https://www.egnomi.gr/

Publication date: 07/02/2019 11:06

Alexa ranking (Greece): 2035

https://www.egnomi.gr/article/100235/pws_na_prostatepseis_ta_passwords.html

Πως να προστατέψεις τα passwords;

Οδηγίες της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου ξεκίνησε η ενημερωτική καμπάνια της **Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών** (ΑΔΑΕ), η οποία επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

http://kataggeilte.blogspot.gr/

Publication date: 07/02/2019 06:09

Alexa ranking (Greece): 0

https://kataggeilte.blogspot.com/2019/02/google.html?utm_source=feedburner&ut...

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων. Αναρτήθηκε από τη Συντακτική ομάδα του Kataggeilte

Αντιδράσεις:

Αποστολή με μήνυμα ηλεκτρονικού ταχυδρομείου BlogThis!Μοιραστείτε το στο TwitterΜοιραστείτε το στο FacebookΚοινοποίηση στο Pinterest

Ετικέτες WEB

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

http://kataggeilte.blogspot.gr/

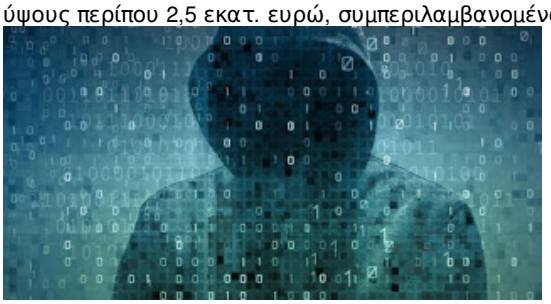
Publication date: 07/02/2019 06:09

Alexa ranking (Greece): 0

https://kataggeilte.blogspot.com/2019/02/google.html?utm_source=feedburner&ut...

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.



Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

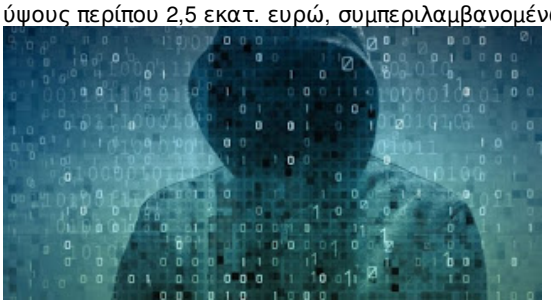
Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.



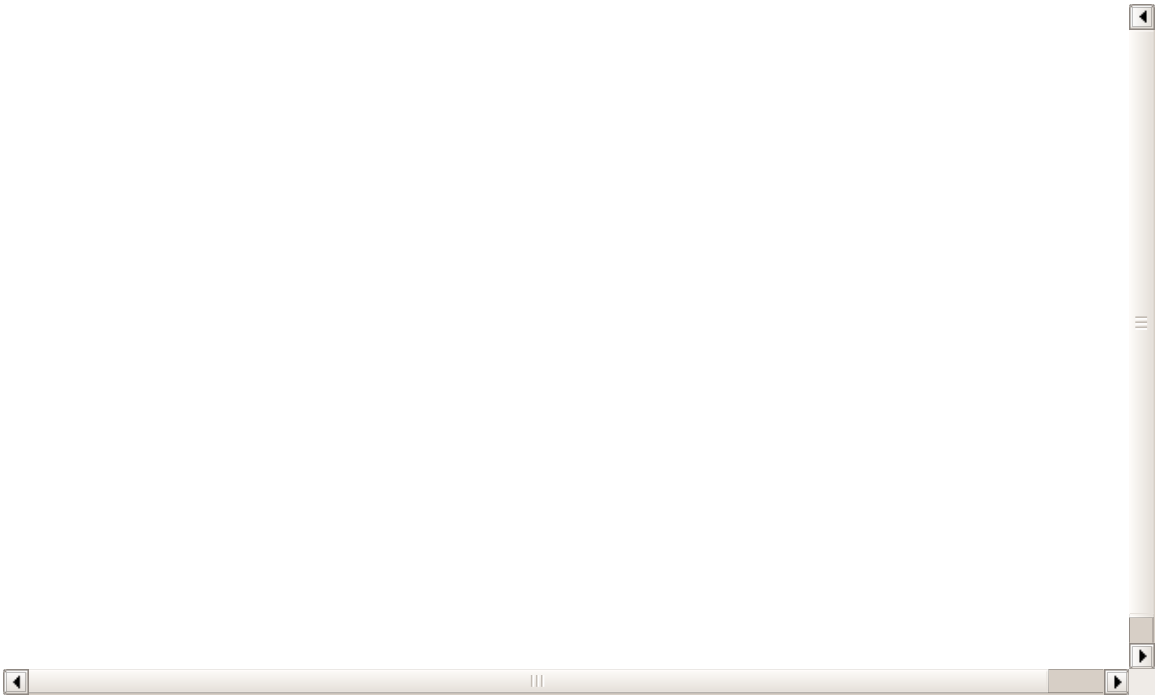
Αναρτήθηκε από τη Συντακτική ομάδα του Kataggeilte
Αντιδράσεις:

Αποστολή με μήνυμα ηλεκτρονικού ταχυδρομείου BlogThis!Μοιραστείτε το στο TwitterΜοιραστείτε το στο FacebookΚοινοποίηση στο Pinterest
Ετικέτες WEB
Αναρτήθηκε από τη Συντακτική ομάδα του Kataggeilte
Αντιδράσεις:

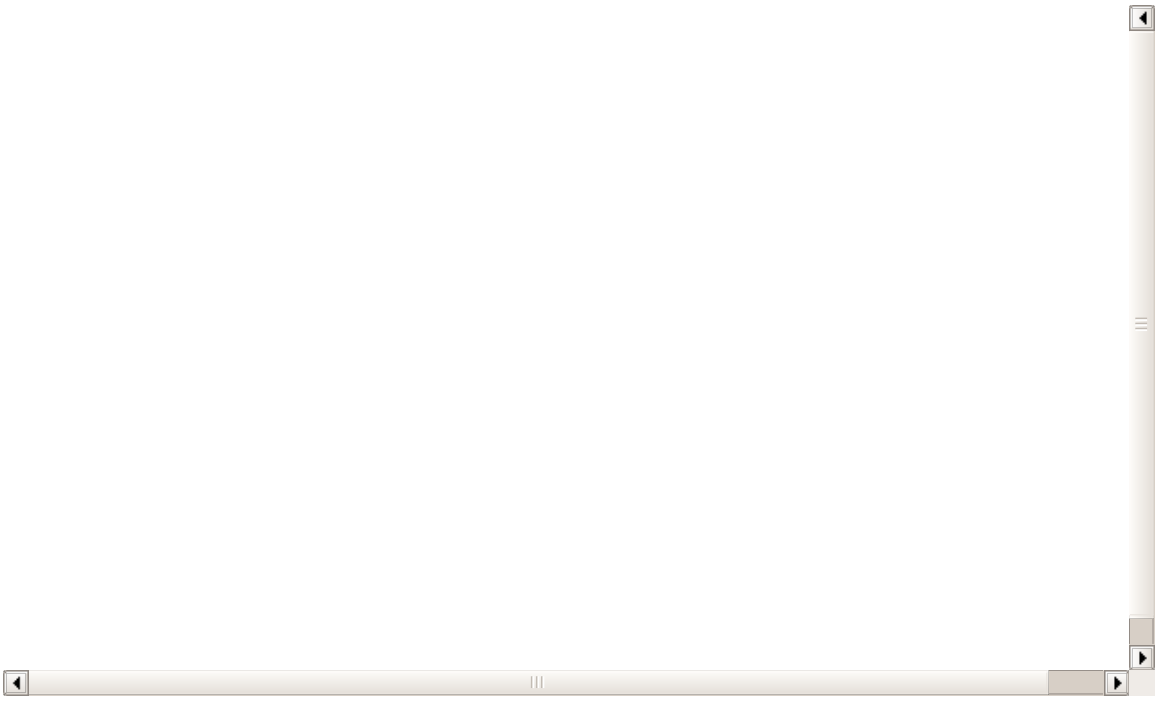
Αποστολή με μήνυμα ηλεκτρονικού ταχυδρομείου BlogThis!Μοιραστείτε το στο TwitterΜοιραστείτε το στο FacebookΚοινοποίηση στο Pinterest
Αποστολή με μήνυμα ηλεκτρονικού ταχυδρομείου BlogThis!Μοιραστείτε το στο TwitterΜοιραστείτε το στο FacebookΚοινοποίηση στο Pinterest
Ετικέτες WEB

Δεν υπάρχουν σχόλια:

Δημοσίευση σχολίου



Δημοσίευση σχολίου



http://www.thrakitoday.com/

Publication date: 07/02/2019 00:26

Alexa ranking (Greece): 16430

http://www.thrakitoday.com/2019/02/blog-post_446.html

Οδηγίες της ΑΔΑΕ για την ασφάλειά σας στο διαδίκτυο

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

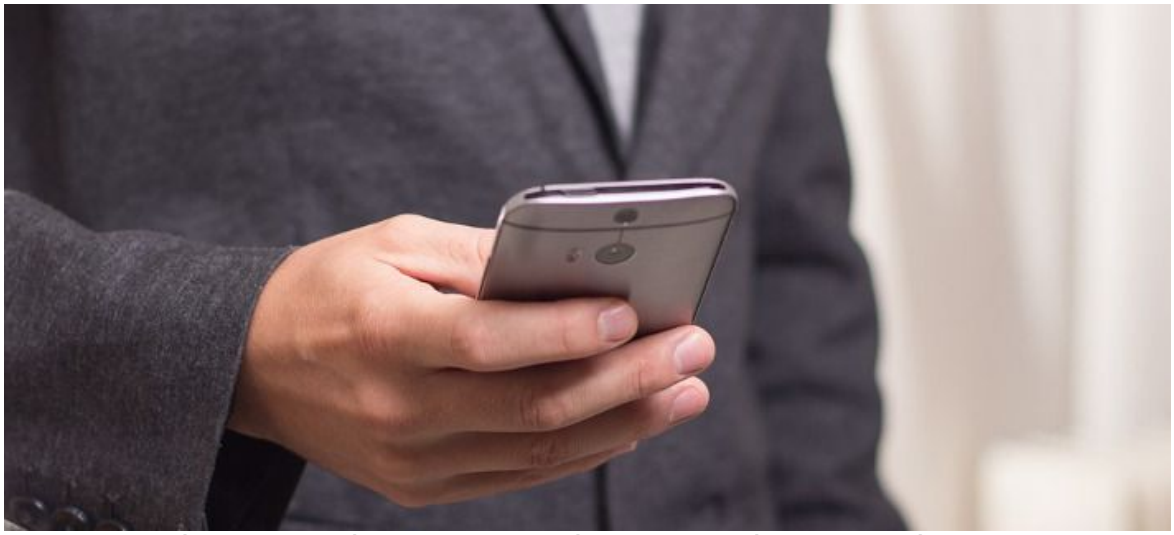
Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://rethemnosnews.gr/
Publication date: 06/02/2019 23:00
Alexa ranking (Greece): 2198
https://rethemnosnews.gr/2019/02/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%84%ce%...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ



Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.
Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:
* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.
Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι,

http://rethemnosnews.gr/
Publication date: 06/02/2019 23:00
Alexa ranking (Greece): 2198
https://rethemnosnews.gr/2019/02/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%84%ce%...

σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

iefimerida.gr

http://www.patrasevents.gr/

Publication date: 06/02/2019 22:11

Alexa ranking (Greece): 658

https://www.patrasevents.gr/article/396411-enas-stous-deka-ellines-thima-ilektroni...

Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Σχετικά...

- Θύμα απάτης έπεσε η Μαρία Μπακοδήμου

- ΣΔΟΕ: Απάτη μέσω Facebook με προϊόντα «μαϊμού» και 70.000 εξαπατημένους πελάτες!

https://www.ersanews.gr/

Publication date: 06/02/2019 21:29

Alexa ranking (Greece): 36272

https://www.ersanews.gr/article/3085350/Prosochi-stous-kodikous-prosvasis-Symv...

Προσοχή στους κωδικούς πρόσβασης. Συμβουλές ασφαλείας

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς...

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: SELEO.GR
06/02 21:15

http://seleo.gr/

Publication date: 06/02/2019 21:18

Alexa ranking (Greece): 538

https://seleo.gr/epistimi/texnologia/291581-prosochh-stoys-kwdikoys-prosbashs-sy...

Προσοχή στους κωδικούς πρόσβασης. Συμβουλές ασφαλείας

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://moneypress.gr/

Publication date: 06/02/2019 16:08

Alexa ranking (Greece): 10917

http://www.moneypress.gr/?p=85498

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο, αναφέρει το in.gr.

Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

Τα τραπεζικά δεδομένα κύρια ανησυχία

Σχετικά με το ποιες πληροφορίες θέλουν να προστατεύσουν περισσότερο, το 59% ανησυχεί κυρίως για τις οικονομικές του πληροφορίες (όπως τραπεζικά δεδομένα), 16% ανησυχεί για τις προσωπικές του πληροφορίες (όπως διεύθυνση κατοικίας), 6% για πληροφορίες σχετικά με προσωπικές στιγμές (όπως φωτογραφίες) και 7% για την παρακολούθηση ηλεκτρονικών μηνυμάτων που στέλνει σε συναδέλφους.

Σε δήλωσή του, ο Manager, Corporate Communication & Public Affairs για Ιταλία, Ελλάδα, Μάλτα, Κλαούντιο Μοντεβέρντε ανέφερε πως η Google δημιουργεί εργαλεία για προστασία σε ό,τι κάνει, ώστε οι χρήστες της να είναι σίγουροι ότι τα προσωπικά τους δεδομένα είναι ασφαλή. Ωστόσο, όπως συμπλήρωσε ο ίδιος, εξακολουθούν να υπάρχουν κάποιες βέλτιστες πρακτικές που μπορεί να ακολουθήσει κανείς και η οικογένειά του, για να διασφαλίσει ότι είναι ασφαλείς όχι μόνο ενώ χρησιμοποιεί το Google αλλά και κατά την πλοήγηση του στο ευρύτερο Διαδίκτυο.

Με αφορμή την Ημέρα Ασφαλούς Διαδικτύου η Google παρουσιάζει μερικές χρήσιμες συμβουλές:

1. Ενημερώστε το λογισμικό σας

Για να προστατεύετε τις δραστηριότητές σας στο διαδίκτυο, είναι πολύ σημαντικό να χρησιμοποιείτε πάντα τις πιο πρόσφατες εκδόσεις λογισμικού, λειτουργικού συστήματος και εφαρμογών σε όλες τις συσκευές σας. Σύμφωνα με τη Google, ορισμένες υπηρεσίες, όπως το Google Chrome, ενημερώνονται αυτόματα ενώ άλλες ειδοποιούν τους χρήστες σχετικά με το πότε πρέπει να τις ενημερώσουν.

2. Χρησιμοποιείτε μοναδικούς, ισχυρούς κωδικούς πρόσβασης

Χρησιμοποιώντας το ίδιο password για να συνδέεστε με διαφορετικούς λογαριασμούς διακινδυνεύετε περισσότερο την ασφάλειά σας. Είναι σαν να χρησιμοποιείτε το ίδιο κλειδί για να ανοίγετε τις πόρτες του σπιτιού, του γραφείου και του αυτοκινήτου σας. Όποιος αποκτήσει πρόσβαση σ' αυτό έχει πρόσβαση σε όλα τα υπάρχοντά σας. Για να περιορίσετε τον κίνδυνο, χρησιμοποιήστε διαφορετικό κωδικό για τον καθένα και επιδιώξτε κάθε κωδικός να είναι δύσκολο να τον μαντέψει κάποιος και να αποτελείται τουλάχιστον από οχτώ χαρακτήρες. Όπως αναφέρει η Google, επιλέξτε να χρησιμοποιήσετε έναν διαχειριστή κωδικών πρόσβασης, όπως αυτός που δημιουργείται στον Chrome σας, για να σας βοηθήσει να δημιουργήσετε, διασφαλίσετε και να ελέγχετε όλους του κωδικούς για τους online λογαριασμούς σας.

3. Κάντε έναν έλεγχο ασφαλείας

Ο Έλεγχος Ασφαλείας της Google, όπως τονίζει η εταιρεία, προσφέρει εξατομικευμένες συμβουλές ασφάλειας που μπορούν να συμβάλουν στην ενίσχυση της ασφάλειας του Google Account σας. Δεν σας βοηθά απλώς να παραμείνετε ασφαλείς όταν χρησιμοποιείτε το Google, αλλά περιέχει χρήσιμες συμβουλές για να είστε ασφαλείς και όταν περιηγείστε γενικά στο διαδίκτυο, όπως το να προσθέσετε την εφαρμογή κλειδώματος οθόνης, να αναθεωρήσετε την πρόσβαση τρίτων στα δεδομένα του Google Account σας και να μάθετε ποια sites και εφαρμογές είναι πιθανόν να έχετε επιτρέψει να συνδεθούν μέσω του Google Account σας. Επισκεφθείτε το https://myaccount.google.com/security-checkup για να κάνετε τον δικό σας

http://moneypress.gr/

Publication date: 06/02/2019 16:08

Alexa ranking (Greece): 10917

http://www.moneypress.gr/?p=85498

Έλεγχο Ασφαλείας.

4. Ορίστε και διατηρήστε ενημερωμένο έναν αριθμό τηλεφώνου ή ένα email ανάκτησης

Η προσθήκη πληροφοριών ανάκτησης, όπως ο αριθμός τηλεφώνου ή το email, μπορεί να σας βοηθήσει να ανακτήσετε πιο γρήγορα το λογαριασμό σας εάν χάσετε την πρόσβαση σ' αυτόν ή δεν μπορείτε να συνδεθείτε. Αν αλλάξουν τα στοιχεία αυτά, θυμηθείτε να ενημερώσετε την εφαρμογή. Σε πολλές περιπτώσεις, ένας αριθμός τηλεφώνου ή μια διεύθυνση email μπορούν να χρησιμοποιηθούν για να ειδοποιηθείτε σχετικά με ύποπτες κινήσεις στο λογαριασμό σας ή για να μπλοκαριστεί κάποιος που θέλει να τον χρησιμοποιήσει χωρίς την άδειά σας. Για παράδειγμα, εάν μια άγνωστη συσκευή χρησιμοποιείται για να συνδεθεί στο Google Account σας, ενδέχεται να σας ζητηθεί να επαληθεύσετε ότι η σύνδεση είναι εξουσιοδοτημένη εισάγοντας έναν κωδικό που αποστέλλεται στον αριθμό τηλεφώνου ανάκτησης. Για να ρυθμίσετε τις πληροφορίες ανάκτησης στο Google Account σας, επισκεφθείτε τη διεύθυνση security.google.com και κάντε κλικ στην επιλογή «Προσωπικές Πληροφορίες».

5. Ορίστε επαλήθευση σε 2 βήματα

Κάντε ένα ακόμη βήμα για τη διασφάλιση των λογαριασμών σας, ορίζοντας επαλήθευση σε 2 βήματα, η οποία απαιτεί να χρησιμοποιήσετε ένα δεύτερο βήμα εκτός από το όνομα χρήστη και τον κωδικό πρόσβασής σας για να συνδεθείτε στο λογαριασμό σας. Παραδείγματα δευτέρων βημάτων επαλήθευσης περιλαμβάνουν: έναν εξαψήφιο κωδικό που δημιουργείται από μια εφαρμογή, μια ερώτηση που λαμβάνετε σε μια αξιόπιστη συσκευή ή τη χρήση ενός κλειδιού φυσικής ασφάλειας (η ισχυρότερη μορφή ενός δεύτερου βήματος). Η δημιουργία επαλήθευσης σε 2 βήματα θα μειώσει σημαντικά την πιθανότητα κάποιος να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο λογαριασμό σας. Αφού ρυθμίσετε την επαλήθευση σε 2 βήματα για έναν λογαριασμό, θυμηθείτε να είστε έτοιμοι για το δεύτερο βήμα επαλήθευσης κάθε φορά που συνδέεστε. Για να ρυθμίσετε την επαλήθευση σε 2 βήματα στο Google Account σας, επισκεφτείτε τη διεύθυνση security.google.com και κάντε κλικ στο κουμπί «Επαλήθευση σε 2 βήματα».

Προστατεύστε τα παιδιά σας

Αν έχετε παιδιά, μιλήστε τους από νωρίς για την ασφάλεια στο Διαδίκτυο και ρυθμίστε τους ψηφιακούς κανόνες για το σπίτι σας. Όπως συστήνει η Google, ακριβώς όπως διδάσκουμε στα παιδιά μας πώς να οδηγούν πριν τους δώσουμε τα κλειδιά του αυτοκινήτου, έτσι είναι χρήσιμο να διδάξετε στα νέα παιδιά τις αρχές της ηλεκτρονικής ασφάλειας πριν τους παραδώσετε μια συσκευή.

Μόλις κερδίσουν την «άδεια οδήγησης» στο Διαδίκτυο, είναι επίσης χρήσιμο να καθορίσετε κάποιους ψηφιακούς κανόνες καθώς αρχίζουν να εξερευνούν. Αν τα παιδιά σας διαθέτουν συσκευή Android ή Chromebook, μπορείτε να χρησιμοποιήσετε την εφαρμογή Family Link για να κάνετε πράγματα όπως διαχείριση των ρυθμίσεων του Λογαριασμού Google, έγκριση ή αποκλεισμό των εφαρμογών και των ιστότοπων που μπορούν να χρησιμοποιήσουν και να ορίσετε χρονικά όρια οθόνης. Μπορείτε να μάθετε περισσότερα στο google.com/familylink.

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Google

https://www.e-simerini.com/a/

Publication date: 06/02/2019 15:48

Alexa ranking (Greece): 0

https://www.e-simerini.com/a/news/%ce%b5%ce%bd%ce%b7%ce%bc%ce%b5%cf%...

