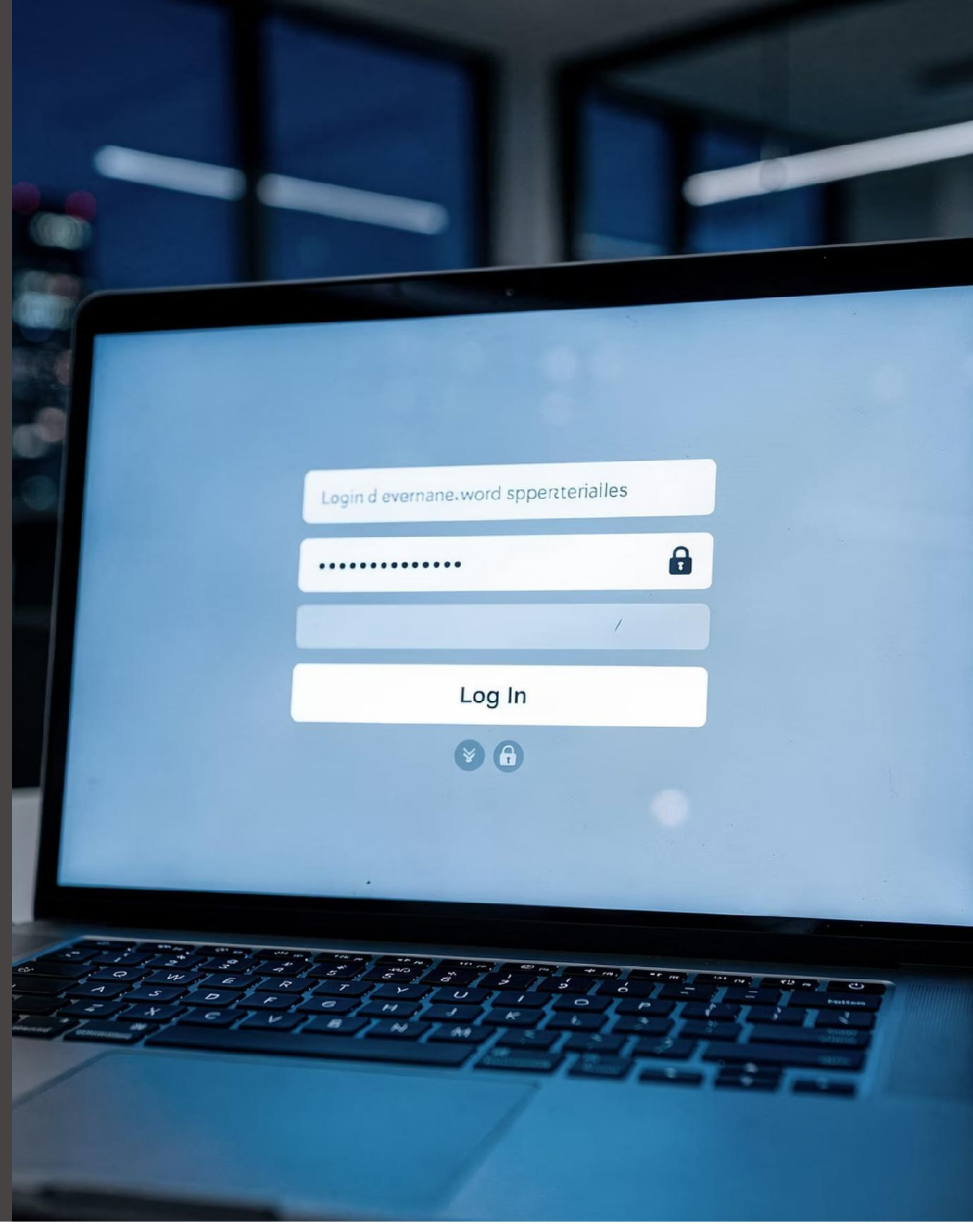
Ενίσχυση της ασφάλειας λογαριασμών email μέσω ρυθμίσεων

Οι λογαριασμοί email αποτελούν έναν από τους πιο συχνούς στόχους κυβερνοεπιθέσεων. Ακόμα και χωρίς εξειδικευμένα εργαλεία, οι σωστές ρυθμίσεις μπορούν να μειώσουν δραστικά τον κίνδυνο παραβίασης. Σε αυτή την παρουσίαση παρουσιάζονται πρακτικά βήματα που αυξάνουν σημαντικά την ασφάλεια — τόσο για εταιρικούς λογαριασμούς (Microsoft 365, Google Workspace) όσο και για ιδρυματικούς.



Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry

safeLine.gr

ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Ενεργοποίηση Πολυπαραγοντικής Αυθεντικοποίησης (MFA)

Η Πολυπαραγοντική Αυθεντικοποίηση είναι το πιο αποτελεσματικό μέτρο προστασίας λογαριασμού. Ακόμα και αν κλαπεί ο κωδικός σας, ο εισβολέας δεν μπορεί να αποκτήσει πρόσβαση χωρίς τον δεύτερο παράγοντα.

✅ Εφαρμογές Authenticator

Google Authenticator, Microsoft Authenticator, Authy — δημιουργούν κωδικούς μίας χρήσης τοπικά, χωρίς εξάρτηση από δίκτυο.

🔑 Passkeys

Σύγχρονη και ανθεκτική στο phishing λύση. Συνιστάται όπου υποστηρίζεται από την πλατφόρμα.

⚠️ SMS — αποφύγετε όπου είναι δυνατό

Ευάλωτο σε SIM-swapping και ανακατεύθυνση κλήσεων. Χρησιμοποιείται μόνο ως έσχατη επιλογή.

- [ ] Ενεργοποιήστε MFA σε **όλους** τους εταιρικούς και ιδρυματικούς λογαριασμούς — χωρίς εξαιρέσεις.

Έλεγχος επιλογών ανάκτησης

Οι επιλογές ανάκτησης αποτελούν συχνά την «πίσω πόρτα» ενός λογαριασμού. Αν ένας εισβολέας αποκτήσει πρόσβαση στο email ή στον αριθμό τηλεφώνου ανάκτησης, μπορεί να επαναφέρει τον κωδικό και να παρακάμψει κάθε άλλη προστασία.

Τι πρέπει να ελέγξετε

- Το εναλλακτικό email ανάκτησης ανήκει σε εσάς και είναι ενεργό
- Ο αριθμός τηλεφώνου είναι επίκαιρος και δεν έχει αλλάξει χέρια
- Δεν υπάρχουν παλιές διευθύνσεις ή αριθμοί που δεν χρησιμοποιείτε πλέον

Πού να το κάνετε

- **Google:** myaccount.google.com → Ασφάλεια → Τρόποι επαλήθευσης
- **Microsoft 365:** mysignins.microsoft.com → Πληροφορίες ασφαλείας
- **Γενικά:** Ελέγχετε τουλάχιστον κάθε 6 μήνες ή μετά από αλλαγή τηλεφώνου

Έλεγχος συνδεδεμένων συσκευών

Κάθε συσκευή που έχει συνδεθεί στον λογαριασμό σας διατηρεί μια ενεργή συνεδρία. Αν κάποια από αυτές τις συσκευές έχει κλαπεί, πουληθεί ή δεν ανήκει πλέον σε εσάς, παραμένει δυνητικός κίνδυνος.

Επισκόπηση ενεργών συνδέσεων

Ελέγξτε τη λίστα όλων των συσκευών που έχουν πρόσβαση στον λογαριασμό — τύπος, τοποθεσία, τελευταία είσοδος.

Αποσύνδεση άγνωστων συσκευών

Οποιαδήποτε συσκευή δεν αναγνωρίζετε πρέπει να αποσυνδεθεί άμεσα και η ενέργεια να καταγραφεί.

Τακτικός έλεγχος ιστορικού

Προγραμματίστε μηνιαίο έλεγχο του ιστορικού σύνδεσης — ιδιαίτερα μετά από αλλαγές προσωπικού ή συσκευής.

