Συμβουλές για την ασφάλεια

των “smartphones**” τηλεφώνων**

Τα smartphones έχουν γίνει πλέον αναπόσπαστο κομμάτι της καθημερινότητάς μας σε τέτοιο βαθμό που οδήγησε στο να αποθηκεύουμε εκεί τεράστιο όγκο πληροφοριών προσωπικού επιπέδου. Για αυτό το λόγο υπάρχει μεγάλη ανάγκη να προστατέψουμε όσο το δυνατόν περισσότερο τα κινητά μας ώστε να μη μπορεί ο οποιοσδήποτε να έχει πρόσβαση σε αυτά γιατί μπορούν να χρησιμοποιηθούν εναντίον μας. Οι παρακάτω συμβουλές μπορούν να βοηθήσουν.

1. **Χρησιμοποιήστε κλείδωμα οθόνης**

Εάν το τηλέφωνό σας κλαπεί ή χαθεί οποιαδήποτε αποτυπώματα δακτύλων μπορεί μερικές φορές να φανούν και να υπάρξει πρόσβαση στην οθόνη. Βάλτε έναν δύσκολο κωδικό, αλλά εύκολο να τον θυμάστε.

2. **Χρησιμοποιήστε κλείδωμα κάρτας SIM**

Το κλείδωμα οθόνης είναι χρήσιμο, αλλά δεν θα εμποδίσει κάποιον να αφαιρέσει την κάρτα SIM από το τηλέφωνό σας και να την χρησιμοποιήσει σε άλλο τηλέφωνο. Για να αποφύγετε κάτι τέτοιο, ρυθμίστε το κλείδωμα της κάρτας SIM με τη μορφή ενός αριθμού PIN.

3. **Προστατεύστε τα ευαίσθητα δεδομένα**

Ενώ τα κλειδώματα εισόδου PIN και κωδικού πρόσβασης είναι χρήσιμα, ένα smartphone είναι στην πραγματικότητα ένας μικρός υπολογιστής με συχνά αφαιρούμενο χώρο αποθήκευσης. Είναι πολύ εύκολο να ανακτήσετε δεδομένα απλά συνδέοντάς τα σε έναν υπολογιστή ή αφαιρώντας τη κάρτα microSD.

4. **Ασύρματη προστασία**

Κάθε συσκευή που μπορεί να αποστέλλει δεδομένα σε ολόκληρη την κλίμακα είναι ανασφαλής. Πάντα να απενεργοποιείτε την ασύρματη σύνδεση όταν δεν χρησιμοποιείται. Εξασφαλίζει ότι οι χρήστες δεν μπορούν να συνδεθούν με τη συσκευή εν αγνοία σας.

5. **Προστατεύστε τη χρήση Bluetooth**

Βεβαιωθείτε ότι το Bluetooth είναι απενεργοποιημένο όταν δεν χρησιμοποιείται. Ρυθμίστε τη ρύθμιση παραμέτρων bluetooth σε 'μη ανιχνεύσιμο', έτσι ώστε οι χρήστες που αναζητούν συσκευές που βρίσκονται σε κοντινή απόσταση να μην μπορούν να δουν τη δική σας.

6. **Ασφάλεια λήψης εφαρμογών**

Μπορεί να μην διαβάζετε τους όρους όταν ανοίγετε μια εφαρμογή, αλλά να είστε προσεκτικοί σε οποιαδήποτε απαίτηση πρόσβασης σε διάφορες λειτουργίες του τηλεφώνου σας, ειδικά αν η εφαρμογή δεν είναι γνωστή.

7. **Περιήγηση στο διαδίκτυο**

Προσέξτε όταν έχετε πρόσβαση σε ένα πρόγραμμα περιήγησης ιστού στο smartphone σας, καθώς μπορεί να είναι εύκολο να δεχτείτε μηνύματα που «πετάγονται». Για παράδειγμα, συμφωνώντας να αποθηκεύσετε τα στοιχεία των χρηστών και τους κωδικούς πρόσβασης μπορεί να είναι εύκολο να το θυμηθείτε αργότερα, αλλά δυστυχώς άλλοι μπορούν να κάνουν το ίδιο εάν αποκτήσουν πρόσβαση στο τηλέφωνό σας.

8. **Απενεργοποιήστε την γεωγραφική ετικέτα**

Πολλές εφαρμογές κοινωνικής δικτύωσης smartphone μεταφέρουν αυτόματα φωτογραφίες στο διαδίκτυο. Το πρόβλημα με αυτό είναι ότι πολλά τηλέφωνα ενσωματώνουν ετικέτες τοποθεσίας, που ονομάζονται επίσης "geotags", απευθείας στα αρχεία φωτογραφιών τους.