ΕΝΗΜΕΡΩΤΙΚΗ ΚΑΜΠΑΝΙΑ ΤΗΣ ΑΑΔΕ ΜΕ ΑΦΟΡΜΗ ΤΗΝ ΠΑΓΚΟΣΜΙΑ ΗΜΕΡΑ ΑΣΦΑΛΟΥΣ ΔΙΑΔΙΚΤΥΟΥ

Επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου

Ενημερωτική καμπάνια της ΑΔΑΕ με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδόθηκε την Τρίτη , με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

https://www.e-simerini.com/a/

Publication date: 06/02/2019 15:48

Alexa ranking (Greece): 0

https://www.e-simerini.com/a/news/%ce%b5%ce%bd%ce%b7%ce%bc%ce%b5%cf%...

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.huffingtonpost.gr/

Publication date: 06/02/2019 13:26

Alexa ranking (Greece): 116

https://www.huffingtonpost.gr/entry/ereena-google-enas-stoes-deka-ellenes-thema...

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου στις 5 Φεβρουαρίου, η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

(Με πληροφορίες από ΑΠΕ-ΜΠΕ, ΑΔΑΕ)

https://www.timesnews.gr/

Publication date: 06/02/2019 13:24

Alexa ranking (Greece): 4064

https://www.timesnews.gr/ereyna-google-enas-stoys-deka-ellines-thyma-i/

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

πηγή: perierga.gr

http://www.perivolos.gr/

Publication date: 06/02/2019 12:32

Alexa ranking (Greece): 20061

http://www.perivolos.gr/article/%CF%80%CF%8E%CF%82-%CE%BD%CE%B1-%CE%B...

Πώς να δημιουργήσετε ισχυρά passwords

Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Οι κωδικοί πρόσβασης είναι ο νούμερο 1 κίνδυνος σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://monomaxoi.com/

Publication date: 06/02/2019 12:08

http://monomaxoi.com/2019/02/06/%ce%ad%cf%81%ce%b5%cf%85%ce%bd%ce%...

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

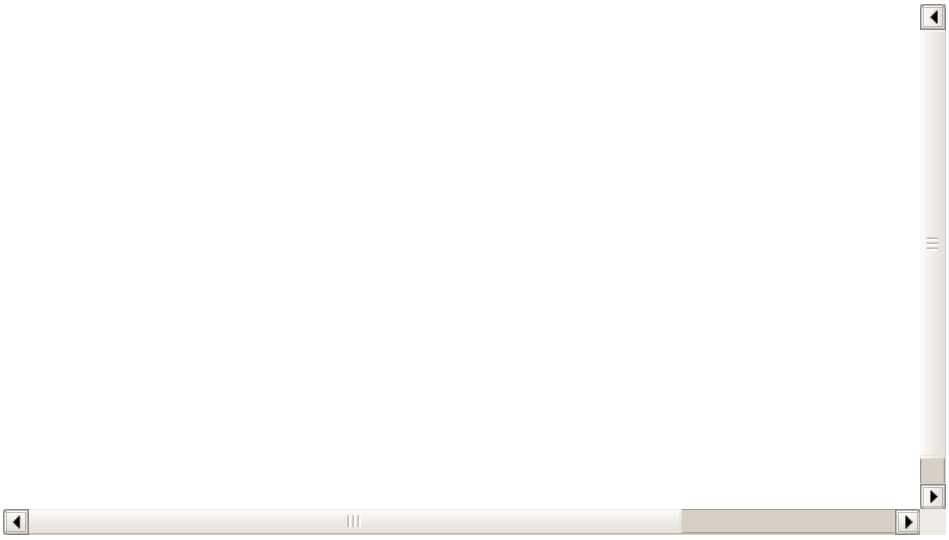
Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).



Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.arttv.gr/

Publication date: 06/02/2019 11:37

http://www.arttv.gr/koinonia/%ce%bc%ce%b1%ce%b6%ce%af-%ce%b3%ce%b9%ce...

«Μαζί για ένα καλύτερο διαδίκτυο».

Παγκόσμια ημέρα ασφαλούς διαδικτύου η 5η Φεβρουαρίου και με το κεντρικό μήνυμα «Μαζί για ένα καλύτερο διαδίκτυο».Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών στην καμπάνιά της εστιάζεται στη προστασία της ιδιωτικότητας των χρηστών του διαδικτύου και τη σημαία των κωδικών πρόσβασης.

https://banks.com.gr/

Publication date: 06/02/2019 10:54

Alexa ranking (Greece): 2869

https://banks.com.gr/adae-pos-profylaksoume-password-apo-tous-chaker/

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.mobilenews.gr/

Publication date: 06/02/2019 10:50

Alexa ranking (Greece): 15451

https://www.mobilenews.gr/oi-tesseris-xrysoi-kanones-gia-toys/

Οι τέσσερις «χρυσοί» κανόνες για τους κωδικούς πρόσβασης

Στην **προστασία της ιδιωτικότητας** των χρηστών του διαδικτύου επικεντρώνεται η **ενημερωτική καμπάνια** (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (**ΑΔΑΕ**), η οποία μεταδίδεται σήμερα, με αφορμή την **Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.**

Το μήνυμά της απαντά στην πάντα επίκαιρη **ερώτηση** για όλους τους **ψηφιακούς** χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά **μέτρα ασφάλειας**.

Η σημασία των **κωδικών πρόσβασης γίνεται** φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, **η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.**

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να **αναζητήσουν** στη **διαδικτυακή** πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει **να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.**

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

• Αφού φτιάξετε ισχυρούς **κωδικούς πρόσβασης**, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

• Εκτός από ισχυρό, το **password** πρέπει να είναι και **μυστικό**. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας **μέσω ηλεκτρονικού ταχυδρομείου.**

• **Σημαντικό** είναι να μην **αποθηκεύετε** τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

• Επιπλέον**, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλο**ς δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το **κεντρικό μήνυμα** της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «**Μαζί για ένα καλύτερο διαδίκτυο**», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η **ψηφιακή τεχνολογία**. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος **κακόβουλων**.

Σε ό,τι αφορά στις εταιρείες παρόχους **υπηρεσιών ηλεκτρονικών επικοινωνιών**, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της **ΑΔΑΕ**. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, **οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.**

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή **περιστατικά ασφάλειας**. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η **ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.**

Μέσα στο 2018 επιβλήθηκαν συνολικά **διοικητικές κυρώσεις** σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και **οκτώ περιπτώσεων επιβολής συστάσεων.**

http://grevenamedia.gr/

Publication date: 06/02/2019 10:34

Alexa ranking (Greece): 6616

http://grevenamedia.gr/adae-pos-na-profylaxoyme-ta-password-apo-toys-chaker/

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://magnesianews.gr/

Publication date: 06/02/2019 10:29

Alexa ranking (Greece): 758

https://magnesianews.gr/perissotera/texnologia/pos-na-profylaxoume-ta-password...

Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.
Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.kontranews.gr/

Publication date: 06/02/2019 10:16

Alexa ranking (Greece): 915

https://www.kontranews.gr/KOINONIA/353573-Ereyna-Google-Enas-stoys-deka-Elle...

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

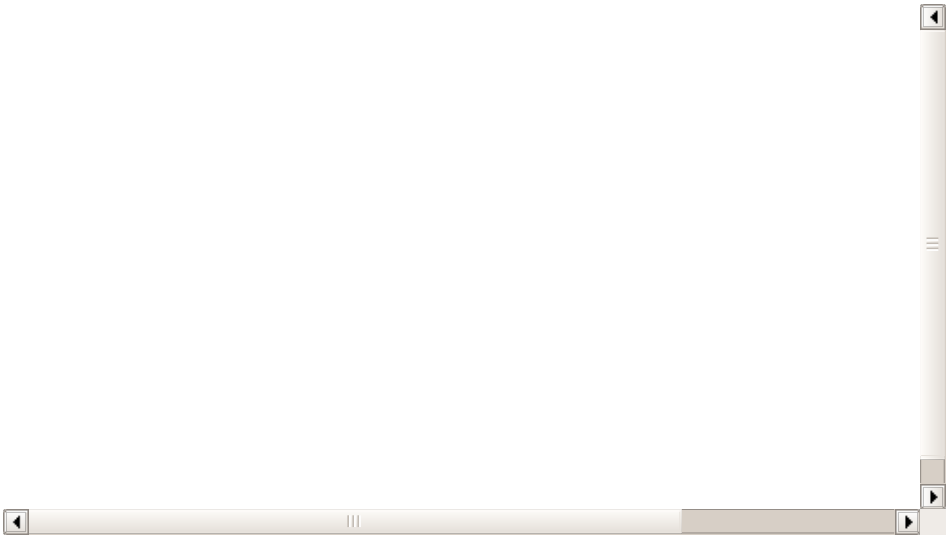
Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).



Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://1news.gr/

Publication date: 06/02/2019 10:15

Alexa ranking (Greece): 12691

https://1news.gr/%ce%ad%cf%81%ce%b5%cf%85%ce%bd%ce%b1-google-%ce%ad...

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

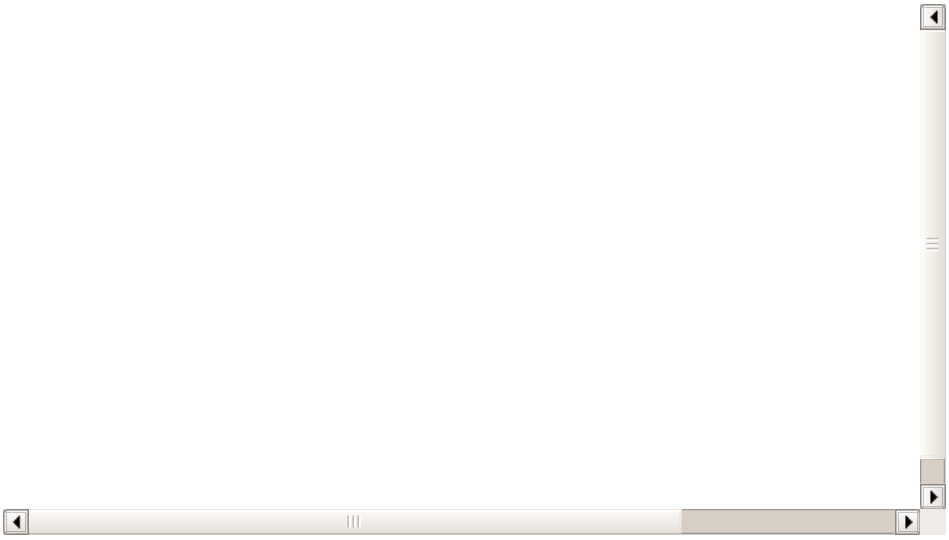
Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).



Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.tromaktiko.gr/

Publication date: 06/02/2019 10:10

Alexa ranking (Greece): 252

https://www.tromaktiko.gr/87216/me-afta-ta-mystika-sta-passwords-den-tha-se-ch...

Με αυτά τα μυστικά στα passwords δεν θα σε χακάρουν ποτέ!

Όταν επιλέγεις έναν κωδικό να βάλεις σε κάποια συσκευή, στο email σου, στα social media, δεν το πολυσκέφτεσαι. Λες «εμένα θα χακάρουν;». Επειδή, όμως, ποτέ δεν ξέρεις αυτά είναι τα μυστικά για καλύτερα passwords.

Φύλαγε τα ρούχα σου για να έχεις τα μισά, έλεγε η γιαγιά μου και είχε απόλυτο δίκαιο. Ποια είναι τα μυστικά για καλύτερα passwords για να μην σε χακάρουν ποτέ;;

Χτες 5 Φεβρουαρίου είναι η Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), σε ενημερώνει και σου λέει όλα τα μυστικά για καλύτερα passwords.

Το μήνυμα καμπάνιας απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Ο κωδικός πρόσβασης είναι πολύ σημαντικός κι εσύ πρέπει να δίνεις την απαραίτητη προσοχή!

Μυστικά για τα καλύτερα passwords και τα μέτρα που πρέπει να λάβεις
Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.
Και... πώς μπορείς να καταλάβεις ότι σε έχουν χακάρει;
Τελειώνει ξαφνικά η μπαταρία του κινητού σου πολύ γρήγορα. Αυτό μπορεί να συμβεί όταν έχεις στο κινητό σου μια άγνωστη εφαρμογή.

Η συσκευή σου ζεσταίνεται ακόμα κι όταν δεν το χρησιμοποιείς. Αυτό είναι ένα ακόμα σημάδι ότι υπάρχει μια άγνωστη εφαρμογή που «τρέχει» στο background.

Γίνεται επανεκκίνηση, απενεργοποίηση, κλήση αριθμών ή εκτέλεση εφαρμογών χωρίς να το έχεις ζητήσει εσύ. Εάν δεν είναι βλάβη του συστήματος, τότε είναι σημάδι ότι σ' έχουν χακάρει.
Υπάρχουν άγνωστοι αριθμοί στις πρόσφατες κλήσεις σου.
Δεν μπορείς ν' απενεργοποιήσεις το κινητό σου και αντ' αυτού ξεκινούν να εκτελούνται διαφορετικές εφαρμογές.

ΠΗΓΗ

http://www.palo.gr/?fcid=5

Publication date: 06/02/2019 09:56

Alexa ranking (Greece): 192

http://www.palo.gr/texnologika-nea/me-ayta-ta-mystika-sta-passwords-den-tha-se-...

Με αυτά τα μυστικά στα passwords δεν θα σε χακάρουν ποτέ! - [Tromaktiko.gr]

Όταν επιλέγεις έναν κωδικό να βάλεις σε κάποια συσκευή, στο email σου, στα social media, δεν το πολυσκέφτεσαι. Λες "εμένα θα χακάρουν;". Επειδή, όμως, ποτέ δεν ξέρεις αυτά είναι τα μυστικά για καλύτερα passwords. Φύλαγε τα ρούχα σου για να έχεις τα μισά, έλεγε η γιαγιά μου και είχε απόλυτο δίκαιο. Ποια είναι τα μυστικά για καλύτερα passwords για να μην σε χακάρουν ποτέ;; Χτες 5 Φεβρουαρίου είναι η Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), σε ενημερώνει και σου λέει όλα τα μυστικά για καλύτερα passwords. Το μήνυμα καμπάνιας απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας. Ο κωδικός πρόσβασης είναι πολύ σημαντικός κι εσύ πρέπει να δίνεις την...

Tromaktiko.gr · πριν από 16 λεπτά ·

Όταν επιλέγεις έναν κωδικό να βάλεις σε κάποια συσκευή, στο email σου, στα social media, δεν το πολυσκέφτεσαι. Λες "εμένα θα χακάρουν;". Επειδή, όμως, ποτέ δεν ξέρεις αυτά είναι τα μυστικά για καλύτερα passwords. Φύλαγε τα ρούχα σου για να έχεις τα μισά, έλεγε η γιαγιά μου και είχε απόλυτο δίκαιο. Ποια είναι τα μυστικά για καλύτερα passwords για να μην σε χακάρουν ποτέ;; Χτες 5 Φεβρουαρίου είναι η Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), σε ενημερώνει και σου λέει όλα τα μυστικά για καλύτερα passwords. Το μήνυμα καμπάνιας απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας. Ο κωδικός πρόσβασης είναι πολύ σημαντικός κι εσύ πρέπει να δίνεις την...

https://www.tromaktiko.gr/

Publication date: 06/02/2019 07:26

Alexa ranking (Greece): 252

https://www.tromaktiko.gr/87636/prosochi-pos-tha-prostateusete-tous-logariasmo...

Προσοχή! Πώς θα προστατεύσετε τους λογαριασμούς σας στο TAXISnet (vid)

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται από χθες (5/2/2019) με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: **Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις**; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, **Τρόι Χαντ**: 21 εκατ. **κωδικοί πρόσβασης** και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Πηγή

http://brb.newsbomb.gr

Publication date: 06/02/2019 06:58

Alexa ranking (Greece): 34

https://www.newsbomb.gr/oikonomia/story/956072/aade-odigies-prostasias-gia-to...

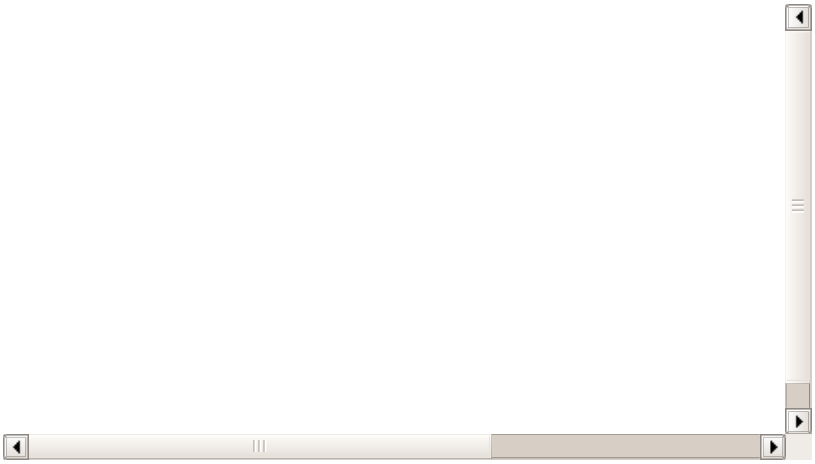
Προσοχή! Πώς θα προστατεύσετε τους λογαριασμούς σας στο TAXISnet (vid)

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται από χθες (5/2/2019) με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: **Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις**; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

- **ΤΟΡ ΘΕΜΑ ΤΩΡΑ: ΣΟΚ στην Κάρυστο: Την κατασπάραξαν άγρια ζώα**

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, **Τρόι Χαντ**: 21 εκατ. **κωδικοί πρόσβασης** και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.



Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://***www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/*** και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους ***http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/***

Πρακτικές οδηγίες

http://brb.newsbomb.gr

Publication date: 06/02/2019 06:58

Alexa ranking (Greece): 34

https://www.newsbomb.gr/oikonomia/story/956072/aade-odigies-prostasias-gia-to...

Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

Εκτός από ισχυρό, **το password πρέπει να είναι και μυστικό**. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε **προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή,** ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

Επιπλέον, **ένα ασφαλές password** θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της **ΑΔΑΕ.**

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά **διοικητικές κυρώσεις σε 41 περιπτώσεις,** συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Διαβάστε επίσης:

Ξαφνικό «κανόνι»: Πτώχευση για γνωστή αεροπορική εταιρεία

Έκτακτο δελτίο επιδείνωσης καιρού: Σε επιφυλακή για τη σφοδρή κακοκαιρία - Θα «ανοίξουν» οι ουρανοί

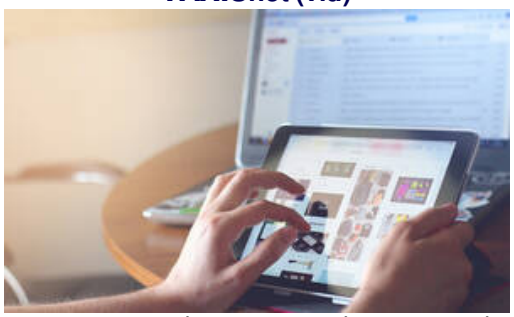
http://www.mykosmos.gr/loc_mk/Default.asp

Publication date: 06/02/2019 06:27

Alexa ranking (Greece): 1184

http://www.mykosmos.gr/loc_mk/news/greece/5473788/prosoxh-pws-tha-prostate...

Ειδήσεις Προσοχή! Πώς θα προστατεύσετε τους λογαριασμούς σας στο TAXISnet (vid)



Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται από χθες (5/2/2019) με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

https://newscast.gr/

Publication date: 06/02/2019 06:14

Alexa ranking (Greece): 28885

https://www.newscast.gr/eidiseis/fp_prosochi_pos_tha_prostateusete_tous_logarias...

Προσοχή! Πώς θα προστατεύσετε τους λογαριασμούς σας στο TAXISnet

Σ

την προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται από χθες (5/2/2019) με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

http://www.fonitisparou.gr/

Publication date: 06/02/2019 05:29

Alexa ranking (Greece): 33090

http://www.fonitisparou.gr/index.php/technology/18217-adae-oi-tesseris-xrysoi-ka...

ΑΔΑΕ: Οι τέσσερις «χρυσοί» κανόνες για τους κωδικούς πρόσβασης

Στην **προστασία της ιδιωτικότητας** των χρηστών του διαδικτύου επικεντρώνεται η **ενημερωτική καμπάνια** (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (**ΑΔΑΕ**), η οποία μεταδίδεται σήμερα, με αφορμή την **Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.**

Το μήνυμά της απαντά στην πάντα επίκαιρη **ερώτηση** για όλους τους **ψηφιακούς** χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά **μέτρα ασφάλειας**.

Η σημασία των **κωδικών πρόσβασης γίνεται** φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, **η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.**

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να **αναζητήσουν** στη **διαδικτυακή** πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει **να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.**

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

• Αφού φτιάξετε ισχυρούς **κωδικούς πρόσβασης**, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

• Εκτός από ισχυρό, το **password** πρέπει να είναι και **μυστικό**. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας **μέσω ηλεκτρονικού ταχυδρομείου.**

• **Σημαντικό** είναι να μην **αποθηκεύετε** τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

• Επιπλέον**, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλο**ς δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το **κεντρικό μήνυμα** της Ημέρας Ασφαλούς Διαδικτύου για φέτος, **«Μαζί για ένα καλύτερο διαδίκτυο»**, υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η **ψηφιακή τεχνολογία**. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος **κακόβουλων**.

