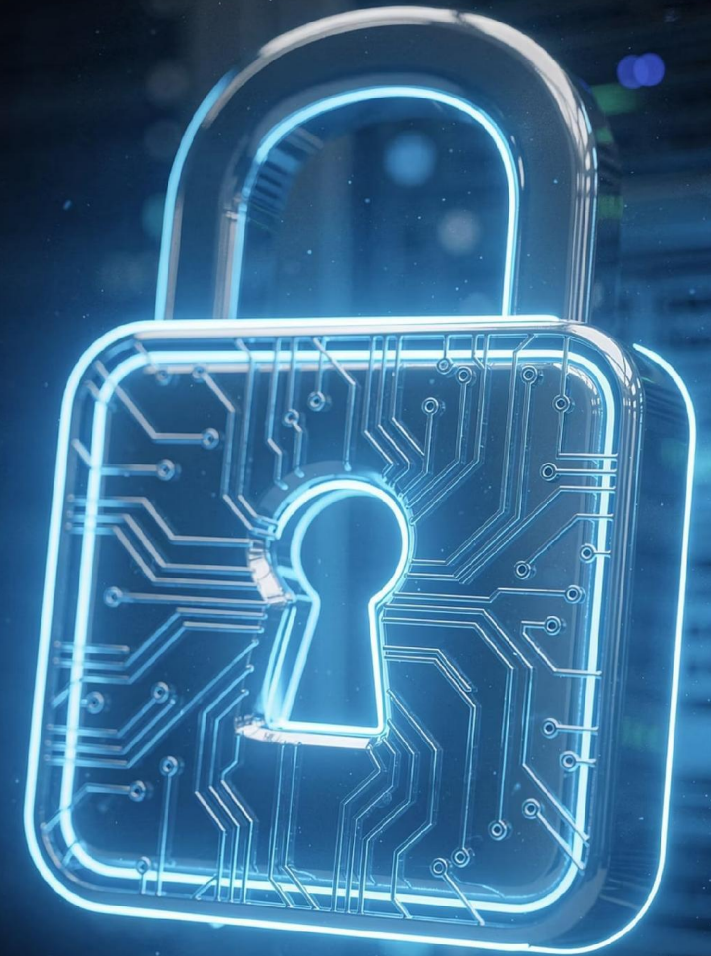


Ασφαλείς κωδικοί πρόσβασης, Password managers, OTP, Authenticators και MFA

Βέλτιστες πρακτικές για την προστασία λογαριασμών και εταιρικών δεδομένων. Μάθετε πώς να θωρακίσετε την επιχείρησή σας από τις πιο συχνές επιθέσεις στα διαπιστευτήρια χρηστών.



Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης



Γιατί οι κωδικοί είναι στόχος

Οι κωδικοί πρόσβασης αποτελούν την πιο συνηθισμένη πύλη εισόδου για επιτιθέμενους. Η κλοπή διαπιστευτηρίων είναι το πρώτο βήμα στην πλειονότητα των παραβιάσεων εταιρικών δεδομένων.

Επαναχρησιμοποίηση κωδικών

Το 85% των χρηστών χρησιμοποιεί τον ίδιο κωδικό σε πολλαπλές υπηρεσίες. Μία παραβίαση αρκεί για να εκτεθούν όλοι οι λογαριασμοί.

Phishing

Οι χρήστες εξαπατώνται μέσω ψεύτικων email ή ιστοσελίδων ώστε να αποκαλύψουν τα διαπιστευτήριά τους σε κακόβουλους παράγοντες.

Διαρροές δεδομένων

Εκατομμύρια κωδικοί κυκλοφορούν στο dark web από προηγούμενες παραβιάσεις γνωστών πλατφορμών και υπηρεσιών.

Πώς κλέβονται οι κωδικοί

Υπάρχουν πολλές μέθοδοι που χρησιμοποιούν οι κυβερνοεγκληματίες για να αποκτήσουν πρόσβαση στα διαπιστευτήριά σας. Η γνώση τους είναι το πρώτο βήμα για την προστασία σας.



Phishing

Ψεύτικα email και ιστοσελίδες που μιμούνται αξιόπιστες υπηρεσίες για την υποκλοπή διαπιστευτηρίων.



Malware & keyloggers

Κακόβουλο λογισμικό που καταγράφει πληκτρολογήσεις ή υποκλέπτει κωδικούς απευθείας από τον browser.



Δημόσιο Wi-Fi

Σε μη κρυπτογραφημένα δίκτυα, τα δεδομένα μπορούν να υποκλαπούν από τρίτους που βρίσκονται στο ίδιο δίκτυο.



Shoulder surfing

Παρατήρηση της πληκτρολόγησης κωδικών σε δημόσιους χώρους, όπως καφετέριες ή αεροδρόμια.



Data breaches

Παραβιάσεις εταιρικών βάσεων δεδομένων που εκθέτουν εκατομμύρια κωδικούς σε κακόβουλους παράγοντες.

