Ασφαλής χρήση εφαρμογών κινητών συσκευών

Οι εφαρμογές κινητών συσκευών αποτελούν αναπόσπαστο κομμάτι της καθημερινής μας ζωής — αλλά και έναν από τους πιο συχνά απειλούμενους τομείς κυβερνοεπιθέσεων. Αυτό το σεμινάριο εξοπλίζει επαγγελματίες και φοιτητές με τις γνώσεις που χρειάζονται για να επιλέγουν, να διαχειρίζονται και να χρησιμοποιούν εφαρμογές με ασφάλεια σε Android και iPhone.

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry
safeLine.gr
ΙΤΕ ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ
Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Γιατί οι εφαρμογές κινητών αποτελούν στόχο επιθέσεων

Τα smartphones μεταφέρουν ένα τεράστιο όγκο ευαίσθητων δεδομένων: τραπεζικές πληροφορίες, επαγγελματικά email, φωτογραφίες, επαφές και τοποθεσία σε πραγματικό χρόνο. Αυτό τα καθιστά εξαιρετικά ελκυστικό στόχο για εγκληματίες του κυβερνοχώρου. Σε αντίθεση με τους παραδοσιακούς υπολογιστές, τα κινητά συχνά στερούνται ισχυρής προστασίας και οι χρήστες τείνουν να είναι λιγότερο προσεκτικοί κατά την εγκατάσταση εφαρμογών.

Τόσο το Android όσο και το iOS αντιμετωπίζουν μοναδικές απειλές. Το Android, λόγω της ανοιχτής αρχιτεκτονικής του, επιτρέπει την εγκατάσταση εφαρμογών από τρίτες πηγές (sideloading), αυξάνοντας τον κίνδυνο κακόβουλου λογισμικού. Το iOS, παρότι πιο κλειστό, δεν είναι άτρωτο — ειδικά σε συσκευές με jailbreak ή μέσω εξελιγμένων phishing επιθέσεων.

3.5M

εφαρμογές στο Google Play

Τεράστιος αριθμός εφαρμογών, πολλές χωρίς επαρκή έλεγχο ασφαλείας

1.8M

εφαρμογές στο App Store

Αυστηρότερος έλεγχος, αλλά όχι ανοσία σε κακόβουλες εφαρμογές

60%

των επιθέσεων μέσω κινητών

Ποσοστό κυβερνοεπιθέσεων που στοχεύουν πλέον κινητές συσκευές

Στόχοι του σεμιναρίου

Το παρόν σεμινάριο καλύπτει τις βασικές αρχές ασφαλούς χρήσης εφαρμογών κινητών συσκευών, με πρακτικές οδηγίες που μπορούν να εφαρμοστούν άμεσα τόσο σε προσωπικό όσο και σε εταιρικό περιβάλλον.

01

Επιλογή ασφαλών εφαρμογών

Κριτήρια αξιολόγησης πριν από κάθε εγκατάσταση

02

Κατανόηση αδειών πρόσβασης

Τι σημαίνουν τα permissions και πότε είναι ύποπτα

03

Αναγνώριση κακόβουλων εφαρμογών

Παραδείγματα fake apps και spyware στην πράξη

04

Προστασία εταιρικών δεδομένων

Εργαλεία και πολιτικές για ασφαλή εταιρική χρήση

05

Πρακτικό checklist

Άμεσα εφαρμόσιμες οδηγίες για κάθε χρήστη

Πώς επιλέγουμε ασφαλείς εφαρμογές

Η πρώτη γραμμή άμυνας είναι η συνειδητή επιλογή εφαρμογών. Πριν πατήσετε "Εγκατάσταση", αφιερώστε λίγα δευτερόλεπτα για να ελέγξετε μερικά βασικά κριτήρια που μπορούν να αποκαλύψουν ύποπτη ή επικίνδυνη εφαρμογή. Η γρήγορη αυτή αξιολόγηση μπορεί να σας γλιτώσει από σοβαρές συνέπειες.

✅ Από πού εγκαθιστάτε

Εγκαταστάστε εφαρμογές **αποκλειστικά** από το Google Play Store ή το Apple App Store. Αποφύγετε APK αρχεία από ιστοσελίδες τρίτων ή links μέσω email/SMS. Ποτέ μην ενεργοποιείτε την επιλογή "Άγνωστες πηγές" στο Android εκτός εάν είστε ειδικός.

