Αθήνα, 26 Απριλίου 2012

ΕΛΛΗΝΙΚΟ ΚΕΝΤΡΟ ΑΣΦΑΛΟΥΣ ΔΙΑΔΙΚΤΥΟΥ
Δράση Ενημέρωσης Saferinternet.gr
ΔΕΛΤΙΟ ΤΥΠΟΥ

Επιλέξτε έναν ισχυρό κωδικό για τις διαδικτυακές σας δραστηριότητες

Το τέλειο *password*, δηλαδή ο μυστικός κωδικός που θα παρέχει απόλυτη ασφάλεια από όσους επιδιώκουν να υποκλέψουν τα προσωπικά μας στοιχεία από τον υπολογιστή μας, δεν έχει εφευρεθεί ακόμα, ωστόσο όλοι μπορούν να θωρακίσουν το *password* τους ώστε να αποφύγουν τις ηλεκτρονικές κακοτοπιές, μικροί και μεγάλοι.

Έρευνες δείχνουν ότι ο μυστικός κωδικός που συνήθως χρησιμοποιούμε για την πρόσβασή μας σε διάφορες διαδικτυακές υπηρεσίες δεν είναι και τόσο ασφαλής όσο πιστεύουμε. Το πιο συχνό λάθος είναι να επιλέγουμε συνηθισμένες λέξεις ή φράσεις τις οποίες τις θυμόμαστε μεν εύκολα, αλλά είναι εξ' ίσου εύκολο να τις μαντέψει και ένας επίδοξος χάκερ. **Το *password* καλό είναι να μην αποτελείται από μία μόνο λέξη**. Σύμφωνα με έρευνα του περιοδικού Forbes που διεξήχθη από εταιρείες που συλλέγουν εξαιρετικά μεγάλο όγκο δεδομένων και ασχολούνται με την ασφάλεια, όπως η splashdata, ανάμεσα στα 25 χειρότερα *passwords* για το 2011 συγκαταλέγονται η ίδια η λέξη "password" στην πρώτη θέση (!) και απλές αγγλικές λέξεις όπως "monkey", "letmein", "trustno1", "dragon", "baseball", "iloveyou" κ.α.

Το *password* πρέπει να είναι μη προσωπικό. Ειδάλλως, με ένα προσωπικό *password* είναι σα να δίνουμε το κλειδί του σπιτιού μας σε οποιονδήποτε γνωστό και άγνωστο. Αποφεύγουμε π.χ. την ημερομηνία των γενεθλίων μας, που πιθανώς να έχουμε δημοσιεύσει σε έναν ιστοχώρο όπως το facebook, δίνοντας έτσι τη δυνατότητα σε οποιονδήποτε να μπει στο λογαριασμό μας πολύ εύκολα, με την ημερομηνία αυτή. Ομοίως, αποφεύγουμε οτιδήποτε θα μπορούσε να μαντέψει κάποιος, όπως π.χ. το τηλέφωνό μας, το όνομα του κατοικίδιου μας, κάποιου κοντινού συγγενή μας κλπ. Επίσης, **ο κωδικός μας δεν πρέπει να είναι προβλέψιμος**. Αποφεύγουμε τυπικούς συνδυασμούς γραμμάτων και αριθμών, όπως «123456», «12345678», «111111», "qwerty", "abcdefg", "abc123", *passwords* που, σύμφωνα με την εταιρεία Imperva σε έρευνα 32 εκατομμυρίων κωδικών που υποκλάπηκαν από την ιστοσελίδα RockYou, κατατάσσονται στις πρώτες θέσεις χρήσης.

Υπάρχουν τρεις απλές συμβουλές που μπορούμε να ακολουθήσουμε για να ενισχύσουμε την ασφάλεια του password μας. Πρώτον, **ο κωδικός μας θα πρέπει να περιέχει τουλάχιστον 8 χαρακτήρες**. Δεύτερον, θα πρέπει να είναι **αναμεμειγμένος με πεζά και κεφαλαία γράμματα, αριθμούς και κάποιους ειδικούς χαρακτήρες** όπως (!@#$%^&*,;"). Τρίτον, χρησιμοποιούμε φαντασία στην επιλογή των λέξεων· είναι σημαντικό να μην είναι μια συνηθισμένη λέξη που μπορεί να υπάρχει στο λεξικό. Μπορούμε π.χ. να επιλέξουμε μια φράση και να μην την χρησιμοποιήσουμε αυτούσια, αλλά να πάρουμε τα πρώτα γράμματα από την κάθε λέξη της φράσης και να δημιουργήσουμε μια νέα λέξη, την οποία όμως θα τη θυμόμαστε εύκολα και θα είναι δύσκολο να τη μαντέψει κάποιος άλλος. Ένα παράδειγμα: από τη φράση «Mou aresoun poli ta lazania me saltsa» δημιουργούμε τον κωδικό «Maptlms», βάζουμε στη μέση και στο τέλος ειδικούς χαρακτήρες ή αλλάζουμε κάποιους όπως το «a» σε «@» και έχουμε έτσι έναν ισχυρό κωδικό → «M@ptlms%».

Ακόμα, όμως, και αν έχουμε επιλέξει το τέλειο *password*, δεν πρέπει να εφησυχάζουμε για την ασφάλεια της ηλεκτρονικής μας επικοινωνίας, γιατί τις περισσότερες φορές δεν τίθεται μόνο θέμα υποκλοπής των στοιχείων μας, αλλά οι επιτήδειοι προσπαθούν μέσα από το λεγόμενο "phishing" να μας παρασύρουν ώστε να δώσουμε μόνοι μας τον κωδικό μας. Ας είμαστε λοιπόν προσεκτικοί, μικροί και μεγάλοι!

Αν θέλετε να ελέγξετε την ασφάλεια του *password* σας υπάρχουν διάφορα sites που μπορείτε να επισκεφθείτε, π.χ. ιδιαίτερα δημοφιλής σε εκπαιδευτικούς και παιδιά είναι ο ιστοχώρος http://howsecureismypassword.net/.

Χρυσός Χορηγός COSMOTE

Με τη συγχρηματοδότηση της Ευρωπαϊκής Επιτροπής