Ασφαλής χρήση antivirus και Microsoft Defender

Ένας πρακτικός οδηγός για εργαζόμενους και χρήστες IT — κατανοήστε τον ρόλο του λογισμικού προστασίας, εξοικειωθείτε με το Microsoft Defender και μάθετε πώς να το χρησιμοποιείτε αποτελεσματικά για την ασφάλεια του συστήματός σας.

Ρόλος προστασίας

Τι κάνει το λογισμικό antivirus και γιατί είναι απαραίτητο

Microsoft Defender

Τα βασικά χαρακτηριστικά και δυνατότητες του ενσωματωμένου εργαλείου

Στόχοι σεμιναρίου

Πρακτικές γνώσεις για την καθημερινή ασφαλή χρήση του υπολογιστή

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry

safeLine.gr

ΙΤΕ
ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Deepfakes: Η νέα απειλή στην Κυβερνοασφάλεια

Αναγνώριση και αντιμετώπιση για επιχειρήσεις — Ενημέρωση και προστασία των εργαζομένων στη σύγχρονη ψηφιακή εποχή.

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry

safeLine.gr

ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Γιατί είναι απαραίτητο το antivirus;

Οι σύγχρονες ψηφιακές απειλές εξελίσσονται συνεχώς και στοχεύουν τόσο εταιρικά όσο και προσωπικά συστήματα. Χωρίς κατάλληλη προστασία, ένας υπολογιστής είναι εκτεθειμένος σε πληθώρα κινδύνων που μπορούν να οδηγήσουν σε απώλεια δεδομένων, οικονομική ζημιά ή παραβίαση εταιρικών πληροφοριών.

Ανίχνευση malware

Εντοπισμός και αφαίρεση κακόβουλου λογισμικού πριν προκαλέσει βλάβη στο σύστημα ή στα αρχεία σας.

Προστασία από ransomware

Αποτροπή κρυπτογράφησης αρχείων από κακόβουλους που απαιτούν λύτρα για την αποκατάστασή τους.

Trojans & spyware

Εντοπισμός προγραμμάτων που μεταμφιέζονται ως νόμιμα ή παρακολουθούν κρυφά τη δραστηριότητά σας.

Μείωση κινδύνου

Ελαχιστοποίηση της πιθανότητας παραβίασης δεδομένων και προστασία της εταιρικής υποδομής.

Γνωριμία με το Microsoft Defender

Το Microsoft Defender είναι το ενσωματωμένο εργαλείο ασφαλείας των Windows, διαθέσιμο χωρίς επιπλέον κόστος. Προσφέρει ένα πλήρες σύνολο δυνατοτήτων που καλύπτουν τις βασικές ανάγκες προστασίας για τους περισσότερους χρήστες και οργανισμούς.

🛡️ Προστασία σε πραγματικό χρόνο

Παρακολουθεί συνεχώς το σύστημα και αποκλείει απειλές τη στιγμή που εμφανίζονται, χωρίς να χρειάζεται χειροκίνητη παρέμβαση.

🔥 Firewall & προστασία δικτύου

Ελέγχει την εισερχόμενη και εξερχόμενη κίνηση δικτύου, αποκλείοντας μη εξουσιοδοτημένες συνδέσεις και ύποπτες επικοινωνίες.

🌐 SmartScreen

Ελέγχει ιστοσελίδες και λήψεις αρχείων σε πραγματικό χρόνο, προειδοποιώντας για γνωστές απειλές phishing και επικίνδυνο περιεχόμενο.

📁 Προστασία από ransomware

Το Controlled Folder Access εμποδίζει μη εξουσιοδοτημένες εφαρμογές να τροποποιήσουν σημαντικούς φακέλους και αρχεία σας.

Διατήρηση ενημερωμένου Defender

Ένα antivirus που δεν είναι ενημερωμένο δεν μπορεί να αναγνωρίσει τις νεότερες απειλές. Οι ενημερώσεις υπογραφών ασφαλείας (virus definitions) εκδίδονται συχνά — μερικές φορές και πολλές φορές την ημέρα — και είναι απαραίτητες για αποτελεσματική προστασία.

Windows Update
Εκτέλεση τακτικά για συστήματα ασφαλείας.

