2 Οκτωβρίου 2014

Καρέ-καρέ πώς θα δημιουργήσετε τον πιο ασφαλή κωδικό πρόσβασης -Οκτώ βήματα [λίστα]

/ Επιστήμες, Τέχνες & Πολιτισμός

Τηλέφωνα, οδοί, ημερομηνίες γέννησης. Αριθμοί και λέξεις που χρησιμοποιούνται συχνά ως κωδικοί πρόσβασης. Κωδικοί πρόσβασης εύκολα προβλέψιμοι που έχουν ως αποτέλεσμα οι χρήστες τους να τίθενται σε μεγάλο κίνδυνο λόγω των χάκερς. Παρακάτω παρουσιάζονται οκτώ τρόποι μέσω των οποίων μπορεί να «χτιστεί» ένας ισχυρός και... άτρωτος κωδικός πρόσβασης που δεν θα μπορέσει να τον σπάσει κανένας χάκερ.

- Αποφύγετε το προφανές

Οσο απίστευτο κι αν ακουγετε υπάρχουν ακόμη χρήστες που βάζουν σε κάρτες, mail και λοιπούς άλλους λογαριασμούς κωδικούς πρόσβασης οπως «123456» ή τη λέξη «password».

- Κάντε ένα αγαπημένο σας μότο κωδικό

Ενας καλός τρόπος για να δημιουργήσετε έναν κωδικό που και ασφαλής θα είναι και δεν θα τον ξεχνάτε είναι να φτιάξετε έναν με μια φράση για εσάς. Για παράδειγμα: «Ο συγκάτοικός μου στο πανεπιστήμιο ήταν από τη Λάρισα» θα μπορουσε να μετατραπεί στον εξής κωδικό «ΟσμσπηατΛΑ».

- Ανακατέψτε γράμματα με αριθμούς

Οι ειδικοί ισχυρίζονται ότι ένας κωδικός που περιλαμβάνει τόσο γράμματα όσο και αριθμούς είναι πολύ πιο ασφαλής από έναν που αποτελείται μόνο από γράμματα ή μόνο από αριθμούς. Αλλά και σε αυτή την περίπτωση δεν πρέπει να χρησιμοποιούνται τα προφανή. Ενας εύκολος τρόπος για να δημιουργηθεί ένας κωδικός είναι να προστεθεί ενδιάμεσα, ακόμη και σπαστά στον κωδικό που προκύπτει από την προσωπική φράση, μια… χρονολογία γέννησης. Για παράδειγμα: «Οσμσπη1984ατΛΑ»

- Χρησιμοποιείστε περισσότερους από 12 χαρακτήρες

Ολοι οι κωδικοί είναι δυνατό να χακευτούν. Ωστόσο, όσο μεγαλύτερος είναι ένας κωδικός τόσο πιο δύσκολο είναι το έργο του επίδοξου χάκερ. Σύμφωνα με τους ερευνητές του πανεπιστημίου της Τζώρτζια θα χρειαστεί 17 χρόνια για να μπορέσει κανείς να σπάσει έναν κωδικό 12 χαρακτήρων.

- Μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης σε όλους τους λογαριασμούς σας

Αν έχετε έναν κωδικό πρόσβασης για όλους τους λογαριασμούς σας τότε ένα χτύπημα σε έναν από αυτούς εκθέτει σε κίνδυνο και όλους τους υπόλοιπους! Φροντίζεται να τους αλλάζετε ανά τακτά χρονικά διαστήματα και αποφεύγετε να επαναχρησιμοποιείτε κωδικούς που έχετε ήδη χρησιμοποιήσει.

- Προσαρμόστε τον κωδικό ανά σελίδα

Αν επιμένετε και θέλετε να έχετε έναν κωδικό για όλους τους λογαριασμούς σας τότε φροντίστε να τον προσαρμόζετε ανάλογα με το πού το χρησιμοποιείτε. Για παράδειγμα αν θέλετε να βάλετε τον παραπάνω κωδικό «Οσμσπη1984ατΛΑ» στο Facebook τότε μετατρέψτε τον σε «FBK. Οσμσπη1984ατΛΑ».

- Να αποσυνδέεστε πάντα

Οσο βολικό, τόσο και επικίνδυνο είναι το να μένει κανείς συνδεδεμένος σε όλους τους λογαριασμούς του. Σε περίπτωση που ένας χάκερ αποκτήσει πρόσβαση σε έναν υπολογιστή με αποθηκευμένους όλους τους κωδικούς πρόσβασης τότε θα μπορέσει μέσα σε ελάχιστο χρόνο και να τους υποκλέψει.

Ενεργοποιήστε την επαλήθευση των δύο κινήσεων
Η επαλήθευση των δύο κινήσεων βοηθά στην περαιτέρω προστασία από τους

χάκερ. Η επαλήθευση των δύο κινήσεων απαιτεί από όποιον την έχει ενεργοποιήσει πέρα από τον κωδικό του να πληκτρολογήσει και τον αριθμό που θα του σταλεί σε μήνυμα.

Πηγή: iefimerida.gr