Σε ό,τι αφορά στις εταιρείες παρόχους **υπηρεσιών ηλεκτρονικών επικοινωνιών**, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της **ΑΔΑΕ**. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, **οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.**

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή **περιστατικά ασφάλειας**. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η **ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.**

Μέσα στο 2018 επιβλήθηκαν συνολικά **διοικητικές κυρώσεις** σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και **οκτώ περιπτώσεων επιβολής συστάσεων.**

http://www.fonitisparou.gr/

Publication date: 06/02/2019 05:29

Alexa ranking (Greece): 33090

http://www.fonitisparou.gr/index.php/technology/18217-adae-oi-tesseris-xrysoi-ka...

Πηγή: cnn.gr

https://www.grtimes.gr/

Publication date: 06/02/2019 01:42

https://www.grtimes.gr/diafora/texnologia/adae-pos-na-profylaxoyme-ta-password...

ΑΔΑΕ: Πως να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://radio4.gr/

Publication date: 06/02/2019 00:50

Alexa ranking (Greece): 38353

https://radio4.gr/%ce%ad%cf%81%ce%b5%cf%85%ce%bd%ce%b1-google-%ce%ad...

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

Σχετικά με το ποιες πληροφορίες θέλουν να προστατεύσουν περισσότερο, το 59% ανησυχεί κυρίως για τις οικονομικές του πληροφορίες (όπως τραπεζικά δεδομένα), 16% ανησυχεί για τις προσωπικές του πληροφορίες (όπως διεύθυνση κατοικίας), 6% για πληροφορίες σχετικά με προσωπικές στιγμές (όπως φωτογραφίες) και 7% για την παρακολούθηση ηλεκτρονικών μηνυμάτων που στέλνει σε συναδέλφους.

Σε δήλωσή του, ο Manager, Corporate Communication & Public Affairs για Ιταλία, Ελλάδα, Μάλτα, Κλαούντιο Μοντεβέρντε ανέφερε πως η Google δημιουργεί εργαλεία για προστασία σε ό,τι κάνει, ώστε οι χρήστες της να είναι σίγουροι ότι τα προσωπικά τους δεδομένα είναι ασφαλή. Ωστόσο, όπως συμπλήρωσε ο ίδιος, εξακολουθούν να υπάρχουν κάποιες βέλτιστες πρακτικές που μπορεί να ακολουθήσει κανείς και η οικογένειά του, για να διασφαλίσει ότι είναι ασφαλείς όχι μόνο ενώ χρησιμοποιεί το Google αλλά και κατά την πλοήγηση του στο ευρύτερο Διαδίκτυο.

Με αφορμή την Ημέρα Ασφαλούς Διαδικτύου η Google παρουσιάζει μερικές χρήσιμες συμβουλές:

1. Ενημερώστε το λογισμικό σας

http://radio4.gr/

Publication date: 06/02/2019 00:50

Alexa ranking (Greece): 38353

https://radio4.gr/%ce%ad%cf%81%ce%b5%cf%85%ce%bd%ce%b1-google-%ce%ad...

Για να προστατεύετε τις δραστηριότητές σας στο διαδίκτυο, είναι πολύ σημαντικό να χρησιμοποιείτε πάντα τις πιο πρόσφατες εκδόσεις λογισμικού, λειτουργικού συστήματος και εφαρμογών σε όλες τις συσκευές σας. Σύμφωνα με τη Google, ορισμένες υπηρεσίες, όπως το Google Chrome, ενημερώνονται αυτόματα ενώ άλλες ειδοποιούν τους χρήστες σχετικά με το πότε πρέπει να τις ενημερώσουν.

2. Χρησιμοποιείτε μοναδικούς, ισχυρούς κωδικούς πρόσβασης

Χρησιμοποιώντας το ίδιο password για να συνδέεστε με διαφορετικούς λογαριασμούς διακινδυνεύετε περισσότερο την ασφάλειά σας. Είναι σαν να χρησιμοποιείτε το ίδιο κλειδί για να ανοίγετε τις πόρτες του σπιτιού, του γραφείου και του αυτοκινήτου σας. Όποιος αποκτήσει πρόσβαση σ' αυτό έχει πρόσβαση σε όλα τα υπάρχοντά σας. Για να περιορίσετε τον κίνδυνο, χρησιμοποιήστε διαφορετικό κωδικό για τον καθένα και επιδιώξτε κάθε κωδικός να είναι δύσκολο να τον μαντέψει κάποιος και να αποτελείται τουλάχιστον από οχτώ χαρακτήρες. Όπως αναφέρει η Google, επιλέξτε να χρησιμοποιήσετε έναν διαχειριστή κωδικών πρόσβασης, όπως αυτός που δημιουργείται στον Chrome σας, για να σας βοηθήσει να δημιουργήσετε, διασφαλίσετε και να ελέγχετε όλους του κωδικούς για τους online λογαριασμούς σας.

3. Κάντε έναν έλεγχο ασφαλείας

Ο Έλεγχος Ασφαλείας της Google, όπως τονίζει η εταιρεία, προσφέρει εξατομικευμένες συμβουλές ασφάλειας που μπορούν να συμβάλουν στην ενίσχυση της ασφάλειας του Google Account σας. Δεν σας βοηθά απλώς να παραμείνετε ασφαλείς όταν χρησιμοποιείτε το Google, αλλά περιέχει χρήσιμες συμβουλές για να είστε ασφαλείς και όταν περιηγείστε γενικά στο διαδίκτυο, όπως το να προσθέσετε την εφαρμογή κλειδώματος οθόνης, να αναθεωρήσετε την πρόσβαση τρίτων στα δεδομένα του Google Account σας και να μάθετε ποια sites και εφαρμογές είναι πιθανόν να έχετε επιτρέψει να συνδεθούν μέσω του Google Account σας. Επισκεφθείτε το https://myaccount.google.com/security-checkup για να κάνετε τον δικό σας Έλεγχο Ασφαλείας.

4. Ορίστε και διατηρήστε ενημερωμένο έναν αριθμό τηλεφώνου ή ένα email ανάκτησης

Η προσθήκη πληροφοριών ανάκτησης, όπως ο αριθμός τηλεφώνου ή το email, μπορεί να σας βοηθήσει να ανακτήσετε πιο γρήγορα το λογαριασμό σας εάν χάσετε την πρόσβαση σ' αυτόν ή δεν μπορείτε να συνδεθείτε. Αν αλλάξουν τα στοιχεία αυτά, θυμηθείτε να ενημερώσετε την εφαρμογή. Σε πολλές περιπτώσεις, ένας αριθμός τηλεφώνου ή μια διεύθυνση email μπορούν να χρησιμοποιηθούν για να ειδοποιηθείτε σχετικά με ύποπτες κινήσεις στο λογαριασμό σας ή για να μπλοκαριστεί κάποιος που θέλει να τον χρησιμοποιήσει χωρίς την άδειά σας. Για παράδειγμα, εάν μια άγνωστη συσκευή χρησιμοποιείται για να συνδεθεί στο Google Account σας, ενδέχεται να σας ζητηθεί να επαληθεύσετε ότι η σύνδεση είναι εξουσιοδοτημένη εισάγοντας έναν κωδικό που αποστέλλεται στον αριθμό τηλεφώνου ανάκτησης. Για να ρυθμίσετε τις πληροφορίες ανάκτησης στο Google Account σας, επισκεφθείτε τη διεύθυνση security.google.com και κάντε κλικ στην επιλογή «Προσωπικές Πληροφορίες».

5. Ορίστε επαλήθευση σε 2 βήματα

Κάντε ένα ακόμη βήμα για τη διασφάλιση των λογαριασμών σας, ορίζοντας επαλήθευση σε 2 βήματα, η οποία απαιτεί να χρησιμοποιήσετε ένα δεύτερο βήμα εκτός από το όνομα χρήστη και τον κωδικό πρόσβασής σας για να συνδεθείτε στο λογαριασμό σας. Παραδείγματα δευτέρων βημάτων επαλήθευσης περιλαμβάνουν: έναν εξαψήφιο κωδικό που δημιουργείται από μια εφαρμογή, μια ερώτηση που λαμβάνετε σε μια αξιόπιστη συσκευή ή τη χρήση ενός κλειδιού φυσικής ασφάλειας (η ισχυρότερη μορφή ενός δεύτερου βήματος). Η δημιουργία επαλήθευσης σε 2 βήματα θα μειώσει σημαντικά την πιθανότητα κάποιος να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο λογαριασμό σας. Αφού ρυθμίσετε την επαλήθευση σε 2 βήματα για έναν λογαριασμό, θυμηθείτε να είστε έτοιμοι για το δεύτερο βήμα επαλήθευσης κάθε φορά που συνδέεστε. Για να ρυθμίσετε την επαλήθευση σε 2 βήματα στο Google Account σας, επισκεφτείτε τη διεύθυνση security.google.com και κάντε κλικ στο κουμπί «Επαλήθευση σε 2 βήματα».

Αν έχετε παιδιά, μιλήστε τους από νωρίς για την ασφάλεια στο Διαδίκτυο και ρυθμίστε τους ψηφιακούς κανόνες για το σπίτι σας. Όπως συστήνει η Google, ακριβώς όπως διδάσκουμε στα παιδιά μας πώς να οδηγούν πριν τους δώσουμε τα κλειδιά του αυτοκινήτου, έτσι είναι χρήσιμο να διδάξετε στα νέα παιδιά τις αρχές της ηλεκτρονικής ασφάλειας πριν τους παραδώσετε μια συσκευή.

Μόλις κερδίσουν την «άδεια οδήγησης» στο Διαδίκτυο, είναι επίσης χρήσιμο να καθορίσετε κάποιους ψηφιακούς κανόνες καθώς αρχίζουν να εξερευνούν. Αν τα παιδιά σας διαθέτουν συσκευή Android ή Chromebook, μπορείτε να χρησιμοποιήσετε την εφαρμογή Family Link για να κάνετε πράγματα όπως διαχείριση των ρυθμίσεων του Λογαριασμού Google, έγκριση ή αποκλεισμό των εφαρμογών και των ιστότοπων που μπορούν να χρησιμοποιήσουν και να ορίσετε χρονικά όρια οθόνης. Μπορείτε να μάθετε περισσότερα στο google.com/familylink.

http://radio4.gr/

Publication date: 06/02/2019 00:50

Alexa ranking (Greece): 38353

https://radio4.gr/%ce%ad%cf%81%ce%b5%cf%85%ce%bd%ce%b1-google-%ce%ad...

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://agrinio24.eu/
Publication date: 06/02/2019 00:07
Alexa ranking (Greece): 11970
https://agrinio24.eu/archives/405069

Πώς να δημιουργήσετε ισχυρά passwords

Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Οι **κωδικοί πρόσβασης** είναι ο νούμερο 1 κίνδυνος σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για **χάκερς** τον Δεκέμβριο.

https://agrinio24.eu/

Publication date: 06/02/2019 00:07

Alexa ranking (Greece): 11970

https://agrinio24.eu/archives/405069

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα **passwords** περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές **password** θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς **ηλεκτρονικών επικοινωνιών**, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγη

http://myportal.gr/

Publication date: 05/02/2019 23:48

Alexa ranking (Greece): 1338

http://myportal.gr/adae-ta-trik-sto-password-gia-na-profylachthoyme-apo-toys-cha...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**
* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς

υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.
Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://thessbomb.blogspot.gr/

Publication date: 05/02/2019 23:24

Alexa ranking (Greece): 0

https://thessbomb.blogspot.com/2019/02/blog-post_517.html

ΑΔΑΕ: Πώς να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

http://thessbomb.blogspot.gr/

Publication date: 05/02/2019 23:24

Alexa ranking (Greece): 0

https://thessbomb.blogspot.com/2019/02/blog-post_517.html

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://newsall.gr/

Publication date: 05/02/2019 23:05

https://newsall.gr/2019/02/05/%ce%ad%cf%81%ce%b5%cf%85%ce%bd%ce%b1-go...

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

Τα τραπεζικά δεδομένα κύρια ανησυχία

Σχετικά με το ποιες πληροφορίες θέλουν να προστατεύσουν περισσότερο, το 59% ανησυχεί κυρίως για τις οικονομικές του πληροφορίες (όπως τραπεζικά δεδομένα), 16% ανησυχεί για τις προσωπικές του πληροφορίες (όπως διεύθυνση κατοικίας), 6% για πληροφορίες σχετικά με προσωπικές στιγμές (όπως φωτογραφίες) και 7% για την παρακολούθηση ηλεκτρονικών μηνυμάτων που στέλνει σε συναδέλφους.

Σε δήλωσή του, ο Manager, Corporate Communication & Public Affairs για Ιταλία, Ελλάδα, Μάλτα, Κλαούντιο Μοντεβέρντε ανέφερε πως η Google δημιουργεί εργαλεία για προστασία σε ό,τι κάνει, ώστε οι χρήστες της να είναι σίγουροι ότι τα προσωπικά τους δεδομένα είναι ασφαλή. Ωστόσο, όπως συμπλήρωσε ο ίδιος, εξακολουθούν να υπάρχουν κάποιες βέλτιστες πρακτικές που μπορεί να ακολουθήσει κανείς και η οικογένειά του, για να διασφαλίσει ότι είναι ασφαλείς όχι μόνο ενώ χρησιμοποιεί το Google αλλά και κατά την πλοήγηση του στο ευρύτερο Διαδίκτυο.

Με αφορμή την Ημέρα Ασφαλούς Διαδικτύου η Google παρουσιάζει μερικές χρήσιμες συμβουλές:

1. Ενημερώστε το λογισμικό σας

https://newsall.gr/

Publication date: 05/02/2019 23:05

https://newsall.gr/2019/02/05/%ce%ad%cf%81%ce%b5%cf%85%ce%bd%ce%b1-go...

Για να προστατεύετε τις δραστηριότητές σας στο διαδίκτυο, είναι πολύ σημαντικό να χρησιμοποιείτε πάντα τις πιο πρόσφατες εκδόσεις λογισμικού, λειτουργικού συστήματος και εφαρμογών σε όλες τις συσκευές σας. Σύμφωνα με τη Google, ορισμένες υπηρεσίες, όπως το Google Chrome, ενημερώνονται αυτόματα ενώ άλλες ειδοποιούν τους χρήστες σχετικά με το πότε πρέπει να τις ενημερώσουν.

2. Χρησιμοποιείτε μοναδικούς, ισχυρούς κωδικούς πρόσβασης

Χρησιμοποιώντας το ίδιο password για να συνδέεστε με διαφορετικούς λογαριασμούς διακινδυνεύετε περισσότερο την ασφάλειά σας. Είναι σαν να χρησιμοποιείτε το ίδιο κλειδί για να ανοίγετε τις πόρτες του σπιτιού, του γραφείου και του αυτοκινήτου σας. Όποιος αποκτήσει πρόσβαση σ' αυτό έχει πρόσβαση σε όλα τα υπάρχοντά σας. Για να περιορίσετε τον κίνδυνο, χρησιμοποιήστε διαφορετικό κωδικό για τον καθένα και επιδιώξτε κάθε κωδικός να είναι δύσκολο να τον μαντέψει κάποιος και να αποτελείται τουλάχιστον από οχτώ χαρακτήρες. Όπως αναφέρει η Google, επιλέξτε να χρησιμοποιήσετε έναν διαχειριστή κωδικών πρόσβασης, όπως αυτός που δημιουργείται στον Chrome σας, για να σας βοηθήσει να δημιουργήσετε, διασφαλίσετε και να ελέγχετε όλους του κωδικούς για τους online λογαριασμούς σας.

3. Κάντε έναν έλεγχο ασφαλείας

Ο Έλεγχος Ασφαλείας της Google, όπως τονίζει η εταιρεία, προσφέρει εξατομικευμένες συμβουλές ασφάλειας που μπορούν να συμβάλουν στην ενίσχυση της ασφάλειας του Google Account σας. Δεν σας βοηθά απλώς να παραμείνετε ασφαλείς όταν χρησιμοποιείτε το Google, αλλά περιέχει χρήσιμες συμβουλές για να είστε ασφαλείς και όταν περιηγείστε γενικά στο διαδίκτυο, όπως το να προσθέσετε την εφαρμογή κλειδώματος οθόνης, να αναθεωρήσετε την πρόσβαση τρίτων στα δεδομένα του Google Account σας και να μάθετε ποια sites και εφαρμογές είναι πιθανόν να έχετε επιτρέψει να συνδεθούν μέσω του Google Account σας. Επισκεφθείτε το https://myaccount.google.com/security-checkup για να κάνετε τον δικό σας Έλεγχο Ασφαλείας.

4. Ορίστε και διατηρήστε ενημερωμένο έναν αριθμό τηλεφώνου ή ένα email ανάκτησης

Η προσθήκη πληροφοριών ανάκτησης, όπως ο αριθμός τηλεφώνου ή το email, μπορεί να σας βοηθήσει να ανακτήσετε πιο γρήγορα το λογαριασμό σας εάν χάσετε την πρόσβαση σ' αυτόν ή δεν μπορείτε να συνδεθείτε. Αν αλλάξουν τα στοιχεία αυτά, θυμηθείτε να ενημερώσετε την εφαρμογή. Σε πολλές περιπτώσεις, ένας αριθμός τηλεφώνου ή μια διεύθυνση email μπορούν να χρησιμοποιηθούν για να ειδοποιηθείτε σχετικά με ύποπτες κινήσεις στο λογαριασμό σας ή για να μπλοκαριστεί κάποιος που θέλει να τον χρησιμοποιήσει χωρίς την άδειά σας. Για παράδειγμα, εάν μια άγνωστη συσκευή χρησιμοποιείται για να συνδεθεί στο Google Account σας, ενδέχεται να σας ζητηθεί να επαληθεύσετε ότι η σύνδεση είναι εξουσιοδοτημένη εισάγοντας έναν κωδικό που αποστέλλεται στον αριθμό τηλεφώνου ανάκτησης. Για να ρυθμίσετε τις πληροφορίες ανάκτησης στο Google Account σας, επισκεφθείτε τη διεύθυνση security.google.com και κάντε κλικ στην επιλογή «Προσωπικές Πληροφορίες».

5. Ορίστε επαλήθευση σε 2 βήματα

Κάντε ένα ακόμη βήμα για τη διασφάλιση των λογαριασμών σας, ορίζοντας επαλήθευση σε 2 βήματα, η οποία απαιτεί να χρησιμοποιήσετε ένα δεύτερο βήμα εκτός από το όνομα χρήστη και τον κωδικό πρόσβασής σας για να συνδεθείτε στο λογαριασμό σας. Παραδείγματα δευτέρων βημάτων επαλήθευσης περιλαμβάνουν: έναν εξαψήφιο κωδικό που δημιουργείται από μια εφαρμογή, μια ερώτηση που λαμβάνετε σε μια αξιόπιστη συσκευή ή τη χρήση ενός κλειδιού φυσικής ασφάλειας (η ισχυρότερη μορφή ενός δεύτερου βήματος). Η δημιουργία επαλήθευσης σε 2 βήματα θα μειώσει σημαντικά την πιθανότητα κάποιος να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο λογαριασμό σας. Αφού ρυθμίσετε την επαλήθευση σε 2 βήματα για έναν λογαριασμό, θυμηθείτε να είστε έτοιμοι για το δεύτερο βήμα επαλήθευσης κάθε φορά που συνδέεστε. Για να ρυθμίσετε την επαλήθευση σε 2 βήματα στο Google Account σας, επισκεφτείτε τη διεύθυνση security.google.com και κάντε κλικ στο κουμπί «Επαλήθευση σε 2 βήματα».

Προστατεύστε τα παιδιά σας

Αν έχετε παιδιά, μιλήστε τους από νωρίς για την ασφάλεια στο Διαδίκτυο και ρυθμίστε τους ψηφιακούς κανόνες για το σπίτι σας. Όπως συστήνει η Google, ακριβώς όπως διδάσκουμε στα παιδιά μας πώς να οδηγούν πριν τους δώσουμε τα κλειδιά του αυτοκινήτου, έτσι είναι χρήσιμο να διδάξετε στα νέα παιδιά τις αρχές της ηλεκτρονικής ασφάλειας πριν τους παραδώσετε μια συσκευή.

Μόλις κερδίσουν την «άδεια οδήγησης» στο Διαδίκτυο, είναι επίσης χρήσιμο να καθορίσετε κάποιους ψηφιακούς κανόνες καθώς αρχίζουν να εξερευνούν. Αν τα παιδιά σας διαθέτουν συσκευή Android ή Chromebook, μπορείτε να χρησιμοποιήσετε την εφαρμογή Family Link για να κάνετε πράγματα όπως διαχείριση των ρυθμίσεων του Λογαριασμού Google, έγκριση ή αποκλεισμό των εφαρμογών και των

https://newsall.gr/

Publication date: 05/02/2019 23:05

https://newsall.gr/2019/02/05/%ce%ad%cf%81%ce%b5%cf%85%ce%bd%ce%b1-go...

ιστότοπων που μπορούν να χρησιμοποιήσουν και να ορίσετε χρονικά όρια οθόνης. Μπορείτε να μάθετε περισσότερα στο google.com/familylink.

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

ΠΗΓΗ:

http://www.in.gr/

Publication date: 05/02/2019 22:47

Alexa ranking (Greece): 38

https://www.in.gr/2019/02/05/greece/ereyna-google-enas-stous-deka-ellines-thyma...

Έρευνα Google: Ένας στους δέκα Έλληνες θύμα ηλεκτρονικής απάτης

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του in.gr

Θύμα ηλεκτρονικής απάτης έχει πέσει ένας στους δέκα Έλληνες, όπως αποκαλύπτει έρευνα της Google, καθώς δεν αλλάζει ποτέ τον κωδικό πρόσβασης του.

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η Google παρουσίασε μια έρευνα που έχει ανατεθεί στη YouGov σχετικά με το θέμα της ιδιωτικής ζωής και της ασφάλειας στο Διαδίκτυο.

Οι Έλληνες που συμμετείχαν στη έρευνα δήλωσαν ότι σε ποσοστό 49% έχουν λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (Phishing). Το 23% έχει εκτεθεί σε κακόβουλο λογισμικό, το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα social media, ενώ το 9% -σχεδόν ένας στους 10- έχει υπάρξει θύμα ηλεκτρονικής απάτης.