🔍 Τι ελέγχουμε

- **Εκδότης:** Είναι γνωστή εταιρεία; Ελέγξτε το επίσημο site
- **Αριθμός λήψεων:** Εκατομμύρια λήψεις = μεγαλύτερη αξιοπιστία
- **Αξιολογήσεις:** Διαβάστε τις αρνητικές κριτικές προσεκτικά
- **Τελευταία ενημέρωση:** Εφαρμογές χωρίς updates για 1+ χρόνια είναι ύποπτες
- **Permissions:** Ελέγξτε τι ζητά η εφαρμογή πριν εγκατασταθεί

⚠ Μια εφαρμογή με λίγες αξιολογήσεις, άγνωστο εκδότη και παλιά ημερομηνία ενημέρωσης είναι ύποπτη — ακόμα και αν βρίσκεται στο επίσημο store.

Άδειες πρόσβασης (Permissions)

Κάθε εφαρμογή ζητά πρόσβαση σε διάφορους πόρους της συσκευής σας. Αυτές οι άδειες πρόσβασης — γνωστές ως **permissions** — είναι το κλειδί για την κατανόηση του τι κάνει πραγματικά μια εφαρμογή στο παρασκήνιο. Η αρχή της ελάχιστης πρόσβασης (principle of least privilege) υπαγορεύει: δίνουμε μόνο ό,τι είναι απολύτως απαραίτητο.

Πριν δεχτείτε ή απορρίψετε ένα αίτημα permission, σκεφτείτε: *Χρειάζεται πραγματικά αυτή η εφαρμογή αυτή την πρόσβαση για να λειτουργήσει;* Μια εφαρμογή πλοήγησης χρειάζεται τοποθεσία. Μια εφαρμογή βιντεοκλήσεων χρειάζεται κάμερα και μικρόφωνο. Αλλά τι λόγο έχει ένα παιχνίδι να χρειάζεται πρόσβαση στις επαφές σας;

Κάμερα

Απαραίτητη για video calls, QR scanners, εφαρμογές φωτογραφίας

Μικρόφωνο

Χρειάζεται σε voice assistants και εφαρμογές ηχογράφησης

Τοποθεσία

Νόμιμη για πλοήγηση, delivery apps, καιρός — ύποπτη για παιχνίδια

Επαφές

Μόνο για messaging apps — ποτέ για games ή εργαλεία παραγωγικότητας

Φωτογραφίες / Αρχεία

Απαραίτητη μόνο για εφαρμογές επεξεργασίας ή αποθήκευσης αρχείων

Bluetooth / Nearby

Για smart devices και wearables — όχι για εφαρμογές που δεν το δικαιολογούν

Επικίνδυνες άδειες: αναγνωρίζουμε την ύποπτη συμπεριφορά

Ένα από τα πιο ισχυρά εργαλεία ανίχνευσης κακόβουλων εφαρμογών είναι η αντιστοίχιση **λειτουργίας εφαρμογής** με τις **άδειες που ζητά**. Αν υπάρχει αναντιστοιχία, κινδυνεύετε. Η λογική είναι απλή: κάθε permission που ζητά μια εφαρμογή πρέπει να δικαιολογείται από την κύρια λειτουργία της.

🎮 Εφαρμογή παιχνιδιού

Ζητά: Επαφές, SMS, Μικρόφωνο, Τοποθεσία

→ **Ύποπτη συμπεριφορά.** Κανένα παιχνίδι δεν χρειάζεται SMS ή επαφές για να λειτουργήσει.

🔦 Εφαρμογή φακού

Ζητά: Τοποθεσία, Επαφές, Αποθήκευση

→ **Κλασικό παράδειγμα** spyware που κρύβεται πίσω από αθώα εφαρμογή.

📖 PDF Reader

Ζητά: Κάμερα, Μικρόφωνο, SMS

→ **Αδικαιολόγητες άδειες.** Ένας αναγνώστης PDF δεν χρειάζεται πρόσβαση σε κάμερα ή μηνύματα.

⊗ Κανόνας: Αν δεν μπορείτε να εξηγήσετε γιατί μια εφαρμογή χρειάζεται ένα permission, μην το δώσετε — ή αφαιρέστε την εφαρμογή.

Ειδοποιήσεις και Push notifications: Το νέο phishing

Τα push notifications έχουν εξελιχθεί σε ένα ισχυρό εργαλείο χειραγώγησης. Το **Notification Phishing** είναι μια τεχνική κατά την οποία κακόβουλες ή παραβιασμένες εφαρμογές στέλνουν ειδοποιήσεις που μιμούνται επίσημες προειδοποιήσεις, δώρα ή ενημερώσεις, με στόχο να σας κάνουν να κλικάρετε σε επικίνδυνους συνδέσμους.

