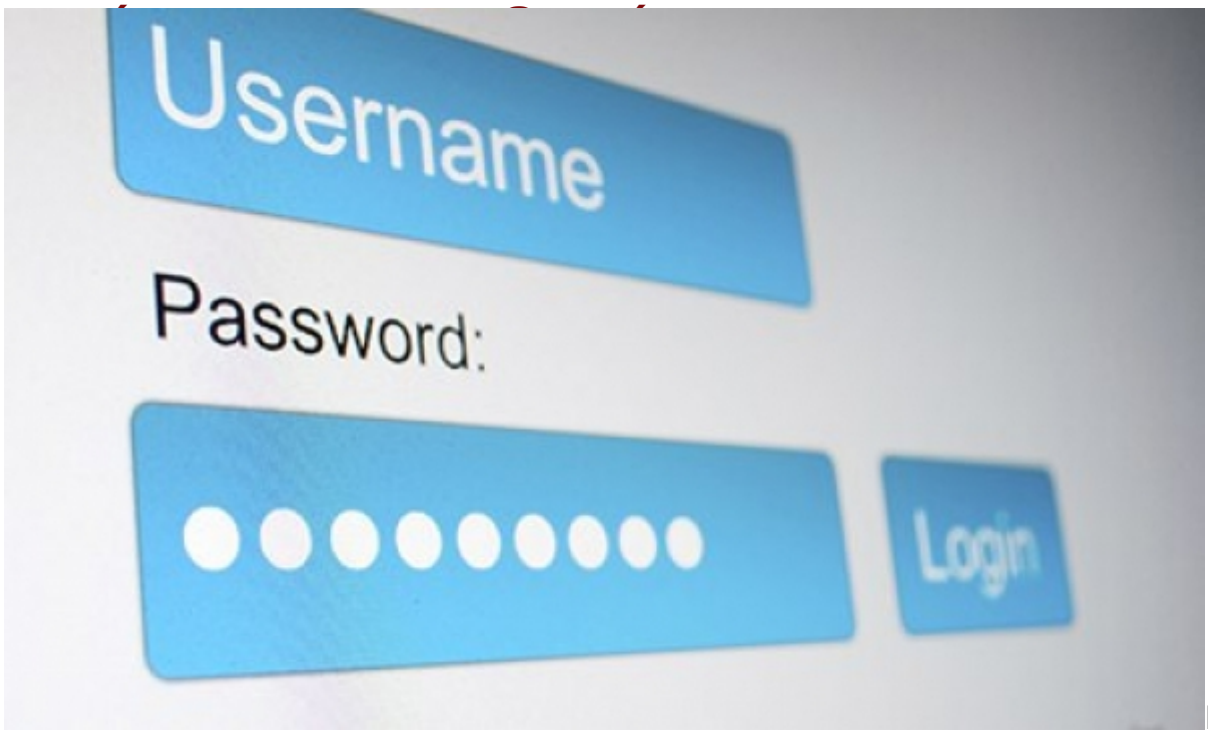
26 Οκτωβρίου 2014

Τα λάθη που κάνετε και είναι επικίνδυνο να σας



Πέρα

από το ότι δεν πρέπει να χρησιμοποιείτε κωδικούς πρόσβασης, όπως το «123456», υπάρχουν και κάποιοι κωδικοί που ναι μεν νομίζετε ότι είναι δύσκολοι, όμως είναι πολύ πιο εύκολο για τους χάκερ να τους σπάσουν από ό, τι εσείς νομίζετε.

