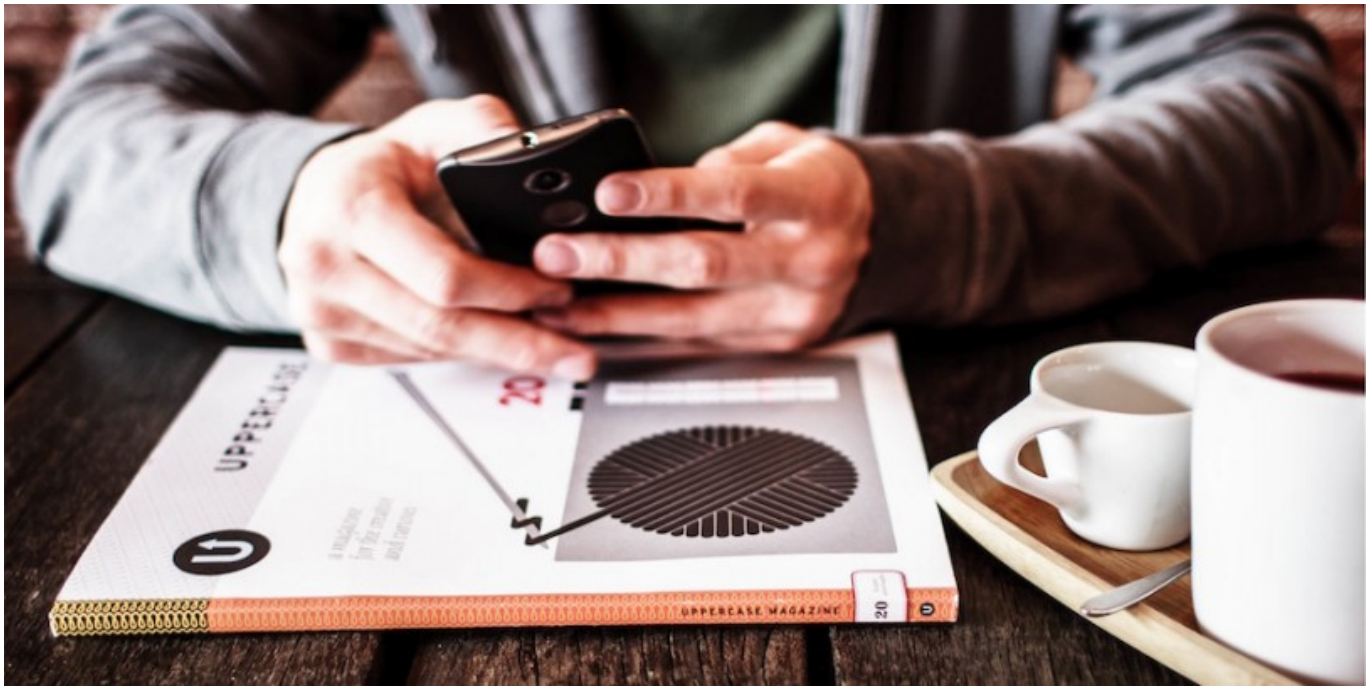
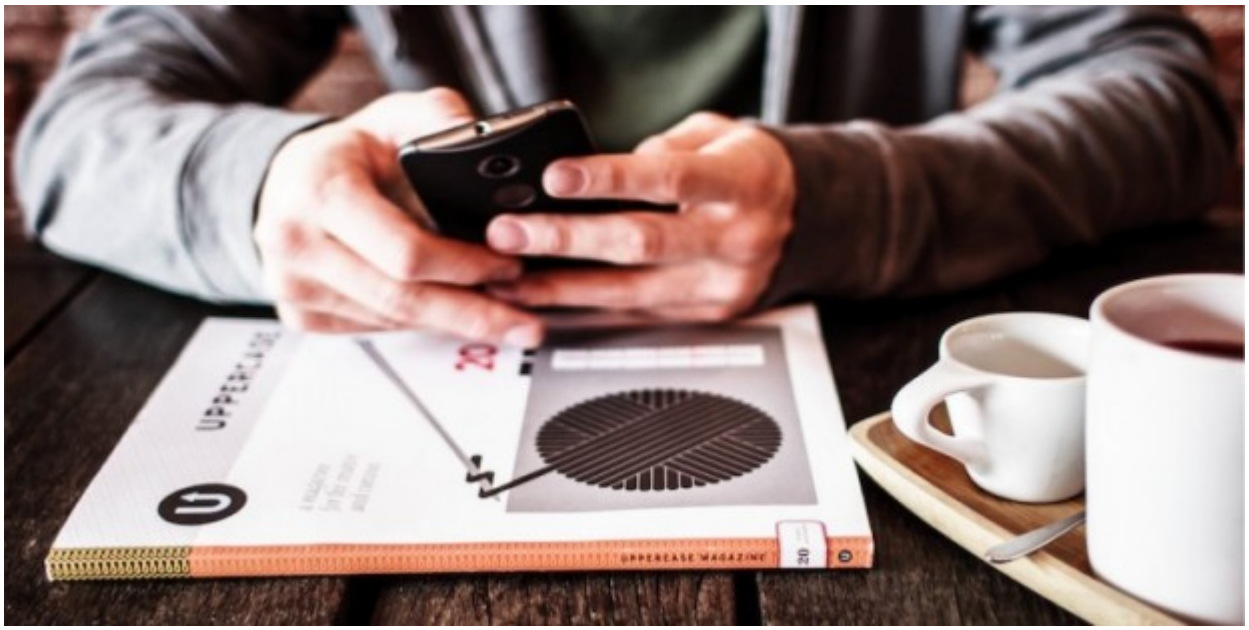
28 Μαρτίου 2016

