



## Κωδικοί πρόσβασης

Το απόρρητο της επικοινωνίας είναι δικαίωμά σου!  
Προστάτεψέ το!

Βασικός κανόνας για την προστασία του απορρήτου των επικοινωνιών σας και της ιδιωτικής σας ζωής είναι να επιλέγετε **ισχυρούς κωδικούς πρόσβασης** (passwords) για κάθε εφαρμογή ή σύνδεση που χρησιμοποιείτε.

*Μην παίρνετε ελαφρά την ασφάλεια. Κωδικοί που είναι εύκολο να προβλεφθούν σας βάζουν σε κίνδυνο. Σκεφθείτε τι θα συμβεί αν κάποιος αποκτήσει πρόσβαση στην ηλεκτρονική σας αλληλογραφία ή στο κινητό σας τηλέφωνο και υποκλέψει όλα σας τα μηνύματα.*

Είναι εύκολο να δημιουργήσετε έναν εξαιρετικά ασφαλή κωδικό πρόσβασης που για να παραβιαστεί θα χρειαστούν χρόνια. Θα πρέπει να είναι μεγάλος (πάνω από 8 χαρακτήρες), σύνθετος (με γράμματα, σύμβολα, αριθμούς) αλλά και να τον θυμάστε, γιατί δεν πρέπει να αποθηκεύεται.

Οι ειδικοί προτείνουν ένα τρόπο για να το πετύχετε: το **passphrase**

**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^**.



# Κωδικοί πρόσβασης

## Κανόνες ασφάλειας

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 ισχυρός, ο κωδικός σας πρέπει να είναι **και μυστικός**. Να ξέρετε ότι καμία εταιρία 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.

Φυσικά, ο ασφαλής κωδικός πρόσβασης που δημιουργήσατε δεν σας προστατεύει αν ένας χάκερ μπορεί να τον παρακάμψει με άλλο τρόπο. **Μάθετε πώς μπορείτε να δημιουργήσετε μια ισχυρή ερώτηση ασφαλείας** (για ανάκτηση κωδικού) που οι χάκερς δεν θα μπορούν να μαντέψουν.

*Επισκεφθείτε την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών ([www.adae.gr](http://www.adae.gr)) και ενημερωθείτε σχετικά με τα μέτρα αυτοπροστασίας που θα πρέπει να εφαρμόζετε για την ασφάλεια του απορρήτου των επικοινωνιών σας.*

**Το απόρρητο της επικοινωνίας είναι δικαίωμά σου! Προστάτεψέ το!**