Από την άλλη, όσον αφορά στις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί ενώ το 11% δεν τον αλλάζει ποτέ.

Το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

Τα τραπεζικά δεδομένα κύρια ανησυχία

Σχετικά με το ποιες πληροφορίες θέλουν να προστατεύσουν περισσότερο, το 59% ανησυχεί κυρίως για τις οικονομικές του πληροφορίες (όπως τραπεζικά δεδομένα), 16% ανησυχεί για τις προσωπικές του πληροφορίες (όπως διεύθυνση κατοικίας), 6% για πληροφορίες σχετικά με προσωπικές στιγμές (όπως φωτογραφίες) και 7% για την παρακολούθηση ηλεκτρονικών μηνυμάτων που στέλνει σε συναδέλφους.

Σε δήλωσή του, ο Manager, Corporate Communication & Public Affairs για Ιταλία, Ελλάδα, Μάλτα, Κλαούντιο Μοντεβέρντε ανέφερε πως η Google δημιουργεί εργαλεία για προστασία σε ό,τι κάνει, ώστε οι χρήστες της να είναι σίγουροι ότι τα προσωπικά τους δεδομένα είναι ασφαλή. Ωστόσο, όπως συμπλήρωσε ο ίδιος, εξακολουθούν να υπάρχουν κάποιες βέλτιστες πρακτικές που μπορεί να ακολουθήσει κανείς και η οικογένειά του, για να διασφαλίσει ότι είναι ασφαλείς όχι μόνο ενώ χρησιμοποιεί το Google αλλά και κατά την πλοήγηση του στο ευρύτερο Διαδίκτυο.

Με αφορμή την Ημέρα Ασφαλούς Διαδικτύου η Google παρουσιάζει μερικές χρήσιμες συμβουλές:

1. Ενημερώστε το λογισμικό σας

Για να προστατεύετε τις δραστηριότητές σας στο διαδίκτυο, είναι πολύ σημαντικό να χρησιμοποιείτε πάντα τις πιο πρόσφατες εκδόσεις λογισμικού, λειτουργικού συστήματος και εφαρμογών σε όλες τις συσκευές σας. Σύμφωνα με τη Google, ορισμένες υπηρεσίες, όπως το Google Chrome, ενημερώνονται αυτόματα ενώ άλλες ειδοποιούν τους χρήστες σχετικά με το πότε πρέπει να τις ενημερώσουν.

2. Χρησιμοποιείτε μοναδικούς, ισχυρούς κωδικούς πρόσβασης

Χρησιμοποιώντας το ίδιο password για να συνδέεστε με διαφορετικούς λογαριασμούς διακινδυνεύετε περισσότερο την ασφάλειά σας. Είναι σαν να χρησιμοποιείτε το ίδιο κλειδί για να ανοίγετε τις πόρτες του σπιτιού, του γραφείου και του αυτοκινήτου σας. Όποιος αποκτήσει πρόσβαση σ' αυτό έχει πρόσβαση σε όλα τα υπάρχοντά σας. Για να περιορίσετε τον κίνδυνο, χρησιμοποιήστε διαφορετικό κωδικό για τον καθένα και επιδιώξτε κάθε κωδικός να είναι δύσκολο να τον μαντέψει κάποιος και να αποτελείται τουλάχιστον από οχτώ χαρακτήρες. Όπως αναφέρει η Google, επιλέξτε να χρησιμοποιήσετε έναν διαχειριστή κωδικών πρόσβασης, όπως αυτός που δημιουργείται στον Chrome σας, για να σας βοηθήσει να δημιουργήσετε, διασφαλίσετε και να ελέγχετε όλους του κωδικούς για τους online λογαριασμούς σας.

3. Κάντε έναν έλεγχο ασφαλείας

Ο Έλεγχος Ασφαλείας της Google, όπως τονίζει η εταιρεία, προσφέρει εξατομικευμένες συμβουλές ασφάλειας που μπορούν να συμβάλουν στην ενίσχυση της ασφάλειας του Google Account σας. Δεν σας βοηθά απλώς να παραμείνετε ασφαλείς όταν χρησιμοποιείτε το Google, αλλά περιέχει χρήσιμες συμβουλές για να είστε ασφαλείς και όταν περιηγείστε γενικά στο διαδίκτυο, όπως το να προσθέσετε την εφαρμογή κλειδώματος οθόνης, να αναθεωρήσετε την πρόσβαση τρίτων στα δεδομένα του Google Account σας και να μάθετε ποια sites και εφαρμογές είναι πιθανόν να έχετε επιτρέψει να συνδεθούν μέσω του Google

http://www.in.gr/

Publication date: 05/02/2019 22:47

Alexa ranking (Greece): 38

https://www.in.gr/2019/02/05/greece/ereyna-google-enas-stous-deka-ellines-thyma...

Account σας. Επισκεφθείτε το https://myaccount.google.com/security-checkup για να κάνετε τον δικό σας Έλεγχο Ασφαλείας.

4. Ορίστε και διατηρήστε ενημερωμένο έναν αριθμό τηλεφώνου ή ένα email ανάκτησης

Η προσθήκη πληροφοριών ανάκτησης, όπως ο αριθμός τηλεφώνου ή το email, μπορεί να σας βοηθήσει να ανακτήσετε πιο γρήγορα το λογαριασμό σας εάν χάσετε την πρόσβαση σ' αυτόν ή δεν μπορείτε να συνδεθείτε. Αν αλλάξουν τα στοιχεία αυτά, θυμηθείτε να ενημερώσετε την εφαρμογή. Σε πολλές περιπτώσεις, ένας αριθμός τηλεφώνου ή μια διεύθυνση email μπορούν να χρησιμοποιηθούν για να ειδοποιηθείτε σχετικά με ύποπτες κινήσεις στο λογαριασμό σας ή για να μπλοκαριστεί κάποιος που θέλει να τον χρησιμοποιήσει χωρίς την άδειά σας. Για παράδειγμα, εάν μια άγνωστη συσκευή χρησιμοποιείται για να συνδεθεί στο Google Account σας, ενδέχεται να σας ζητηθεί να επαληθεύσετε ότι η σύνδεση είναι εξουσιοδοτημένη εισάγοντας έναν κωδικό που αποστέλλεται στον αριθμό τηλεφώνου ανάκτησης. Για να ρυθμίσετε τις πληροφορίες ανάκτησης στο Google Account σας, επισκεφθείτε τη διεύθυνση security.google.com και κάντε κλικ στην επιλογή «Προσωπικές Πληροφορίες».

5. Ορίστε επαλήθευση σε 2 βήματα

Κάντε ένα ακόμη βήμα για τη διασφάλιση των λογαριασμών σας, ορίζοντας επαλήθευση σε 2 βήματα, η οποία απαιτεί να χρησιμοποιήσετε ένα δεύτερο βήμα εκτός από το όνομα χρήστη και τον κωδικό πρόσβασής σας για να συνδεθείτε στο λογαριασμό σας. Παραδείγματα δευτέρων βημάτων επαλήθευσης περιλαμβάνουν: έναν εξαψήφιο κωδικό που δημιουργείται από μια εφαρμογή, μια ερώτηση που λαμβάνετε σε μια αξιόπιστη συσκευή ή τη χρήση ενός κλειδιού φυσικής ασφάλειας (η ισχυρότερη μορφή ενός δεύτερου βήματος). Η δημιουργία επαλήθευσης σε 2 βήματα θα μειώσει σημαντικά την πιθανότητα κάποιος να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο λογαριασμό σας. Αφού ρυθμίσετε την επαλήθευση σε 2 βήματα για έναν λογαριασμό, θυμηθείτε να είστε έτοιμοι για το δεύτερο βήμα επαλήθευσης κάθε φορά που συνδέεστε. Για να ρυθμίσετε την επαλήθευση σε 2 βήματα στο Google Account σας, επισκεφτείτε τη διεύθυνση security.google.com και κάντε κλικ στο κουμπί «Επαλήθευση σε 2 βήματα».

Προστατεύστε τα παιδιά σας

Αν έχετε παιδιά, μιλήστε τους από νωρίς για την ασφάλεια στο Διαδίκτυο και ρυθμίστε τους ψηφιακούς κανόνες για το σπίτι σας. Όπως συστήνει η Google, ακριβώς όπως διδάσκουμε στα παιδιά μας πώς να οδηγούν πριν τους δώσουμε τα κλειδιά του αυτοκινήτου, έτσι είναι χρήσιμο να διδάξετε στα νέα παιδιά τις αρχές της ηλεκτρονικής ασφάλειας πριν τους παραδώσετε μια συσκευή.

Μόλις κερδίσουν την «άδεια οδήγησης» στο Διαδίκτυο, είναι επίσης χρήσιμο να καθορίσετε κάποιους ψηφιακούς κανόνες καθώς αρχίζουν να εξερευνούν. Αν τα παιδιά σας διαθέτουν συσκευή Android ή Chromebook, μπορείτε να χρησιμοποιήσετε την εφαρμογή Family Link για να κάνετε πράγματα όπως διαχείριση των ρυθμίσεων του Λογαριασμού Google, έγκριση ή αποκλεισμό των εφαρμογών και των ιστότοπων που μπορούν να χρησιμοποιήσουν και να ορίσετε χρονικά όρια οθόνης. Μπορείτε να μάθετε περισσότερα στο google.com/familylink.

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Σημειώνεται ότι, μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

ΑΔΑΕ: Πώς να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: in.gr

http://www.loutrakiblog.gr/

Publication date: 05/02/2019 20:06

Alexa ranking (Greece): 2283

http://www.loutrakiblog.gr/2019/02/blog-post_74.html

ΑΔΑΕ: Οι τέσσερις «χρυσοί» κανόνες για τους κωδικούς πρόσβασης

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου...
Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

• Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

• Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

• Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

• Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά στις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών

http://www.loutrakiblog.gr/
Publication date: 05/02/2019 20:06
Alexa ranking (Greece): 2283
http://www.loutrakiblog.gr/2019/02/blog-post_74.html

επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

cnn.gr

http://www.lamiakos-typos.gr/

Publication date: 05/02/2019 20:01

Alexa ranking (Greece): 8284

http://www.lamiakos-typos.gr/ellada-eidiseis/prosohi-stoys-kodikoys-prosvasis-syni...

Προσοχή στους κωδικούς πρόσβασης συνιστά στους χρήστες η ΑΔΑΕ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/ article/ symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/ enimerosi-christon-kai- syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://anakalipto.blogspot.gr/
Publication date: 05/02/2019 19:56
Alexa ranking (Greece): 0
https://anakalipto.blogspot.com/2019/02/blog-post_4.html

Οι τέσσερις «χρυσοί» κανόνες για τους κωδικούς πρόσβασης

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν

http://anakalipto.blogspot.gr/
Publication date: 05/02/2019 19:56
Alexa ranking (Greece): 0
https://anakalipto.blogspot.com/2019/02/blog-post_4.html

ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

• Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

• Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

• Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

• Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά στις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν

http://anakalipto.blogspot.gr/
Publication date: 05/02/2019 19:56
Alexa ranking (Greece): 0
https://anakalipto.blogspot.com/2019/02/blog-post_4.html

εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

cnn.gr

http://fonografos.net/v1/

Publication date: 05/02/2019 19:52

Alexa ranking (Greece): 3679

https://fonografos.net/v1/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%84%ce%b1-%cf%8...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**
* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο»,

υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.
Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ | iefimerida.gr

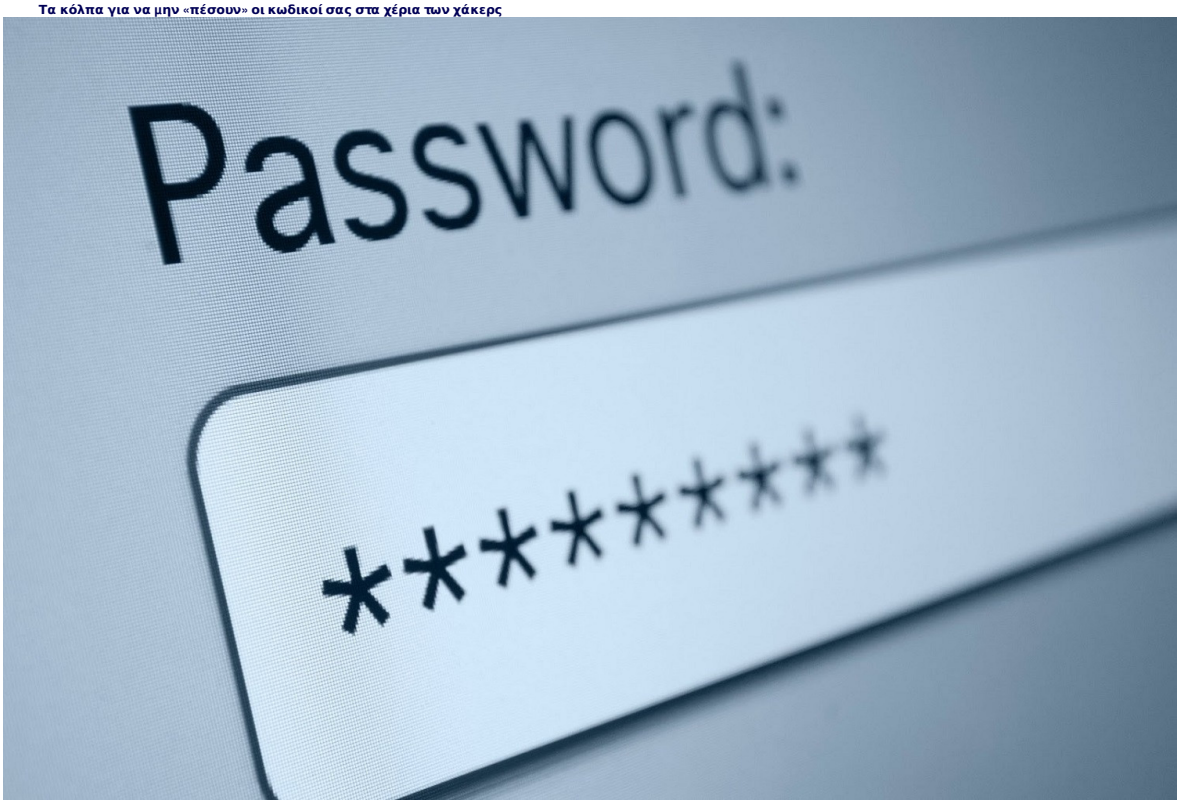
http://teleytaiaexodos.blogspot.gr/

Publication date: 05/02/2019 19:28

Alexa ranking (Greece): 0

http://teleytaiaexodos.blogspot.com/2019/02/blog-post_61.html

Τα κόλπα για να μην «πέσουν» οι κωδικοί σας στα χέρια των χάκερς



Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα

αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή, μέσω kozanara

https://www.ersanews.gr/

Publication date: 05/02/2019 19:23

Alexa ranking (Greece): 36272

https://www.ersanews.gr/article/3082683/ADAE-Pos-na-profylachthoume-apo-tous-...

ΑΔΑΕ: Πώς να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες:

Πηγή: MADATA.GR
05/02 19:23

http://monomaxoi.com/

Publication date: 05/02/2019 18:12

http://monomaxoi.com/2019/02/05/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%84%ce...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

http://monomaxoi.com/

Publication date: 05/02/2019 18:12

http://monomaxoi.com/2019/02/05/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%84%ce...

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

iefimerida.gr

https://thecaller.gr/

Publication date: 05/02/2019 17:58

Alexa ranking (Greece): 292

https://thecaller.gr/tech/adae-ta-mystika-gia-na-profylachtoyme-apo-toys-chaker/

ΑΔΑΕ: Τα μυστικά για να προφυλαχτούμε από τους χάκερ

Η νέα ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύο επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου.

Με το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Τονίζει δε ότι η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαν: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.flowmagazine.gr/

Publication date: 05/02/2019 17:52

https://www.flowmagazine.gr/adae_pos_na_profulaksoume_ta_password_apo_tous...

ΑΔΑΕ: Πώς να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: in.gr

http://www.enallaktikos.gr/

Publication date: 05/02/2019 17:32

Alexa ranking (Greece): 1019

http://www.enallaktikos.gr/ar45059el-adae-prosoxi-stoys-kwdikoys-prosvasis-odigie...

ΑΔΑΕ: Προσοχή στους κωδικούς πρόσβασης - Οδηγίες για ασφαλή passwords

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης www.adae.gr/nomothetiko-plaisio και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους www.adae.gr/cybersecurity

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις

http://www.enallaktikos.gr/

Publication date: 05/02/2019 17:32

Alexa ranking (Greece): 1019

http://www.enallaktikos.gr/ar45059el-adae-prosoxi-stoys-kwdikoys-prosvasis-odigie...

περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης www.adae.gr/nomothetiko-plaisio και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους www.adae.gr/cybersecurity

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

http://www.enallaktikos.gr/

Publication date: 05/02/2019 17:32

Alexa ranking (Greece): 1019

http://www.enallaktikos.gr/ar45059el-adae-prosoxi-stoys-kwdikoys-prosvasis-odigie...

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας

http://www.enallaktikos.gr/

Publication date: 05/02/2019 17:32

Alexa ranking (Greece): 1019

http://www.enallaktikos.gr/ar45059el-adae-prosoxi-stoys-kwdikoys-prosvasis-odigie...

καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης www.adae.gr/nomothetiko-plaisio και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους www.adae.gr/cybersecurity

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.enallaktikos.gr/

Publication date: 05/02/2019 17:32

Alexa ranking (Greece): 1019

http://www.enallaktikos.gr/ar45059el-adae-prosoxi-stoys-kwdikoys-prosvasis-odigie...

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης www.adae.gr/nomothetiko-plaisio και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους www.adae.gr/cybersecurity

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

http://www.enallaktikos.gr/

Publication date: 05/02/2019 17:32

Alexa ranking (Greece): 1019

http://www.enallaktikos.gr/ar45059el-adae-prosoxi-stoys-kwdikoys-prosvasis-odigie...

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.asfalisinet.gr/

Publication date: 05/02/2019 17:29

Alexa ranking (Greece): 5781

https://www.asfalisinet.gr/%ce%bf%ce%b9-%ce%b9%cf%83%cf%87%cf%85%cf%81...

Οι ισχυροί κωδικοί πρόσβασης στο διαδίκτυο ασπίδα για την ιδιωτικότητα [Video]

Ραδιοφωνική καμπάνια και ενημερωτικό video της ΑΔΑΕ με αφορμή την Ημέρα Ασφαλούς Διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται το ΕΝΗΜΕΡΩΤΙΚΟ VIDEO και η ΡΑΔΙΟΦΩΝΙΚΗ ΚΑΜΠΑΝΙΑ της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατομ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Η είδηση κάνει ακόμη πιο επίκαιρη τη ραδιοφωνική καμπάνια της ΑΔΑΕ για τους κωδικούς πρόσβασης. Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής **ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης** και **ποια μέτρα** θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, ***«Μαζί για ένα καλύτερο διαδίκτυο»***, υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις. Μέσα στο 2018, επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

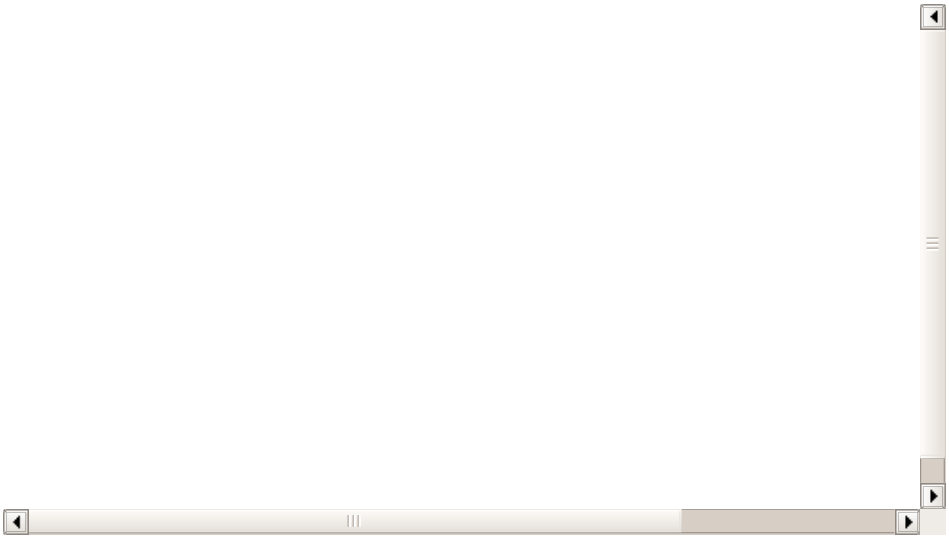
Δείτε το βίντεο για ασφαλείς κωδικούς πρόσβασης

https://www.asfalisinet.gr/

Publication date: 05/02/2019 17:29

Alexa ranking (Greece): 5781

https://www.asfalisinet.gr/%ce%bf%ce%b9-%ce%b9%cf%83%cf%87%cf%85%cf%81...



http://www.topontiki.gr/

Publication date: 05/02/2019 16:34

Alexa ranking (Greece): 214

http://www.topontiki.gr/article/308275/adae-pos-na-profylahthoyme-apo-toys-haker

ΕΛΛΑΔΑ

5.2.2019 / ΤΟ ΠΟΝΤΙΚΙ WEB

ΑΔΑΕ: Πώς να προφυλαχθούμε από τους χάκερ

-
- EMAIL
- Εκτύπωση

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

http://www.topontiki.gr/

Publication date: 05/02/2019 16:34

Alexa ranking (Greece): 214

http://www.topontiki.gr/article/308275/adae-pos-na-profylahthoyme-apo-toys-haker

- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: **in.gr**
ΑΔΑΕ
προστασία

http://kefaloniapress.gr/

Publication date: 05/02/2019 16:27

Alexa ranking (Greece): 1566

http://www.kefaloniapress.gr/2019/02/05/adae-ta-trik-sto-password-gia-na-profylac...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.
Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**
* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

http://kefaloniapress.gr/

Publication date: 05/02/2019 16:27

Alexa ranking (Greece): 1566

http://www.kefaloniapress.gr/2019/02/05/adae-ta-trik-sto-password-gia-na-profylac...

