Ασφαλής εγκατάσταση και χρήση εφαρμογών σε υπολογιστές

Ένας πρακτικός οδηγός για υπαλλήλους και διαχειριστές IT — κατανοήστε τους κινδύνους, αναγνωρίστε τις απειλές και εφαρμόστε ασφαλείς πρακτικές εγκατάστασης λογισμικού στο εργασιακό περιβάλλον.

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry

safeLine.gr

ΙΤΕ
ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Στόχοι σεμιναρίου

Οι εφαρμογές αποτελούν μία από τις πιο συχνές πύλες εισόδου για κακόβουλο λογισμικό. Κατανοώντας πώς λειτουργούν οι επιθέσεις, μπορούμε να τις αποτρέψουμε αποτελεσματικά.

⚠️ Γιατί οι εφαρμογές αποτελούν κίνδυνο

Κάθε εγκατάσταση λογισμικού από αναξιόπιστη πηγή ανοίγει θύρα για εισβολείς στο σύστημά σας.

🦠 Πώς εισέρχεται το Malware

Μέσω crack, trojan, ψεύτικων ενημερώσεων ή επιπλέον λογισμικού που «κρύβεται» στην εγκατάσταση.

🎯 Στόχοι του σεμιναρίου

Αναγνώριση επικίνδυνων πηγών, σωστός έλεγχος πριν την εγκατάσταση και εφαρμογή καλών πρακτικών.

Από πού εγκαθιστούμε λογισμικό;

Η επιλογή της σωστής πηγής είναι το πρώτο και πιο κρίσιμο βήμα ασφάλειας. Πάντα να κατεβάζετε λογισμικό αποκλειστικά από εγκεκριμένες πηγές.

✅ Αξιόπιστες πηγές

- Επίσημη ιστοσελίδα κατασκευαστή
- Microsoft Store
- Εγκεκριμένο εταιρικό Software Portal

❌ Πηγές που ΑΠΑΓΟΡΕΥΟΝΤΑΙ

- Torrent & Warez sites
- Crack & keygen ιστοσελίδες
- Άγνωστα download sites
- Μη επαληθευμένοι τρίτοι πωλητές

Κίνδυνοι από μη αξιόπιστο λογισμικό

Η εγκατάσταση λογισμικού από αναξιόπιστες πηγές εκθέτει ολόκληρη την επιχείρηση σε σοβαρές απειλές. Ακολουθούν οι πιο συχνές κατηγορίες κακόβουλου λογισμικού.

Ransomware

Κρυπτογραφεί τα αρχεία σας και απαιτεί λύτρα για την αποκατάστασή τους.

Spyware & keyloggers

Καταγράφουν κωδικούς, πλήκτρα και δραστηριότητα χωρίς να το αντιληφθείτε.

Trojans & backdoors

Δίνουν πρόσβαση σε εισβολείς στο σύστημά σας από απόσταση.

Cryptominers

Χρησιμοποιούν τους πόρους του υπολογιστή σας κρυφά για εξόρυξη κρυπτονομισμάτων.

Προσοχή κατά την εγκατάσταση

Πολλά προγράμματα «κρύβουν» επιπλέον λογισμικό στη διαδικασία εγκατάστασης. Το να πατάτε αδιάκριτα **Next** → **Next** → **Finish** είναι μια συνηθισμένη παγίδα που αξιοποιούν κακόβουλοι εκδότες.

☐ Additional software

Ελέγξτε αν προτείνεται εγκατάσταση επιπλέον προγραμμάτων — συνήθως είναι ήδη τσεκαρισμένα.

☐ Browser extensions & toolbars

Αρνηθείτε κάθε επέκταση ή toolbar που δεν έχετε ζητήσει — συχνά συλλέγουν δεδομένα.

☐ Αλλαγές search engine

Μερικά προγράμματα αλλάζουν τον μηχανισμό αναζήτησης του browser σας χωρίς ενημέρωση.

☐ Startup programs

Ελέγξτε ποια προγράμματα εκκινούν αυτόματα μαζί με τα Windows — απενεργοποιήστε τα μη απαραίτητα.