Ενημέρωση υπογραφών
Αυτόματη λήψη νεότερων definitions.

Αυτόματες ενημερώσεις
Ενεργοποιημένες για συνεχή προστασία.

Τακτικός έλεγχος
Εβδομαδιαίος έλεγχος κατάστασης Defender.

Βεβαιωθείτε ότι το Windows Update είναι ενεργοποιημένο και ότι δεν αναβάλλετε τις ενημερώσεις. Ο τακτικός έλεγχος της κατάστασης του Defender από τις **Ρυθμίσεις** → **Ενημέρωση & Ασφάλεια** → **Windows Security** σας εξασφαλίζει ότι το σύστημά σας είναι πάντα προστατευμένο.

Προστασία σε πραγματικό χρόνο

Η προστασία σε πραγματικό χρόνο είναι η πρώτη γραμμή άμυνας του Microsoft Defender. Λειτουργεί αθόρυβα στο παρασκήνιο, παρακολουθώντας κάθε αρχείο που ανοίγετε, κάθε πρόγραμμα που εκτελείται και κάθε σύνδεση που πραγματοποιείται. **Δεν πρέπει ποτέ να απενεργοποιηθεί.**

Real-time protection

Συνεχής παρακολούθηση του συστήματος για ύποπτη δραστηριότητα και άμεση αντίδραση σε απειλές.

Cloud-delivered protection

Χρησιμοποιεί τη βάση δεδομένων του Microsoft cloud για ανίχνευση νέων, άγνωστων απειλών σε milliseconds.

Automatic sample submission

Αποστέλλει αυτόματα ύποπτα αρχεία στη Microsoft για ανάλυση, βελτιώνοντας συνολικά την ασφάλεια.

Tamper protection

Αποτρέπει κακόβουλο λογισμικό από το να απενεργοποιήσει ή να τροποποιήσει τις ρυθμίσεις του Defender.

Προγραμματισμένες σαρώσεις

Πέρα από την προστασία σε πραγματικό χρόνο, οι τακτικές σαρώσεις εξασφαλίζουν ότι κανένα κρυμμένο απειλητικό αρχείο δεν παραμένει ανεντόπιστο στο σύστημά σας. Το Microsoft Defender προσφέρει τρεις τύπους σάρωσης ανάλογα με τις ανάγκες.

1

⚡ Γρήγορη σάρωση

Ελέγχει τις πιο κοινές τοποθεσίες απειλών. Ιδανική για καθημερινή χρήση, διαρκεί μόνο λίγα λεπτά.

2

🔍 Πλήρης σάρωση

Σαρώνει ολόκληρο το σύστημα. Συνιστάται εβδομαδιαία ή μετά από ύποπτη δραστηριότητα. Διαρκεί περισσότερο.

3

🔒 Offline scan

Εκτελείται κατά την επανεκκίνηση, πριν φορτωθεί το λειτουργικό σύστημα. Ανιχνεύει επίμονες απειλές που αποφεύγουν τη συνήθη ανίχνευση.

ⓘ Χρησιμοποιήστε το **Offline Scan** όταν υποψιάζεστε σοβαρή μόλυνση που δεν αντιμετωπίστηκε με τις συνήθεις σαρώσεις.

Προστασία από ransomware

Το ransomware είναι από τις πιο καταστροφικές μορφές κυβερνοεπίθεσης — κρυπτογραφεί τα αρχεία σας και απαιτεί λύτρα για την επαναφορά τους. Το Microsoft Defender προσφέρει ειδικά εργαλεία για την αντιμετώπισή του.

Controlled Folder Access

Προστατεύει συγκεκριμένους φακέλους (Έγγραφα, Εικόνες, κ.ά.) από μη εξουσιοδοτημένες εφαρμογές. Μόνο εγκεκριμένα προγράμματα μπορούν να κάνουν αλλαγές.

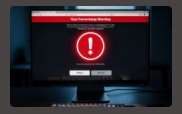
Αντίγραφα ασφαλείας & ανάκτηση

Ακόμα και με ενεργή προστασία, τα τακτικά backups είναι αναντικατάστατα. Χρησιμοποιήστε **OneDrive** ή εξωτερικό αποθηκευτικό μέσο. Σε περίπτωση επίθεσης, η ανάκτηση αρχείων από αντίγραφο ασφαλείας είναι ο πιο αξιόπιστος τρόπος αποκατάστασης.

