Greek

ΟΙ ΔΕΚΑ ΚΑΛΥΤΕΡΕΣ ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

1. Οι χάκερς χρησιμοποιούν ηλεκτρονικά μηνύματα «ψαρέματος» (phishing) για να αποκτήσουν πρόσβαση στις ασφαλείς πληροφορίες σας. Να είστε προσεκτικοί σε όλες τις επικοινωνίες που λαμβάνετε και αν νομίζετε ότι κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου είναι ύποπτο, μην κάνετε κλικ σε συνδέσμους και μην ανοίγετε συνημμένα αρχεία.

2. Βελτιώστε την ασφάλειά σας στο διαδίκτυο καθορίζοντας δύο κωδικούς. Η προσθήκη ενός ακόμη κωδικού πιστοποίησης της ταυτότητάς σας καθιστά δυσκολότερη την πρόσβαση των επιτιθέμενων στα δεδομένα σας.

3. Μην ενεργοποιείτε πάντα τη γεωγραφική θέση. Είναι σύνηθες οι ιστότοποι να σας ζητούν να δηλώσετε την τοποθεσία σας. Με τον τρόπο αυτό, δημιουργούν ένα προφίλ γύρω από την τοποθεσία και τα ενδιαφέροντά σας. Αντ' αυτού, επιλέξτε χειροκίνητα την τοποθεσία σας για καλύτερη προστασία των δεδομένων σας.

4. Εγκαταστήστε προγράμματα φραγής διαφημίσεων - οι διαφημίσεις ενδέχεται να σας παρακολουθούν στο παρασκήνιο. Χρησιμοποιήστε φραγές διαφημίσεων για να απενεργοποιήσετε την παρακολούθηση και την ανάλυση από δεύτερα και τρίτα μέρη.

5. Να είστε επιφυλακτικοί με τα δημόσια δίκτυα Wi-Fi - αυτά είναι συχνά λιγότερο ασφαλή από τα κανονικά δίκτυα και παρέχουν πρόσβαση σε περισσότερα δεδομένα από τα απαραίτητα όταν παρέχουν σύνδεση στο Διαδίκτυο.

6. Έχετε δικαίωμα να ρωτήσετε γιατί συλλέγονται οποιεσδήποτε πληροφορίες για εσάς. Αυτό περιλαμβάνει, για παράδειγμα, πολιτειακούς κυβερνητικούς οργανισμούς και άλλους φορείς. Η πολιτική απορρήτου τους μπορεί να περιέχει αυτές τις πληροφορίες.

7. Διατηρείτε τα έγγραφα και τα αρχεία σας ασφαλή, εάν περιέχουν ευαίσθητες ή προσωπικές πληροφορίες. Εξετάστε το ενδεχόμενο χρήσης κρυπτογράφησης για το κλείδωμα φορητών σκληρών δίσκων και USB, ώστε να αποτρέψετε τη μη εξουσιοδοτημένη πρόσβαση σε περίπτωση κακής τοποθέτησής τους

8. Διατηρείτε τους κωδικούς πρόσβασης, τους κωδικούς PIN και άλλους κωδικούς πρόσβασης εμπιστευτικούς και ασφαλείς. Η χρήση ενός διαχειριστή κωδικών πρόσβασης είναι ένας καλός τρόπος για να διατηρείτε τους κωδικούς πρόσβασης και σύνδεσης (login) σας ασφαλή, καθώς αποθηκεύονται σε κρυπτογραφημένες βάσεις δεδομένων.

9. Ενεργοποιήστε τις ρυθμίσεις απορρήτου και επανεξετάστε τις τακτικά όταν χρησιμοποιείτε διαδικτυακά μέσα κοινωνικής δικτύωσης και ιστότοπους δικτύωσης (π.χ. Facebook, Twitter). Εξετάστε το ενδεχόμενο να κάνετε τα προφίλ σας στα μέσα κοινωνικής δικτύωσης εμπιστευτικά.

10. Πετάτε με ασφάλεια (π.χ. με καταστροφέα εγγράφων) την αλληλογραφία που περιέχει προσωπικά στοιχεία. Ποτέ μην τοποθετείτε ευαίσθητα έγγραφα που περιέχουν τα προσωπικά σας στοιχεία στον κάδο ανακύκλωσης.