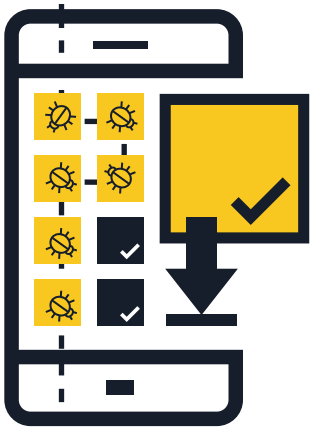
MOBILE MALWARE

ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΘΕΙΤΕ

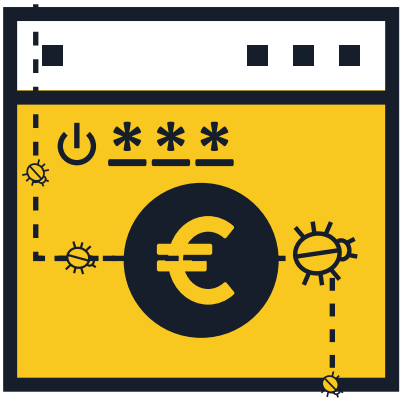


1 Εγκαταστήστε εφαρμογές μόνο από αξιόπιστες πηγές

- **Κάντε αγορές μόνο από αξιόπιστα καταστήματα εφαρμογών** — Πριν κατεβάσετε μια εφαρμογή, βρείτε πληροφορίες γι' αυτή και τους δημιουργούς της. Προσοχή στους συνδέσμους που λαμβάνετε μέσω email ή SMS, που μπορεί να σας παραπλανήσουν ώστε να εγκαταστήσετε εφαρμογές από τρίτες ή μη έμπιστες πηγές.
- **Ελέγξτε τις κριτικές και τις βαθμολογίες άλλων χρηστών,** εφόσον είναι διαθέσιμες.
- **Διαβάστε τις άδειες πρόσβασης που ζητά η εφαρμογή** — Ελέγξτε σε ποιες κατηγορίες δεδομένων θα μπορεί να έχει πρόσβαση, καθώς και αν θα μοιράζεται πληροφορίες για εσάς με εξωτερικές οντότητες. Αν πιστεύετε ότι οι όροι είναι ύποπτοι ή σας κάνουν να αισθάνεστε άβολα, μην κατεβάζετε την εφαρμογή.

2 Μην κάνετε κλικ σε συνδέσμους ή επισυναπτόμενα αρχεία που εμπεριέχονται σε μη ζητηθέντα (spam) emails ή μηνύματα SMS

- **Μην εμπιστεύεστε συνδέσμους που εμπεριέχονται σε μη ζητηθέντα (spam) emails ή γραπτά μηνύματα (SMS και MMS)** — Διαγράψτε τα αμέσως μόλις τα λάβετε.
- **Ελέγξτε προσεκτικά τυχόν συντετμημένα URLs και QR codes** — θα μπορούσαν να οδηγήσουν σε ιστοτόπους με βλαβερό περιεχόμενο ή σε απευθείας εγκατάσταση κακόβουλου λογισμικού στη συσκευή σας. Προτού κάνετε κλικ, χρησιμοποιήστε έναν ιστότοπο προεπισκόπησης του URL για να βεβαιωθείτε ότι η διεύθυνση ιστού είναι ορθή. Προτού σαρώσετε ένα QR code, επιλέξτε έναν αναγνώστη QR που δημιουργεί προεπισκόπηση του ενσωματωμένου ιστοτόπου και χρησιμοποιήστε λογισμικό προστασίας για φορητές συσκευές που σας προειδοποιεί για επικίνδυνους συνδέσμους.



3 Πραγματοποιήστε έξοδο από ιστοτόπους μετά την ολοκλήρωση μιας πληρωμής

- **Ποτέ μην αποθηκεύετε ονόματα χρηστών και κωδικούς πρόσβασης στον περιηγητή ή στις εφαρμογές της φορητής σας συσκευής** — Αν το τηλέφωνό σας ή το tablet χαθεί ή κλαπεί, οποιοσδήποτε θα μπορούσε να εισέλθει στους λογαριασμούς σας. Μετά την ολοκλήρωση της συναλλαγή σας, κάντε log out από το λογαριασμό σας αντί να κλείσετε απλά τον περιηγητή.
- **Αποφύγετε την είσοδο στους online τραπεζικούς σας λογαριασμούς και τις διαδικτυακές αγορές μέσω δημόσιων Wi-Fi δικτύων** — Χρησιμοποιήστε τις mobile banking εφαρμογές σας και πραγματοποιήστε συναλλαγές μόνο μέσα από δίκτυα που γνωρίζετε και εμπιστεύεστε.
- **Δώστε μεγάλη προσοχή στο URL του ιστοτόπου** — Βεβαιωθείτε ότι η διεύθυνση URL του ιστοτόπου είναι η σωστή, πριν κάνετε log in ή αποστείλετε ευαίσθητα δεδομένα σε αυτόν. Θα ήταν προτιμότερο να εγκαταστήσετε στη συσκευή σας την επίσημη εφαρμογή της τράπεζάς σας για να είστε σίγουροι ότι συνδέεστε πάντα στον σωστό ιστότοπο.