Τύποι επιθέσεων κωδικών

Οι επιτιθέμενοι χρησιμοποιούν αυτοματοποιημένες τεχνικές για να σπάσουν κωδικούς σε ελάχιστο χρόνο. Η κατανόηση αυτών των μεθόδων εξηγεί γιατί η πολυπλοκότητα και η μοναδικότητα κάθε κωδικού είναι κρίσιμη.

#ΒΙΑΙΗ ΕΠΙΘΕΣΗ#



#ΛΕΞΙΚΟΓΡΑΦΙΚΗ ΕΠΙΘΕΣΗ#



#ΔΙΑΣΠΟΡΑ ΚΩΔΙΚΩΝ#



#ΠΑΡΑΒΙΑΣΗ ΔΕΔΟΜΕΝΩΝ#



Αδύναμοι vs Ισχυροί κωδικοί

Η επιλογή κωδικού είναι η πρώτη γραμμή άμυνας. Παρακάτω βλέπετε τη διαφορά μεταξύ κωδικών που παραβιάζονται σε δευτερόλεπτα και κωδικών που απαιτούν χρόνια.

Αδύναμοι Κωδικοί

- **password123** — από τους πιο κοινούς παγκοσμίως
- **Company2026** — προβλέψιμος, βασισμένος σε δεδομένα
- **12345678** — σπάει σε κλάσματα δευτερολέπτου
- **Όνομα + ημερομηνία** — εύκολα μαντεύσιμος από κοινωνική μηχανική

Ισχυροί Κωδικοί

- **Μοναδικός κωδικός** — διαφορετικός για κάθε υπηρεσία
- **Passphrase** — συνδυασμός άσχετων λέξεων, π.χ. Πορτοκάλι! Βουνό#Θάλασσα
- **Τυχαίος κωδικός** — 16+ χαρακτήρες με σύμβολα και αριθμούς
- **Δημιουργημένος από Password Manager** — η ασφαλέστερη επιλογή

Χρόνος παραβίασης κωδικού

Ο χρόνος που απαιτείται για να σπάσει ένας κωδικός εξαρτάται άμεσα από το μήκος και την πολυπλοκότητά του. Τα σύγχρονα συστήματα μπορούν να δοκιμάζουν **δισεκατομμύρια** συνδυασμούς ανά δευτερόλεπτο.

<1s

Απλοί κωδικοί

Κωδικοί όπως "123456" ή "password" παραβιάζονται σε λιγότερο από ένα δευτερόλεπτο.

11h

8 χαρακτήρες

Ένας τυχαίος κωδικός 8 χαρακτήρων με ανάμεικτους χαρακτήρες παραβιάζεται σε λίγες ώρες.

300+yr

12–16 χαρακτήρες

Ένας σύνθετος κωδικός 12–16 χαρακτήρων απαιτεί εκατοντάδες χρόνια για να παραβιαστεί.

∞

20+ τυχαίοι

Ένας τυχαίος κωδικός 20+ χαρακτήρων είναι πρακτικά αδύνατο να παραβιαστεί με brute force.





Τι είναι ένα passphrase;

Ένα passphrase είναι μια σειρά από **4–5 τυχαίες, άσχετες μεταξύ τους λέξεις** που σχηματίζουν έναν κωδικό. Είναι εξαιρετικά δύσκολο να παραβιαστεί, ενώ παράλληλα παραμένει εύκολο στην απομνημόνευση

❏ Παράδειγμα passphrase: **Πορτοκάλι!Βουνό#Θάλασσα2026** — 28 χαρακτήρες, εύκολο να θυμάστε, εξαιρετικά δύσκολο να σπάσει.

Γιατί λειτουργεί;

- Μεγάλο μήκος χωρίς προσπάθεια απομνημόνευσης
- Οι τυχαίες λέξεις δεν ακολουθούν κανένα μοτίβο
- Η προσθήκη συμβόλων αυξάνει δραματικά την πολυπλοκότητα

Σε σχέση με τον παραδοσιακό κωδικό;

- Πιο εύκολο να θυμάστε από τυχαίους χαρακτήρες
- Πολύ μεγαλύτερο μήκος από τυπικούς κωδικούς
- Ιδανικό για master password σε Password Manager

Δημιουργία ισχυρού passphrase

Ακολουθήστε αυτά τα τέσσερα βήματα για να δημιουργήσετε ένα passphrase που θα σας προστατεύει αποτελεσματικά, χωρίς να χρειαστεί να το σημειώσετε πουθενά.

Προσθέστε αριθμούς

Βάλτε αριθμούς ανάμεσα ή στο τέλος.

Προσθέστε σύμβολα

Χρησιμοποιήστε ! # @ για πολυπλοκότητα.

Επιλέξτε λέξεις

4–5 άσχετες λέξεις, π.χ. πορτοκάλι βουνό θάλασσα.

