21 Ιανουαρίου 2016

Social media: 6 πράγματα που σας κάνουν ευάλωτους!

/ Πεμπτουσία

Image not found or type unknown

Υπάρχουν κάποια πράγματα που πιθανόν κάνετε στα social media και σας κάνουν ευάλωτους σε hacks κι επιθέσεις.

Το ηλεκτρονικό έγκλημα είναι μια πραγματική και διαδεδομένη απειλή οπότε πρέπει να αυξήσετε την ασφάλεια σας στο διαδίκτυο και σαφώς και στα social media. Αυτά είναι τα 6 πράγματα που πρέπει να προσέξετε:

Δέχεστε followers ή αιτήματα φιλίας από ανθρώπους που δεν γνωρίζετε!

Επιτρέποντας σε αγνώστους να βλέπουν το Facebook, το Twitter, το Instagram σας και άλλα σας προφίλ σε social media, τους παρέχετε ουσιαστικά πρόσβαση στα προσωπικά σας στοιχεία. Δεν θα τα λέγατε αυτά σε ξένους στο δρόμο επειδή θα ήταν περίεργο κι επικίνδυνο. Το ίδιο ισχύει και online.

Σύμφωνα με μια έρευνα του Kaspersky Lab, το 31% των χρηστών δέχονται συνδέσεις με ανθρώπους που δεν ξέρουν. Αυτό μπορεί να τους εκθέσει σε ακόμα πιο άγνωστα άτομα και ακόμα και σε διαφημιστές και σε εγκληματίες του κυβερνοχώρου.

Πατάτε links που σας στέλνουν οι διαδικτυακοί σας φίλοι χωρίς να ρωτάτε τι είναι!

Συνήθως οι φίλοι κοινοποιούν links από αστείες εικόνες ή ενδιαφέροντα άρθρα. Αλλά δεν είναι κακό αν είστε επιφυλακτικός για links που φαίνονται πονηρά ή προέρχονται από κάποιον που δεν γνωρίζετε ή έχετε μιλήσει σπάνια. Η έρευνα έδειξε ότι 26% των χρηστών θα πατούσαν κλικ σε κάποιο link που θα τους αποστελλόταν χωρίς δισταγμό και ανησυχία.

Μοιράζεστε προσωπικές λεπτομέρειες!

Δεν είναι μόνο τα τραπεζικά στοιχεία που πρέπει να προστατεύετε! Οι λογαριασμοί μπορούν να δημιουργηθούν με πολύ λίγα στοιχεία όποτε αν είναι κάτι που δεν θέλετε να μοιραστείτε με τον εργοδότη σας, με ξένους και με τους φίλους σας μην το βάζετε online.

Περίπου το 1/3 των χρηστών των social media που ρωτήθηκαν μοιράζονται τα posts τους, τα check-in κι άλλες πληροφορίες όχι μόνο με τους φίλους τους αλλά με οποιοδήποτε είναι online. Αυτό αφήνει την πόρτα ορθάνοιχτη για τους εγκληματίες του κυβερνοχώρου να επιτεθούν καθώς οι χρήστες αγνοούν πόσο δημόσιες μπορούν να είναι οι πληροφορίες τους.

Παραμελείτε τις ρυθμίσεις απορρήτου

Αν υπάρχουν κάποιες συγκεκριμένες λεπτομέρειες, φωτογραφίες, status ή άλλες πληροφορίες που δεν θέλετε να τις ξέρουν άλλοι σιγουρευτείτε ότι χρησιμοποιείτε την προστασία που παρέχεται. Παρότι πάνω από τα ¾ των χρηστών του διαδικτύου χρησιμοποιούν social media, υπάρχει σαφής έλλειψη ευαισθητοποίησης για θέματα ασφαλείας.

Όλοι σας οι κωδικοί είναι ίδιοι ή είναι αποθηκευμένοι στον browser σας

Αν και είναι πολύ βολικό να έχετε τους κωδικούς σας αποθηκευμένους και να μπαίνουν κατευθείαν μόλις κάνετε log in, αν κάποιος χακάρει τον browser σας θα αποκτήσει πρόσβαση στα πάντα. Οι ισχυροί κωδικοί πρόσβασης αποτελούνται από

συνδυασμό αριθμών, γραμμάτων και κεφαλαίων και μικρών και χαρακτήρων. Πρέπει να είναι ισχυροί και να τους θυμάστε αλλά μην είναι προφανείς οπότε ξεχάστε τα γενέθλια σας!

Δεν έχετε λογισμικό ασφαλείας!

Σε συνδυασμό με την επαγρύπνηση και την κοινή λογική, το λογισμικό ασφαλείας προστατεύει τη ψηφιακή σας ζωή από απειλές του Διαδικτύου και προστατεύει την ιδιωτική σας ζωή και ταυτότητα. Οι χρήστες των social media παίζουν ένα επικίνδυνο παιχνίδι και ουσιαστικά δίνουν σε ξένους εύκολη πρόσβαση στα προσωπικά τους στοιχεία.

Για να δείτε αν είστε αρκετά ενημερωμένοι για την ασφάλεια σας στο διαδίκτυο κάντε το τεστ εδώ

Πηγή: secnews.gr