Συμβουλές Ιδιωτικότητας για τα Μέσα Κοινωνικής Δικτύωσης

Χρηστάκης Νόνης, φοιτητής και μέλος του **CYberSafety Youth Panel Κύπρου**

Ενημερωθείτε σχετικά με τις ρυθμίσεις απορρήτου

Το πρώτο βήμα, που αρκετοί αγνοούμε, πριν ανοίξουμε έναν λογαριασμό σε τέτοιου είδους ιστοτόπους, είναι να ενημερωθούμε, αναφορικά με τις πολιτικές απορρήτου που ακολουθούν. Το ξέρουμε και συμφωνούμε ότι, το να διαβάσει κάποιος το μακροσκελές κείμενο, που αναφέρεται στους όρους χρήσης, είναι εξαιρετικά ανιαρό, όμως είναι ένα «αναγκαίο κακό» και θα πρέπει να γίνεται. Σε αυτό το κείμενο, περιλαμβάνονται σημαντικές πληροφορίες, όσον αφορά στους πιθανούς κινδύνους, αλλά και πληροφορίες για το πώς ο χρήστης θα αξιοποιήσει στο έπακρο τις ρυθμίσεις ιδιωτικότητας του εκάστοτε μέσου.

Προσοχή στους ύποπτους συνδέσμους

Σχεδόν όλοι μας, έχουμε λάβει στο inbox μας μηνύματα με ερωτήσεις του τύπου: «Είστε εσείς σε αυτό το βίντεο;», συνοδευόμενα και από κάποιο σύνδεσμο. Να ξέρετε ότι πρόκειται για κάποιο spam ή ιό και δεν πρέπει να κάνετε κλικ στον σύνδεσμο. Αν κάνατε κλικ σε έναν τέτοιο σύνδεσμο, φροντίστε να αλλάξετε τον κωδικό πρόσβασής σας, να προειδοποιήσετε τους/τις φίλους/ες σας ότι πρόκειται για κάποιας μορφής απάτη και επικοινωνήστε με την εξυπηρέτηση του εκάστοτε ιστοτόπου, ώστε να λάβετε την απαραίτητη καθοδήγηση και να καταγγείλετε το γεγονός.

Φροντίστε ο κωδικός ασφαλείας σας να είναι ισχυρός

Αν και ένα απλός κωδικός ασφαλείας (password) είναι σχετικά εύκολο να απομνημονευτεί από εμάς (για παράδειγμα ο αριθμός τηλεφώνου μας), είναι εξίσου εύκολο και για κάποιον να το «μαντέψει». Όταν ορίζουμε τον κωδικό πρόσβασης για τον λογαριασμό μας, θα πρέπει να αποφεύγουμε τις απλές λέξεις ή μία σειρά από αριθμούς, αφού, σε μια τέτοια περίπτωση, κάποιος θα είχε τη δυνατότητα να τον αποκρυπτογραφήσει, μέσα σε ένα πολύ μικρό χρονικό διάστημα. Ένας ισχυρός κωδικός ασφαλείας αποτελείται από μία μίξη από χαρακτήρες (τόσο κεφαλαίους όσο και μικρούς), αριθμούς και σύμβολα.

Αναθεωρήστε τον κωδικό σας

Όσο σημαντική είναι η θέσπιση ενός ισχυρού κωδικού πρόσβασης, άλλο τόσο είναι και η αναθεώρησή του. Ιδανικά, αλλάζετε τον κωδικό σας κάθε μήνα. Επίσης, είναι σημαντικό να αποφεύγετε την επαναχρησιμοποίηση κωδικών που έχετε χρησιμοποιήσει κατά το παρελθόν.

Αποφύγετε τη χρήση ενός ενιαίου κωδικού για όλους τους λογαριασμούς σας

Σε καμία περίπτωση μην κάνετε χρήση του ίδιου κωδικού σε όλους τους λογαριασμούς σας. Αυτό είναι σημαντικό, γιατί, σε περίπτωση που πέσετε θύμα επίθεσης σε έναν από τους λογαριασμούς σας, κατά πάσα πιθανότητα θα επηρεάσει και όλους τους υπόλοιπους.

Αποφύγετε συνδέσμους με παραπλανητικούς τίτλους

Πολλές φορές, θα έχετε συναντήσει δημοσιεύσεις τίτλων, όπως για παράδειγμα: «Δείτε τι θα γίνει στο επόμενο επεισόδιο της σειράς Χ» ή «Έσκασε νέα μεταγραφή. Δείτε ποιος παίκτης έρχεται». Αν και τις περισσότερες φορές πρόκειται για clickbait, υπάρχουν περιπτώσεις που οδηγούν σε άλλες σελίδες που περιέχουν κακόβουλο λογισμικό. Οπότε, σκεφτείτε το καλά πριν πατήσετε, για να ακολουθήσετε τον σύνδεσμο.

Χρησιμοποιήστε όλες τις δυνατότητες ταυτοποίησης

Ορισμένα μέσα κοινωνικής δικτύωσης περιλαμβάνουν παραπάνω από ένα στάδια ταυτοποίησης των χρηστών τους. Αυτό συνήθως περιλαμβάνει την εισαγωγή κάποιου κωδικού που ο χρήστης λαμβάνει με SMS. Αυτό το βήμα όχι μόνο αποτελεί ένα επιπλέον μέτρο ασφάλειας, αλλά, σε πολλές περιπτώσεις, προειδοποιεί και τον χρήστη, όταν κάποιος προσπαθεί να αποκτήσει πρόσβαση στον λογαριασμό του.

Δώστε ιδιαίτερη έμφαση, όταν δημοσιεύετε κάποιο περιεχόμενο

Μεγάλη προσοχή θα πρέπει να αφιερώνετε και κατά τη διαδικασία της κοινοποίησης περιεχομένου. Κάποιοι ιστότοποι προτρέπουν τους χρήστες να κάνουν εμφανή τα posts τους σε όλους τους υπόλοιπους. Οπότε, πριν αρχίσετε να κοινοποιείτε τις φωτογραφίες ή την τοποθεσία σας, επιλέγετε, ανάλογα, το σύνολο των χρηστών, που θα μπορούν να βλέπουν τη δημοσίευση (π.χ., μόνο οι φίλοι σας, μόνο εσείς).