Ασφαλής περιήγηση στο Διαδίκτυο

Ένας πρακτικός οδηγός για την προστασία σας κατά την πλοήγηση στο διαδίκτυο — από τις βασικές ρυθμίσεις του browser έως τις πιο συχνές παγίδες που θέτουν σε κίνδυνο τα δεδομένα σας.

🎯 Στόχος

Κατανόηση των κινδύνων και εφαρμογή σωστών ρυθμίσεων σε Chrome, Edge και Firefox.

👥 Για ποιους

Χρήστες διαδικτύου και επαγγελματίες πληροφορικής που θέλουν ασφαλέστερη εμπειρία.

✅ Αποτέλεσμα

Πρακτικές γνώσεις που μπορείτε να εφαρμόσετε άμεσα στον browser σας.

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry

safeLine.gr

ΙΤΕ
ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Γιατί η ασφαλής περιήγηση είναι σημαντική;

Κάθε φορά που ανοίγετε έναν browser, εκτίθεστε σε δεκάδες αόρατες απειλές. Τα προσωπικά σας δεδομένα, οι κωδικοί σας και η ταυτότητά σας μπορούν να τεθούν σε κίνδυνο σε δευτερόλεπτα.

🔐 Προστασία δεδομένων

Προσωπικές πληροφορίες, κωδικοί και οικονομικά στοιχεία μπορούν να υποκλαπούν από κακόβουλους τρίτους που παρακολουθούν την κυκλοφορία σας στο διαδίκτυο.

🎣 Phishing

Ψεύτικες ιστοσελίδες που μιμούνται τράπεζες, υπηρεσίες email ή κυβερνητικές υπηρεσίες προσπαθούν να αποσπάσουν τα διαπιστευτήριά σας.

🦠 Malware

Κακόβουλο λογισμικό μπορεί να εγκατασταθεί στον υπολογιστή σας χωρίς να το αντιληφθείτε, απλά επισκεπτόμενοι μια μολυσμένη ιστοσελίδα.

Κίνδυνοι από μη ασφαλείς ιστοσελίδες

Δεν χρειάζεται να κατεβάσετε κάτι για να μολυνθεί ο υπολογιστής σας. Οι σύγχρονες απειλές εκμεταλλεύονται αδυναμίες του ίδιου του browser.

Drive-by downloads

Αυτόματη λήψη κακόβουλου αρχείου μόλις φορτωθεί η σελίδα, χωρίς καμία ενέργεια από τον χρήστη.

Malvertising

Κακόβουλες διαφημίσεις σε νόμιμες ιστοσελίδες που ανακατευθύνουν σε επικίνδυνα sites ή εκτελούν scripts.

Fake updates

Ψεύτικα μηνύματα που σας καλούν να «ενημερώσετε» τον browser ή το Flash, εγκαθιστώντας στην πραγματικότητα malware.

Browser exploits

Εκμετάλλευση γνωστών ή άγνωστων αδυναμιών (zero-day) στον browser για απόκτηση πρόσβασης στο σύστημά σας.

Τι μπορεί να συμβεί;

Οι συνέπειες μιας ανασφαλούς περιήγησης μπορεί να είναι καταστροφικές — από οικονομική ζημία έως πλήρη απώλεια ελέγχου του συστήματός σας.

🔑 Κλοπή κωδικών

Keyloggers και phishing forms υποκλέπτουν τα διαπιστευτήριά σας για email, τράπεζες και υπηρεσίες.

💰 Ransomware

Τα αρχεία σας κρυπτογραφούνται και ζητείται λύτρα για την επαναφορά τους. Συχνά μέσω drive-by downloads.

🍪 Υποκλοπή cookies

Τα session cookies κλέβονται και χρησιμοποιούνται για πρόσβαση σε λογαριασμούς χωρίς κωδικό.

👁️ Παρακολούθηση

Trackers και spyware καταγράφουν τις κινήσεις σας, τις αγορές σας και ακόμα και τις πληκτρολογήσεις σας.

Αναγνώριση ασφαλών ιστοσελίδων

Πριν εισάγετε οποιοδήποτε προσωπικό στοιχείο σε μια ιστοσελίδα, ελέγξτε αυτά τα βασικά σημεία ασφαλείας.

1 HTTPS & λουκέτο

Βεβαιωθείτε ότι η διεύθυνση ξεκινά με **https://** και υπάρχει το εικονίδιο λουκέτου στη γραμμή διευθύνσεων. Το HTTP (χωρίς S) σημαίνει μη κρυπτογραφημένη σύνδεση.