ⓘ Στο **Google Admin Console** και στο **Microsoft Entra ID** μπορείτε να εκτελέσετε μαζική αποσύνδεση συσκευών για ολόκληρο τον οργανισμό.

Έλεγχος εφαρμογών τρίτων

Εφαρμογές τρίτων που συνδέθηκαν στον λογαριασμό email με OAuth ή API κλειδιά μπορούν να διαβάζουν, να τροποποιούν ή να διαγράφουν μηνύματα — ακόμα και αν έχουν παύσει να χρησιμοποιούνται.

Αφαιρέστε ανενεργές εφαρμογές

Οποιαδήποτε εφαρμογή δεν χρησιμοποιείτε πλέον πρέπει να αφαιρεθεί από τις εξουσιοδοτήσεις. Η αδράνεια δεν σημαίνει ακινδυνότητα — η εφαρμογή εξακολουθεί να έχει πρόσβαση.

Αρχή ελαχίστων δικαιωμάτων

Δώστε σε κάθε εφαρμογή μόνο τα απολύτως απαραίτητα δικαιώματα. Αποφύγετε εφαρμογές που ζητούν πλήρη πρόσβαση στα email αν δεν υπάρχει σαφής λόγος.

Τακτικός έλεγχος αδειών

Ελέγχετε τις συνδεδεμένες εφαρμογές κάθε τρίμηνο. Στο Google: myaccount.google.com → Ασφάλεια → Εφαρμογές τρίτων με πρόσβαση.

Ρυθμίσεις προώθησης και κανόνων

Η αυτόματη προώθηση email και οι κρυφοί κανόνες (Rules/Filters) είναι μια από τις πιο συχνές τακτικές που χρησιμοποιούν επιτιθέμενοι μετά από παραβίαση λογαριασμού — για να παρακολουθούν αθόρυβα την αλληλογραφία.

Τι να αναζητήσετε

- Κανόνες που προωθούν αυτόματα email σε εξωτερικές διευθύνσεις
- Φίλτρα που σημειώνουν μηνύματα ως αναγνωσμένα ή τα μεταφέρουν σε φάκελο
- Ρυθμίσεις SMTP relay που δεν έχετε ορίσει εσείς

Πού να ελέγξετε

- **Gmail:** Ρυθμίσεις → Φίλτρα και αποκλεισμένες διευθύνσεις + Προώθηση/POP/IMAP
- **Outlook:** Ρυθμίσεις → Αλληλογραφία → Κανόνες
- **Microsoft 365 Admin:** Security & Compliance Center → Mail flow rules

⚠ Οποιοσδήποτε κανόνας προωθεί email εκτός οργανισμού χωρίς τεκμηριωμένη επιχειρηματική αιτιολογία πρέπει να απενεργοποιείται άμεσα.

Ειδοποιήσεις ασφαλείας

Οι ειδοποιήσεις ασφαλείας λειτουργούν ως πρώτη γραμμή άμυνας σε πραγματικό χρόνο. Επιτρέπουν την έγκαιρη ανίχνευση ύποπτης δραστηριότητας πριν η ζημιά γίνει μη αναστρέψιμη.

Ειδοποιήσεις σύνδεσης

Ενεργοποιήστε ειδοποιήσεις για κάθε νέα σύνδεση από άγνωστη συσκευή ή τοποθεσία. Λαμβάνετε ειδοποίηση μέσω email ή push notification.

Έλεγχος νέων συσκευών

Κάθε νέα συσκευή που αποκτά πρόσβαση στον λογαριασμό πρέπει να επιβεβαιώνεται από εσάς. Μη εγκεκριμένες συσκευές να αποκλείονται αυτόματα.

Αναφορά ύποπτης δραστηριότητας

Εκπαιδεύστε τους χρήστες να αναφέρουν άμεσα κάθε ασυνήθιστη ειδοποίηση στο τμήμα IT — ακόμα και αν δεν φαίνεται σοβαρή.