9. **Εγκαταστήστε λογισμικό προστασίας από ιούς**

Οι δυνατότητες των smartphones πλησιάζουν τις δυνατότητες ενός υπολογιστή, αλλά οι περισσότεροι άνθρωποι δεν έχουν καμία μορφή προστασίας, αν και μπορούν να αντιμετωπίσουν παρόμοιες απειλές.

10. **Απομακρυσμένο καθάρισμα**

Αν συμβεί το χειρότερο και το τηλέφωνο σας χαθεί ή κλαπεί, ίσως θελήσετε να προστατέψετε τα δεδομένα σας διαγράφοντας γρήγορα και απομακρυσμένα τα δεδομένα σας.

Δυστυχώς αυτές οι απλές συμβουλές δεν είναι αρκετές στην προστασία του κινητού σας τηλεφώνου από επίδοξους hackers.

Τα τελευταία χρόνια οι εταιρίες που κατασκευάζουν τα “έξυπνα” κινητά έχουν ενσωματώσει τη λεγόμενη τεχνολογία sandbox ώστε να δημιουργήσει στο κινητό τηλέφωνο ένα απομονωμένο, ασφαλές περιβάλλον που μιμείται ένα ολόκληρο υπολογιστικό σύστημα για την εκτέλεση ύποπτων προγραμμάτων, την παρακολούθηση της συμπεριφοράς τους και την κατανόηση του σκοπού τους, δίχως να εκτίθεται σε κίνδυνο το δίκτυο του οργανισμού.

Ωστόσο, υπήρξαν και κακόβουλα λογισμικά τύπου botnet κατά το παρελθόν τα οποία δεν τους σταμάτησε, έτσι οι κατασκευαστές αποφάσισαν να πάνε ακόμα ένα βήμα μπροστά, απομονώνοντας και το hardware των συσκευών.

Μια τεχνική, που ακούει στο όνομα έμπιστο περιβάλλον εκτέλεσης (συντ. στα Αγγλικά «TEE»), είναι πλέον διαδεδομένη σχεδόν σε όλα τα σύγχρονα smartphones.

Ένα έμπιστο περιβάλλον εκτέλεσης (TEE – Trusted Execution Environment) είναι ένα θεωρητικά απαραβίαστο ασφαλές περιβάλλον, υποβοηθούμενο από υλικό, όπου μπορεί να εκτελείται κώδικας απομονωμένος από το υπόλοιπο σύστημα.

Τα περισσότερα Android προσφέρουν την τεχνολογία TrustZone της ARM, η οποία αποτελείται από δύο εικονικούς επεξεργαστές, έναν "ασφαλή" και έναν "μη ασφαλή". Τα iPhone και τα Mac με αναγνωριστικό αφής ή αναγνωριστικό προσώπου χρησιμοποιούν ξεχωριστό επεξεργαστή (Secure Enclave) για να χειριστούν τα βιομετρικά στοιχεία του κάθε χρήστη. Και στις δύο περιπτώσεις, το TEE χρησιμοποιείται στον επεξεργαστή εφαρμογών ή σε ένα τσιπ που τρέχει μη ασφαλές λογισμικό. Και εδώ ωστόσο έχουν γίνει αναφορές για υποκλοπή δεδομένων, λόγω διάφορων σφαλμάτων λογισμικού.

Έτσι περνάμε στο επόμενο βήμα που θα είναι η εξωτερική επεξεργασία δεδομένων, κατά την οποία χρήστες, οργανισμοί και άλλοι φορείς, θα απομονώνουν πολύτιμες πληροφορίες εξωτερικά. Φανταστείτε ένα φορητό υπολογιστή με επεξεργαστή σε μέγεθος ενός smartwatch, ο οποίος θα λειτουργεί ανεξάρτητα από το smartphone και δεν θα εκτελεί κώδικα τρίτου μέρους. Αυτή η συσκευή θα επιτρέπει στο χρήστη να επικοινωνεί με ασφάλεια, καθώς δεν θα έχει σημεία εισόδου για επίθεση.

Αναμένεται ότι μέσω αυτής της μεθόδου μεγάλες εταιρίες αλλά και κρατικές υπηρεσίες να προστατεύσουν τα δεδομένα τους στο μέλλον χρησιμοποιώντας αυτήν την τεχνολογία.