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.epixeiro.gr/

Publication date: 05/02/2019 15:56

Alexa ranking (Greece): 1260

http://www.epixeiro.gr/article/112617

Οι ισχυροί κωδικοί πρόσβασης στο διαδίκτυο ασπίδα για την ιδιωτικότητα [video]

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται το ενημερωτικό video και η ραδιοφωνική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: «*Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις;*». Πρώτα απ' όλα, όπως σημειώνει η ΑΔΑΕ, ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατομ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή ***πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες,*** σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε **ισχυρούς κωδικούς πρόσβασης**, **διαφορετικούς** για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να **τους ανανεώνετε τακτικά** (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι **και μυστικό.** Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι **να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης** στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει **μόνο αν** ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). **Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας** που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «***Μαζί για ένα καλύτερο διαδίκτυο***», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

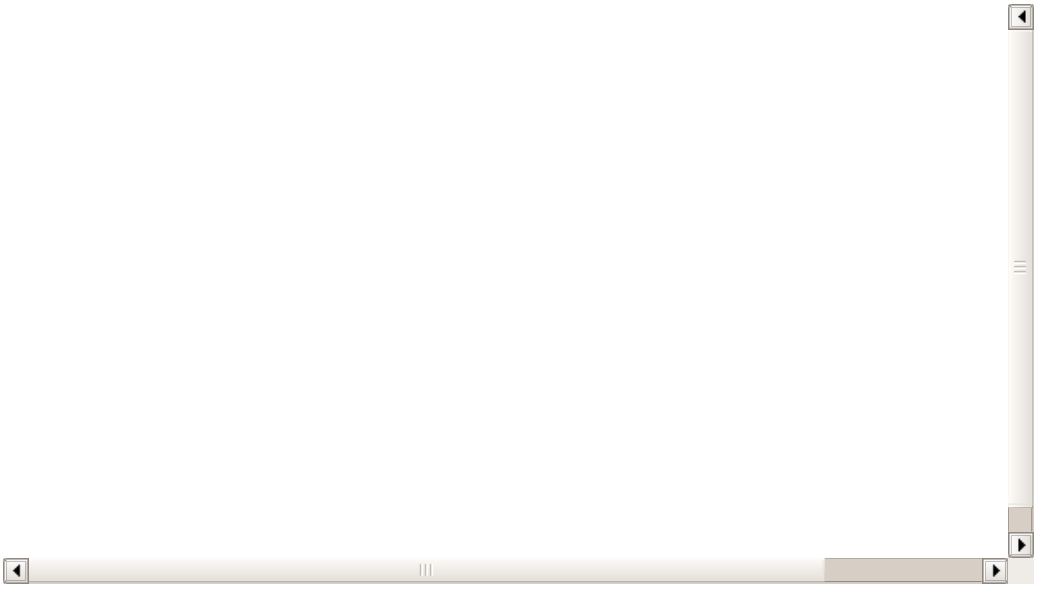
Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις. Μέσα στο 2018, επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.epixeiro.gr/

Publication date: 05/02/2019 15:56

Alexa ranking (Greece): 1260

http://www.epixeiro.gr/article/112617



https://www.parapolitikakritis.gr/
Publication date: 05/02/2019 15:41
Alexa ranking (Greece): 1608
https://www.parapolitikakritis.gr/pagkosmia-imera-asfaloys-diadiktyoy-pos-na-prof...

Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου : Πώς να προφυλάξετε τα password σας

Από **Παπ_Editor**

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ(1): 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

https://www.parapolitikakritis.gr/

Publication date: 05/02/2019 15:41

Alexa ranking (Greece): 1608

https://www.parapolitikakritis.gr/pagkosmia-imera-asfaloys-diadiktyoy-pos-na-prof...

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.enikonomia.gr/

Publication date: 05/02/2019 15:39

Alexa ranking (Greece): 813

http://www.enikonomia.gr/timeliness/207556,chrisimes-symvoules-gia-prostasia-ap...

Χρήσιμες συμβουλές για προστασία από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: ΑΠΕ- ΜΠΕ

http://www.enikonomia.gr/
Publication date: 05/02/2019 15:39
Alexa ranking (Greece): 813
http://www.enikonomia.gr/timeliness/207556,chrisimes-symvoules-gia-prostasia-ap...

#ΔΙΑΔΙΚΤΥΟ #ΑΣΦΑΛΕΙΑ #ΚΩΔΙΚΟΙ #ΟΔΗΓΙΕΣ

- share
-
-
-
-

http://dhmak-elta.blogspot.com/
Publication date: 05/02/2019 14:58
Alexa ranking (Greece): 24939
http://dhmak-elta.blogspot.com/2019/02/blog-post_53.html

ΑΔΑΕ: Πώς να προφυλάξετε τους κωδικούς σας από τους χάκερς

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς

http://dhmak-elta.blogspot.com/
Publication date: 05/02/2019 14:58
Alexa ranking (Greece): 24939
http://dhmak-elta.blogspot.com/2019/02/blog-post_53.html

υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων. eisodima

https://www.typosthes.gr/

Publication date: 05/02/2019 14:02

Alexa ranking (Greece): 830

https://www.typosthes.gr/koinonia/176285_prosohi-stoys-kodikoys-prosbasis-oi-4-...

Προσοχή στους κωδικούς πρόσβασης – Οι 4 «χρυσοί» κανόνες

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου, σύμφωνα με το ΑΠΕ-ΜΠΕ.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

• Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

• Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

• Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

• Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://ioannina24.gr/

Publication date: 05/02/2019 13:13

Alexa ranking (Greece): 13514

http://ioannina24.gr/%CE%B5%CE%B9%CE%B4%CE%B7%CF%83%CE%B5%CE%B9%...

Η ΑΔΑΕ προειδοποιεί: Προσοχή στους κωδικούς πρόσβασης

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας. Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής. Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους >http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/ Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα: * Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον). * Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου. * Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού. * Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν. Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων. Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας. Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις. Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

- -- Πηγή: RIZOPOULOSPOST.gr

http://ioannina24.gr/

Publication date: 05/02/2019 13:13

Alexa ranking (Greece): 13514

http://ioannina24.gr/%CE%B5%CE%B9%CE%B4%CE%B7%CF%83%CE%B5%CE%B9%...

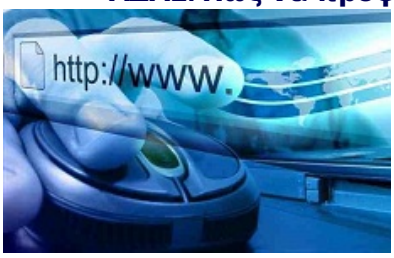
http://www.eisodima.gr/

Publication date: 05/02/2019 13:13

Alexa ranking (Greece): 13407

http://www.eisodima.gr/2019/02/blog-post_49.html

ΑΔΑΕ: Πώς να προφυλάξετε τους κωδικούς σας από τους χάκερς



Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

(ΤΡ 5/2/19)

https://agrinio24.eu/
Publication date: 05/02/2019 12:57
Alexa ranking (Greece): 11970
https://agrinio24.eu/archives/404290

Οδηγίες της ΑΔΑΕ για την ασφάλειά σας στο διαδίκτυο

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

https://agrinio24.eu/

Publication date: 05/02/2019 12:57

Alexa ranking (Greece): 11970

https://agrinio24.eu/archives/404290

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

tovima.gr

https://agrinio24.eu/

Publication date: 05/02/2019 12:57

Alexa ranking (Greece): 11970

https://agrinio24.eu/archives/404290

http://radio4.gr/

Publication date: 05/02/2019 12:56

Alexa ranking (Greece): 38353

https://radio4.gr/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%80%cf%89%cf%82-%ce%bd...

ΑΔΑΕ: Πως να προφυλάξουμε τα password από τους χάκερ

ΑΔΑΕ: Πως να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

http://radio4.gr/

Publication date: 05/02/2019 12:56

Alexa ranking (Greece): 38353

https://radio4.gr/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%80%cf%89%cf%82-%ce%bd...

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.briefingnews.gr/

Publication date: 05/02/2019 12:51

Alexa ranking (Greece): 3462

https://www.briefingnews.gr/oikonomia/adae-pos-na-profylaxoyme-ta-password-a...

ΑΔΑΕ: Πως να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://1news.gr/

Publication date: 05/02/2019 12:46

Alexa ranking (Greece): 12691

https://1news.gr/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%84%ce%b1-%cf%84%cf%81...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ

Κοινοποίηση

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς

https://1news.gr/
Publication date: 05/02/2019 12:46
Alexa ranking (Greece): 12691
https://1news.gr/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%84%ce%b1-%cf%84%cf%81...

υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.
Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

iefimerida.gr

https://www.ersanews.gr/

Publication date: 05/02/2019 12:45

Alexa ranking (Greece): 36272

https://www.ersanews.gr/article/3080885/Odigies-tis-ADAE-gia-tin-asfaleia-sas-sto-...

Οδηγίες της ΑΔΑΕ για την ασφάλειά σας στο διαδίκτυο

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Πηγή: ΤΟ ΒΗΜΑ
05/02 10:27

https://www.wepost.gr/

Publication date: 05/02/2019 12:40

Alexa ranking (Greece): 3656

https://www.wepost.gr/%cf%80%cf%8e%cf%82-%ce%bd%ce%b1-%ce%b4%ce%b7%...

Πώς να δημιουργήσετε ισχυρά passwords

Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η σημερινή

Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Οι **κωδικοί πρόσβασης** είναι ο νούμερο 1 κίνδυνος σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς **ηλεκτρονικών επικοινωνιών**, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.sepe.gr/
Publication date: 05/02/2019 12:36
Alexa ranking (Greece): 9461
http://www.sepe.gr/gr/InformationTechnology/it-article/12852166/i-adae-proeidop...

Η ΑΔΑΕ προειδοποιεί-Πώς θα δημιουργήσετε ισχυρούς κωδικούς πρόσβασης

Πληροφορική

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Δείτε περισσότερα: skai.gr

https://www.tovima.gr/

Publication date: 05/02/2019 12:36

Alexa ranking (Greece): 156

https://www.tovima.gr/2019/02/05/finance/odigies-tis-adae-gia-tin-asfaleia-sas-sto-...

Οδηγίες της ΑΔΑΕ για την ασφάλειά σας στο διαδίκτυο

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

ToBHMA Team

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου

https://www.tovima.gr/

Publication date: 05/02/2019 12:36

Alexa ranking (Greece): 156

https://www.tovima.gr/2019/02/05/finance/odigies-tis-adae-gia-tin-asfaleia-sas-sto-...

2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Δείτε επίσης

- ΑΔΑΕ
- ασφάλεια στο διαδίκτυο
- Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

https://typos-i.gr/

Publication date: 05/02/2019 12:32

Alexa ranking (Greece): 4230

https://typos-i.gr/article/8yma-hlektronikhs-apaths-enas-stoys-10-ellhnes

Θύμα ηλεκτρονικής απάτης ένας στους 10 Έλληνες

Ένας στους δέκα Έλληνες έχει υπάρξει θύμα ηλεκτρονικής απάτης, ενώ δεν αλλάζει ποτέ τον κωδικό πρόσβασής του (password). Αυτό αποκαλύπτει, με αφορμή τη φετινή Ημέρα Ασφαλούς Διαδικτύου, μια νέα έρευνα της Google. Η ασφάλεια στο διαδίκτυο είναι σημαντική, αλλά αρκετοί Έλληνες μάλλον δεν κάνουν ούτε τα βασικά για να προστατευθούν.

Όσον αφορά τους διαδικτυακούς κινδύνους, οι Έλληνες ερωτηθέντες δήλωσαν ότι το 9% έχει πέσει θύμα ηλεκτρονικής απάτης, το 49% έχει λάβει μηνύματα ηλεκτρονικού «ψαρέματος» (phishing), το 23% έχει εκτεθεί σε κακόβουλο λογισμικό και το 13% έχει πέσει θύμα μη εξουσιοδοτημένης πρόσβασης στα προφίλ που διατηρεί στα μέσα κοινωνικής δικτύωσης.

Όσον αφορά τις διαδικτυακές ρυθμίσεις, το 34% χρησιμοποιεί τον ίδιο κωδικό πρόσβασης (password) για μερικές ή και όλες τις ηλεκτρονικές υπηρεσίες που χρησιμοποιεί, ενώ το 11% δεν τον αλλάζει ποτέ.

Τέλος, το 20% δεν έχει χρησιμοποιήσει ποτέ ένα δεύτερο επίπεδο προστασίας στον λογαριασμό του, όπως η επαλήθευση σε δύο στάδια, ενώ το 38% τη χρησιμοποιεί μόνο σε μερικούς λογαριασμούς αλλά όχι σε όλους.

Στην ερώτηση «πόσες φορές ενημερώνετε το πρόγραμμα περιήγησής σας», το 22% των ερωτηθέντων λέει ότι το κάνει αρκετές φορές τον ίδιο μήνα, αλλά το 12% δήλωσε ότι το ενημερώνει λιγότερο από μία φορά κάθε έξι μήνες, ενώ παραπάνω από το 14% δήλωσε ότι δεν το ενημερώνει ποτέ.

Ποιες όμως είναι οι πληροφορίες που θέλουν οι Έλληνες να προστατεύσουν περισσότερο; Το 59% ανησυχεί κυρίως για τις οικονομικές του πληροφορίες (όπως τραπεζικά δεδομένα), το 16% ανησυχεί για τις προσωπικές του πληροφορίες (όπως διεύθυνση κατοικίας), το 6% για πληροφορίες σχετικά με προσωπικές στιγμές (όπως φωτογραφίες) και το 7% για την παρακολούθηση ηλεκτρονικών μηνυμάτων που στέλνει σε συναδέλφους.

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα

https://typos-i.gr/

Publication date: 05/02/2019 12:32

Alexa ranking (Greece): 4230

https://typos-i.gr/article/8yma-hlektronikhs-apaths-enas-stoys-10-ellhnes

πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://dete.gr/

Publication date: 05/02/2019 12:27

Alexa ranking (Greece): 886

https://dete.gr/%ce%91%ce%94%ce%91%ce%95-%ce%a4%ce%b1-%cf%84%cf%81%...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.
Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**
* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.
Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς,

https://dete.gr/

Publication date: 05/02/2019 12:27

Alexa ranking (Greece): 886

https://dete.gr/%ce%91%ce%94%ce%91%ce%95-%ce%a4%ce%b1-%cf%84%cf%81%...

όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://keramidi-valtou.blogspot.gr/
Publication date: 05/02/2019 12:22
Alexa ranking (Greece): 0
https://keramidi-valtou.blogspot.com/2019/02/adae-ta-trik-sto-password-gia-na-pr...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ..

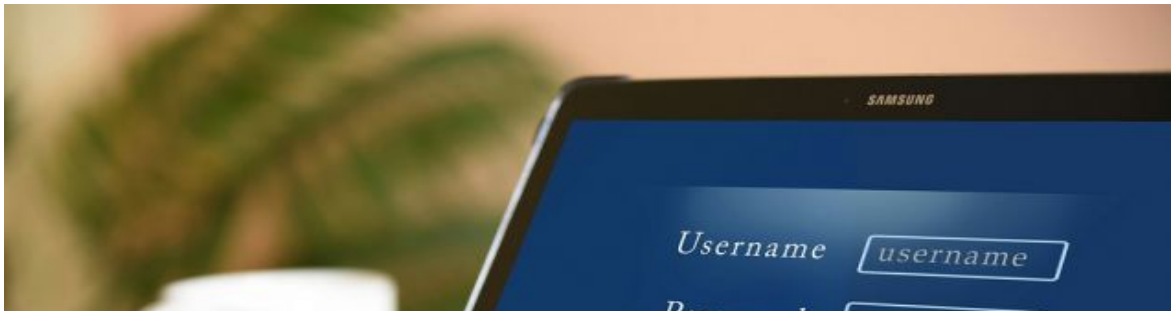
Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.
Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**
* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.



https://keramidi-valtou.blogspot.gr/

Publication date: 05/02/2019 12:22

Alexa ranking (Greece): 0

https://keramidi-valtou.blogspot.com/2019/02/adae-ta-trik-sto-password-gia-na-pr...

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.
Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας.

Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.
Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.
Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

NewsOne

Πηγή ανάρτησης: **www.newsone.gr**

https://www.daily-news.gr/

Publication date: 05/02/2019 12:18

Alexa ranking (Greece): 22904

https://www.daily-news.gr/technologia/%cf%80%cf%8e%cf%82-%ce%bd%ce%b1-%c...

Πώς να δημιουργήσετε ισχυρά passwords

Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Οι **κωδικοί πρόσβασης** είναι ο νούμερο 1 κίνδυνος σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

googletag.cmd.push(function() { googletag.display('div-gpt-ad-1539094824448-0'); });

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για **χάκερς** τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα **passwords** περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε

https://www.daily-news.gr/

Publication date: 05/02/2019 12:18

Alexa ranking (Greece): 22904

https://www.daily-news.gr/technologia/%cf%80%cf%8e%cf%82-%ce%bd%ce%b1-%c...

μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές **password** θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς **ηλεκτρονικών επικοινωνιών**, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

ΑΞΙΟΛΟΓΗΣΤΕ ΤΟ ΑΡΘΡΟ

localStorage.clear();

Πηγή

http://www.sport-fm.gr/

Publication date: 05/02/2019 12:16

Alexa ranking (Greece): 48

http://www.sport-fm.gr/article/epikairotita/i-adae-proeidopoiei-pws-tha-dimiourgis...

Η ΑΔΑΕ προειδοποιεί - Πώς θα δημιουργήσετε ισχυρούς κωδικούς πρόσβασης

Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις;

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

•Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

•Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

•Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

•Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.sport-fm.gr/
Publication date: 05/02/2019 12:16
Alexa ranking (Greece): 48
http://www.sport-fm.gr/article/epikairotita/i-adae-proeidopoiei-pws-tha-dimiourgis...

Πηγή: **skai.gr**

https://www.eleftheriaonline.gr/

Publication date: 05/02/2019 12:10

Alexa ranking (Greece): 1123

https://www.eleftheriaonline.gr/new/item/177367-prosoxi-stous-kodikoys-prosvasis...

Προσοχή στους κωδικούς πρόσβασης συνιστά στους χρήστες η ΑΔΑΕ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

ΑΠΕ-ΜΠΕ

https://www.typosthes.gr/

Publication date: 05/02/2019 12:09

Alexa ranking (Greece): 830

https://www.typosthes.gr/koinonia/176285_prosohi-stoys-kodikoys-prosbasis-synis...

Προσοχή στους κωδικούς πρόσβασης συνιστά στους χρήστες η ΑΔΑΕ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου, σύμφωνα με το ΑΠΕ-ΜΠΕ.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

• Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

• Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

• Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

• Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.athensmagazine.gr/

Publication date: 05/02/2019 12:09

Alexa ranking (Greece): 330

https://www.athensmagazine.gr/article/tech/385128-pagkosmia-hmera-asfaloys-pl...

Παγκόσμια Ημέρα Ασφαλούς Πλοήγησης στο Διαδίκτυο: Έξυπνα τρικ στο password για να προφυλαχθείς από τους χάκερ!

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία.

Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας.

Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

http://www.athensmagazine.gr/

Publication date: 05/02/2019 12:09

Alexa ranking (Greece): 330

https://www.athensmagazine.gr/article/tech/385128-pagkosmia-hmera-asfaloys-pl...

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.mononews.gr/

Publication date: 05/02/2019 12:06

Alexa ranking (Greece): 471

https://www.mononews.gr/society/simvoules-apo-adae-pos-tha-dimiourgisete-ischi...

Συμβουλές από ΑΔΑΕ: Πώς θα δημιουργήσετε ισχυρούς κωδικούς πρόσβασης

Από
NewsRoom
-

Με νέα καμπάνια υποδέχεται η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), τη σημερινή ημέρα, που έχει οριστεί ως Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Κεντρικό μήνυμα της καμπάνιας είναι η προστασία της ιδιωτικότητας των χρηστών και στόχος της είναι να μπορέσει να λύσει τον κύριο προβληματισμό τους: ποια στοιχεία αποτελούν τους πιο επιρρεπείς στόχους σε κυβερνοεπιθέσεις και τι μπορούμε εμείς να κάνουμε γι' αυτό;

Το πρώτο και απλούστερο βήμα που μπορούμε να κάνουμε προκειμένου να προστατεύσουμε τα προσωπικά μας στοιχεία στο διαδίκτυο είναι να χρησιμοποιούμε κωδικούς πρόσβασης. Η λογική, με την οποία ορίζουμε ένα συγκεκριμένο κωδικό και ο τρόπος που τον χρησιμοποιούμε είναι μείζονος σημασίας, γεγονός που επισφραγίστηκε από ένα μεγάλο γεγονός του περασμένου Δεκέμβρη: ένα εκτεταμένο περιστατικό υποκλοπής, με την ανάρτηση 21 εκατομμυρίων κωδικών πρόσβασης και προσωπικών email, σε ένα φόρουμ για χάκερς.