Ρυθμίσεις απορρήτου

Πολλές πλατφόρμες email εκθέτουν από προεπιλογή πληροφορίες σχετικά με τον χρήστη — όνομα, φωτογραφία, κατάσταση online, ακόμα και γεωγραφική τοποθεσία. Ο περιορισμός αυτών των πληροφοριών μειώνει την επιφάνεια κοινωνικής μηχανικής (social engineering).

→ Απόκρυψη προσωπικών πληροφοριών

Αφαιρέστε ή αποκρύψτε στοιχεία όπως αριθμό τηλεφώνου, εικόνα προφίλ και τίτλο εργασίας από το δημόσιο προφίλ του λογαριασμού.

→ Περιορισμός κοινοποίησης στοιχείων

Ρυθμίστε ποιοι μπορούν να βλέπουν την κατάσταση «online», το ιστορικό δραστηριότητας ή τα στοιχεία επικοινωνίας σας. Περιορίστε σε «Μόνο Οργανισμός» ή «Μόνο Επαφές».

→ Έλεγχος δικαιωμάτων εφαρμογών

Επανεξετάστε ποιες εφαρμογές έχουν δικαίωμα ανάγνωσης επαφών, ημερολογίου ή αρχείων. Ακόμα και εφαρμογές παραγωγικότητας μπορεί να συλλέγουν περισσότερα δεδομένα από ό,τι χρειάζεται.

Προστασία εταιρικών λογαριασμών

Οι εταιρικοί λογαριασμοί απαιτούν πρόσθετα στρώματα προστασίας πέρα από τις βασικές ρυθμίσεις. Η ολιστική προσέγγιση συνδυάζει ισχυρά διαπιστευτήρια, σωστή διαχείριση κωδικών και ασφαλές περιβάλλον εργασίας.

🔐 Ισχυροί & μοναδικοί κωδικοί

Χρησιμοποιήστε κωδικούς τουλάχιστον 16 χαρακτήρων με συνδυασμό γραμμάτων, αριθμών και ειδικών χαρακτήρων. Ποτέ ίδιος κωδικός σε δύο υπηρεσίες.

🗝️ Password manager

Εργαλεία όπως Bitwarden, 1Password ή KeePass επιτρέπουν τη διαχείριση εκατοντάδων μοναδικών κωδικών με ασφάλεια — χωρίς την ανάγκη απομνημόνευσης.

🔄 Τακτικές ενημερώσεις

Διατηρείτε πάντα ενημερωμένο το λειτουργικό σύστημα και τον browser. Οι ενημερώσεις ασφαλείας κλείνουν γνωστές ευπάθειες που εκμεταλλεύονται επιτιθέμενοι.

🌐 VPN όταν απαιτείται

Χρησιμοποιείτε VPN εταιρικής εμπιστοσύνης όταν εργάζεστε από δημόσια δίκτυα Wi-Fi ή απομακρυσμένες τοποθεσίες.

Checklist ασφάλειας email

Χρησιμοποιήστε την παρακάτω λίστα ως οδηγό ελέγχου για κάθε λογαριασμό στον οργανισμό σας. Συνιστάται επαλήθευση τουλάχιστον κάθε τρίμηνο.

Βασικά μέτρα

- [x] MFA ενεργοποιημένο (Authenticator ή Passkey)
- [x] Έλεγχος και ενημέρωση επιλογών ανάκτησης
- [x] Αποσύνδεση άγνωστων συνδεδεμένων συσκευών
- [x] Αφαίρεση ανενεργών εφαρμογών τρίτων

Προχωρημένος έλεγχος

- [x] Έλεγχος κανόνων προώθησης και φίλτρων
- [x] Ενεργοποιημένες ειδοποιήσεις ασφαλείας
- [x] Ρυθμίσεις απορρήτου περιορισμένες
- [x] Ισχυροί κωδικοί μέσω Password Manager
- [x] Ενημερωμένο λειτουργικό και browser

Ο συστηματικός έλεγχος αυτής της λίστας μειώνει σημαντικά την πιθανότητα παραβίασης και διασφαλίζει συμμόρφωση με βέλτιστες πρακτικές ασφάλειας.