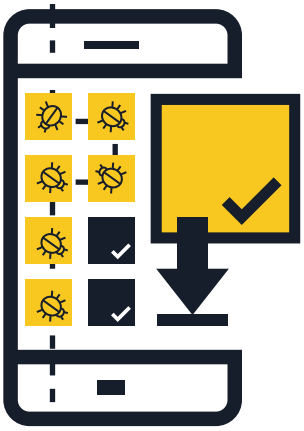
Κακόβουλο λογισμικό στα κινητά

Μικρές συμβουλές ασφάλειας για το κινητό και το tablet σου



1 Να κατεβάζεις εφαρμογές μόνο από αξιόπιστες πηγές

- **Να αγοράζεις μόνο από αξιόπιστα app stores**

Πριν κατεβάσεις μια εφαρμογή, κάνε μια μικρή έρευνα για αυτήν αλλά και τον εκδότη της. Να είσαι επιφυλακτικός με συνδέσμους (links) που λαμβάνεις στο email σου ή μέσω μηνυμάτων στο κινητό σου τα οποία σε παροτρύνουν να κατεβάσεις εφαρμογές από άγνωστες και πιθανώς μη αξιόπιστες πηγές.

- **Έλεγξε τα σχόλια και τις βαθμολογίες άλλων χρηστών** αν υπάρχει η δυνατότητα.
- **Διάβασε τις άδειες που ζητάει η εφαρμογή**

Έλεγξε σε ποια δεδομένα έχει πρόσβαση η εφαρμογή και αν μοιράζεται τα δεδομένα σου με τρίτους. Εάν δεν είσαι σίγουρος και δεν συμφωνείς με τους όρους χρήσης της εφαρμογής, μην την κατεβάσεις.

2 Μην μεταβαίνεις σε συνδέσμους και μην ανοίγεις συνημμένα αρχεία από spam email ή μηνύματα στο κινητό σου

- **Μην εμπιστεύεσαι συνδέσμους από ανεπιθύμητα emails ή μηνύματα** (SMS and MMS) — Διάγραψέ τα μόλις τα λάβεις.
- **Να ελέγχεις τις συντομευμένες διευθύνσεις URL και τα QR codes**

Υπάρχει περίπτωση να οδηγούν σε επικίνδυνα sites ή στην λήψη κακόβουλου λογισμικού στη συσκευή σου. Μπορείς να χρησιμοποιήσεις ένα εργαλείο προεπισκόπησης URL για να επιβεβαιώσεις αν μία ιστοσελίδα είναι έγκυρη. Πριν διαβάσεις ένα QR code, επέλεξε έναν QR reader ο οποίος περιλαμβάνει προεπισκόπηση του site στο οποίο οδηγεί το QR code καθώς και λογισμικό ασφάλειας για κινητές συσκευές που σε προειδοποιεί σε περίπτωση επικίνδυνου συνδέσμου.

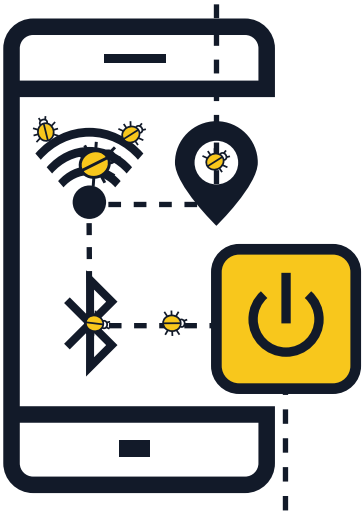
3 Να κάνεις αποσύνδεση από τα sites μετά από online πληρωμές

- **Ποτέ να μην αποθηκεύεις στον browser του κινητού σου usernames ή passwords** – Αν το κινητό σου χαθεί ή κλαπεί, θα μπορεί ο οποιοσδήποτε να μπει στους λογαριασμούς σου. Μόλις ολοκληρώσεις τις συναλλαγές σου από κάποιο ηλεκτρονικό κατάστημα, κάνε αμέσως αποσύνδεση και μην κλείνεις απλώς τον browser.
- **Μη μπαίνεις σε τραπεζικούς λογαριασμούς και μην κάνεις ηλεκτρονικές αγορές όταν είσαι συνδεδεμένος σε δημόσια free Wi-Fi** Τέτοιου είδους συναλλαγές θα πρέπει να γίνονται μόνο από ασφαλή δίκτυα.
- **Έλεγξε το URL του site** – Πριν βάλεις σε κάποιο site τους κωδικούς σου ή δώσεις ευαίσθητες πληροφορίες, έλεγξε ότι η διεύθυνση URL που εμφανίζεται στον browser σου είναι όντως η σωστή. Μπορείς να κατεβάσεις την επίσημη εφαρμογή της τράπεζάς σου για να είσαι σίγουρος ότι συνδέεσαι πάντα στο πραγματικό site.

