14 Απριλίου 2021

«Προσέχετε τι ανεβάζετε! Το Ιντερνετ δεν είναι παιδική χαρά»

/ Επιστήμες, Τέχνες & Πολιτισμός



Ειδικός σε θέματα ψηφιακής ασφάλειας δίνει μέσα από «ΤΑ ΝΕΑ» επτά πολύ σημαντικές συμβουλές στους χρήστες των μέσων κοινωνικής δικτύωσης ώστε να θωρακίσουν, στο μέτρο που είναι δυνατό, τα προσωπικά τους δεδομένα



Μετά το πρώτο σοκ από την κυβερνοεπίθεση με διαρροή-μαμούθ προσωπικών δεδομένων 533 εκατομμυρίων χρηστών του Facebook παγκοσμίως και 617.000 χρηστών στην Ελλάδα, οι ειδικοί για την ασφάλεια στο Διαδίκτυο κρούουν τον κώδωνα του κινδύνου προτείνοντας απλούς τρόπους προφύλαξης από κακόβουλες επιθέσεις που μπορεί να μας στοιχίσουν πολύ ακριβά. Ο Κωνσταντίνος Βαβούσης από τον ελληνικό ιστότοπο για θέματα ψηφιακής ασφάλειας, secnews.gr, προτείνει τι μπορεί να κάνει ο καθένας μας για να θωρακίσει τα προσωπικά του δεδομένα. «Δεν είναι παιδική χαρά το Διαδίκτυο όπως νομίζουν κάποιοι», σημειώνει μιλώντας στα «ΝΕΑ».

Αναλυτικά τα επτά βήματα που προτείνει:

1.Προστατεύουμε τον κωδικό πρόσβασης. Δεν χρησιμοποιούμε τον ίδιο κωδικό για όλα τα κοινωνικά δίκτυα. Σε κανέναν άλλον ιστότοπο δεν χρησιμοποιούμε τον ίδιο κωδικό. Και προφανώς δεν τον μοιραζόμαστε με κανέναν.

2.Δεν αποκαλύπτουμε ποτέ στοιχεία σύνδεσης. Για παράδειγμα, μας στέλνουν ένα fishing mail που λέει: «συνδεθείτε με το email και τον κωδικό σας, μπείτε εδώ». Κανένας δεν πρέπει να μας ζητήσει στοιχεία πρόσβασης και εμείς δεν πρέπει να τα δίνουμε. Οταν θέλουμε να συνδεθούμε σε κάποιο μέσο κοινωνικής δικτύωσης θα πρέπει μόνοι μας να πληκτρολογούμε τη διεύθυνση, ειδικά αν έχουμε οποιαδήποτε αμφιβολία, και να πατάμε «Log in». E-mail που μας στέλνουν σε Facebook και

Twitter είναι πιθανότητα fishing (ηλεκτρονικό ψάρεμα).

3.Οταν χρησιμοποιούμε κοινό υπολογιστή, κάνουμε πάντα αποσύνδεση. Καθίσαμε στο πανεπιστήμιο, στο Ιντερνετ καφέ, στο αεροδρόμιο για να δούμε το mail μας, το Twitter μας, πάντα «Log off». Ακόμα και από υπολογιστή φίλου μας.

4.Δεν αποδεχόμαστε αιτήματα φιλίας από άτομα που δεν γνωρίζουμε. Υπάρχουν απατεώνες που χρησιμοποιούν ψεύτικους λογαριασμούς. Είχαμε περιπτώσεις που ισχυρίζονταν κάποιοι ότι είναι βετεράνοι πολέμου και απευθύνονταν σε κυρίες συγκεκριμένου ηλικιακού γκρουπ και προφίλ για να τους αποσπάσουν χρήματα. Να κρατάμε στον νου ότι ποτέ δεν ξέρουμε ποιος βρίσκεται πραγματικά στην άλλη άκρη του καλωδίου. Ας σκεφτούμε μόνο ότι κάποιος αγνώστου ταυτότητος που θα δει πού μένουμε και τι κάνουμε μπορεί να απειλήσει την ίδια μας τη ζωή.