Χρήση μίας φορές

Χρησιμοποιήστε το μόνο για μία υπηρεσία.

Θυμηθείτε: ένα passphrase χρησιμοποιείται **μόνο μία φορά**. Για κάθε υπηρεσία, δημιουργήστε διαφορετικό. Ένας Password Manager αναλαμβάνει να τα θυμάται για εσάς.



Γιατί δεν πρέπει να επαναχρησιμοποιούμε κωδικούς

Η επαναχρησιμοποίηση κωδικών είναι μία από τις πιο επικίνδυνες συνήθειες στον ψηφιακό κόσμο. Όταν μία υπηρεσία παραβιαστεί, **όλοι οι λογαριασμοί σας με τον ίδιο κωδικό τίθενται σε κίνδυνο.**

- Παραβίαση κάποιας υπηρεσίας
Μια γνωστή πλατφόρμα παραβιάζεται και ο κωδικός σας εκτίθεται στο dark web.
- Credential Stuffing
Αυτοματοποιημένα εργαλεία δοκιμάζουν τα κλεμμένα διαπιστευτήρια σε δεκάδες άλλες υπηρεσίες.
- Πρόσβαση σε εταιρικά συστήματα
Εάν ο ίδιος κωδικός χρησιμοποιείται και για εταιρικό email ή VPN, ο επιτιθέμενος αποκτά πλήρη πρόσβαση.

Τι είναι ένας Password Manager;

Ένας Password manager είναι ένα εξειδικευμένο εργαλείο που αποθηκεύει και διαχειρίζεται με ασφάλεια όλους τους κωδικούς πρόσβασής σας. Χρειάζεται να θυμάστε **μόνο έναν master κωδικό** — τον υπόλοιπο κόσμο τον διαχειρίζεται ο manager.



Δημιουργία

Παράγει αυτόματα ισχυρούς, τυχαίους κωδικούς μεγάλου μήκους για κάθε υπηρεσία.



Κρυπτογραφημένη αποθήκευση

Όλοι οι κωδικοί αποθηκεύονται κρυπτογραφημένοι. Ακόμα και αν παραβιαστεί ο manager, τα δεδομένα είναι αναγνώσιμα μόνο με τον master κωδικό.



Αυτόματη συμπλήρωση

Αναγνωρίζει τις ιστοσελίδες και συμπληρώνει αυτόματα τα διαπιστευτήρια χωρίς χειροκίνητη εισαγωγή.



Συγχρονισμός

Διαθέσιμος σε όλες τις συσκευές σας — υπολογιστή, κινητό, tablet — με πλήρη συγχρονισμό.

Παραδείγματα Password Managers



Bitwarden



1Password



Dashlane



Proton Pass



Πολλοί browsers (Chrome, Safari, Firefox) και smartphones προσφέρουν επίσης βασικό password management.

Επίδειξη password manager

Ας δούμε βήμα προς βήμα πώς λειτουργεί στην πράξη ένας Password Manager στην καθημερινή εταιρική χρήση.



