Μόνο μικρός αριθμός νέων κατανοεί τους κινδύνους που συνδέονται με την ενεργό χρήση των κοινωνικών δικτύων. Αυτό υποστηρίζει νέα έρευνα της Kaspersky Lab και της B2B International.

Όπως προκύπτει από τα στοιχεία της μελέτης, σε μεγαλύτερο κίνδυνο βρίσκονται όσοι χρησιμοποιούν φορητές συσκευές για να επισκέπτονται μέσα κοινωνικής δικτύωσης.

Αναλυτικότερα, η έρευνα δείχνει, ότι η επικοινωνία μέσω κοινωνικών δικτύων αποτελεί μία από τις πιο δημοφιλείς δραστηριότητες στο διαδίκτυο. Συνολικά, η κοινωνική δικτύωση ήταν η τρίτη δημοφιλέστερη δραστηριότητα μετά από την πρόσβαση και την ανάγνωση των μηνυμάτων ηλεκτρονικού ταχυδρομείου. Ακόμα πιο δημοφιλής είναι η χρήση των κοινωνικών δικτύων σε ό,τι αφορά στις φορητές συσκευές, καθώς καταλαμβάνει τη δεύτερη θέση.

Οι συμμετέχοντες στην έρευνα δήλωσαν σε ποσοστό 78%, ότι δεν πιστεύουν πως οι ηλεκτρονικοί εγκληματίες ενδιαφέρονται γι' αυτούς ή ότι δεν τους απασχολεί καθόλου το συγκεκριμένο θέμα. Ένας στους δέκα χρήστες μοιράζεται ιδιωτικές πληροφορίες με αγνώστους, ενώ 15% των ερωτηθέντων χρησιμοποιούν τα κοινωνικά δίκτυα για ανταλλαγή πληροφοριών που δεν θα αποκάλυπταν ποτέ στην πραγματική ζωή.

Επιπλέον, 12% των ερωτηθέντων εισάγουν δεδομένα σε διαδικτυακούς λογαριασμούς ενώ βρίσκεται συνδεδεμένο σε δημόσια δίκτυα Wi-Fi. Μόλις 18% πιστεύουν, ότι αποκαλύπτουν περισσότερες προσωπικές πληροφορίες απ' όσο πρέπει στα κοινωνικά δίκτυα. Επίσης, μόλις 7% των ερωτηθέντων δήλωσαν, ότι οι κωδικοί πρόσβασης στα μέσα κοινωνικής δικτύωσης είναι μεταξύ των τριών ειδών πληροφοριών που φοβούνται να χάσουν.

Όπως επισημαίνει η Kaspersky, η απρόσεκτη συμπεριφορά των νέων μπορεί να οδηγήσει σε δυσάρεστες συνέπειες. Οι επιτιθέμενοι ψάχνουν συχνά στα κοινωνικά δίκτυα για πληροφορίες που έχουν αφήσει οι χρήστες εν αγνοία τους.

Οι πληροφορίες αυτές μπορεί να συμβάλουν σε ένα έγκλημα. Μεταξύ άλλων, οι διευθύνσεις ηλεκτρονικού ταχυδρομείου μπορεί να χρησιμοποιηθούν για απάτες, ενώ κάποιες πληροφορίες μπορεί να βοηθήσουν τους εγκληματίες να «σπάσουν» κωδικούς πρόσβασης ή να προσδιορίσουν τη θέση ενός χρήστη. Επιπλέον, αν οι ψηφιακοί απατεώνες αποκτήσουν πρόσβαση στους λογαριασμούς των νέων, έχουν ακόμη περισσότερες ευκαιρίες στη διάθεση τους, όπως η αποστολή κακόβουλων συνδέσεων και αρχείων στους «φίλους» του θύματος, η υποκλοπή προσωπικών δεδομένων που αργότερα θα πουληθούν στη μαύρη αγορά κ.α., τονίζεται στην έρευνα.

Επίσης, η έρευνα δείχνει ότι 40% των νέων αντιμετώπισαν ύποπτα μηνύματα που τους ζητούσαν να ακολουθήσουν έναν άγνωστο σύνδεσμο ή να «κατεβάσουν» ένα δυνητικά κακόβουλο αρχείο. Ταυτόχρονα, 21% των νέων έλαβαν μήνυμα ηλεκτρονικού ταχυδρομείου που ισχυριζόταν ότι προέρχεται από κάποιο κοινωνικό δίκτυο, σε μια προσπάθεια υποκλοπής των στοιχείων του λογαριασμού του χρήστη.

Επιπλέον, οι χρήστες φορητών συσκευών βάζουν συχνά τους εαυτούς τους σε ακόμη μεγαλύτερο κίνδυνο. Μόλις 6% των ερωτηθέντων δήλωσαν ότι ηλεκτρονικοί εγκληματίες είχαν «εισβάλει» στους λογαριασμούς τους σε κοινωνικά δίκτυα, ενώ το αντίστοιχο ποσοστό ανάμεσα σε κατόχους υπολογιστών- ταμπλετών με λειτουργικό Android ανήλθε στο 13%.

Επιπρόσθετα, ο αριθμός των θυμάτων ποικίλλει όχι μόνο ανάλογα με τη συσκευή που χρησιμοποιείται, αλλά και βάσει του τόπου κατοικίας των νέων. Για παράδειγμα, 16% των νέων στην Κίνα και την περιοχή Ασίας- Ειρηνικού ανέφεραν ότι έπεσαν θύματα μη εξουσιοδοτημένης πρόσβασης σε λογαριασμούς κοινωνικών δικτύων. Το αντίστοιχο ποσοστό στη Ρωσία έφτασε το 19%, ενώ σαφώς μικρότερα ήταν τα μεγέθη στην Ιαπωνία (2%) και στη Βόρεια Αμερική (4%).

**Απλοί κανόνες προστασίας**

Για την προστασία τους απέναντι σε απάτες στα κοινωνικά δίκτυα, οι χρήστες μπορούν να ακολουθήσουν μερικούς απλούς κανόνες:

Χρήση ισχυρών κωδικών πρόσβασης και απενεργοποίηση της λειτουργίας αυτόματης συμπλήρωσης, ειδικά αν η σύνδεση στο λογαριασμό γίνεται μέσω «έξυπνων» κινητών τηλεφώνων και υπολογιστών-ταμπλετών.

Περιορισμός των πληροφοριών που κοινοποιούνται στο δίκτυο. Προτείνεται οι χρήστες να διαχωρίσουν τους «φίλους» τους σε ομάδες, ώστε να μοιράζονται κάτι πολύ προσωπικό μόνο με εκείνους που πραγματικά εμπιστεύονται.

Γενικά, οι χρήστες δεν πρέπει να «κατεβάζουν» αρχεία ή να «ακολουθούν» ηλεκτρονικούς συνδέσμους, αν δεν είναι σίγουροι ποιος τα έχει στείλει και γιατί.
Πριν από την εισαγωγή των στοιχείων σύνδεσης, οι χρήστες πρέπει να βεβαιωθούν ότι δεν έχουν επισκεφθεί μια πλαστή σελίδα που έχει ως σκοπό την υποκλοπή τους.

Συνίσταται η χρήση ασφαλών συνδέσεων δικτύου και να αποφεύγεται η εισαγωγή στοιχείων πρόσβασης όταν γίνεται χρήση ενός hotspot.

**Το άρθρο πάρθηκε απ’ τη σελίδα:**

https://www.newsbeast.gr/technology/arthro/733706/oi-kindunoi-ton-koinonikon-diktuon