4 Να κάνεις αναβάθμιση λογισμικού του λειτουργικού συστήματος των εφαρμογών σου

- **Όταν σου ζητάει το κινητό σου αναβάθμιση του λειτουργικού συστήματος θα πρέπει να το κάνεις** — Έχοντας τις πιο πρόσφατες εκδόσεις εξασφαλίζεις μεγαλύτερη ασφάλεια και ταχύτητα για την συσκευή σου.

5 Να κλείνεις το Wi-Fi, τον εντοπισμό θέσης και το Bluetooth της συσκευής σου όταν δεν τα χρησιμοποιείς



- **Να κλείνεις το Wi-Fi από το κινητό σου όταν δεν το χρησιμοποιείς**

Επιτήδειοι μπορούν να αποκτήσουν πρόσβαση στην συσκευή σου αν το δίκτυο που είσαι συνδεδεμένος δεν είναι ασφαλές. Χρησιμοποίησε 3G ή 4G σύνδεση αντί για hotspot. Μπορείς επίσης να χρησιμοποιήσεις Virtual Private Network (VPN) για κρυπτογραφημένη μετάδοση των δεδομένων.

- **Μην επιτρέπεις στις εφαρμογές να έχουν πρόσβαση στην τοποθεσίας σου, εκτός αν όντως υπάρχει τέτοια ανάγκη** - Αυτή η πληροφορία μπορεί να χρησιμοποιηθεί από τρίτους για στοχευμένη διαφήμιση ή άλλους σκοπούς.
- **Να κλείνεις το Bluetooth της συσκευής σου όταν δεν το χρησιμοποιείς**

Βεβαιώσου ότι είναι απενεργοποιημένο και όχι απλώς σε invisible mode. Συνήθως οι προεπιλεγμένες ρυθμίσεις του Bluetooth είναι τέτοιες ώστε να επιτρέπεται να συνδεθούν άλλοι στην συσκευή σου χωρίς εσύ να το γνωρίζεις. Υπάρχει κίνδυνος κάποιος επιτήδειος να συνδεθεί στην συσκευή σου και να αντιγράψει τα δεδομένα σου, ή ακόμα και να πάρει τον έλεγχο της συσκευής σου εξ' αποστάσεως και να κάνει κλήσεις ή να στέλνει μηνύματα που μπορεί να οδηγήσουν σε μεγάλες χρεώσεις.

6 Προσοχή στα προσωπικά σου δεδομένα

- **Ποτέ μην στέλνεις τα προσωπικά σου δεδομένα** απαντώντας σε emails ή μηνύματα που υποτιθέμενα προέχονται από την τράπεζα σου ή κάποιον άλλο οργανισμό. Επικοινώνησε μαζί τους για να εξακριβώσεις την εγκυρότητα των ισχυρισμών τους.
- **Να ελέγχεις τακτικά τους λογαριασμούς του κινητού σου για τυχόν ύποπτες χρεώσεις** - Αν εντοπίσεις χρεώσεις που δεν έχεις κάνει ποτέ, ενημέρωσε αμέσως τον πάροχο κινητής τηλεφωνίας σου.

7 Μην ξεκλειδώνεις με παράνομους τρόπους το κινητό σου (jailbreaking)

- Το Jailbreaking είναι η κατάργηση των δικλίδων ασφαλείας του λειτουργικού συστήματος με σκοπό την απόκτηση πλήρους πρόσβασης στο λειτουργικό σύστημα και στα χαρακτηριστικά του. **Το Jailbreaking μπορεί να εξασθενίσει σημαντικά την ασφάλεια της συσκευής σου** δημιουργώντας κενά ασφαλείας τα οποία το καθιστούν πιο ευάλωτο.

8 Πάντα να κρατάς αντίγραφο ασφαλείας (back up) των δεδομένων σου

- **Πολλά κινητά και tablets κρατάνε αυτόματα αντίγραφο ασφαλείας των δεδομένων της συσκευής** - Έλεγξε τις επιλογές που σου προσφέρει το λειτουργικό σύστημα της συσκευής σου. Με την δημιουργία αντιγράφου ασφαλείας μπορείς να επαναφέρεις τα δεδομένα σου σε περίπτωση απώλειας, κλοπής, ή καταστροφής της συσκευής σου.

9 Εγκατέστησε μια εφαρμογή που προστατεύει το κινητό σου από διάφορες απειλές

- Όλα τα λειτουργικά συστήματα διατρέχουν κίνδυνο να προσβληθούν από κάποιο κακόβουλο λογισμικό. Αν υπάρχει η δυνατότητα, εγκατέστησε μια **εφαρμογή προστασίας** που να ανιχνεύει και να προλαμβάνει από τους ιούς, τα spyware (λογισμικά κατασκοπίας) και άλλες κακόβουλες εφαρμογές, και κατά συνέπεια διασφαλίζει την ιδιωτικότητα των δεδομένων και της συσκευής σου.