Δημιουργία

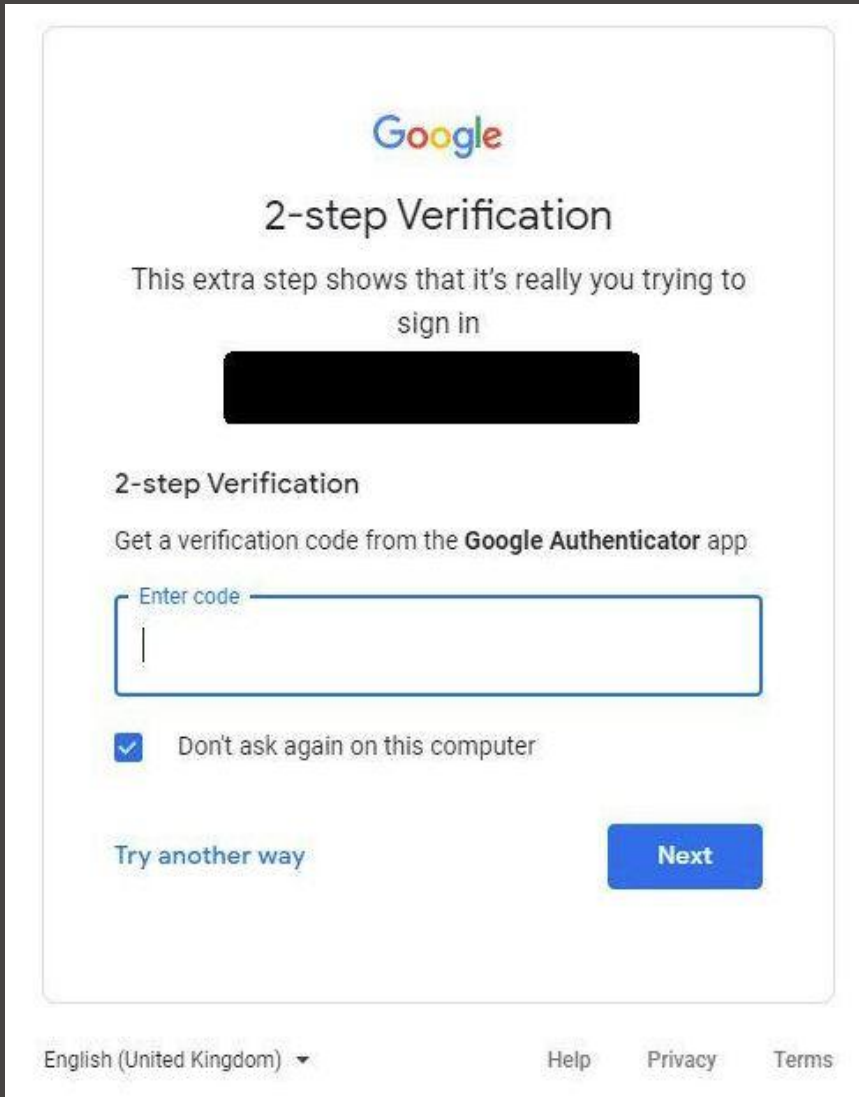
Αποθήκευση

Αυτόματη
συμπλήρωση

Ασφαλής
κοινή χρήση

Η **ασφαλής κοινή χρήση** είναι ιδιαίτερα σημαντική σε εταιρικά περιβάλλοντα: μοιραστείτε πρόσβαση χωρίς να αποκαλύψετε ποτέ τον πραγματικό κωδικό σε συναδέλφους.

Two-Factor Authentication



The screenshot shows the Google 2-step Verification process. At the top is the Google logo, followed by the text "2-step Verification". Below this, it says "This extra step shows that it's really you trying to sign in" with a blacked-out area representing the user's name. The section is titled "2-step Verification" again, with the instruction "Get a verification code from the Google Authenticator app". There is a text input field labeled "Enter code" with a cursor. Below the field is a checked checkbox labeled "Don't ask again on this computer". At the bottom left is a link "Try another way" and at the bottom right is a blue "Next" button. The footer contains "English (United Kingdom)" with a dropdown arrow, and links for "Help", "Privacy", and "Terms".

- Το **2FA (Two-Factor Authentication)** είναι ένα σύστημα ασφαλείας που απαιτεί δύο διαφορετικά βήματα επαλήθευσης για να συνδεθείς σε έναν λογαριασμό.
- Εκτός από το password, χρειάζεται επίσης:
 - One Time Password (OTP) μέσω SMS ή email
 - Push notification στο κινητό
 - Επιβεβαίωση μέσω authenticator app
 - Βιομετρική επαλήθευση (δακτυλικό αποτύπωμα)
- **Ακόμα και αν κάποιος κλέψει το password, δεν μπορεί να συνδεθεί χωρίς το δεύτερο βήμα.**



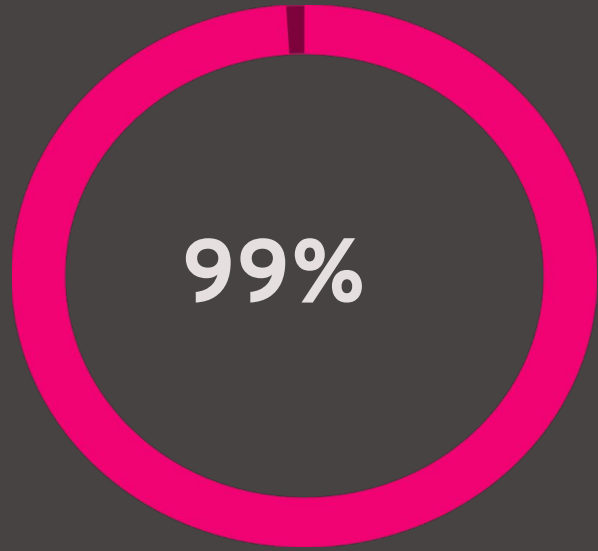
Γιατί είναι σημαντικό το 2FA;

Προστασία από κλεμμένα passwords: ακόμα και αν το password σου εμπλακεί σε υποκλοπή προσωπικών δεδομένων, το 2FA εμποδίζει κάθε προσπάθεια σύνδεσης από τρίτους.

Άμυνα κατά phishing: σε περίπτωση που κάποιος μπει σε ψεύτικη σελίδα και δώσει τον κωδικό του, ο επιτιθέμενος δεν μπορεί να προχωρήσει χωρίς το 2FA.