- Δημιουργείτε backup τουλάχιστον εβδομαδιαία
- Αποθηκεύετε αντίγραφα εκτός δικτύου (offline)
- Ελέγχετε ότι τα backups είναι αναξιόπιστα ανακτήσιμα

Microsoft Defender SmartScreen

Το SmartScreen λειτουργεί ως φίλτρο ασφαλείας για τον περιηγητή σας και τις λήψεις αρχείων. Ελέγχει σε πραγματικό χρόνο κάθε ιστοσελίδα που επισκέπτεστε και κάθε αρχείο που κατεβάζετε, συγκρίνοντάς τα με βάσεις δεδομένων γνωστών απειλών.



Έλεγχος ιστοσελίδων

Κάθε URL που επισκέπτεστε αξιολογείται αυτόματα. Αν η σελίδα είναι γνωστή για phishing ή διανομή malware, το SmartScreen εμφανίζει προειδοποίηση πριν φορτωθεί.

Έλεγχος λήψεων

Πριν εκτελεστεί ένα αρχείο που κατεβάσατε, το SmartScreen ελέγχει τη φήμη του. Αρχεία άγνωστης ή κακής φήμης σημειώνονται και αποκλείονται.

Προειδοποιήσεις phishing

Μην αγνοείτε ποτέ τις προειδοποιήσεις SmartScreen. Ακόμα κι αν η σελίδα φαίνεται νόμιμη, η προειδοποίηση βασίζεται σε επαληθευμένη επικίνδυνη δραστηριότητα.

Καλές πρακτικές ασφάλειας

Η τεχνολογία μόνη της δεν αρκεί — η ασφάλεια εξαρτάται και από τη συμπεριφορά μας. Ακολουθώντας μερικές βασικές αρχές, μειώνετε σημαντικά τον κίνδυνο μόλυνσης ή παραβίασης.

Μην απενεργοποιείτε το Antivirus

Ακόμα και αν κάποια εφαρμογή ζητά να το κάνετε "προσωρινά", αυτό είναι συχνά σημάδι κακόβουλου λογισμικού. Επικοινωνήστε με το IT πριν από οποιαδήποτε αλλαγή.

Σαρώστε USB και νέες λήψεις

Κάθε εξωτερική συσκευή ή αρχείο που κατεβάζετε από το διαδίκτυο μπορεί να περιέχει απειλή. Εκτελέστε σάρωση πριν ανοίξετε οποιοδήποτε αρχείο.

Συνδυάστε με MFA και ενημερώσεις

Το antivirus είναι ένα επίπεδο προστασίας. Η πολυπαραγοντική ταυτοποίηση (MFA) και οι τακτικές ενημερώσεις συστήματος ενισχύουν σημαντικά την συνολική ασφάλεια.

Checklist ασφάλειας

Χρησιμοποιήστε αυτήν τη λίστα για να επαληθεύσετε ότι το σύστημά σας είναι σωστά διαμορφωμένο και προστατευμένο. Ελέγξτε τακτικά κάθε σημείο — ιδανικά μία φορά την εβδομάδα.

Βασικές ρυθμίσεις

- [x] Defender ενημερωμένος με τελευταίες υπογραφές ασφαλείας
- [x] Real-time Protection ενεργή και λειτουργεί κανονικά
- [x] SmartScreen ενεργό στον browser και στο σύστημα

Τακτικές ενέργειες

- [x] Τακτικές σαρώσεις προγραμματισμένες (γρήγορη / πλήρης)
- [x] Controlled Folder Access ενεργοποιημένο για σημαντικούς φακέλους
- [ ] Αντίγραφο ασφαλείας (backup) δημιουργημένο πρόσφατα
- [ ] Ενημερώσεις Windows εγκατεστημένες χωρίς αναβολή

- [ ] Αν κάποιο από τα παραπάνω δεν ισχύει για το σύστημά σας, επικοινωνήστε άμεσα με την ομάδα IT του οργανισμού σας.