Την αποκάλυψη του τεράστιου επεισοδίου έκανε ο ερευνητής σε θέματα ασφαλείας, Τρόι Χαντ, που τόνισε πως το εν λόγω περιστατικό αποτελεί τη μεγαλύτερη συγκέντρωση υποκλαπέντων στοιχείων στην ιστορία του Διαδικτύου. Ο Χαντ εξήγησε πως ο λόγος που η λίστα με τα στοιχεία αυτά ήταν εξαιρετικά χρήσιμη για τους κακόβουλους χρήστες, είναι ότι πολλοί χρήστες χρησιμοποιούν ένα κωδικό, για πολλές υπηρεσίες. Επομένως, με ένα κωδικό για κάθε χρήστη, που είχαν στα στοιχεία που συγκέντρωσαν, μπορούσαν θεωρητικά, να παραβιάσουν πολλές από τις εφαρμογές που χρησιμοποιεί ένας άνθρωπος, και να έχουν, άρα, πολλαπλό κέρδος.

Στον ιστότοπο της ΑΔΑΕ, οι χρήστες του Διαδικτύου μπορούν να ενημερωθούν για τους τρόπους, με τους οποίους μπορούν να δημιουργήσουν κωδικούς υψηλής προστασίας και χαμηλής δυνατότητας παραβίασης, καθώς και για τα μέτρα προστασίας, που πρέπει να παίρνουν, προκειμένου να εξασφαλίζουν το απόρρητο των επικοινωνιών τους.

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

«Μαζί για ένα καλύτερο διαδίκτυο» είναι η κεντρική ιδέα της φετινής Παγκόσμιας Ημέρας Ασφαλούς Διαδικτύου, και επιθυμεί να υπογραμμίσει ότι η εξασφάλιση της ασφαλούς διαδικτυακής πλοήγησης είναι ένα ζήτημα που αφορά όλους, από τον απλό χρήστη, έως τις μεγάλες εταιρείες, τους ειδικούς ηλεκτρονικών υπολογιστών και τις κυβερνήσεις.

Είναι υποχρέωση του κάθε χρήστη να απολαμβάνει τις διαρκώς εξελισσόμενες δυνατότητες της ψηφιακής τεχνολογίας, παραμένοντας συνειδητοποιημένος ως προς τους κινδύνους που ενέχονται σε αυτή και παίρνοντας δραστικά μέτρα ασφαλείας.

Η ΑΔΑΕ επικεντρώνεται ιδιαίτερα και στις οδηγίες ασφαλείας, σε ό,τι αφορά στις εταιρείες παρόχους, στις οποίες επιθυμεί να εμφυσήσει μια γενικότερη κουλτούρα ασφαλείας.

Στοχεύοντας στην πρόληψη και τον περιορισμό των κινδύνων, αναφορικά με την ιδιωτικότητα της επικοινωνίας, η Αρχή χρησιμοποιεί τις εξουσίες της, επιβάλλοντας μια σειρά μέτρων ασφαλείας στους παρόχους. Οι «Πολιτικές Ασφαλείας» εφαρμόζονται πλέον από τις μεγαλύτερες εταιρείες παρόχων, που καλύπτουν το 95% της αγοράς ηλεκτρονικών επικοινωνιών.

Σε δεύτερο στάδιο, η Αρχή λειτουργεί ελεγκτικά, για να εξασφαλίσει ότι οι Κανονισμοί εφαρμόζονται κατά το δοκούν, ενώ ταυτόχρονα εξετάζει και καταγγελίες χρηστών. Όταν και όπου παρατηρούνται παραβιάσεις επί των κανονισμών, η Αρχή επιβάλλει διοικητικές κυρώσεις.

http://www.mononews.gr/

Publication date: 05/02/2019 12:06

Alexa ranking (Greece): 471

https://www.mononews.gr/society/simvoules-apo-adae-pos-tha-dimiourgisete-ischi...

Συγκεκριμένα, το περασμένο έτος, επιβλήθηκαν συνολικά 41 διοικητικές κυρώσεις, στις οποίες συμπεριλαμβάνονταν και 8 περιστατικά σύστασης, συνολικού χρηματικού ύψους 2,5 εκατομμυρίων.

https://www.kostoday.com/

Publication date: 05/02/2019 12:06

Alexa ranking (Greece): 4405

https://www.kostoday.com/%CF%84%CE%B5%CF%87%CE%BD%CE%BF%CE%BB%C...

Παγκόσμια ημέρα ασφαλούς διαδικτύου: Καμπάνια της ΑΔΑΕ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα Τρίτη, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/> και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων. πηγή thetoc.gr

https://www.kostoday.com/

Publication date: 05/02/2019 12:06

Alexa ranking (Greece): 4405

https://www.kostoday.com/%CF%84%CE%B5%CF%87%CE%BD%CE%BF%CE%BB%C...

http://www.dimokratiki.gr/

Publication date: 05/02/2019 11:57

Alexa ranking (Greece): 704

https://www.dimokratiki.gr/05-02-2019/pagkosmia-imera-asfaloys-diadiktyoy-kamp...

δημοκρατική Παγκόσμια ημέρα ασφαλούς διαδικτύου: Καμπάνια της ΑΔΑΕ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα Τρίτη, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/> και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων. πηγή thetoc.gr

https://www.msn.com/el-gr/

Publication date: 05/02/2019 11:54

Alexa ranking (Greece): 71

https://www.msn.com/el-gr/news/techandscience/%ce%b1%ce%b4%ce%b1%ce%b...

ΑΔΑΕ: Οι τέσσερις «χρυσοί» κανόνες για τους κωδικούς πρόσβασης

www.cnn.gr

Στην **προστασίατης ιδιωτικότητας** των χρηστών του διαδικτύου επικεντρώνεται η **ενημερωτική καμπάνια** (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (**ΑΔΑΕ**), η οποία μεταδίδεται σήμερα, με αφορμή την **Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.**

Το μήνυμά της απαντά στην πάντα επίκαιρη **ερώτηση** για όλους τους **ψηφιακούς** χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά **μέτρα ασφάλειας**.

Η σημασία των **κωδικών πρόσβασης γίνεται** φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, **η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.**

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να **αναζητήσουν** στη **διαδικτυακή** πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει **να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.**

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

• Αφού φτιάξετε ισχυρούς **κωδικούς πρόσβασης**, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

• Εκτός από ισχυρό, το **password** πρέπει να είναι και **μυστικό**. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας **μέσω ηλεκτρονικού ταχυδρομείου.**

• **Σημαντικό** είναι να μην **αποθηκεύετε** τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

• Επιπλέον**, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλο**ς δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το **κεντρικόμήνυμα** της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «**Μαζί για ένα καλύτερο διαδίκτυο**», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η **ψηφιακήτεχνολογία**. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος **κακόβουλων**.

Σε ό,τι αφορά στις εταιρείες παρόχους **υπηρεσιών ηλεκτρονικών επικοινωνιών**, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της **ΑΔΑΕ**. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, **οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.**

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή **περιστατικάασφάλειας**. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η **ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.**

https://www.msn.com/el-gr/

Publication date: 05/02/2019 11:54

Alexa ranking (Greece): 71

https://www.msn.com/el-gr/news/techandscience/%ce%b1%ce%b4%ce%b1%ce%b...

Μέσα στο 2018 επιβλήθηκαν συνολικά **διοικητικέςκυρώσεις** σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και **οκτώ περιπτώσεων επιβολής συστάσεων.**

http://www.kontranews.gr/

Publication date: 05/02/2019 11:46

Alexa ranking (Greece): 915

https://www.kontranews.gr/KOINONIA/353481-ADAE-Pos-tha-demioyrgesete-ischyr...

ΑΔΑΕ: Πώς θα δημιουργήσετε ισχυρούς κωδικούς πρόσβασης

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

• Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

• Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

• Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

• Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά στις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.voria.gr/

Publication date: 05/02/2019 11:44

Alexa ranking (Greece): 362

https://www.voria.gr/article/kampania-tis-adae-gia-tin-prostasia-ton-christon-sto-di...

ΚΑΜΠΑΝΙΑ ΤΗΣ ΑΔΑΕ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΧΡΗΣΤΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς

Στην **προστασία της ιδιωτικότητας των χρηστών του διαδικτύου** επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της **Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών** (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.voria.gr/

Publication date: 05/02/2019 11:44

Alexa ranking (Greece): 362

https://www.voria.gr/article/kampania-tis-adae-gia-tin-prostasia-ton-christon-sto-di...

http://www.kerdos.gr/

Publication date: 05/02/2019 11:44

Alexa ranking (Greece): 3714

http://www.kerdos.gr/%CE%B5%CF%80%CE%B9%CF%83%CF%84%CE%AE%CE%BC...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

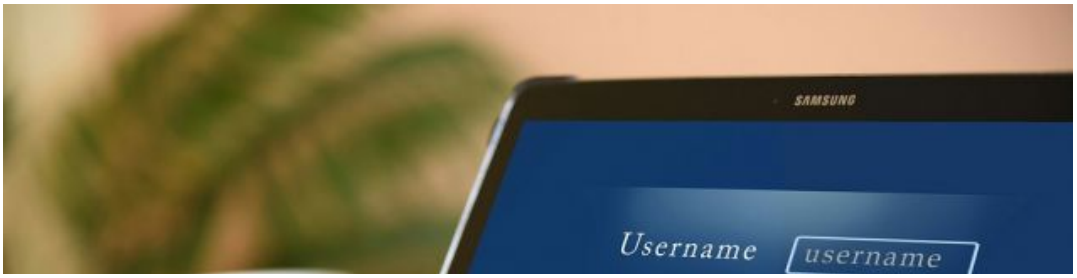
Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.



http://www.kerdos.gr/

Publication date: 05/02/2019 11:44

Alexa ranking (Greece): 3714

http://www.kerdos.gr/%CE%B5%CF%80%CE%B9%CF%83%CF%84%CE%AE%CE%BC...

Πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.
Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Κέρδος online 5/2/2019 11:42

http://www.voreini.gr/

Publication date: 05/02/2019 11:44

Alexa ranking (Greece): 11566

http://www.voreini.gr/technology/i-ischyri-kodiki-prosvasis-sto-diad/

Οι ισχυροί κωδικοί πρόσβασης στο διαδίκτυο ασπίδα για την ιδιωτικότητα

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται το ενημερωτικό video και η ραδιοφωνική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: *Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις;* Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατομ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή ***πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες,*** σημειώνει ο ερευνητής.

Η είδηση κάνει ακόμη πιο επίκαιρη τη **ραδιοφωνική καμπάνια της ΑΔΑΕ για τους κωδικούς πρόσβασης.** Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «***Μαζί για ένα καλύτερο διαδίκτυο***», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

http://www.voreini.gr/

Publication date: 05/02/2019 11:44

Alexa ranking (Greece): 11566

http://www.voreini.gr/technology/i-ischyri-kodiki-prosvasis-sto-diad/

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις. Μέσα στο 2018, επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.dailythess.gr/

Publication date: 05/02/2019 11:42

Alexa ranking (Greece): 2026

https://www.dailythess.gr/aade-odigies-gia-ischyra-password-me-aformi-tin-pagkos...

ΑΑΔΕ: Οδηγίες για... ισχυρά password και ασφαλή πλοήγηση στο διαδίκτυο
5 Φεβρουαρίου 2019 - 11:40

ΑΑΔΕ: Οδηγίες για... ισχυρά password και ασφαλή πλοήγηση στο διαδίκτυο

dailythess

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την

https://www.dailythess.gr/

Publication date: 05/02/2019 11:42

Alexa ranking (Greece): 2026

https://www.dailythess.gr/aade-odigies-gia-ischyra-password-me-aformi-tin-pagkos...

πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://halkidikivoice.gr/

Publication date: 05/02/2019 11:42

Alexa ranking (Greece): 0

https://halkidikivoice.gr/ellada/item/5366-enhmerwtikh-kampania-aade-pagosmia-...

Ενημερωτική καμπάνια της ΑΔΑΕ με αφορμή τη σημερινή Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις;

Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας. Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης εδώ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους εδώ.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

• Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

• Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

• Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

• Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

[ΑΠΕ-ΜΠΕ]

http://halkidikivoice.gr/

Publication date: 05/02/2019 11:42

Alexa ranking (Greece): 0

https://halkidikivoice.gr/ellada/item/5366-enhmerwtikh-kampania-aade-pagosmia-...

http://news24world.com/

Publication date: 05/02/2019 11:41

Alexa ranking (Greece): 4915

http://news24world.com/pos-na-dimiourgisete-ischyra-passwords/

Πώς να δημιουργήσετε ισχυρά passwords

Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η σημερινή

Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Οι **κωδικοί πρόσβασης** είναι ο νούμερο 1 κίνδυνος σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για **χάκερς** τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα **passwords** περιλαμβάνουν τα παρακάτω μέτρα:

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς **ηλεκτρονικών επικοινωνιών**, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://ipop.gr/
Publication date: 05/02/2019 11:40
Alexa ranking (Greece): 1703
https://ipop.gr/texnologia/me-ayta-ta-mystika-sta-passwords-den-tha-se-chakaroyn...

Με αυτά τα μυστικά στα passwords δεν θα σε χακάρουν ποτέ!

Όταν επιλέγεις έναν κωδικό να βάλεις σε κάποια συσκευή, στο email σου, στα social media, δεν το πολυσκέφτεσαι. Λες «εμένα θα χακάρουν;». Επειδή, όμως, ποτέ δεν ξέρεις αυτά είναι τα μυστικά για καλύτερα passwords.

Φύλαγε τα ρούχα σου για να έχεις τα μισά, έλεγε η γιαγιά μου και είχε απόλυτο δίκαιο. Ποια είναι τα μυστικά για καλύτερα passwords για να μην σε χακάρουν ποτέ;;

Σήμερα 5 Φεβρουαρίου είναι η Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου και η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), σε ενημερώνει και σου λέει όλα τα μυστικά για καλύτερα passwords.

Το μήνυμα καμπάνιας απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Ο κωδικός πρόσβασης είναι πολύ σημαντικός κι εσύ πρέπει να δίνεις την απαραίτητη προσοχή!

Μυστικά για τα καλύτερα passwords και τα μέτρα που πρέπει να λάβεις

Και... πώς μπορείς να καταλάβεις ότι σε έχουν χακάρει;

Διαβάστε επίσης:

https://stergiog.blogspot.com/

Publication date: 05/02/2019 11:32

Alexa ranking (Greece): 3235

https://stergiog.blogspot.com/2019/02/password.html

ΑΔΑΕ: Πως να προφυλάξουμε τα password από τους χάκερ

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.
Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς

υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: in.gr

** Οι απόψεις του ιστολογίου μπορεί να μη συμπίπτουν με τις απόψεις του/της αρθρογράφου ή τα περιεχόμενα του άρθρου.*

http://fibernews.gr/

Publication date: 05/02/2019 11:31

Alexa ranking (Greece): 0

http://fibernews.gr/index.php/news/item/23487-passwords

Πώς να δημιουργήσετε ισχυρά passwords

- February 5, 2019
- Written by NEWSROOM
- Published in NEWS
- 0 comments

Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Οι **κωδικοί πρόσβασης** είναι ο νούμερο 1 κίνδυνος σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για **χάκερς** τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα **passwords** περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

http://fibernews.gr/

Publication date: 05/02/2019 11:31

Alexa ranking (Greece): 0

http://fibernews.gr/index.php/news/item/23487-passwords

- Επιπλέον, ένα ασφαλές **password** θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς **ηλεκτρονικών επικοινωνιών**, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://magdasnews.gr/

Publication date: 05/02/2019 11:30

Alexa ranking (Greece): 9067

https://magdasnews.gr/%cf%80%cf%8e%cf%82-%ce%bd%ce%b1-%ce%b4%ce%b7%...

Πώς να δημιουργήσετε ισχυρά passwords

Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Οι **κωδικοί πρόσβασης** είναι ο νούμερο 1 κίνδυνος σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για **χάκερς** τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα **passwords** περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές **password** θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

https://magdasnews.gr/

Publication date: 05/02/2019 11:30

Alexa ranking (Greece): 9067

https://magdasnews.gr/%cf%80%cf%8e%cf%82-%ce%bd%ce%b1-%ce%b4%ce%b7%...

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς **ηλεκτρονικών επικοινωνιών**, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

ΑΞΙΟΛΟΓΗΣΤΕ ΤΟ ΑΡΘΡΟ

Πηγή: newsbeast.gr

http://www.amna.gr/

Publication date: 05/02/2019 11:28

Alexa ranking (Greece): 643

http://www.amna.gr/feeds/logosupload.php?id=331475

Ενημερωτική καμπάνια της ΑΔΑΕ με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ **και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους** http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

*** Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).**

*** Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.**

*** Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.**

*** Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.**

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν

http://www.amna.gr/

Publication date: 05/02/2019 11:28

Alexa ranking (Greece): 643

http://www.amna.gr/feeds/logosupload.php?id=331475

εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.amna.gr/

Publication date: 05/02/2019 11:28

Alexa ranking (Greece): 643

http://www.amna.gr/feeds/logosupload.php?id=331486

Προσοχή στους κωδικούς πρόσβασης συνιστά στους χρήστες η ΑΔΑΕ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ **και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους** http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

*** Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).**

*** Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.**

*** Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.**

*** Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.**

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

http://www.amna.gr/

Publication date: 05/02/2019 11:28

Alexa ranking (Greece): 643

http://www.amna.gr/feeds/logosupload.php?id=331486

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.mycampus.gr/

Publication date: 05/02/2019 11:28

Alexa ranking (Greece): 8481

https://www.mycampus.gr/deite-ta-mystika-gia-na-prostateysete-toys-kodikoys-sas-...

Δείτε τα μυστικά για να προστατεύσετε τους κωδικούς σας από τους χάκερς!

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα 05/02, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής, αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σε ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους, επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:
Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου. Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών
Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας, με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: dikaiologitika.gr

https://www.cnn.gr/

Publication date: 05/02/2019 11:27

Alexa ranking (Greece): 92

https://www.cnn.gr/tech/story/164573/adae-oi-tesseris-xrysoi-kanones-gia-toys-kod...

ΑΔΑΕ: Οι τέσσερις «χρυσοί» κανόνες για τους κωδικούς πρόσβασης

Newsroom , CNN Greece

Στην **προστασία της ιδιωτικότητας** των χρηστών του διαδικτύου επικεντρώνεται η **ενημερωτική καμπάνια** (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (**ΑΔΑΕ**), η οποία μεταδίδεται σήμερα, με αφορμή την **Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.**

Το μήνυμά της απαντά στην πάντα επίκαιρη **ερώτηση** για όλους τους **ψηφιακούς** χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά **μέτρα ασφάλειας**.

Η σημασία των **κωδικών πρόσβασης γίνεται** φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, **η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.**

Video: GDPR: Όλα όσα πρέπει να ξέρουμε για τον Γενικό Κανονισμό για την Προστασία Δεδομένων

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να **αναζητήσουν** στη **διαδικτυακή** πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει **να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.**

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

• Αφού φτιάξετε ισχυρούς **κωδικούς πρόσβασης**, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

• Εκτός από ισχυρό, το **password** πρέπει να είναι και **μυστικό**. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας **μέσω ηλεκτρονικού ταχυδρομείου.**

• **Σημαντικό** είναι να μην **αποθηκεύετε** τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

• Επιπλέον**, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλο**ς δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το **κεντρικό μήνυμα** της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «**Μαζί για ένα καλύτερο διαδίκτυο**», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η **ψηφιακή τεχνολογία**. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος **κακόβουλων**.

Σε ό,τι αφορά στις εταιρείες παρόχους **υπηρεσιών ηλεκτρονικών επικοινωνιών**, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της **ΑΔΑΕ**. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, **οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.**

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή **περιστατικά ασφάλειας**. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η **ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.**

https://www.cnn.gr/

Publication date: 05/02/2019 11:27

Alexa ranking (Greece): 92

https://www.cnn.gr/tech/story/164573/adae-oi-tesseris-xrysoi-kanones-gia-toys-kod...

Μέσα στο 2018 επιβλήθηκαν συνολικά **διοικητικές κυρώσεις** σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και **οκτώ περιπτώσεων επιβολής συστάσεων.**

http://www.skai.gr/default.aspx?pid=2&la=1&si=1

Publication date: 05/02/2019 11:27

http://www.skai.gr/news/technology/article/396113/i-adae-proeidopoiei-pos-tha-di...

https://www.evrytanika.gr/
Publication date: 05/02/2019 11:26
Alexa ranking (Greece): 3191
https://www.evrytanika.gr/index.php?option=com_content&view=article&id=13027...

ΑΔΑΕ: Οι τέσσερις «χρυσοί» κανόνες για τους κωδικούς πρόσβασης

https://www.biscotto.gr/

Publication date: 05/02/2019 11:18

Alexa ranking (Greece): 6095

https://www.biscotto.gr/deite-ta-mystika-gia-na-prostatepsete-toys-kodikoys-sas-ap...

Δείτε τα μυστικά για να προστατέψετε τους κωδικούς σας από τους χάκερς

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα 05/02, με αφορμή την **Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.**

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής, αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σε ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους, επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

https://www.biscotto.gr/

Publication date: 05/02/2019 11:18

Alexa ranking (Greece): 6095

https://www.biscotto.gr/deite-ta-mystika-gia-na-prostatepsete-toys-kodikoys-sas-ap...

Εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας, με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, **οι μεγαλύτερες εταιρείες πάροχοι**, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, **εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.**

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: dikaiologitika.gr

https://www.ersanews.gr/

Publication date: 05/02/2019 11:16

Alexa ranking (Greece): 36272

https://www.ersanews.gr/article/3080561/Pagkosmia-imera-asfalous-diadiktyou

Παγκόσμια ημέρα ασφαλούς διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα Τρίτη, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.Το μήνυμά της απαντά στην πάντα [...]

Πηγή: MATRIX24.GR
05/02 08:52

http://www.rizopoulospost.com/

Publication date: 05/02/2019 11:15

Alexa ranking (Greece): 4806

http://www.rizopoulospost.com/h-adae-proeidopoiei-prosoxh-stous-kwdikous-pros...