⚠ Διαβάζετε ΠΑΝΤΑ κάθε βήμα της εγκατάστασης. Ποτέ μην πατάτε Next χωρίς να ελέγξετε τι συμφωνείτε.

Ψεύτικες ενημερώσεις — ένας διαδεδομένος κίνδυνος

Οι επιτήδειοι δημιουργούν πανομοιότυπες σελίδες και παράθυρα που μιμούνται γνωστές εφαρμογές. Εάν δεν εγκαταστήσετε την «ενημέρωση», στην πραγματικότητα κατεβάζετε malware.

❌ Fake Chrome update

Εμφανίζεται ως επείγουσα ενημέρωση του browser, αλλά εγκαθιστά adware ή spyware.

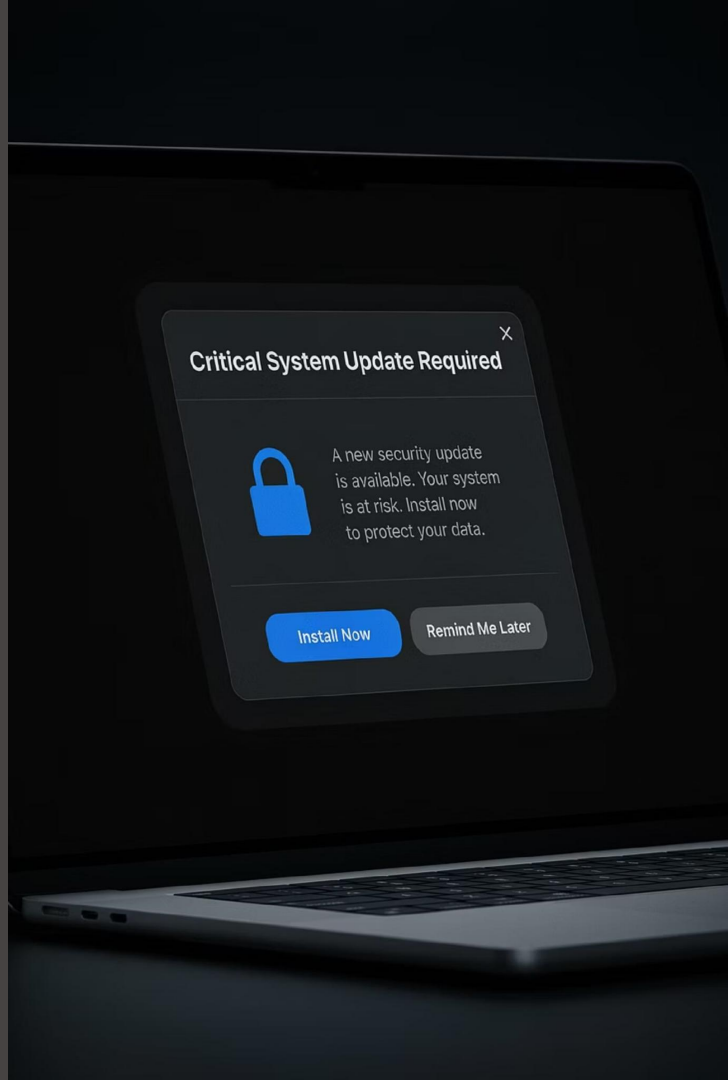
❌ Fake Adobe / VLC

Ψεύτικα popup ζητούν «αναβάθμιση» δημοφιλών εφαρμογών για να εισάγουν κακόβουλο κώδικα.

❌ Fake Zoom / Microsoft

Στοχεύουν επαγγελματίες με απομίμηση εταιρικών εργαλείων που χρησιμοποιούνται καθημερινά.

Κανόνας: Οι ενημερώσεις γίνονται ΜΟΝΟ μέσα από την ίδια την εφαρμογή ή τα Windows Update — ποτέ μέσω αναδυόμενων παραθύρων από ιστοσελίδες.



Ψηφιακές υπογραφές — πώς επαληθεύουμε τον εκδότη

Πριν από κάθε εγκατάσταση, ελέγξτε αν το αρχείο φέρει έγκυρη ψηφιακή υπογραφή. Αυτός είναι ο πιο αξιόπιστος τρόπος να επιβεβαιώσετε ότι το λογισμικό προέρχεται από τον πραγματικό κατασκευαστή.