2 Έλεγχος domain

Διαβάστε προσεκτικά το domain. Το **paypa1.com** δεν είναι το **paypal.com**. Ελέγξτε το TLD (.com, .gr) και αποφύγετε ύποπτα subdomains.

3 Πιστοποιητικό SSL

Κάντε κλικ στο λουκέτο για να δείτε λεπτομέρειες του πιστοποιητικού. Βεβαιωθείτε ότι εκδόθηκε για τον σωστό οργανισμό.

4 Typosquatting

Κακόβουλοι καταχωρούν domains με τυπογραφικά λάθη (π. χ. **goo**o**gle.com**) για να παγιδεύσουν χρήστες που πληκτρολογούν λανθασμένα.

Chrome – ρυθμίσεις ασφαλείας

Το Google Chrome διαθέτει ισχυρά ενσωματωμένα εργαλεία ασφαλείας. Ακολουθήστε αυτές τις συστάσεις για μέγιστη προστασία.

🟢 Προτεινόμενες ρυθμίσεις

- **Safe Browsing → Ενισχυμένη προστασία**: Ενεργοποιήστε την «Ενισχυμένη προστασία» στις Ρυθμίσεις → Απόρρητο & Ασφάλεια για προηγμένη ανίχνευση απειλών σε πραγματικό χρόνο.
- **HTTPS-Only Mode**: Ενεργοποιήστε στις Ρυθμίσεις → Ασφάλεια → Πάντα χρήση ασφαλών συνδέσεων.
- **Secure DNS**: Χρησιμοποιήστε DNS-over-HTTPS με παρόχους όπως το Cloudflare (1.1.1.1) ή το Google (8.8.8.8).

🔴 Μη προτεινόμενες ρυθμίσεις

- Απενεργοποίηση Safe Browsing — σας αφήνει εκτεθειμένους σε phishing και malware χωρίς προειδοποίηση.
- Αποδοχή HTTP χωρίς προειδοποίηση — επιτρέπει μη κρυπτογραφημένες συνδέσεις.
- Χρήση μη αξιόπιστου DNS — τα αιτήματά σας μπορούν να παρακολουθηθούν ή να ανακατευθυνθούν.

Διαδρομή: Chrome → Ρυθμίσεις → Απόρρητο και ασφάλεια → Ασφάλεια

Edge – Ρυθμίσεις ασφαλείας

Το Microsoft Edge προσφέρει μοναδικά εργαλεία ασφαλείας βαθιά ενσωματωμένα με το Windows Defender ecosystem.

🟢 Προτεινόμενες ρυθμίσεις

- **Microsoft Defender SmartScreen**: Ενεργοποιήστε για αυτόματο αποκλεισμό επικίνδυνων ιστοσελίδων και αρχείων. Ρυθμίσεις → Απόρρητο, αναζήτηση και υπηρεσίες → Ασφάλεια.
- **Tracking Prevention → Αυστηρό**: Αποκλείει trackers από ιστοσελίδες που δεν έχετε επισκεφτεί. Ρυθμίσεις → Απόρρητο → Πρόληψη παρακολούθησης.
- **Secure DNS**: Ενεργοποιήστε DNS-over-HTTPS με αξιόπιστο πάροχο.

🔴 Μη Προτεινόμενες ρυθμίσεις

- Απενεργοποίηση SmartScreen — αφαιρεί ένα κρίσιμο επίπεδο προστασίας κατά phishing.
- Tracking Prevention σε «Βασικό» — επιτρέπει στους περισσότερους trackers να λειτουργούν.
- Αποδοχή όλων των αιτημάτων cookie τρίτων χωρίς έλεγχο.

Διαδρομή: Edge → Ρυθμίσεις → Απόρρητο, αναζήτηση και υπηρεσίες

Firefox – Ρυθμίσεις ασφαλείας

Ο Firefox είναι γνωστός για την ισχυρή του δέσμευση στην προστασία της ιδιωτικότητας και προσφέρει από προεπιλογή πιο αυστηρές ρυθμίσεις από τους ανταγωνιστές.

