20 Σεπτεμβρίου 2016

Έξι τρωτά σημεία της παρουσίας στο διαδίκτυο: πως να προστατεθείτε

/ Πεμπτουσία

Image not found or type unknown

Στην εποχή μας, το internet αποτελεί αναπόσπαστο κομμάτι της καθημερινότητάς μας. Όμως μαζί με τα πλεονεκτήματα που μας προσφέρει, έρχονται και τα προβλήματα και ένα από αυτά είναι η διαρροή προσωπικών μας πληροφοριών σε τρίτους. Σας παραθέτουμε λοιπόν 6 περιπτώσεις που είστε εκτεθειμένοι σε κινδύνους online, χωρίς να το υποψιάζεστε, καθώς και πώς να προστατευτείτε.

1 Όταν χρησιμοποιούμε δημόσια Wi-Fi

Τα δημόσια δίκτυα Wi-Fi είναι εγγενώς μη ασφαλή. Επειδή ο καθένας μπορεί να έχει πρόσβαση στο ίδιο δημόσιο hotspot, οποιαδήποτε πληροφορία μπορείτε να στείλετε ή να λάβετε μέσω δημοσίου Wi-Fi θα μπορούσε να είναι ευάλωτη σε αδιάκριτα μάτια. Αυτό σημαίνει ότι όλα τα μηνύματα που στέλνετε online ή οι κωδικοί πρόσβασης που εισάγετε θα μπορούσαν να υποκλαπούν από τρίτους, στο

ίδιο δίκτυο.

Πώς να προστατευτείτε: Περιορίστε τη χρήση των δημόσιων Wi-Fi και ενημερωθείτε για τους κινδύνους που εμπλέκονται. Βεβαιωθείτε ότι έχετε επιλέξει ένα νόμιμο hotspot και να αποφύγετε τη χρήση ιστοσελίδων που παρέχουν πρόσβαση σε ευαίσθητες οικονομικές πληροφορίες ή τη χρήση προσωπικών σας email όταν σερφάρετε στο διαδίκτυο σε δημόσια Wi-Fi.

2. Όταν δίνετε προσωπικές πληροφορίες μέσω e-mail

Το ηλεκτρονικό ταχυδρομείο είναι ένα από τα πιο δημοφιλή μέσα επικοινωνίας. Είναι δελεαστικό να χρησιμοποιήσετε το email κατά την ανταλλαγή προσωπικών πληροφοριών, όπως κωδικούς πρόσβασης επειδή είναι βολικό, αλλά αυτό μπορεί να ενέχει κινδύνους. Ακόμα και αν είστε εντελώς σίγουρος ότι η σύνδεσή σας είναι ασφαλής, δεν ξέρετε ότι του παραλήπτη είναι και αυτό σημαίνει ότι τα ευαίσθητα προσωπικά σας δεδομένα θα μπορούσαν να βρεθούν σε κίνδυνο.

Πώς να προστατευτείτε: Μην περιλαμβάνετε τίποτα σημαντικές προσωπικές πληροφορίες σε ένα email. Όποτε είναι δυνατόν, θα πρέπει να χρησιμοποιείτε μια ασφαλή υπηρεσία ηλεκτρονικού ταχυδρομείου που προσφέρει ένα υψηλότερο επίπεδο προστασίας.

3. Όταν κάνετε απρόσεκτα post στα social media

Τα μέσα κοινωνικής δικτύωσης σας αναδεικνύουν τη ζωή σας. Ωστόσο, ανάλογα με τις ρυθμίσεις απορρήτου σας και τις ενέργειες των συνδέσεων σας, τα post αυτά μπορεί να φαίνονται σε λάθος ανθρώπους. Είναι δυνατόν να εκθέσετε ιδιωτικές ή ευαίσθητες πληροφορίες σε εγκληματίες που μπορεί να διαρρήξουν το σπίτι σας ή να επιτεθούν στην ψηφιακή σας ταυτότητα.

Πώς να προστατευτείτε: Μην δημοσιεύετε οτιδήποτε στα social media και επιπλέον ελέγξτε διπλά όλες τις ρυθμίσεις απορρήτου σας για να βεβαιωθείτε ότι είστε πιο ασφαλείς.

4. Όταν συμπληρώνετε ηλεκτρονικές φόρμες

Οι περισσότερες ιστοσελίδες αυτές τις μέρες να ζητούν για κάποιο είδος προσωπικών πληροφοριών, είτε αυτό είναι μια διεύθυνση email ή ακόμα και περισσότερα προσωπικά στοιχεία για να αποκτήσετε πρόσβαση σε αυτές. Αυτό δεν είναι εγγενώς επικίνδυνο – οι περισσότερες είναι στην πραγματικότητα πολύ αξιόπιστες – αλλά αν δεν είστε προσεκτικοί, τα προσωπικά σας στοιχεία θα μπορούσαν να χρησιμοποιηθούν για αμφισβητήσιμους σκοπούς.

Πώς να προστατευτείτε: Να είστε ενήμεροι για τις ιστοσελίδες που χρησιμοποιείτε και για το πώς χρησιμοποιούνται οι πληροφορίες σας. Οι περισσότερες νόμιμες ιστοσελίδες θα έχουν πολιτικές απορρήτου που εξηγούν πώς θα χρησιμοποιηθούν τα προσωπικά σας στοιχεία.

5. Όταν χρησιμοποιείτε αδύναμους ή συνηθισμένους κωδικούς πρόσβασης.

Οι περίπλοκοι κωδικοί πρόσβασης είναι δύσκολοι, έτσι οι περισσότεροι άνθρωποι επιλέγουν απλούστερες εναλλακτικές και έχουν την τάση να χρησιμοποιούν αυτούς τους απλούς κωδικούς πρόσβασης ξανά και ξανά. Ωστόσο, κάτι τέτοιο μπορεί να αφήσει τα δεδομένα σας ευάλωτα σε επιθέσεις. Οι χάκερ μπορούν εύκολα να μαντέψουν απλούς κωδικούς πρόσβασης και από τη στιγμή που τους γνωρίζουν, μπορούν να τους εφαρμόσουν σε σελίδες σε όλο το Διαδίκτυο για να αποκτήσουν ακόμη μεγαλύτερη πρόσβαση σε προσωπικούς σας λογαριασμούς.

Πώς να προστατευτείτε: Βεβαιωθείτε ότι όλοι οι κωδικοί πρόσβασης σας είναι ισχυροί, συνδυάζοντας κεφαλαία και μικρά γράμματα, αριθμούς και σύμβολα. Χρησιμοποιήστε διαφορετικούς κωδικούς πρόσβασης για κάθε τοποθεσία και θυμηθείτε να τους αλλάζετε σε τακτά χρονικά διαστήματα.

6. Όταν αποδέχεστε πολιτικές απορρήτου, χωρίς να τις διαβάζετε

Οι περισσότερες online σελίδες θα σας πουν να δεχτείτε μια πολιτική προστασίας. Οι περισσότεροι χρήστες απλά κάνουν κλικ, χωρίς να τις διαβάζουν. Και ενώ στις περισσότερες περιπτώσεις αυτό δεν θα σας βλάψει, είναι μια μη ασφαλής πρακτική σε γενικές γραμμές.

Πώς να προστατευτείτε: Αγνοείστε τις πολιτικές απορρήτου και εξοικειωθείτε με το πώς διάφορες οργανώσεις παρακολουθούν τις δραστηριότητες και τις πληροφορίες σας online.

Πηγή: www.secnews.gr