Publisher verification

Κάντε δεξί κλικ στο αρχείο → Properties → Digital Signatures. Ελέγξτε ότι το όνομα εκδότη ταιριάζει με τον αναμενόμενο κατασκευαστή.

Code signing certificate

Ένα έγκυρο πιστοποιητικό υπογραφής κώδικα εγγυάται ότι το αρχείο δεν έχει τροποποιηθεί από τρίτους.

Windows SmartScreen

Το SmartScreen ειδοποιεί αυτόματα για αρχεία με άγνωστο ή μη αξιόπιστο εκδότη. Μην το παρακάμπτετε.

Microsoft Defender

Εκτελέστε σάρωση με Defender πριν από κάθε εγκατάσταση για πρόσθετη επαλήθευση ασφάλειας.

Δικαιώματα διαχειριστή — Administrator vs standard user

Η καθημερινή χρήση του υπολογιστή ως **Administrator** αυξάνει δραματικά τον κίνδυνο μόλυνσης. Ένα κακόβουλο πρόγραμμα που εκτελείται με δικαιώματα διαχειριστή μπορεί να πάρει τον πλήρη έλεγχο του συστήματος.

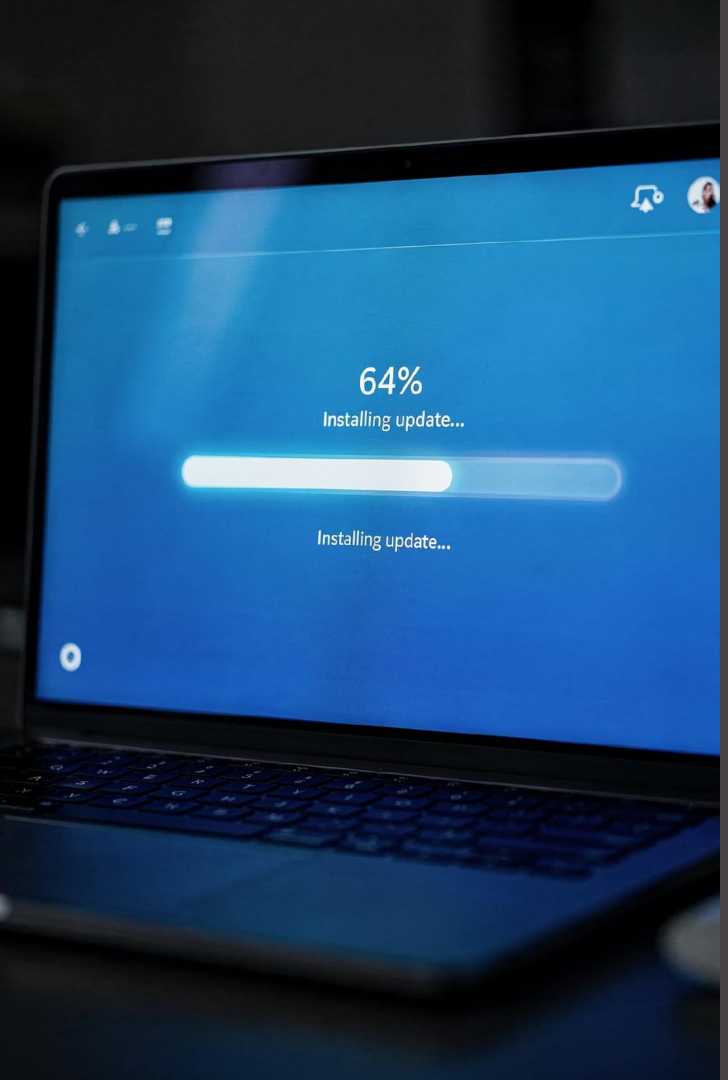
👤 Administrator

- Πλήρης πρόσβαση στο σύστημα
- Εγκατάσταση/διαγραφή λογισμικού
- Τροποποίηση ρυθμίσεων ασφάλειας
- Αλλαγή λογαριασμών χρηστών
- ⚠️ Malware αποκτά τον ίδιο έλεγχο

👤 Standard user

- Περιορισμένη πρόσβαση στο σύστημα
- Δεν μπορεί να εγκαταστήσει λογισμικό χωρίς έγκριση
- Malware δεν μπορεί να αλλάξει συστημικά αρχεία
- ✅ Συνιστάται για καθημερινή χρήση

Χρησιμοποιείτε Administrator ΜΟΝΟ όταν χρειάζεται — και μόνο για συγκεκριμένες εργασίες.