4 Ενημερώνετε τακτικά το λειτουργικό σύστημα και τις εφαρμογές

- **Αμέσως όταν λαμβάνετε ειδοποίηση ότι αυτές είναι διαθέσιμες, εγκαταστήστε τις ενημερώσεις του λειτουργικού συστήματος της φορητής συσκευής σας** — Έχοντας εγκατεστημένες τις πιο πρόσφατες ενημερώσεις, διασφαλίζετε όχι μόνο την ασφάλεια της συσκευής σας, αλλά και τη βέλτιστη και αποδοτικότερη λειτουργία της.

5 Απενεργοποιήστε το Wi-Fi, τις υπηρεσίες τοποθεσίας και το Bluetooth όταν δεν τα χρησιμοποιείτε

- **Απενεργοποιήστε το Wi-Fi όταν δεν το χρησιμοποιείτε** — Οι κυβερνοεγκληματίες θα μπορούσαν να προσπελάσουν τα δεδομένα σας όταν η σύνδεση που χρησιμοποιείτε δεν είναι ασφαλής. Αν είναι εφικτό, χρησιμοποιήστε 3G ή 4G σύνδεση δεδομένων αντί να συνδεθείτε σε ένα hotspot. Εξετάστε επίσης τη χρήση μιας υπηρεσίας virtual private network (VPN), ώστε τα δεδομένα σας να κρυπτογραφούνται κατά τη μετάδοσή τους.
- **Μην επιτρέπετε στις εφαρμογές να χρησιμοποιήσουν την τοποθεσία σας, παρά μόνο αν είναι αναγκαίο** — Αυτού του είδους η πληροφορία μπορεί να διαμοιραστεί ή να διαρρεύσει και τελικά να χρησιμοποιηθεί για την προβολή διαφημίσεων με βάση την τοποθεσία σας.
- **Απενεργοποιήστε το Bluetooth όταν δεν το χρειάζεστε** — Βεβαιωθείτε ότι είναι απενεργοποιημένο και όχι απλά αόρατο. Συνήθως, με βάση τις εργοστασιακές ρυθμίσεις της συσκευής σας, οποιοσδήποτε μπορεί να συνδεθεί σε αυτή χωρίς να το γνωρίζετε. Κακόβουλοι χρήστες θα μπορούσαν να αντιγράψουν τα αρχεία σας, να προσπελάσουν άλλες συνδεδεμένες συσκευές ή ακόμα και να αποκτήσουν απομακρυσμένη πρόσβαση στη συσκευή σας για να πραγματοποιήσουν κλήσεις και να στείλουν μηνύματα, κάτι που θα οδηγούσε σε αυξημένες χρεώσεις στο λογαριασμό του κινητού σας τηλεφώνου.

6 Μην αποκαλύπτετε προσωπικές πληροφορίες

- **Μην απαντάτε στέλνοντας προσωπικές πληροφορίες** σε μηνύματα SMS ή emails που ισχυρίζονται πως είναι από την τράπεζά σας ή κάποιο άλλο οργανισμό. Αντί αυτού, επικοινωνήστε απευθείας με το φορέα, για να επιβεβαιώσετε το αίτημά τους.
- **Ελέγχετε τακτικά τους λογαριασμούς κινητής τηλεφωνίας για τυχόν υπερβολικές χρεώσεις** — αν εντοπίσετε κινήσεις που δεν έχουν γίνει από εσάς, επικοινωνήστε αμέσως με τον πάροχο των υπηρεσιών.

7 Jailbreak: ξανασκεφτείτε το!

- Με τον όρο jailbreak αναφερόμαστε στη διαδικασία αφαίρεσης των περιορισμών ασφαλείας που έχουν ορισθεί από τον πωλητή του λειτουργικού συστήματος, ώστε να μπορεί κάποιος να έχει πλήρη πρόσβαση στο λειτουργικό σύστημα και στα χαρακτηριστικά του — **Το jailbreak της συσκευής εξασθενεί την ασφάλειά της,** δημιουργώντας κενά ασφάλειας που ενδεχομένως δεν είναι άμεσα εμφανή.

8 Δημιουργήστε αντίγραφα ασφαλείας των δεδομένων σας

- **Πολλά smartphones και tablets έχουν τη δυνατότητα ασύρματης δημιουργίας αντιγράφων ασφαλείας των δεδομένων** — Ελέγξτε τις διαθέσιμες επιλογές, με βάση το λειτουργικό σας σύστημα. Με τη δημιουργία αντιγράφων ασφαλείας των δεδομένων του smartphone ή του tablet σας, μπορείτε εύκολα να ανακτήσετε προσωπικά δεδομένα αν η συσκευή χαθεί, κλαπεί ή καταστραφεί.

9 Εγκαταστήστε λογισμικό ασφάλειας για φορητές συσκευές

- Όλα τα λειτουργικά συστήματα κινδυνεύουν να μολυνθούν. Αν υπάρχει διαθέσιμο, **χρησιμοποιήστε λογισμικό ασφάλειας για φορητές συσκευές,** το οποίο ανιχνεύει και σας προστατεύει από malware, spyware και κακόβουλες εφαρμογές, αλλά και αντικλεπτικές λύσεις και λύσεις προστασίας της ιδιωτικότητας.

EUROPOL EC3 European Cybercrime Centre
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#MobileMalware