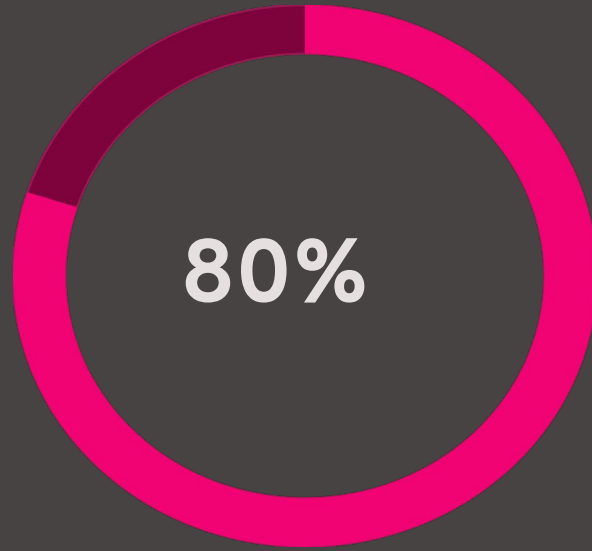
Ευρεία υποστήριξη: σχεδόν κάθε μεγάλη πλατφόρμα (Gmail, Instagram, TikTok, Discord, Facebook, Microsoft) υποστηρίζει πλέον ενεργοποίηση 2FA.

2FA & Modern Cybersecurity



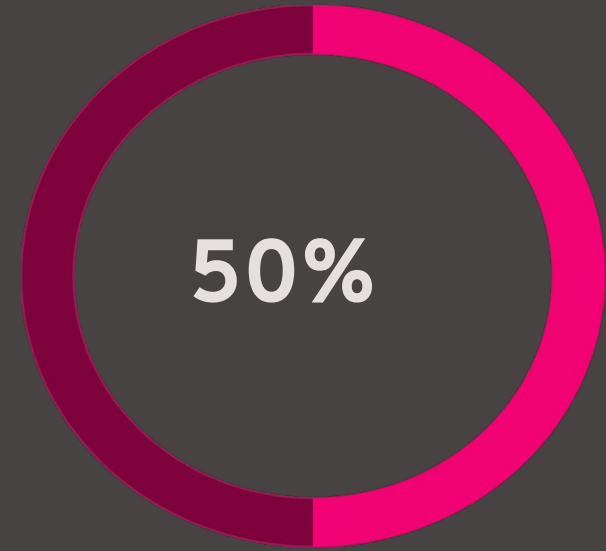
Αποτροπή Επιθέσεων

Σύμφωνα με τη Microsoft, το MFA μπλοκάρει πάνω από το 99% των αυτοματοποιημένων επιθέσεων σε λογαριασμούς.



Credential Stuffing

Περίπου 8 στις 10 παραβιάσεις βασίζονται σε κλεμμένα ή επαναχρησιμοποιημένα credentials — ακριβώς αυτό που το 2FA αντιμετωπίζει.



Μειωμένος Κίνδυνος

Ακόμα και η απλούστερη μορφή 2FA (SMS) μειώνει σημαντικά τον κίνδυνο παραβίασης σε σχέση με μόνο password.

OTP – One Time Password



- Το OTP είναι ένας **προσωρινός κωδικός μιας χρήσης** που αποστέλλεται αυτόματα για να επιβεβαιώσει μια σύνδεση ή συναλλαγή. Ισχύει μόνο για λίγα δευτερόλεπτα ή λεπτά και αχρηστεύεται αμέσως μετά τη χρήση του.
- Παραδίδεται
 - Με SMS στο κινητό
 - Με Email
 - Μέσω Authenticator app (π.χ. Google/ Microsoft Authenticator)



Γιατί είναι σημαντικό το OTP;

- Το OTP εμποδίζει την μη εξουσιοδοτημένη πρόσβαση σε Gmail, Instagram, Facebook και άλλες πλατφόρμες, ακόμα και αν το password είναι γνωστό.
- Οι τράπεζες χρησιμοποιούν OTP για κάθε συναλλαγή, εξασφαλίζοντας ότι μόνο ο πραγματικός κάτοχος του λογαριασμού μπορεί να εγκρίνει πληρωμές.
- Σε όλες τις online υπηρεσίες το OTP χρησιμοποιείται ευρέως ως επιπλέον επίπεδο επαλήθευσης ταυτότητας.

Το password μόνο του δεν αρκεί πλέον. Το OTP είναι το επιπλέον βήμα που κάνει τη διαφορά.

OTP & Online απάτες

Phishing emails: Ψεύτικα emails που μοιάζουν από τράπεζες ή γνωστές υπηρεσίες σε ζητούν να "επιβεβαιώσεις" τα στοιχεία σου και να δώσεις το OTP σου.

Smishing (SMS απάτες): Ψεύτικα SMS με συνδέσμους που οδηγούν σε σελίδες όπου σου ζητείται ο κωδικός επαλήθευσης.

Fake support calls: Κάποιος προσποιείται υπάλληλο υποστήριξης τράπεζας ή εταιρείας και ζητά το OTP για να "επιλύσει" ένα πρόβλημα.