Ολοι οι κωδικοί θα μπορούσαμε να πούμε πως είναι εύκολος στόχος για τους χάκερ, παρόλο που κάθε ένας έχει μήκος εννέα ή περισσότερους χαρακτήρες και περιέχει ένα μείγμα από γράμματα, αριθμούς και σύμβολα. Πώς, λοιπόν, μπορούν αυτοί οι φαινομενικά ισχυροί κωδικοί πρόσβασης να είναι τόσο αδύναμοι και πώς ένας χάκερ μπορεί να τους βρει;

Το πιο πιθανό είναι να τους κλέψει μέσω της παραβίασης από μία βάση δεδομένων πελατών, όπως έγινε πρόσφατα με το iCloud της Apple και το τεράστιο σκάνδαλο με γυμνές φωτογραφίες σταρ του Χόλιγουντ. Δεδομένου ότι πολλοί κωδικοί πρόσβασης αποθηκεύονται με τέτοιο τρόπο που να μην μπορούν να διαβαστούν άμεσα από τους απλούς ανθρώπους, οι χάκερ χρησιμοποιούν συχνά ένα λογισμικό για τους σπάσουν.

Σε μια μελέτη του 2013 για την DARPA (Federal Defense Advanced Research Projects Agency) η εταιρεία συμβούλων ασφαλείας KoreLogic διαπίστωσε ότι

ανάμεσα στις χιλιάδες των χρηστών του δείγματος περίπου οι μισοί είχαν βασιστεί σε μόλις πέντε πρότυπα για να φτιάξουν τους κωδικούς πρόσβασής τους και 85% είχαν βασιστεί σε 100 διαφορετικά.

Αυτά είναι τα τρία πιο κοινά πρότυπα που βρήκε η έρευνα ότι εμπιστεύεται η πλειοψηφία των χρηστών και που αν τα χρησιμοποιήσει κανείς, τότε ο κωδικός τους σπάει πολύ εύκολα:

• Ενα κεφαλαίο γράμμα, στη συνέχεια πέντε πεζά και μετά δύο αριθμοί (Παράδειγμα: Dulith57)
• Ενα κεφαλαίο γράμμα, στη συνέχεια έξι πεζά και μετά δύο αριθμοί (Παράδειγμα: Abugmar64)
• Ενα κεφαλαίο γράμμα, στη συνέχεια τρία πεζά και μετά τέσσερις αριθμοί (Παράδειγμα: Itio1981)

Ποια είναι τα λάθη που κάνετε:

• Ξεκινάτε με ένα κεφαλαίο γράμμα και συνεχίζετε με πεζά γράμματα
• Όταν ένας κωδικός πρόσβασης δεν είναι αρκετά μακρύς, προσθέτετε ένα με δύο τυχαία γράμματα
• Βάζετε αριθμούς, δύο ή τέσσερις, πριν ή μετά από τα γράμματα
• Όταν ένας ειδικός χαρακτήρας απαιτείται χρησιμοποιείτε το θαυμαστικό (!) και κυρίως το βάζετε στο τέλος
• Δεν χρησιμοποιείτε δύο ειδικούς χαρακτήρες στον ίδιο κωδικό πρόσβασης

Πώς να δημιουργήσετε πιο ισχυρούς κωδικούς πρόσβασης:

• Αποφύγετε να ξεκινά ο κωδικός πρόσβασης σας με ένα κεφαλαίο γράμμα ή ίσως ακόμη και χωρίς κάποιο γράμμα
• Δημιουργήστε ένα αρκτικόλεξο χρησιμοποιώντας το πρώτο γράμμα κάθε λέξης σε πρόταση που δεν θα ξεχάσετε. Παράδειγμα: t2cmlp,@yh από το «Try to crack my latest password, all you hackers» (σσ: Προσπαθήστε να σπάσετε τον τελευταίο κωδικό μου όλοι εσείς οι χάκερ).
• Αντισταθείτε στη φυσική τάση να χρησιμοποιείτε βασικές λέξεις και φράσεις
• Βάλτε πολλούς ειδικούς χαρακτήρες στον ίδιο κωδικό πρόσβασης
• Μην βάζετε τους αριθμούς τον έναν δίπλα στον άλλο

Πηγές:protothema.gr- onlycy.com