Ενημερώσεις λογισμικού — η πρώτη γραμμή άμυνας

Το μη ενημερωμένο λογισμικό αποτελεί από τις συχνότερες αιτίες επιτυχημένων κυβερνοεπιθέσεων. Οι ενημερώσεις δεν φέρνουν μόνο νέες λειτουργίες — διορθώνουν κρίσιμα κενά ασφάλειας.

Browser & Office

Chrome, Firefox, Edge και Microsoft Office πρέπει να ενημερώνονται αυτόματα. Ελέγξτε τις ρυθμίσεις.

PDF Reader & Java

Εφαρμογές όπως Adobe Reader και Java αποτελούν συχνό στόχο. Ενεργοποιήστε αυτόματες ενημερώσεις.

Drivers & .NET

Οι drivers και το .NET framework χρειάζονται τακτική ενημέρωση μέσω Windows Update για μέγιστη ασφάλεια.

Επικίνδυνες κατηγορίες εφαρμογών

Ορισμένες κατηγορίες λογισμικού ενέχουν εξαιρετικά υψηλό κίνδυνο ανεξαρτήτως προέλευσης. Αποφύγετε τις παντελώς ή χρησιμοποιήστε τις μόνο κατόπιν έγκρισης από το IT.

🔓 Cracks & keygens

Παράνομα εργαλεία παράκαμψης αδειών λογισμικού — περιέχουν σχεδόν πάντα malware.

🖥️ Unknown Remote Access tools

Εργαλεία απομακρυσμένης πρόσβασης από άγνωστους εκδότες δίνουν πλήρη έλεγχο σε τρίτους.

🛡️ Fake antivirus

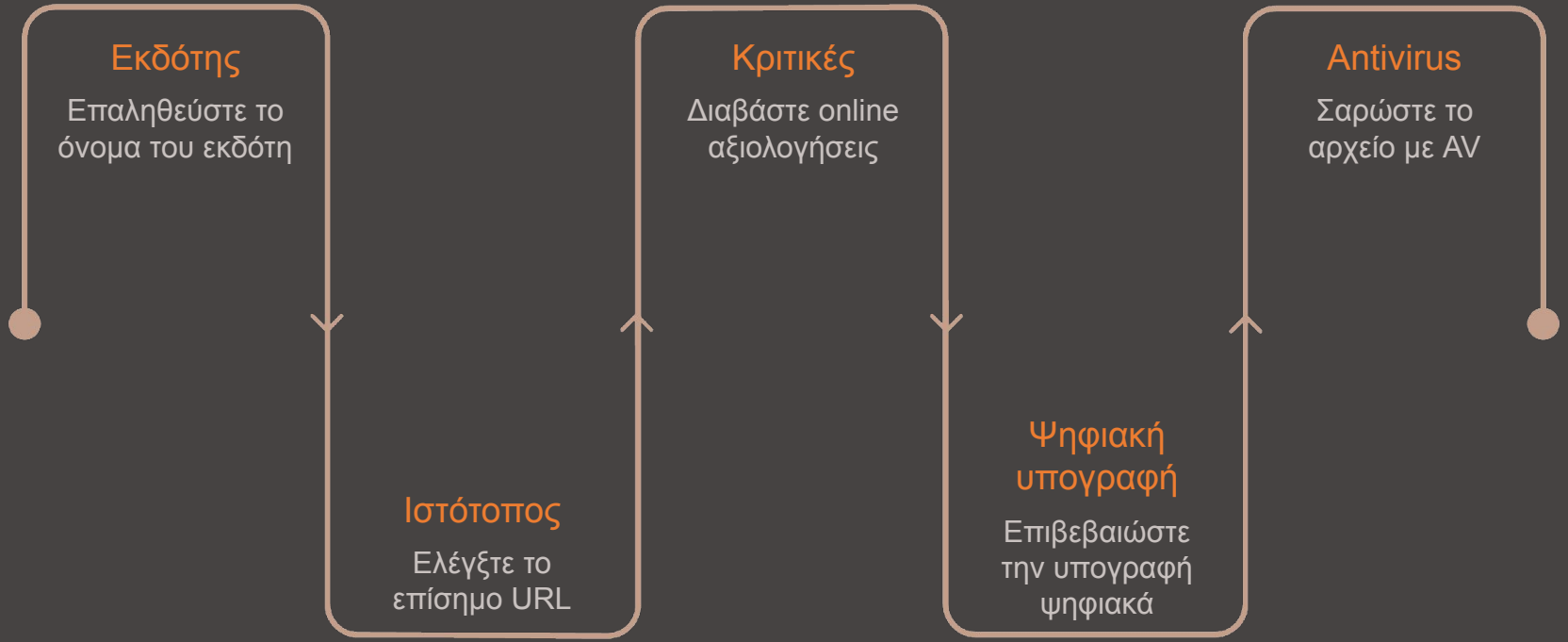
Προγράμματα που προσποιούνται ότι προστατεύουν ενώ στην πραγματικότητα μολύνουν το σύστημα.