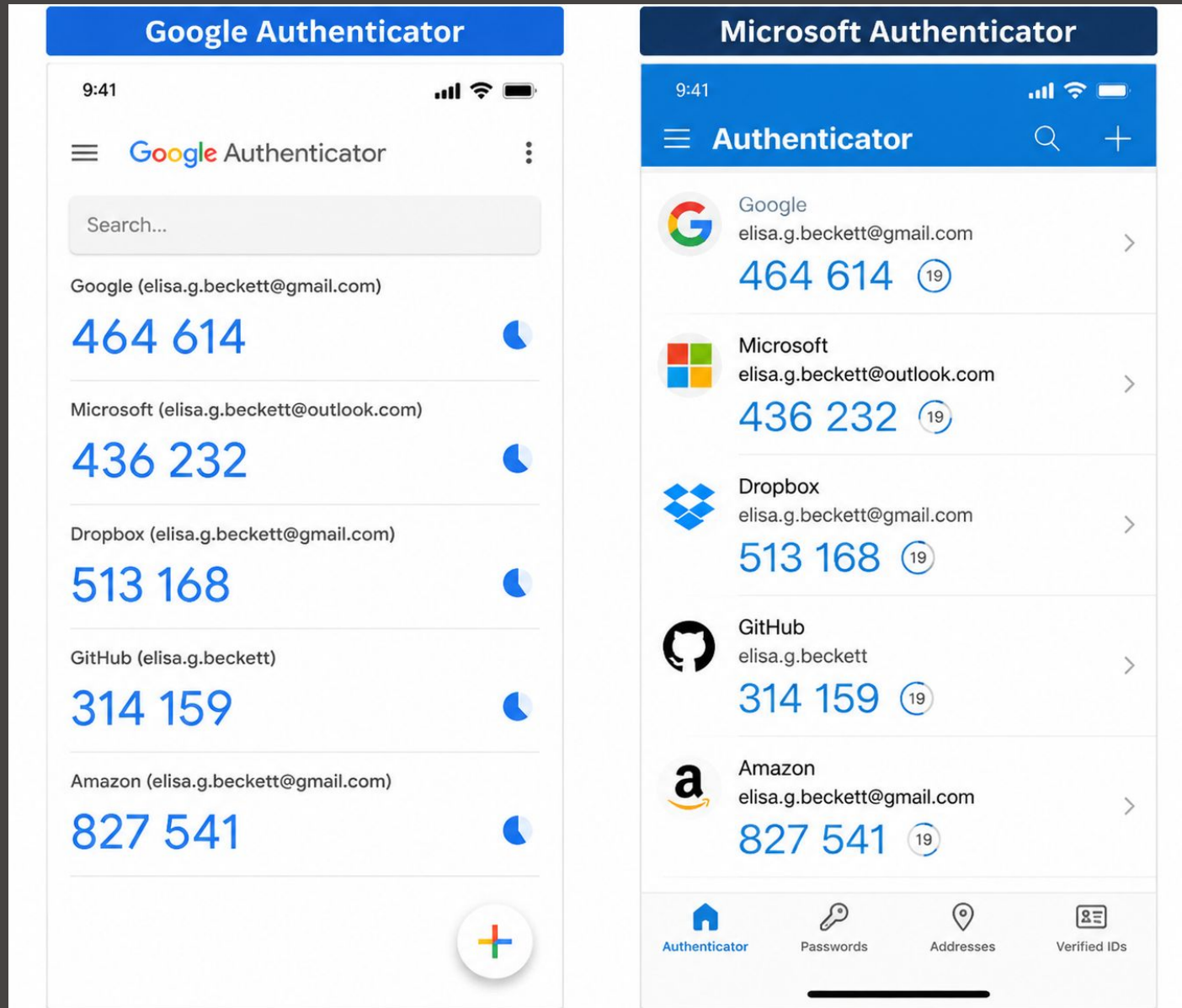


Κανείς δεν έχει λόγο να σου ζητήσει OTP. Μην το μοιράζεσαι ποτέ — ούτε σε τηλεφωνικές κλήσεις, ούτε σε SMS, ούτε σε email.

Τι είναι τα Password Authenticators;

- Οι εφαρμογές authenticator αποτελούν ένα επιπλέον επίπεδο προστασίας για τους ψηφιακούς λογαριασμούς. Δημιουργούν αυτόματα προσωρινούς κωδικούς ασφαλείας (OTPs) που χρησιμοποιούνται για την επιβεβαίωση της ταυτότητας κατά τη σύνδεση.
- Αντί για SMS, η εφαρμογή δημιουργεί έναν νέο μοναδικό κωδικό κάθε 30 δευτερόλεπτα. Ο κωδικός αυτός είναι έγκυρος μόνο για το συγκεκριμένο χρονικό διάστημα και δεν μπορεί να επαναχρησιμοποιηθεί.
- Ακόμα και αν κάποιος γνωρίζει το password, δεν μπορεί να συνδεθεί χωρίς τον προσωρινό κωδικό που παράγεται αποκλειστικά από τη συσκευή του χρήστη. Το password μόνο του δεν αρκεί πλέον.
- Κάθε φορά που συνδέεται, το σύστημα ζητά και τον κωδικό από την εφαρμογή. Έτσι, επιβεβαιώνεται ότι η σύνδεση γίνεται από τον πραγματικό χρήστη και όχι από κάποιον άλλο.