🟢 Προτεινόμενες ρυθμίσεις

- **Enhanced Tracking Protection** → **Αυστηρό**: Αποκλείει trackers, crypto miners, fingerprinters και cookies παρακολούθησης. Ρυθμίσεις → Απόρρητο & Ασφάλεια.
- **HTTPS-Only Mode**: Ενεργοποιήστε «Μόνο HTTPS» και στα δύο παράθυρα (κανονικό και ιδιωτικό). Αποτρέπει τη σύνδεση σε μη ασφαλείς σελίδες.
- **DNS over HTTPS**: Χρησιμοποιήστε Max Protection με αξιόπιστο πάροχο.

🔴 Μη Προτεινόμενες ρυθμίσεις

- ETP σε «Τυπικό» ή «Απενεργοποιημένο» — αφήνει ανοιχτό το tracking και τους crypto miners.
- Απενεργοποίηση HTTPS-Only — επιτρέπει μη κρυπτογραφημένες συνδέσεις χωρίς προειδοποίηση.
- Χρήση προεπιλεγμένου συστήματος DNS χωρίς κρυπτογράφηση.

Διαδρομή: Firefox → Ρυθμίσεις → Απόρρητο & Ασφάλεια

Pop-ups & redirects

Τα pop-ups και τα αυτόματα redirects είναι από τους πιο κοινούς φορείς κακόβουλου περιεχομένου. Ο σωστός χειρισμός τους είναι απαραίτητος.

🟢 Σωστή αντιμετώπιση

- **Ενεργοποιήστε τον αποκλεισμό pop-ups** σε όλους τους browsers — είναι συνήθως ενεργός από προεπιλογή.
- **Αποκλείστε αυτόματα τα redirects**: Chrome/Edge/Firefox → Ρυθμίσεις → Δικαιώματα ιστοτόπου → Pop-ups και ανακατευθύνσεις → Αποκλεισμός.
- **Εξαιρέσεις μόνο για εμπιστευμένες σελίδες** (π.χ. εταιρικές εφαρμογές) που γνωρίζετε και χρειάζονται pop-ups για λειτουργικούς λόγους.

🔴 Τι να αποφύγετε

- Να κλικάρετε «Επιτρέψτε» σε pop-up αιτήματα από άγνωστες ιστοσελίδες.
- Να ακολουθείτε redirects από αναδυόμενα παράθυρα που ισχυρίζονται ότι «ο υπολογιστής σας είναι μολυσμένος».
- Να απενεργοποιείτε τον αποκλεισμό pop-ups γενικά για να λειτουργεί μία ιστοσελίδα.

Downloads & εκτελέσιμα αρχεία

Τα κακόβουλα αρχεία συχνά μεταμφιέζονται σε νόμιμα. Πριν ανοίξετε οποιοδήποτε αρχείο από το διαδίκτυο, γνωρίστε τις επικίνδυνες επεκτάσεις.

⚠️ Επικίνδυνες επεκτάσεις

.exe .msi .bat .cmd .scr .ps1 .js .vbs — Εκτελέσιμα αρχεία που μπορούν να τρέξουν κώδικα απευθείας στο σύστημά σας. Ποτέ μην τα ανοίγετε αν δεν γνωρίζετε 100% την πηγή.

🛡️ Έλεγχος με Windows Defender

Πριν ανοίξετε οποιοδήποτε ληφθέν αρχείο, κάντε δεξί κλικ → «Σάρωση με Microsoft Defender». Εναλλακτικά, χρησιμοποιήστε το **virustotal.com** για online σάρωση.

🟢 Προτεινόμενη πρακτική

Αποθηκεύστε πρώτα, σαρώστε μετά, ανοίξτε τελευταία. Προτιμήστε λήψεις απευθείας από επίσημες ιστοσελίδες.

🔴 Μη προτεινόμενη πρακτική

Λήψη εκτελέσιμων από email, forums ή άγνωστα sites. Άνοιγμα αρχείων χωρίς προηγούμενη σάρωση.

JavaScript – ασφαλής χρήση

Η JavaScript είναι απαραίτητη για τη λειτουργία του σύγχρονου διαδικτύου, αλλά αποτελεί και το κύριο εργαλείο κακόβουλων επιθέσεων στον browser.

🟢 **Προτεινόμενη προσέγγιση**

- Επιτρέψτε JavaScript **μόνο σε αξιόπιστες ιστοσελίδες** που επισκέπτεστε τακτικά.
- Χρησιμοποιήστε extensions όπως το **uBlock Origin** που φιλτράρει κακόβουλα scripts χωρίς να σπάει τη λειτουργία νόμιμων σελίδων.
- Ενημερώνετε πάντα τον browser — τα patches κλείνουν γνωστά JavaScript exploits.