Η βασική ερώτηση πριν κάνετε κλικ σε οποιαδήποτε ειδοποίηση: *"Περίμενα αυτό το μήνυμα; Το έστειλε κάποιος που εμπιστεύομαι;"* Αν η απάντηση είναι όχι, μην πατήσετε τίποτα.

Fake updates

Ειδοποιήσεις που σας λένε να "ενημερώσετε" μια εφαρμογή μέσω link — αντί από το επίσημο store. Στην πραγματικότητα εγκαθιστάτε malware.

Ψεύτικα δώρα

"Κερδίσατε ένα iPhone! Κάντε κλικ εδώ για να το παραλάβετε." Κλασική τεχνική απάτης που εκμεταλλεύεται την περιέργεια και την απληστία.

Ψεύτικες προειδοποιήσεις

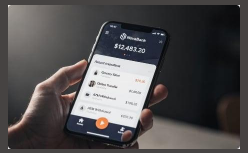
"Η συσκευή σας έχει ιό! Εγκαταστήστε αμέσως αυτό το antivirus." Δημιουργούν πανικό για να σας κάνουν να ενεργήσετε χωρίς σκέψη.

Πότε πατάμε "Να επιτρέπεται";

Μόνο όταν μια εφαρμογή έχει σαφή λόγο να σας στέλνει ειδοποιήσεις (π.χ. τραπεζική εφαρμογή για συναλλαγές). Απορρίψτε notifications από εφαρμογές που δεν τις χρειάζονται.

Κακόβουλες εφαρμογές: γνωρίστε την απειλή

Οι κακόβουλες εφαρμογές δεν είναι πάντα προφανείς. Πολλές μιμούνται γνωστά εργαλεία ή προσφέρουν πραγματική λειτουργικότητα ενώ παράλληλα συλλέγουν δεδομένα ή κλέβουν πληροφορίες στο παρασκήνιο. Η κατανόηση των κατηγοριών τους σας βοηθά να τις αναγνωρίσετε εγκαίρως.



Fake banking apps

Μιμούνται γνωστές τράπεζες pixel-perfect. Κλέβουν credentials και PIN. Πάντα κατεβάζετε τραπεζικές εφαρμογές αποκλειστικά από το επίσημο site της τράπεζας.

Fake QR Scanner & PDF Reader

Απλές εφαρμογές που κρύβουν adware ή spyware. Χρησιμοποιήστε τον ενσωματωμένο scanner της κάμερας του κινητού σας — δεν χρειάζεστε εξωτερική εφαρμογή.

Spyware & stalkerware

Εγκαθίστανται συχνά χωρίς γνώση του χρήστη. Παρακολουθούν τοποθεσία, μηνύματα και κλήσεις. Ιδιαίτερα επικίνδυνα σε περιβάλλον οικιακής ή εταιρικής παρακολούθησης.

Fake Crypto wallet apps

Στοχεύουν επενδυτές κρυπτονομισμάτων. Μόλις εισαγάγετε το seed phrase σας, οι εγκληματίες έχουν πλήρη πρόσβαση στα κεφάλαιά σας. Μη μετανοήσιμη απώλεια.

Ενημερώσεις εφαρμογών: Η πιο εύκολη άμυνα

Οι ενημερώσεις εφαρμογών και λειτουργικού συστήματος είναι η απλούστερη και πιο αποτελεσματική μορφή κυβερνοάμυνας. Κάθε ενημέρωση φέρνει διορθώσεις ευπαθειών (patches) που αν παραμείνουν ανεπίδοτες, αποτελούν ανοιχτές πόρτες για επιτιθέμενους. Πολλές από τις μεγαλύτερες κυβερνοεπιθέσεις εκμεταλλεύτηκαν γνωστές ευπάθειες για τις οποίες υπήρχε ήδη patch — το οποίο οι θύματα απλά δεν είχαν εγκαταστήσει.

1

Automatic updates

Ενεργοποιήστε τις αυτόματες ενημερώσεις για όλες τις εφαρμογές. Δεν απαιτεί καμία ενέργεια από εσάς μετά την αρχική ρύθμιση.

2

Security patches

Εγκαθιστάτε αμέσως τα security updates του λειτουργικού συστήματος. Αυτά έχουν απόλυτη προτεραιότητα — ακόμα και αν η ενημέρωση είναι μεγάλη.