Δημοφιλείς Password Authenticator εφαρμογές



Τι είναι το MFA;

Ο Πολυπαραγοντικός Έλεγχος Ταυτότητας (MFA) προσθέτει ένα επιπλέον επίπεδο ασφάλειας πέρα από τον κωδικό. Ακόμα και αν κλαπεί ο κωδικός σας, ο επιτιθέμενος δεν μπορεί να συνδεθεί χωρίς τον δεύτερο παράγοντα.

ΠΑΡΑΓΟΝΤΕΣ ΓΝΩΣΗΣ & ΚΑΤΟΧΗΣ



Κάτι που γνωρίζω
(π.χ. κωδικός
πρόσβασης)

Κάτι που έχω
(π.χ. smartphone,
token)

ΠΑΡΑΓΟΝΤΕΣ ΕΙΝΑΙ (ΒΙΟΜΕΤΡΙΚΑ)



Κάτι που είμαι
(π.χ. δακτυλικό αποτύπωμα,
πρόσωπο)

Η ενεργοποίηση MFA μειώνει τον κίνδυνο παραβίασης λογαριασμού κατά **περισσότερο από 99%** σύμφωνα με έρευνες της Microsoft.

SMS OTP, Authenticator Apps και Passkeys

Δεν είναι όλες οι μέθοδοι MFA εξίσου ασφαλείς. Επιλέξτε την κατάλληλη μέθοδο ανάλογα με το επίπεδο ασφάλειας που απαιτεί η επιχείρησή σας.



SMS OTP

Εύκολο, αλλά λιγότερο ασφαλές. Ευάλωτο σε SIM-swapping και υποκλοπή. Αποδεκτό ως ελάχιστο επίπεδο προστασίας, αλλά όχι προτεινόμενο για υψηλής αξίας λογαριασμούς.



Authenticator Apps

Η προτεινόμενη λύση. Εφαρμογές όπως Google Authenticator, Microsoft Authenticator ή Aegis παράγουν κωδικούς μίας χρήσης (TOTP) τοπικά, χωρίς δικτυακή εξάρτηση.



Passkeys

Η σύγχρονη προστασία. Βασίζονται σε κρυπτογραφία δημόσιου κλειδιού. Δεν υπάρχει κωδικός να κλαπεί — η πιστοποίηση γίνεται με βιομετρικά ή PIN της συσκευής.

Τι είναι τα Passkeys;

Τα Passkeys αντικαθιστούν πλήρως τους παραδοσιακούς κωδικούς. Χρησιμοποιούν κρυπτογραφία δημόσιου-ιδιωτικού κλειδιού: **το ιδιωτικό κλειδί παραμένει πάντα στη συσκευή σας και δεν μεταδίδεται ποτέ στον διακομιστή.**



Βασίζονται στο FIDO2

Διεθνές πρότυπο ασφαλείας υποστηριζόμενο από Google, Apple, Microsoft και εκατοντάδες άλλες εταιρείες.



Βιομετρικά ή PIN

Η επαλήθευση γίνεται με δακτυλικό αποτύπωμα, αναγνώριση προσώπου ή PIN συσκευής — γρήγορα και εύκολα.



Ανθεκτικά στο Phishing

Επειδή δεν υπάρχει κωδικός να υποκλαπεί, τα passkeys είναι θεμελιωδώς ανθεκτικά σε phishing επιθέσεις.



Phishing Fatigue — Η Κόπωση του MFA

Η Phishing Fatigue (ή MFA Fatigue) είναι μια εξελιγμένη τεχνική κοινωνικής μηχανικής. Ο επιτιθέμενος στέλνει **συνεχόμενα αιτήματα έγκρισης MFA** μέχρι ο χρήστης, από κούραση ή σύγχυση, να εγκρίνει κατά λάθος.

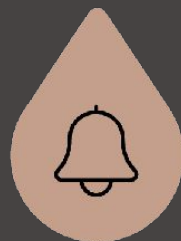
Κλεμμένος κωδικός

Ο επιτιθέμενος κατέχει τον κωδικό πρόσβασης



Λανθασμένη έγκριση

Ο χρήστης εγκρίνει κατά λάθος και χάνεται ο έλεγχος



Επιμονή ειδοποιήσεων

Επαναλαμβανόμενα αιτήματα έγκρισης MFA



Κανόνας: Ποτέ μην εγκρίνετε αίτημα MFA που δεν ξεκινήσατε εσείς. Αν λάβετε απρόσμενη ειδοποίηση, αλλάξτε κωδικό αμέσως και ειδοποιήστε το IT.