Η ΑΔΑΕ προειδοποιεί: Προσοχή στους κωδικούς πρόσβασης

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ" όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ" ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους >http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://securityreport.gr/

Publication date: 05/02/2019 11:05

Alexa ranking (Greece): 17042

https://securityreport.gr/news/security-news/item/6759-enimerotiki-kampania-tis-a...

Ενημερωτική καμπάνια της ΑΔΑΕ με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών-ΑΔΑΕ..

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://securityreport.gr/

Publication date: 05/02/2019 11:05

Alexa ranking (Greece): 17042

https://securityreport.gr/news/security-news/item/6759-enimerotiki-kampania-tis-a...

ΑΠΕ ΜΠΕ

https://analitis.gr/

Publication date: 05/02/2019 11:04

Alexa ranking (Greece): 3097

https://analitis.gr/prosoxh-stoys-kwdikoys-prosbashs-synista-stoys-xrhstes-h-adae/

Προσοχή στους κωδικούς πρόσβασης συνιστά στους χρήστες η ΑΔΑΕ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.matrix24.gr/

Publication date: 05/02/2019 11:04

Alexa ranking (Greece): 2093

http://www.matrix24.gr/2019/02/pagkosmia-imera-asfalous-diadiktiou/

Παγκόσμια ημέρα ασφαλούς διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα Τρίτη, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.economy365.gr/

Publication date: 05/02/2019 11:04

Alexa ranking (Greece): 2567

http://www.economy365.gr/article/109118/pos-na-dimioyrgisete-ishyra-passwords

Πώς να δημιουργήσετε ισχυρά passwords

Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Οι **κωδικοί πρόσβασης** είναι ο νούμερο 1 κίνδυνος σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

http://www.economy365.gr/

Publication date: 05/02/2019 11:04

Alexa ranking (Greece): 2567

http://www.economy365.gr/article/109118/pos-na-dimioyrgisete-ishyra-passwords

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

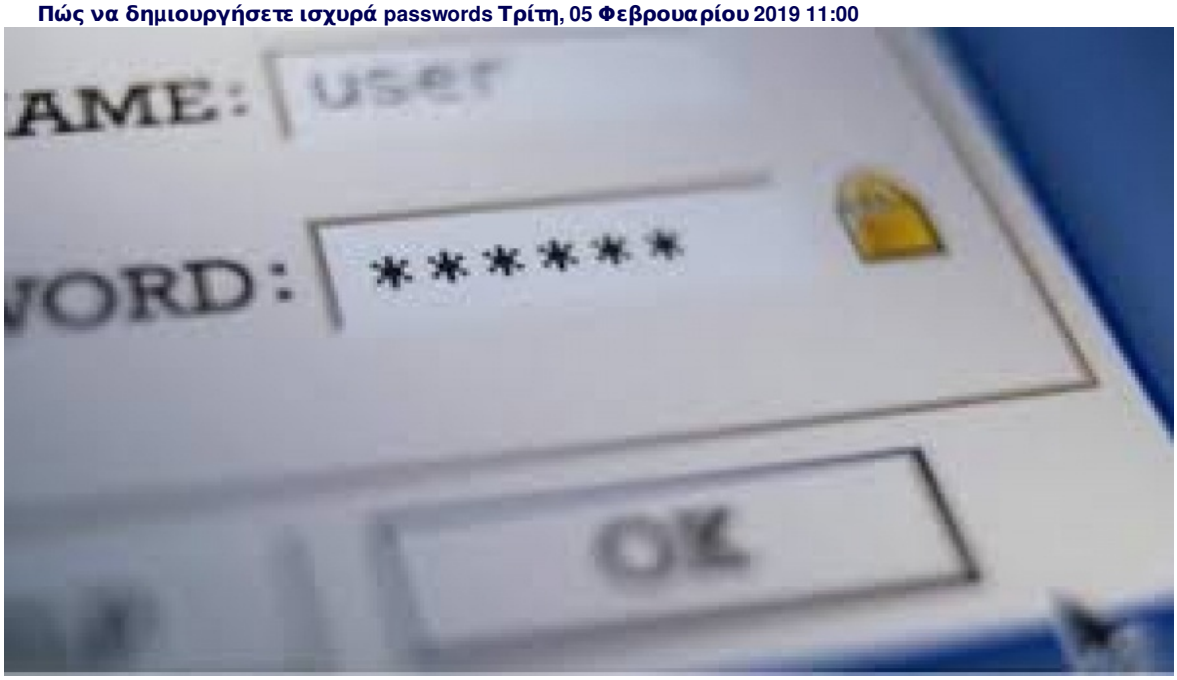
http://www.toxwni.gr/

Publication date: 05/02/2019 10:56

Alexa ranking (Greece): 1795

http://www.toxwni.gr/kainotomia/205199-pos-na-dimiourgisete-isxira-passwords

Πώς να δημιουργήσετε ισχυρά passwords Τρίτη, 05 Φεβρουαρίου 2019 11:00



Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Οι κωδικοί πρόσβασης είναι ο νούμερο 1 κίνδυνος σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασηςhttp://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς

ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.newsbeast.gr/

Publication date: 05/02/2019 10:54

Alexa ranking (Greece): 49

https://www.newsbeast.gr/technology/arthro/4490228/pos-na-dimioyrgisete-ischyr...

Πώς να δημιουργήσετε ισχυρά passwords

Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου η σημερινή

Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Οι **κωδικοί πρόσβασης** είναι ο νούμερο 1 κίνδυνος σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής που αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για **χάκερς** τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα **passwords** περιλαμβάνουν τα παρακάτω μέτρα:

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς **ηλεκτρονικών επικοινωνιών**, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.alfavita.gr/

Publication date: 05/02/2019 10:54

Alexa ranking (Greece): 114

https://www.alfavita.gr/koinonia/280288_symboyles-gia-asfales-diadiktyo-kai-ishyro...

Συμβουλές για ασφαλές διαδίκτυο και «ισχυρούς» κωδικούς

Για την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης (http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/) και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους (http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/)

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://aftodioikisi.isol-servers.net/

Publication date: 05/02/2019 10:53

Alexa ranking (Greece): 0

https://www.aftodioikisi.gr/koinonia/pagkosmia-imera-asfaloys-diadiktyoy-ti-na-pro...

Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου: Τι να προσέχετε με τους κωδικούς πρόσβασης

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται το ενημερωτικό video και η ραδιοφωνική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://analitis.gr/

Publication date: 05/02/2019 10:51

Alexa ranking (Greece): 3097

https://analitis.gr/enhmerwtikh-kampania-ths-adae-me-aformh-thn-pagkosmia-hm...

Ενημερωτική καμπάνια της ΑΔΑΕ με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://pelop.gr/default.aspx?page=home

Publication date: 05/02/2019 10:42

http://pelop.gr:80/default.aspx?page=article&DocID=506111

Τι συστήνει η ΑΔΑΕ για ισχυρούς κωδικούς

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: iefimerida.gr

https://sofokleous10.gr/

Publication date: 05/02/2019 10:41

Alexa ranking (Greece): 5319

https://sofokleous10.gr/index.php/component/k2/item/185848-adae-pos-na-profyl...

ΑΔΑΕ: Πως να προφυλάξουμε τα password από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί...

Read more https://thetimes.gr/%CE%B1%CE%B4%CE%B1%CE%B5-%CF%80%CF%89%CF%82-%CE%BD%CE%B1-%CF%80%CF%81%CE%BF%CF%86%CF%85%CE%BB%CE%AC%CE%BE%CE%BF%CF%85%CE%BC%CE%B5-%CF%84%CE%B1-password-%CE%B1%CF%80%CF%8C-%CF%84%CE%BF%CF%85%CF%82/

http://eretikos.gr/
Publication date: 05/02/2019 10:40
Alexa ranking (Greece): 1120
https://eretikos.gr/ellada/etsi-tha-prostateyteite-apo-toys-chakers-ta-trik-kai-oi-kodi...

Έτσι θα... προστατευτείτε από τους χάκερς! Τα «τρικ» και οι κωδικοί

ΦΩΤΟ ΑΡΧΕΙΟΥ: EUROKINISSI

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου από τους χάκερς επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Πώς θα προστατευτείτε από τους χάκερς;

http://eretikos.gr/

Publication date: 05/02/2019 10:40

Alexa ranking (Greece): 1120

https://eretikos.gr/ellada/etsi-tha-prostateyteite-apo-toys-chakers-ta-trik-kai-oi-kodi...

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

– Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

– Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

SOS. Τα μικρά παιδιά εκτεθειμένα στους κινδύνους των social media

– Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

– Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Προσοχή ειδικά οι... μη ειδικοί

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Οι εταιρείες και οι χάκερς

http://eretikos.gr/

Publication date: 05/02/2019 10:40

Alexa ranking (Greece): 1120

https://eretikos.gr/ellada/etsi-tha-prostateyteite-apo-toys-chakers-ta-trik-kai-oi-kodi...

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.pelop.gr/

Publication date: 05/02/2019 10:38

Alexa ranking (Greece): 1616

http://www.pelop.gr/?page=article&srv=10&DocID=506111

Τι συστήνει η ΑΔΑΕ για ισχυρούς κωδικούς

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.
Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:
* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.
Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: iefimerida.gr

http://www.thesstoday.gr/

Publication date: 05/02/2019 10:37

Alexa ranking (Greece): 1683

https://thesstoday.gr/%ce%b7-%ce%b1%ce%b4%ce%b1%ce%b5-%cf%80%cf%81%c...

Η ΑΔΑΕ προειδοποιεί: Προσοχή στους κωδικούς πρόσβασης

Προσοχή στους κωδικούς πρόσβασης, τονίζει προς τους χρήστες η Αρχή Διασφάλιση του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) στην νέα ενημερωτική καμπάνια με αφορμή τη σημερινή Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Η καμπάνια της ΑΔΑΕ επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου και το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους. Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

– Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

– Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

– Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

– Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία.

Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων. Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.

Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας. Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας.

Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις. Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

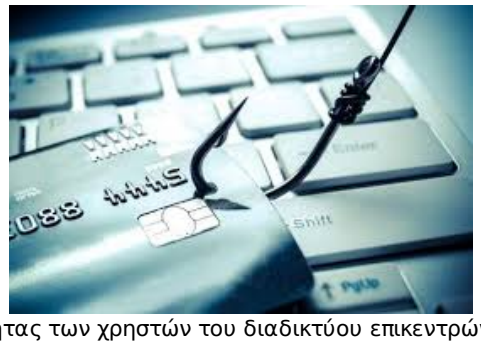
https://indicator.gr/

Publication date: 05/02/2019 10:33

Alexa ranking (Greece): 3574

https://indicator.gr/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%80%cf%89%cf%82-%ce%...

ΑΔΑΕ: Πως θα προφυλάξετε τα password από τους χάκερ



Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ(1): 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.
Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.sepe.gr/

Publication date: 05/02/2019 10:31

Alexa ranking (Greece): 9461

http://www.sepe.gr/gr/researchscience/researchscience-article/12851532/pagkosm...

Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου : Πώς να προφυλάξετε τα password σας

Έρευνα & Επιστήμες

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας. Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ(1): 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής. Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα: Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον). Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου. Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού. Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν. Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων. Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας. Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να

διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις. Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.lifo.gr/

Publication date: 05/02/2019 10:29

Alexa ranking (Greece): 40

https://www.lifo.gr/now/tech_science/225148/i-adae-proeidopoiei-prosoxi-stoys-ko...

Tech & Science

Η ΑΔΑΕ προειδοποιεί: Προσοχή στους κωδικούς πρόσβασης

Πρακτικές οδηγίες σχετικά με τα passwords και πώς να δημιουργήσετε ισχυρούς κωδικούς πρόσβασης

NEWSROOM
5.2.2019 | 10:09

Η ΑΔΑΕ προειδοποιεί: Προσοχή στους κωδικούς πρόσβασης

Προσοχή στους κωδικούς πρόσβασης, τονίζει προς τους χρήστες η Αρχή Διασφάλιση του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) στην νέα ενημερωτική καμπάνια με αφορμή τη σημερινή Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Η καμπάνια της ΑΔΑΕ επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου και το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις;

Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

https://www.lifo.gr/

Publication date: 05/02/2019 10:29

Alexa ranking (Greece): 40

https://www.lifo.gr/now/tech_science/225148/i-adae-proeidopoiei-prosoxi-stoys-ko...

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.lifo.gr/

Publication date: 05/02/2019 10:29

Alexa ranking (Greece): 40

https://www.lifo.gr/now/tech_science/225148/i-adae-proeidopoiei-prosoxi-stoys-ko...

Με πληροφορίες από ΑΠΕ-ΜΠΕ

Πρακτικές οδηγίες σχετικά με τα passwords και πώς να δημιουργήσετε ισχυρούς κωδικούς πρόσβασης

Προσοχή στους κωδικούς πρόσβασης, τονίζει προς τους χρήστες η Αρχή Διασφάλιση του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) στην νέα ενημερωτική καμπάνια με αφορμή τη σημερινή Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Η καμπάνια της ΑΔΑΕ επικεντρώνεται στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου και το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις;

Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.

Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το

https://www.lifo.gr/

Publication date: 05/02/2019 10:29

Alexa ranking (Greece): 40

https://www.lifo.gr/now/tech_science/225148/i-adae-proeidopoiei-prosoxi-stoys-ko...

παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Με πληροφορίες από ΑΠΕ-ΜΠΕ

Οι New York Times αναζητούν την σαγηνευτικότερη μουσική του κόσμου στην Ήπειρο

Μαχαιρώματα, εμπρησμοί αιθουσών, bullying στους δασκάλους: Η καθημερινή κόλαση ενός εκπαιδευτικού

Αληθινά εγκλήματα που έγιναν υλικό τέχνης

ΜΟΥΣΙΚΗ Οι New York Times αναζητούν την σαγηνευτικότερη μουσική του κόσμου στην Ήπειρο

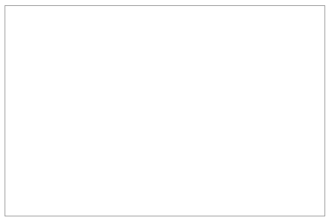
https://www.lifo.gr/
Publication date: 05/02/2019 10:29
Alexa ranking (Greece): 40
https://www.lifo.gr/now/tech_science/225148/i-adae-proeidopoiei-prosoxi-stoys-ko...

ΕΛΛΑΔΑ Η μητέρα του Βαγγέλη Γιακουμάκη μιλά στο LIFO.gr και μας δείχνει τις παιδικές φωτογραφίες του

ΚΟΣΜΟΣ Τι συμβαίνει αν μετανιώσεις τον επαναπροσδιορισμό φύλου;

ΠΡΟΣΩΠΑ Μια σπάνια τηλεοπτική συνέντευξη του Μισέλ Φουκώ: Αν ο Άνθρωπος είναι νεκρός, όλα είναι δυνατά!

ΜΟΥΣΙΚΗ Sid & Nancy: 40 χρόνια μετά τον θάνατο του Sid Vicious, το μυστήριο παραμένει γύρω από το τραγικό ζεύγος του πανκ



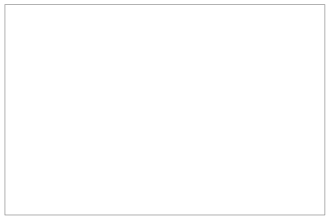
ΚΟΣΜΟΣ Camping House: ένα σπίτι στην Τζιά που προσφέρει μόνο τα απαραίτητα

LGBTQI+ Ισχύει η δεξιά στροφή σημαντικού ποσοστού των γκέι ανδρών;

https://www.lifo.gr/
Publication date: 05/02/2019 10:29
Alexa ranking (Greece): 40
https://www.lifo.gr/now/tech_science/225148/i-adae-proeidopoiei-prosoxi-stoys-ko...

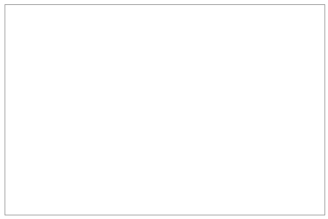
ΤΕΧΝΕΣ Κλαρίνα μέσα στα νερά του Βοϊδομάτη: Ο θρήνος και η έκσταση του δημοτικού τραγουδιού

ΔΙΕΘΝΗ Νεπάλ: Μια 21χρονη πέθανε από ασφυξία σε «καλύβα για την έμμηνο ρύση»



ΑΘΛΗΤΙΣΜΟΣ Γιατί οι παίκτες του ράγκμπι πεθαίνουν ξαφνικά λίγο μετά τον αγώνα; Τα ανησυχητικά κρούσματα

ΔΙΕΘΝΗ Το Instagram θα θολώνει φωτογραφίες μετά τον θάνατο της Μόλι Ράσελ



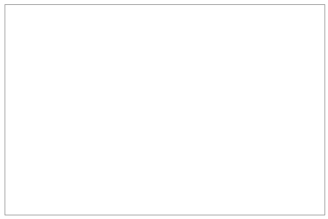
ΑΝΘΡΩΠΟΙ Η Madonna στη Eurovision - Ποιος πληρώνει το τεράστιο ποσό για την εμφάνιση

https://www.lifo.gr/
Publication date: 05/02/2019 10:29
Alexa ranking (Greece): 40
https://www.lifo.gr/now/tech_science/225148/i-adae-proeidopoiei-prosoxi-stoys-ko...

ΕΛΛΑΔΑ Σε σχολείο στην Καλαμαριά κάνουν κατάληψη για να διώξουν 12χρονο μαθητή με μαθησιακές δυσκολίες

TECH & SCIENCE Κατακόρυφη η αύξηση κρουσμάτων του καρκίνου του στόματος- Αυτοί είναι οι παράγοντες κινδύνου

ΑΘΛΗΤΙΣΜΟΣ Σοκ στο χάντμπολ - Αυτοκτόνησε ο 29χρονος διεθνής Μπόσκοβιτς



ΠΟΛΙΤΙΚΗ Για σκι στο Βελούχι ο Μητσοτάκης

ΦΩΤΟΓΡΑΦΙΑ Ο υπέροχος, τρελός, ανεκτίμητος κόσμος της μητρότητας

https://www.lifo.gr/
Publication date: 05/02/2019 10:29
Alexa ranking (Greece): 40
https://www.lifo.gr/now/tech_science/225148/i-adae-proeidopoiei-prosoxi-stoys-ko...

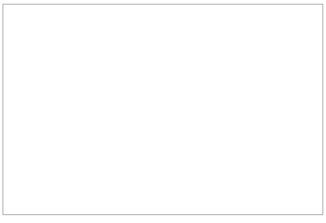
ΑΛΜΑΝΑΚ Οι Κουβανοί. Ένας Δεκέμβριος στην Κούβα.

ΦΩΤΟΓΡΑΦΙΑ Προσπαθώντας να βγεις στην επιφάνεια

DESIGN Μέσα στο μαγνητικό βασίλειο του Τάκι, του μεγαλύτερου εν ζωή Έλληνα καλλιτέχνη

ΕΙΚΑΣΤΙΚΑ Στην γκαλερί Allouche Benias ο Φαϊτάκης συνυπάρχει με τους ATH Kids

ΦΩΤΟΓΡΑΦΙΑ Η ανείπωτη βία του πολέμου στη Συρία



ΦΩΤΟΓΡΑΦΙΑ Πόσες φορές μπορείς να ερωτευτείς;

https://www.lifo.gr/
Publication date: 05/02/2019 10:29
Alexa ranking (Greece): 40
https://www.lifo.gr/now/tech_science/225148/i-adae-proeidopoiei-prosoxi-stoys-ko...

ΦΩΤΟΓΡΑΦΙΑ Οι εξορκίστριες τη Λευκορωσίας

https://www.tanea.gr/

Publication date: 05/02/2019 10:29

Alexa ranking (Greece): 134

https://www.tanea.gr/2019/02/05/economy/economy-greece/pagkosmia-imera-asf...

Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου : Πώς να προφυλάξετε τα password σας

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ(1): 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://thetimes.gr/

Publication date: 05/02/2019 10:23

Alexa ranking (Greece): 5867

https://thetimes.gr/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%80%cf%89%cf%82-%ce%...

ΑΔΑΕ: Πως να προφυλάξουμε τα password από τους χάκερ

https://www.dikaiologitika.gr/

Publication date: 05/02/2019 10:18

Alexa ranking (Greece): 46

https://www.dikaiologitika.gr/eidhseis/kosmos/243360/ta-kolpa-gia-na-min-pesoun-...

Τα κόλπα για να μην «πέσουν» οι κωδικοί σας στα χέρια των χάκερς

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

https://www.dikaiologitika.gr/

Publication date: 05/02/2019 10:18

Alexa ranking (Greece): 46

https://www.dikaiologitika.gr/eidhseis/kosmos/243360/ta-kolpa-gia-na-min-pesoun-...

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.in.gr/

Publication date: 05/02/2019 10:16

Alexa ranking (Greece): 38

https://www.in.gr/2019/02/05/tech/adae-pos-na-profylaksoume-ta-password-apo-t...

ΑΔΑΕ: Πως να προφυλάξουμε τα password από τους χάκερ

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου in.gr

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://www.pentapostagma.gr/

Publication date: 05/02/2019 10:14

Alexa ranking (Greece): 89

https://www.pentapostagma.gr/2019/02/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%84...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερς

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.
Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**
* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

https://www.pentapostagma.gr/

Publication date: 05/02/2019 10:14

Alexa ranking (Greece): 89

https://www.pentapostagma.gr/2019/02/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%84...

Πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.
Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.thetoc.gr/

Publication date: 05/02/2019 10:12

Alexa ranking (Greece): 224

http://www.thetoc.gr/koinwnia/article/pagkosmia-imera-asfalous-diadiktuou-kamp...