3

Καθαρισμός

Διαγράψτε εφαρμογές που δεν χρησιμοποιείτε. Κάθε εγκατεστημένη εφαρμογή είναι ένα πιθανό σημείο επίθεσης, ακόμα και αν δεν την ανοίγετε ποτέ.

Προστασία εταιρικών δεδομένων

Στο εταιρικό περιβάλλον, η ασφάλεια κινητών συσκευών απαιτεί πολύπλοκη προσέγγιση. Μια μόνο παραβιασμένη συσκευή μπορεί να δώσει πρόσβαση σε ολόκληρο το εταιρικό δίκτυο. Για αυτό, οι οργανισμοί συνδυάζουν τεχνολογικά εργαλεία με αυστηρές πολιτικές χρήσης. Το BYOD (Bring Your Own Device) αποτελεί ιδιαίτερη πρόκληση, καθώς ανακατεύει προσωπικά και επαγγελματικά δεδομένα στην ίδια συσκευή.

Τεχνολογικά μέτρα

- **PIN & Βιομετρικά:** Κλείδωμα οθόνης ως πρώτη γραμμή άμυνας
- **Κρυπτογράφηση:** Προστασία δεδομένων ακόμα και σε κλοπή συσκευής
- **MFA:** Πολυπαραγοντική ταυτοποίηση για όλες τις εταιρικές εφαρμογές
- **Remote wipe:** Απομακρυσμένη διαγραφή δεδομένων σε περίπτωση απώλειας

Mobile Device Management (MDM)

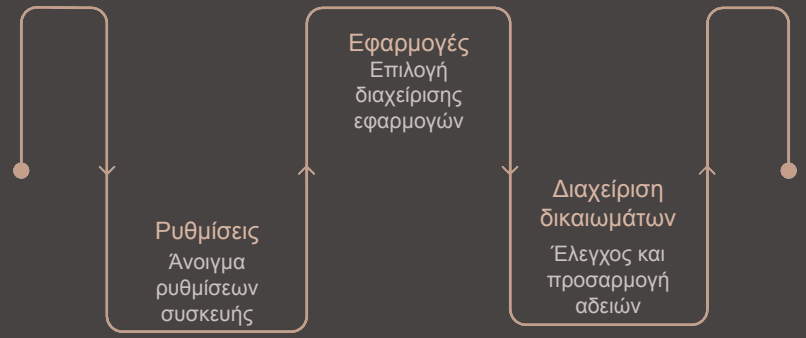
Το MDM επιτρέπει στο τμήμα IT να διαχειρίζεται συσκευές εξ αποστάσεως: να επιβάλει πολιτικές ασφαλείας, να εγκαθιστά ή να απεγκαθιστά εφαρμογές, να κρυπτογραφεί δεδομένα και να κλειδώνει ή να σβήνει απομακρυσμένα μια χαμένη συσκευή. Αποτελεί βασικό εργαλείο κάθε σύγχρονης εταιρείας.

Αν η εταιρεία σας έχει MDM, μην το παρακάμψετε ποτέ — υπάρχει για την προστασία και των δικών σας δεδομένων.

Έλεγχος δικαιωμάτων: οδηγός βήμα-βήμα

Ο τακτικός έλεγχος των αδειών πρόσβασης που έχετε παραχωρήσει σε εφαρμογές είναι μια συνήθεια που πρέπει να καλλιεργήσετε. Συνιστάται να κάνετε αυτόν τον έλεγχο τουλάχιστον μία φορά το μήνα ή μετά από κάθε μεγάλη ενημέρωση του λειτουργικού. Η διαδικασία διαφέρει ελαφρά μεταξύ Android και iPhone, αλλά είναι εξίσου απλή και στις δύο πλατφόρμες.

🤖 Android



Μπορείτε επίσης να δείτε ποιες εφαρμογές χρησιμοποιούν κάμερα/μικρόφωνο από το **Privacy Dashboard** (Android 12+). Ελέγξτε κάθε permission και ανακαλέστε όσες δεν δικαιολογούνται.

🍎 iPhone

Το iOS σας επιτρέπει να επιλέξετε **"Μόνο κατά τη χρήση"** για την τοποθεσία — μια πολύ χρήσιμη επιλογή που περιορίζει την παρακολούθηση στο παρασκήνιο. Χρησιμοποιήστε την πάντα.

Πραγματικά παραδείγματα: καλό vs. κακό

Ας δούμε δύο χαρακτηριστικά παραδείγματα που απεικονίζουν ξεκάθαρα τη διαφορά μεταξύ μιας νόμιμης και μιας ύποπτης εφαρμογής. Το κλειδί είναι πάντα η **αναλογία** μεταξύ λειτουργίας και αιτούμενων αδειών.