MFA Bombing

Το MFA Bombing είναι η εντατική εκδοχή της Phishing Fatigue. Ο επιτιθέμενος χρησιμοποιεί αυτοματοποιημένα εργαλεία για να πλημμυρίσει τη συσκευή του θύματος με δεκάδες ειδοποιήσεις εντός λεπτών.

Μαζικές ειδοποιήσεις

Δεκάδες push notifications αποστέλλονται αυτόματα, δημιουργώντας πανικό και σύγχυση στον χρήστη.

Ψυχολογική πίεση

Στόχος είναι να κουράσει τον χρήστη ώστε να εγκρίνει απλά «για να σταματήσουν» οι ειδοποιήσεις.

Η σωστή αντίδραση

Ποτέ μην εγκρίνετε άγνωστο αίτημα. Αγνοήστε τις ειδοποιήσεις, κλειδώστε τον λογαριασμό και επικοινωνήστε με το IT τμήμα αμέσως.



Πραγματικά περιστατικά κυβερνοεπιθέσεων

Οι παρακάτω υποθέσεις δείχνουν ότι ακόμα και μεγάλες εταιρείες με πόρους δεν είναι άτρωτες. Κάθε περιστατικό κρύβει ένα διδακτικό μάθημα για τις επιχειρήσεις.



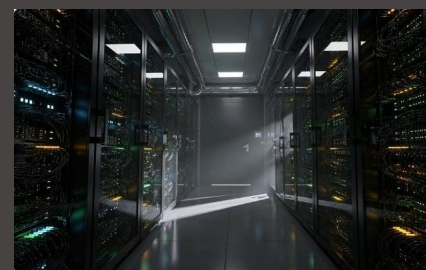
Uber (2022)

Επίθεση μέσω social engineering σε contractor. Ο επιτιθέμενος χρησιμοποίησε MFA Bombing για να αποκτήσει πρόσβαση σε εσωτερικά συστήματα.



Colonial pipeline

Ransomware μέσω κλεμμένου κωδικού VPN χωρίς MFA. Αποτέλεσμα: διακοπή τροφοδοσίας καυσίμων στις ανατολικές ΗΠΑ και λύτρα \$4.4 εκ.



LastPass

Παραβίαση του ίδιου του Password Manager. Κλάπηκαν κρυπτογραφημένα vaults — υπενθύμιση ότι ο master κωδικός πρέπει να είναι εξαιρετικά ισχυρός.

Βέλτιστες πρακτικές για επιχειρήσεις

Εφαρμόστε αυτές τις πρακτικές στην επιχείρησή σας για να δημιουργήσετε μια ισχυρή πρώτη γραμμή άμυνας έναντι κυβερνοεπιθέσεων.



Χρησιμοποιήστε Password Manager

Αναπτύξτε εταιρικό Password Manager για όλους τους εργαζομένους. Εξαλείψτε τη χρήση κοινών ή αδύναμων κωδικών.



Ενεργοποιήστε MFA παντού

Email, VPN, cloud services, ERP — κανένα κρίσιμο σύστημα χωρίς MFA. Προτιμήστε Authenticator Apps έναντι SMS.



Μοναδικός κωδικός ανά υπηρεσία

Κανένας κωδικός δεν χρησιμοποιείται δύο φορές. Ο Password Manager το διαχειρίζεται αυτόματα.



Έλεγχος διαρροών

Χρησιμοποιήστε υπηρεσίες όπως HaveIBeenPwned για να ελέγχετε τακτικά αν εταιρικά email έχουν εκτεθεί σε παραβιάσεις.



Ενημέρωση λογισμικού

Διατηρείτε ενημερωμένα λειτουργικά συστήματα, browsers και εφαρμογές. Πολλές παραβιάσεις εκμεταλλεύονται γνωστές ευπάθειες.

Σύνοψη & ερωτήσεις

Καλύψαμε τα βασικά εργαλεία και πρακτικές για την ασφάλεια των εταιρικών σας λογαριασμών. Εφαρμόστε τα σήμερα — η κυβερνοασφάλεια ξεκινά με μικρές, συνεπείς αλλαγές.

Ισχυροί κωδικοί

Μακριά, μοναδικά, με passphrases ή τυχαίους χαρακτήρες.

Password Manager

Ένας κωδικός για να τους κυβερνά όλους — ο master κωδικός.

MFA / Passkeys

Δεύτερο επίπεδο προστασίας σε κάθε κρίσιμο σύστημα.

Επαγρύπνηση

Ποτέ μην εγκρίνετε αίτημα MFA που δεν ξεκινήσατε εσείς.