🔑 Password recovery Tools

Εργαλεία ανάκτησης κωδικών από αναξιόπιστες πηγές μπορούν να εξάγουν credentials σε τρίτους.

Έλεγχος πριν την εγκατάσταση — 6 βήματα

Πριν εγκαταστήσετε οποιοδήποτε λογισμικό, ακολουθήστε αυτή τη λίστα ελέγχου. Λίγα λεπτά προφύλαξης μπορούν να αποτρέψουν σοβαρά περιστατικά ασφάλειας.



Κάθε βήμα αποτελεί ανεξάρτητη γραμμή άμυνας. Παραλείποντας έστω και ένα, αυξάνετε τον κίνδυνο σημαντικά. Σε περίπτωση αμφιβολίας, απευθυνθείτε πάντα στο τμήμα IT.

Checklist ασφαλούς εγκατάστασης

Χρησιμοποιήστε αυτή τη λίστα ως ημερήσιο οδηγό ασφάλειας για κάθε εγκατάσταση λογισμικού στο εργασιακό σας περιβάλλον.

Πηγή & επαλήθευση

- [x] Λήψη μόνο από Official Website ή Microsoft Store
- [x] Έλεγχος ψηφιακής υπογραφής (Publisher)
- [x] Σάρωση αρχείου με Microsoft Defender
- [x] Επαλήθευση hash όπου απαιτείται

Ρυθμίσεις & συστήματα

- [x] Ενεργοποιημένο Windows SmartScreen
- [x] Χρήση Standard User για καθημερινή εργασία
- [x] Αυτόματες ενημερώσεις ενεργοποιημένες
- [x] Τακτικό backup δεδομένων

Σε κάθε περίπτωση αμφιβολίας — πριν εγκαταστήσετε οτιδήποτε — επικοινωνήστε με το τμήμα IT.

Συμπεράσματα

> Η ασφαλής εγκατάσταση λογισμικού είναι μία από τις σημαντικότερες άμυνες απέναντι στις κυβερνοεπιθέσεις.

Επιλέγετε πάντα αξιόπιστες πηγές

Επίσημες ιστοσελίδες, Microsoft Store και εγκεκριμένο εταιρικό portal είναι οι μόνες αποδεκτές επιλογές.

Ελέγχετε πριν εγκαταστήσετε

Ψηφιακή υπογραφή, εκδότης, antivirus σάρωση και κριτικές αποτρέπουν την πλειονότητα των απειλών.

Ενημερώνετε τακτικά και χρησιμοποιείτε standard user

Τα ενημερωμένα συστήματα και οι περιορισμένοι λογαριασμοί μειώνουν δραστικά την επιφάνεια επίθεσης.