Προσοχή! Έτσι θα καταλάβετε αν παρακολουθούν το κινητό σας

/ Επιστήμες, Τέχνες & Πολιτισμός





Φωτο:banknxt.com

Οι ειδικοί στην ασφάλεια των επικοινωνιών λένε πώς αν θέλετε να είστε 100% σίγουροι ότι δεν παρακολουθούνται αυτά που λέτε ή γράφετε στο κινητό σας δεν έχετε παρά να το κλείσετε.

Διαβάστε μερικά απλά βήματα για να αποφύγετε την παρακολούθηση.

Σε περίπτωση που δεν μπορείτε να το αποφύγετε στην αρχή, πως αφαιρείτε τον κοριό

Με επαναφορά των εργοστασιακών ρυθμίσεων

Είναι ίσως η πιο αποτελεσματική μέθοδος για να σβήσετε το κατασκοπευτικό λογισμικό που ενδέχεται να έχει εγκατασταθεί στο κινητό σας. Μπορείτε να το κάνετε μόνοι σας ή, εναλλακτικά, να επισκεφθείτε ένα κατάστημα κινητής τηλεφωνίας και να ζητήσετε να γίνει επαναφορά εργοστασιακών ρυθμίσεων (factory reset) στη συσκευή σας. Η λειτουργία είναι διαθέσιμη σε όλα τα τηλέφωνα (Android, iPhone, BlackBerry κ.λπ.). Η διαδικασία αυτή θα επαναφέρει το τηλέφωνό σας στην κατάσταση που ήταν όταν το αγοράσατε. Μην ξεχάσετε να δημιουργήσετε προηγουμένως αντίγραφα ασφαλείας (backup), αν δεν θέλετε να χάσετε αρχεία.

Με ενημέρωση του λειτουργικού συστήματος

Η αναβάθμιση ή εγκατάσταση από την αρχή του λειτουργικού συστήματος (software) του τηλεφώνου σας θα επιφέρει ανάλογο αποτέλεσμα με αυτό της επαναφοράς εργοστασιακών ρυθμίσεων. Το καλό είναι ότι με αυτή τη μέθοδο δεν θα σβηστούν οι εφαρμογές και τα δεδομένα σας, αλλά θα είστε σίγουροι ότι το κατασκοπευτικό λογισμικό θα αφαιρεθεί. Και αυτό διότι οι εφαρμογές παρακολούθησης εγκαθίστανται στο λειτουργικό σύστημα της συσκευής.