Παγκόσμια ημέρα ασφαλούς διαδικτύου: Καμπάνια της ΑΔΑΕ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης Απορρήτου των Επικοινωνιών

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα Τρίτη, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/> και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://newsone.gr/

Publication date: 05/02/2019 10:06

Alexa ranking (Greece): 311

https://www.newsone.gr/texnologia/adae-ta-trik-sto-password-gia-na-profylachtho...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

http://newsone.gr/

Publication date: 05/02/2019 10:06

Alexa ranking (Greece): 311

https://www.newsone.gr/texnologia/adae-ta-trik-sto-password-gia-na-profylachtho...

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

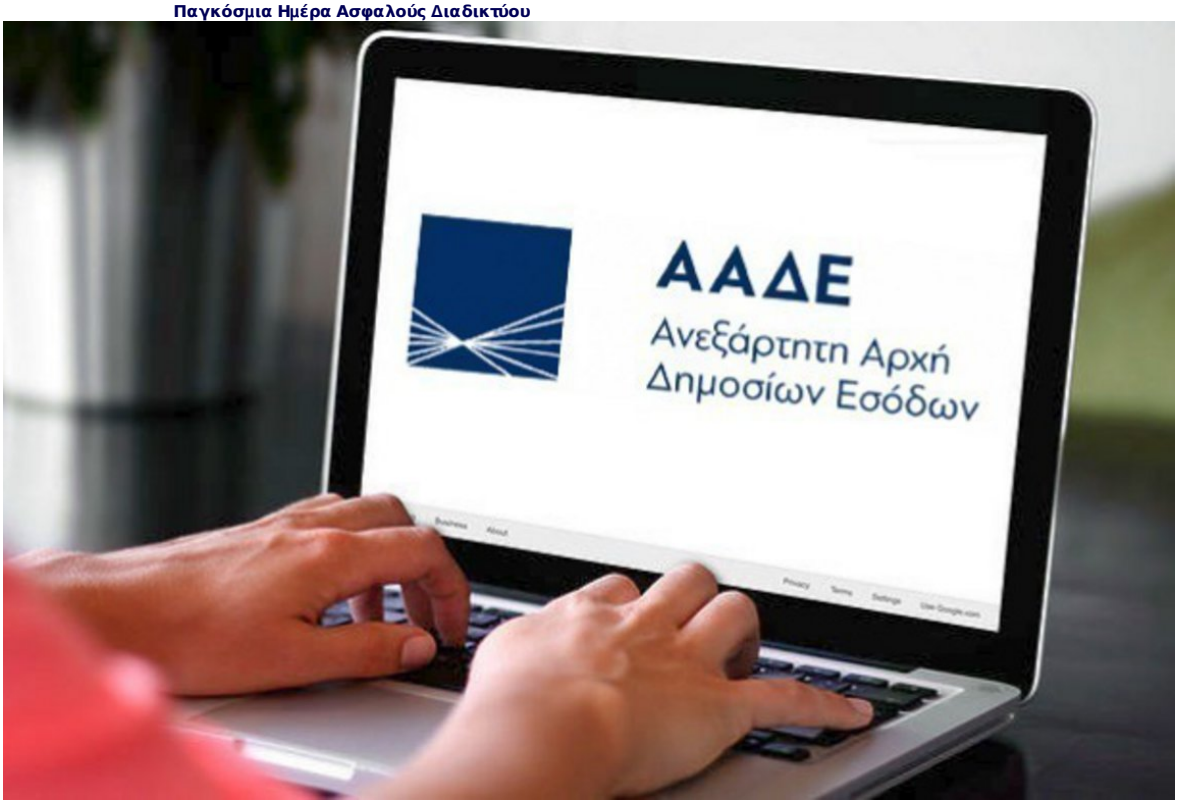
http://www.real.gr/

Publication date: 05/02/2019 10:04

Alexa ranking (Greece): 235

http://www.real.gr/texnologia/arthro/aade_prosoxi_stous_kodikous_prosbasis_to_...

ΑΑΔΕ: Προσοχή στους κωδικούς πρόσβασης - Το μήνυμα με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου



Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το **πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης**

και **ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου** των επικοινωνιών τους

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://emvolos.gr/

Publication date: 05/02/2019 10:03

Alexa ranking (Greece): 831

https://emvolos.gr/enimerotiki-kampania-tis-adae-me-aformi-ti-simerini-pagkosmia...

Ενημερωτική καμπάνια της ΑΔΑΕ με αφορμή τη σημερινή Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Προσοχή στους κωδικούς πρόσβασης

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που

https://emvolos.gr/
Publication date: 05/02/2019 10:03
Alexa ranking (Greece): 831
https://emvolos.gr/enimerotiki-kampania-tis-adae-me-aformi-ti-simerini-pagkosmia...

προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

ΑΠΕ-ΜΠΕ

https://www.movenews.gr/

Publication date: 05/02/2019 10:03

Alexa ranking (Greece): 12097

https://www.movenews.gr/aade-oi-isxyroi-kvdikoi-prosbashs-sto-diadiktyo-aspida-g...

ΑΑΔΕ: Οι ισχυροί κωδικοί πρόσβασης στο διαδίκτυο ασπίδα για την ιδιωτικότητα

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται το ενημερωτικό video και η ραδιοφωνική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ : 21 εκατομ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Η είδηση κάνει ακόμη πιο επίκαιρη τη ραδιοφωνική καμπάνια της ΑΔΑΕ για τους κωδικούς πρόσβασης. Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Οι ειδικοί προτείνουν ένα τρόπο για να το πετύχετε: το **passphrase**

https://www.movenews.gr/
Publication date: 05/02/2019 10:03
Alexa ranking (Greece): 12097
https://www.movenews.gr/aade-oi-isxyroi-kvdikoi-prosbashs-sto-diadiktyo-aspida-g...

ΒΗΜΑ 1: Επιλέξτε **μια σύντομη φράση** που σας αρέσει και θα μπορείτε να τη θυμάστε εύκολα (π.χ. ένα στίχο από το αγαπημένο σας τραγούδι).

ΒΗΜΑ 2: **Ενώστε τη** φράση σε μια λέξη βάζοντας το **πρώτο γράμμα κάθε λέξης με ΚΕΦΑΛΑΙΑ**

ΒΗΜΑ 3: **Προσθέστε σύμβολα ή αριθμούς χρησιμοποιώντας ένα συγκεκριμένο τρόπο,** π.χ. «το τελευταίο γράμμα σε κάθε λέξη της φράσης να αλλάζει σε σύμβολο ή αριθμό». Στο παράδειγμα παρακάτω, το σύμβολο ή ο αριθμός επιλέγεται με βάση τη διάταξη στο πληκτρολόγιο. (π.χ. ο αριθμός 3 αντικαθιστά το γράμμα ε επειδή βρίσκεται πάνω από το γράμμα αυτό στο πληκτρολόγιο).

π.χ. η φράση «***Μάντεψε τον κωδικό μου***» μπορεί να γίνει Μαντεψ3Το^Κωδικ9Μο^

ΒΗΜΑ 4: Κάντε τον κωδικό σας **μοναδικό για κάθε εφαρμογή ή σύνδεση** χρησιμοποιώντας παραλλαγές. Ένας τρόπος είναι να προσθέσετε στον κωδικό σας χαρακτηριστικά από μια εφαρμογή. Για παράδειγμα, για το Facebook, προσθέστε το γράμμα F και τον αριθμό 4 που βρίσκεται πάνω από το γράμμα αυτό, και ο κωδικός γίνεται F4Μαντεψ3Το^Κωδικ9Μο^.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις. Μέσα στο 2018, επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://e-volos.gr/

Publication date: 05/02/2019 10:02

Alexa ranking (Greece): 3276

https://e-volos.gr/%ce%b1%ce%b4%ce%b1%ce%b5-%cf%84%ce%b1-%cf%84%cf%8...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο.
Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**
* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.
Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Πηγή: iefimerida.gr

http://parallaximag.gr/

Publication date: 05/02/2019 10:01

Alexa ranking (Greece): 672

https://parallaximag.gr/life/technologia/ta-4-vimata-pou-mas-kanounatrotous-stis-k...

Τα 4 βήματα που μας κάνουν"άτρωτους" στις κυβερνοεπιθέσεις

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι **η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.** Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, **η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.** Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

ΠΗΓΗ: ΑΠΕ ΜΠΕ

http://itsecuritypro.gr/

Publication date: 05/02/2019 09:59

Alexa ranking (Greece): 0

https://www.itsecuritypro.gr/oi-ischyroi-kodikoi-prosvasis-sto-diadiktyo-aspida-gia-t...

Οι ισχυροί κωδικοί πρόσβασης στο διαδίκτυο ασπίδα για την ιδιωτικότητα

Ραδιοφωνική καμπάνια και ενημερωτικό video της ΑΔΑΕ με αφορμή την Ημέρα Ασφαλούς Διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται το ενημερωτικό video και η ραδιοφωνική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τους ψηφιακούς χρήστες: *Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις;* Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατομ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή ***πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες,*** σημειώνει ο ερευνητής.

Η είδηση κάνει ακόμη πιο επίκαιρη τη **ραδιοφωνική καμπάνια της ΑΔΑΕ για τους κωδικούς πρόσβασης.** Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

- Αφού φτιάξετε **ισχυρούς κωδικούς πρόσβασης**, **διαφορετικούς** για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να **τους ανανεώνετε τακτικά** (κάθε 6 μήνες τουλάχιστον).
- Εκτός από ισχυρό, το password πρέπει να είναι **και μυστικό.** Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
- Σημαντικό είναι **να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης** στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
- Επιπλέον, ένα ασφαλές password θα σας προστατεύει **μόνο αν** ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). **Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας** που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «***Μαζί για ένα καλύτερο διαδίκτυο***», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

http://itsecuritypro.gr/

Publication date: 05/02/2019 09:59

Alexa ranking (Greece): 0

https://www.itsecuritypro.gr/oi-ischyroi-kodikoi-prosvasis-sto-diadiktyo-aspida-gia-t...

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις. Μέσα στο 2018, επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

[1] Πηγή The Guardian: https://www.theguardian.com/technology/2019/jan/17/breached-data-largest-collection-ever-seen-email-password-hacking» \l «img-1

https://left.gr/
Publication date: 05/02/2019 09:58
Alexa ranking (Greece): 524
https://left.gr/news/prosohi-stoys-kodikoys-prosvasis-i-aade-me-aformi-tin-pagkos...

«Προσοχή στους κωδικούς πρόσβασης»: Η ΑΑΔΕ με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Ενημερωτική καμπάνια της ΑΔΑΕ με αφορμή τη σημερινή Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

https://left.gr/

Publication date: 05/02/2019 09:58

Alexa ranking (Greece): 524

https://left.gr/news/prosohi-stoys-kodikoys-prosvasis-i-aade-me-aformi-tin-pagkos...

ΑΠΕ-ΜΠΕ

http://www.ipaideia.gr/

Publication date: 05/02/2019 09:58

Alexa ranking (Greece): 627

https://www.ipaideia.gr/endiaferouses-eidiseis/aade-prosoxi-stous-kodikous-prosv...

ΑΑΔΕ: Προσοχή στους κωδικούς πρόσβασης

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους >http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.ipaideia.gr/

Publication date: 05/02/2019 09:58

Alexa ranking (Greece): 627

https://www.ipaideia.gr/endiaferouses-eidiseis/aade-prosoxi-stous-kodikous-prosv...

http://www.iefimerida.gr/

Publication date: 05/02/2019 09:58

Alexa ranking (Greece): 27

https://www.iefimerida.gr/news/476736/adae-ta-trik-sto-password-gia-na-profylaht...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

http://www.iefimerida.gr/

Publication date: 05/02/2019 09:58

Alexa ranking (Greece): 27

https://www.iefimerida.gr/news/476736/adae-ta-trik-sto-password-gia-na-profylaht...

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.iefimerida.gr/

Publication date: 05/02/2019 09:58

Alexa ranking (Greece): 27

https://www.iefimerida.gr/news/476736/adae-ta-trik-sto-password-gia-na-profylaht...

ΑΔΑΕ: Τα τρικ στο password για να προφυλαχθούμε από τους χάκερς

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους.

Ενδεικτικά, **πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:**

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις.

http://www.iefimerida.gr/

Publication date: 05/02/2019 09:58

Alexa ranking (Greece): 27

https://www.iefimerida.gr/news/476736/adae-ta-trik-sto-password-gia-na-profylaht...

Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ.
Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.avgi.gr/

Publication date: 05/02/2019 09:52

Alexa ranking (Greece): 488

http://www.avgi.gr/article/10951/9564419/prosoche-stous-kodikous-prosbases-toni...

Προσοχή στους κωδικούς πρόσβασης, τονίζει η ΑΑΔΕ με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους >http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

- A
- A
- A

Email Εκτυπωση
Κατηγορία
Οικονομικά Νέα Ροη κατηγοριας

Όπως αναφέρει η χθεσινή «Εστία», αποδίδοντας την πληροφορία σε συνεργάτες του Κ. Μητσοτάκη, ο πρόεδρος της Ν.Δ. εξέφρασε στη Μέρκελ τη διαφωνία του με τη Συνθήκη των Πρεσπών, λέγοντας «δεν θα...

https://www.economistas.gr/

Publication date: 05/02/2019 09:51

Alexa ranking (Greece): 755

https://www.economistas.gr/tehnologia/7272_aade-prosohi-stoys-kodikoys-prosba...

ΑΑΔΕ: Προσοχή στους κωδικούς πρόσβασης στο Διαδίκτυο

- #Διαδίκτυο

Newsroom 05/02/2019 09:32 ΤΕΧΝΟΛΟΓΙΑ

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης (http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis) και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους (www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies)

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

http://www.patranews.gr/

Publication date: 05/02/2019 09:48

Alexa ranking (Greece): 5490

http://www.patranews.gr/politiki/enimerotiki-kampania-tis-adae-me-aformi-ti-simer...

Ενημερωτική καμπάνια της ΑΔΑΕ με αφορμή τη σημερινή Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Προσοχή στους κωδικούς πρόσβασης, τονίζει προς τους χρήστες η ανεξάρτητη Αρχή

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gi... και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enim...

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

• Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

• Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

• Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

• Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

Δ.Β.

Πηγή: ΑΠΕ-ΜΠΕ

http://www.palo.gr/?fcid=5

Publication date: 05/02/2019 09:46

Alexa ranking (Greece): 192

http://www.palo.gr/texnologika-nea/psifoforia/20743097/

Ενημερωτική καμπάνια της ΑΔΑΕ με αφορμή τη σημερινή Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου. Προσοχή στους κωδικούς πρόσβασης, τονίζει προς τους χρήστες η ανεξάρτητη Αρχή - [Patranews.gr]

ΠΕΡΙΛΗΨΗ ΕΙΔΗΣΗΣ

- * Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό.
- * Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή.
- Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ.ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.AAAEmail
- Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας.

http://www.avgi.gr/

Publication date: 05/02/2019 09:42

Alexa ranking (Greece): 488

https://www.avgi.gr/article/10951/9564419/prosoche-stous-kodikous-prosbases-to...

Προσοχή στους κωδικούς πρόσβασης, τονίζει η ΑΑΔΕ με αφορμή τη σημερινή Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.

Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.

Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.

Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους >http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/

Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:

* Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).

* Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.

* Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.

* Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.

Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.

Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.

Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.

Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.

- A
- A
- A

Email Εκτυπωση
Κατηγορία
Οικονομικά Νέα Ροη κατηγοριας

Όπως αναφέρει η χθεσινή «Εστία», αποδίδοντας την πληροφορία σε συνεργάτες του Κ. Μητσοτάκη, ο πρόεδρος της Ν.Δ. εξέφρασε στη Μέρκελ τη διαφωνία του με τη Συνθήκη των Πρεσπών, λέγοντας «δεν θα...

https://ergasianews.gr/
Publication date: 05/02/2019 00:00
Alexa ranking (Greece): 5475
https://ergasianews.gr/2019/02/05/%ce%b7-%ce%b1%ce%b4%ce%b1%ce%b5-%cf%...

Η ΑΔΑΕ προειδοποιεί-Πώς θα δημιουργήσετε ισχυρούς κωδικούς πρόσβασης

Στην προστασία της ιδιωτικότητας των χρηστών του διαδικτύου επικεντρώνεται η ενημερωτική καμπάνια (ραδιόφωνο, video) της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), η οποία μεταδίδεται σήμερα, με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου.
Το μήνυμά της απαντά στην πάντα επίκαιρη ερώτηση για όλους τούς ψηφιακούς χρήστες: Τι μπορεί να μας καταστήσει ευάλωτους στόχους σε πιθανές κυβερνοεπιθέσεις; Πρώτα απ' όλα ο κωδικός πρόσβασης σε συνδέσεις και εφαρμογές στο διαδίκτυο, αν από άγνοια ή αμέλεια δεν εφαρμόζονται βασικά μέτρα ασφάλειας.
Η σημασία των κωδικών πρόσβασης γίνεται φανερή από το σοβαρό και εκτεταμένο περιστατικό υποκλοπής αποκάλυψε πρόσφατα ο ερευνητής σε θέματα ασφάλειας, Τρόι Χαντ[1]: 21 εκατ. κωδικοί πρόσβασης και προσωπικά email χρηστών συγκεντρώθηκαν και αναρτήθηκαν σ' ένα φόρουμ για χάκερς τον Δεκέμβριο. Η συγκέντρωση των υποκλαπέντων στοιχείων, η μεγαλύτερη στην ιστορία του Διαδικτύου, έχει αξία για τους κακόβουλους επειδή πολλοί χρήστες χρησιμοποιούν τους ίδιους κωδικούς και τα ίδια ψευδώνυμα για διαφορετικές υπηρεσίες, σημειώνει ο ερευνητής.
Οι ενδιαφερόμενοι ψηφιακοί χρήστες μπορούν να αναζητήσουν στη διαδικτυακή πύλη της Αρχής ενημέρωση για το πώς να δημιουργήσουν ισχυρούς κωδικούς πρόσβασης http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/symboyles-gia-toys-kodikoys-prosbasis/ και ποια μέτρα θα πρέπει να εφαρμόζουν για την προστασία του απορρήτου των επικοινωνιών τους http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/enimerosi-gia-prostasia-toy-aporritoy-ton-epikoinonion/ilektronikes-epikoinonies/
Ενδεικτικά, πρακτικές οδηγίες σχετικά με τα passwords περιλαμβάνουν τα παρακάτω μέτρα:
•Αφού φτιάξετε ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε, θα πρέπει να τους ανανεώνετε τακτικά (κάθε 6 μήνες τουλάχιστον).
•Εκτός από ισχυρό, το password πρέπει να είναι και μυστικό. Να ξέρετε ότι καμία εταιρεία που προσφέρει νόμιμη υπηρεσία δεν θα σας ζητήσει να στείλετε τον κωδικό σας μέσω ηλεκτρονικού ταχυδρομείου.
•Σημαντικό είναι να μην αποθηκεύετε τον κωδικό σας σε προγράμματα πλοήγησης στο διαδίκτυο ή σε μια εφαρμογή, ιδιαίτερα αν χρησιμοποιείτε έναν κοινόχρηστο υπολογιστή. Καλύτερα ακόμη, απενεργοποιήστε την επιλογή απομνημόνευσης κωδικού.
•Επιπλέον, ένα ασφαλές password θα σας προστατεύει μόνο αν ένας κακόβουλος δεν μπορέσει να το παρακάμψει με άλλο τρόπο (π.χ. με την ερώτηση ασφάλειας για την ανάκτηση του password). Θα πρέπει να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας που οι χάκερς δεν θα μπορούν να μαντέψουν.
Το κεντρικό μήνυμα της Ημέρας Ασφαλούς Διαδικτύου για φέτος, «Μαζί για ένα καλύτερο διαδίκτυο», υπογραμμίζει ότι η ασφάλεια του κυβερνοχώρου δεν αφορά μόνο τους ειδικούς στους ηλεκτρονικούς υπολογιστές, ή μεγάλες εταιρείες και κυβερνήσεις. Αφορά όλους μας που αξιοποιούμε τις εκπληκτικές δυνατότητες που μας προσφέρει η ψηφιακή τεχνολογία. Γνωρίζοντας τους πιθανούς κινδύνους και υιοθετώντας τους κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, αποφεύγουμε να γινόμαστε στόχος κακόβουλων.
Σε ό,τι αφορά τις εταιρείες παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών, η καλλιέργεια μιας κουλτούρας ασφάλειας είναι επίσης σημαντική και αποτελεί κύριο μέλημα της ΑΔΑΕ. Με βάση τις αρμοδιότητές της, η Αρχή επιβάλλει στους παρόχους την εφαρμογή μέτρων ασφάλειας με στόχο την πρόληψη και τον περιορισμό των κινδύνων ως προς την ιδιωτικότητα της επικοινωνίας. Έτσι, σήμερα, οι μεγαλύτερες εταιρείες πάροχοι, οι οποίες εξυπηρετούν πάνω από το 95% της αγοράς ηλεκτρονικών επικοινωνιών, εφαρμόζουν εγκεκριμένες Πολιτικές Ασφάλειας.
Επίσης, η Αρχή ελέγχει τις εταιρείες, με σκοπό να διερευνήσει αν εφαρμόζουν ορθά τους Κανονισμούς, όπως υποχρεούνται, αλλά και για να διερευνήσει καταγγελίες πολιτών ή περιστατικά ασφάλειας. Στις περιπτώσεις που παρατηρείται παραβίαση της σχετικής νομοθεσίας από τους παρόχους, η ΑΔΑΕ επιβάλλει διοικητικές κυρώσεις.
Μέσα στο 2018 επιβλήθηκαν συνολικά διοικητικές κυρώσεις σε 41 περιπτώσεις, συνολικού ύψους περίπου 2,5 εκατ. ευρώ, συμπεριλαμβανομένων και οκτώ περιπτώσεων επιβολής συστάσεων.