🟢 Εφαρμογή τράπεζας — λογικές άδειες

- ✓ **Κάμερα:** Για σκανάρισμα εγγράφων και QR πληρωμών
- ✓ **Notifications:** Για ειδοποιήσεις συναλλαγών σε πραγματικό χρόνο
- ✓ **Biometrics:** Για ασφαλή είσοδο με δακτυλικό αποτύπωμα ή Face ID
- ✓ **Internet:** Απαραίτητο για κάθε online εφαρμογή

→ Όλες οι άδειες δικαιολογούνται από τη λειτουργία της εφαρμογής.

🔴 Εφαρμογή φακού — ύποπτες άδειες

- ❌ **Contacts:** Ένας φακός δεν χρειάζεται τις επαφές σας
- ❌ **SMS:** Αδικαιολόγητη — σήμα spyware ή adware
- ❌ **Location:** Γιατί χρειάζεται GPS μια εφαρμογή φωτισμού;
- ❌ **Microphone:** Εντελώς άσχετο με τη λειτουργία

→ Κλασικό παράδειγμα κακόβουλης εφαρμογής. Άμεση απεγκατάσταση.

Checklist ασφαλούς χρήσης mobile apps

Χρησιμοποιήστε αυτό το checklist ως οδηγό αξιολόγησης για κάθε συσκευή και κάθε εφαρμογή. Μπορείτε να το μοιραστείτε με συναδέλφους ή να το ενσωματώσετε σε εταιρικές πολιτικές ασφαλείας. Ένα ολοκληρωμένο checklist καλύπτει τόσο την εγκατάσταση όσο και τη συνεχή συντήρηση της ασφάλειας της συσκευής.

- [ ] Εγκατάσταση μόνο από επίσημα stores (Google Play / App Store)
- [ ] Έλεγχος εκδότη, αξιολογήσεων και ημερομηνίας ενημέρωσης
- [ ] Ενεργοποίηση αυτόματων ενημερώσεων εφαρμογών
- [ ] Εγκατάσταση security patches λειτουργικού αμέσως
- [ ] Ενεργοποίηση MFA σε όλες τις κρίσιμες εφαρμογές
- [ ] Χρήση βιομετρικού κλειδώματος οθόνης
- [ ] Μηνιαίος έλεγχος permissions εφαρμογών
- [ ] Ανάκληση αδειών που δεν χρησιμοποιούνται
- [ ] Τακτικό backup δεδομένων συσκευής
- [ ] Χρήση Password Manager για εφαρμογές
- [ ] Χρήση VPN σε δημόσιο Wi-Fi
- [ ] Διαγραφή εφαρμογών που δεν χρησιμοποιούνται

Αν ολοκληρώσετε όλα τα βήματα, η συσκευή σας έχει επαγγελματικό επίπεδο προστασίας. Επαναλαμβάνετε τον έλεγχο κάθε μήνα.

Συμπεράσματα

Η ασφαλής χρήση εφαρμογών κινητών συσκευών δεν απαιτεί εξειδικευμένες τεχνικές γνώσεις — απαιτεί **συνείδηση και συνήθεια**. Οι πιο αποτελεσματικές άμυνες είναι συχνά οι πιο απλές: ελέγξτε τι εγκαθιστάτε, ποιος το έφτιαξε, και τι πρόσβαση ζητά.

Ελέγχετε πάντα τα permissions

Κάθε άδεια που δίνετε αποτελεί δυνητική έκθεση δεδομένων. Δίνετε μόνο ό,τι είναι απολύτως απαραίτητο και ανακαλείτε ό,τι δεν χρειάζεται πλέον.

Εγκαθιστάτε μόνο από επίσημα καταστήματα

Το Google Play και το App Store δεν εγγυώνται 100% ασφάλεια, αλλά προσφέρουν σημαντική φιλτράρισμα. Τρίτες πηγές δεν προσφέρουν τίποτα.

Διατηρείτε πάντα ενημερωμένη τη συσκευή

Οι ενημερώσεις κλείνουν γνωστές ευπάθειες. Κάθε μέρα χωρίς update είναι μια μέρα που οι επιτιθέμενοι έχουν πλεονέκτημα.

Αναφέρετε ύποπτες εφαρμογές στο IT

Αν εντοπίσετε κάτι ύποπτο, μην το κρατήσετε για τον εαυτό σας. Η έγκαιρη αναφορά μπορεί να προστατεύσει ολόκληρη την εταιρεία από μια επίθεση.