Πώς εντοπίζετε την εισβολή

1. Απενεργοποιήστε τη συσκευή
2. Παρατηρήστε αν υπάρχει ασυνήθιστη «συμπεριφορά» (π.χ. η οθόνη ενεργοποιείται μόνη της ή φωτίζονται τα πλήκτρα)
3. Ελέγξτε αν η μπαταρία είναι ζεστή. Αυτό μπορεί να σημαίνει ότι το τηλέφωνο δεν είναι στην πραγματικότητα κλειστό αλλά τρέχει κρυφά κάποιο πρόγραμμα
4. Ενεργοποιήστε ξανά το τηλέφωνο
5. Παρατηρήστε αν ακούγονται ασυνήθιστοι ήχοι όταν πραγματοποιείτε μια κλήση

Προστατέψτε τα δεδομένα σας

1. Να έχετε τη συσκευή πάντοτε μαζί σας και να μην επιτρέπετε σε κανέναν να τη χρησιμοποιήσει. Οποιοσδήποτε έρθει σε επαφή με το κινητό σας, έστω για λίγα δευτερόλεπτα, μπορεί να εγκαταστήσει πρόγραμμα παρακολούθησης (spyware)

2. Ορίστε κωδικό πρόσβασης (password) στο τηλέφωνό σας για να το ασφαλίσετε από μη εξουσιοδοτημένη χρήση
3. Μην επιτρέπετε πρόσβαση σε άγνωστες συνδέσεις Bluetooth
4. Μην κατεβάζετε αρχεία από το Διαδίκτυο στο τηλέφωνό σας
5. Απενεργοποιήστε ή περιορίστε την πρόσβαση στο Ιντερνετ από το κινητό σας

Στοπ στις υποκλοπές

1. Αφαιρέστε την μπαταρία του κινητού όταν δεν είναι σε χρήση
2. Χρησιμοποιήστε ένα καρτοκινητό για προστασία σε εξαιρετικά ευαίσθητες συνομιλίες
3. Εάν παρατηρήσετε ασυνήθιστη συμπεριφορά στο τηλέφωνο, ενημερώστε τον τηλεπικοινωνιακό πάροχό σας
4. Απενεργοποιήστε τη λειτουργία ασύρματου Ίντερνετ (WiFi) στο κινητό σας. Σερφάρετε μόνο από σημεία που γνωρίζετε ότι είναι ασφαλή, όπως το σπίτι ή το γραφείο
5. Να θυμάστε ότι το λογισμικό spyware σπανίως μολύνει τα τηλέφωνα που δεν έχουν πρόσβαση στο Ίντερνετ
6. Μην αποκαλύπτετε από το τηλέφωνο απόρρητες πληροφορίες, αν υποψιάζεστε ότι το κινητό σας έχει «μολυνθεί»
7. Κάντε επαναφορά των εργοστασιακών ρυθμίσεων στο κινητό σας για να αφαιρέσετε τυχόν λογισμικό παρακολούθησης
8. Εγκαταστήστε πρόγραμμα εντοπισμού κακόβουλου λογισμικού και ιών (antivirus) στο τηλέφωνό σας
9. Απενεργοποιήστε το GPS όταν δεν το χρησιμοποιείτε. Μπορεί να χρησιμοποιηθεί από επιτήδειους για να δουν πού βρίσκεται το τηλέφωνο σας (και ο κάτοχός του)
10. Απενεργοποιήστε το Bluetooth όταν δεν το χρησιμοποιείτε. Ανοίξτε το μόνο όταν θέλετε να μεταφέρετε επαφές, αρχεία κ.λπ.

Πηγή:newsbomb.gr