5.Δεν κάνουμε κλικ ποτέ σε ύποπτους συνδέσμους. Παράδειγμα, κάποιος φίλος – που πιθανότατα έχει χακαριστεί και ο ίδιος – μοιράστηκε μαζί μας έναν σύνδεσμο με θέματα κυρίως επικαιρότητας ή συνδέσμους από πορνογραφικό υλικό. «Διέρρευσαν οι προσωπικές φωτογραφίες του τάδε ή της τάδε ηθοποιού». Ολα αυτά διασπείρονται μέσω των μέσων κοινωνικής δικτύωσης και μαζί τους τα κακόβουλα λογισμικά.



«Αυτό που θα πρέπει να μας τρομάξει δεν είναι τόσο η διαρροή όσο το τι μπορεί να κάνει κανείς με αυτά τα στοιχεία», λέει ο Κωνσταντίνος Βαβούσης

6.Ολα τα κοινωνικά δίκτυα έχουν επιπλέον ρυθμίσεις ασφαλείας. Καλό είναι να τις ενεργοποιούμε. Ενεργοποίηση, ταυτοποίηση δύο παραγόντων, το γνωστό ως «two factor authentication». Ειδικά με το Instagram γίνεται χαμός γιατί οι περισσότεροι επειδή είναι καινούριο μέσο πιστεύουν ότι οι χάκερ δεν ενδιαφέρονται. Παρ' όλ' αυτά, πολλοί διάσημοι την έχουν πατήσει. Ενεργοποιήστε το two factor authentication. Ενας επιπλέον κωδικός είναι πέραν του κωδικού που έχουμε βάλει και έρχεται ένα μήνυμα επιβεβαίωσης από την ειδική υπηρεσία των social network στο κινητό που μας βοηθά να κρατάμε τον λογαριασμό μας ασφαλή. Είναι η βέλτιστη μέθοδος ασφάλειας.

7.Οι χρήστες συνήθως πελαγώνουν με τους κωδικούς γιατί νομίζουν ότι πρέπει να τους θυμούνται με αποτέλεσμα να τους σημειώνουν πρόχειρα σε τεφτέρια ή σε αρχεία στην επιφάνεια εργασίας. Αυτό είναι λάθος. Υπάρχουν κρυπτογραφημένες εφαρμογές που διαφυλάσσουν τους κωδικούς μας, όπως το «keep us» ή το «last pass», που είναι αποθετήρια κωδικών. Χρειαζόμαστε μόνο έναν master κωδικό που θα τον απομνημονεύσουμε και που θα είναι περίπλοκος – κεφαλαία, πεζά, αριθμούς, γράμματα, σύμβολα, πάνω από 12-14 χαρακτήρες. Μπαίνοντας σε αυτή την εφαρμογή θα έχουμε όλους τους κωδικούς μας αποθηκευμένους. Και φροντίζουμε οι κωδικοί να μη μας θυμίζουν τίποτα. Για να συνδεθούμε τους κάνουμε αντιγραφή

επικόλληση από την εφαρμογή.

Τέλος, για να διαπιστώσει κανείς αν ο λογαριασμός του είναι ένας από τους εκατομμύρια που δέχθηκαν την επίθεση μπορεί να «μπει» στο ακόλουθο link https://www.haveibeenpwned.com/ και βάζοντας το e-mail του στο ειδικό πεδίο να ενημερωθεί σχετικά. Ο Κωνσταντίνος Βαβούσης προειδοποιεί: «Αυτό που θα πρέπει να μας τρομάξει δεν είναι τόσο η διαρροή όσο το τι μπορεί να κάνει κανείς με αυτά τα στοιχεία. Οταν κάποιος ξέρει ότι αυτά είναι τα στοιχεία μας μπορεί να ενορχηστρώσει μια επόμενη στοχευμένη επίθεση. Αρα, η διαρροή μάς προβληματίζει για τον όγκο της και σε δεύτερο επίπεδο για το γεγονός ότι τα στοιχεία που διέρρευσαν τα ανήρτησαν οι χρήστες οικειοθελώς. Μεγάλη προσοχή στο τι ανεβάζουμε. Στο κυβερνοχώρο δεν είναι όλοι φίλοι μας».

Πηγή: tanea.gr