🔴 Κίνδυνοι από κακόβουλα scripts

- **Cryptojacking**: Scripts που χρησιμοποιούν τον επεξεργαστή σας για mining κρυπτονομισμάτων.
- **Keylogging**: Καταγραφή πληκτρολογήσεων και κλοπή κωδικών σε πραγματικό χρόνο.
- **Drive-by exploits**: Εκμετάλλευση browser vulnerabilities μέσω κακόβουλου JS κώδικα.

Cookies – παρακολούθηση & εκκαθάριση

Τα cookies δεν είναι από μόνα τους επικίνδυνα, αλλά μπορούν να χρησιμοποιηθούν για παρακολούθηση, κλοπή session και στοχευμένη διαφήμιση χωρίς τη συγκατάθεσή σας.

Third-party cookies

Τοποθετούνται από διαφημιστικά δίκτυα για να παρακολουθούν την περιήγησή σας σε πολλαπλές ιστοσελίδες. Αποκλείστε τα στις ρυθμίσεις του browser σας.

Session tracking

Τα session cookies μπορούν να υποκλαπούν μέσω XSS επιθέσεων ή man-in-the-middle attacks, δίνοντας πρόσβαση στους λογαριασμούς σας.

Τακτική εκκαθάριση

Διαγράψτε cookies και cache τακτικά: Ctrl+Shift+Delete σε όλους τους browsers. Σκεφτείτε αυτόματη εκκαθάριση κατά το κλείσιμο του browser.

- 🟢 Προτεινόμενο: Αποκλεισμός third-party cookies + αυτόματη εκκαθάριση κατά κλείσιμο. 🔴 Μη προτεινόμενο: Αποδοχή όλων των cookies χωρίς έλεγχο.

Browser extensions – ασφαλής χρήση

Τα extensions επεκτείνουν τις δυνατότητες του browser, αλλά έχουν πρόσβαση σε ευαίσθητα δεδομένα. Λάθος επιλογή μπορεί να μετατρέψει ένα χρήσιμο εργαλείο σε spyware.

🟢 Ασφαλής εγκατάσταση

- Εγκαταστήστε extensions **αποκλειστικά** από επίσημα stores: Chrome Web Store, Microsoft Edge Add-ons, Firefox Add-ons (AMO).
- Ελέγξτε τον αριθμό χρηστών, τις κριτικές και την ημερομηνία τελευταίας ενημέρωσης.
- Αναθεωρήστε τα εγκατεστημένα extensions τακτικά και αφαιρέστε όσα δεν χρησιμοποιείτε.

🔴 Τι να προσέχετε

- **Υπερβολικά δικαιώματα**: Ένα extension μετατροπής PDF δεν χρειάζεται πρόσβαση σε όλες τις ιστοσελίδες και το ιστορικό σας.
- **Εγκατάσταση από τρίτες πηγές**: Αρχεία .crx ή .xpi από άγνωστα sites μπορεί να είναι κακόβουλα.
- **Clone extensions**: Αντίγραφα δημοφιλών extensions με παρόμοια ονόματα που κλέβουν δεδομένα.

Site permissions – δικαιώματα ιστοτόπων

Οι ιστοσελίδες μπορούν να ζητήσουν πρόσβαση σε ευαίσθητες λειτουργίες της συσκευής σας. Γνωρίστε τους κινδύνους πριν πατήσετε «Επιτρέψτε».

Κάμερα

Επιτρέψτε μόνο σε εφαρμογές βιντεοκλήσεων (Zoom, Teams). Ποτέ σε άγνωστες ή αναπάντεχες σελίδες.

Μικρόφωνο

Μόνο για εφαρμογές που χρειάζονται φωνή. Αποκλείστε από προεπιλογή και επιτρέψτε κατά περίπτωση.

Τοποθεσία

Εξαιρετικά ευαίσθητο. Επιτρέψτε μόνο σε χάρτες και υπηρεσίες εντοπισμού που εμπιστεύεστε.

Ειδοποιήσεις & clipboard

Το clipboard μπορεί να περιέχει κωδικούς. Οι ειδοποιήσεις χρησιμοποιούνται για spam. Αποκλείστε και τα δύο ως προεπιλογή.

🟢 Προτεινόμενο: Ρύθμιση όλων των δικαιωμάτων σε «Να ερωτάται» — ποτέ σε «Να επιτρέπεται» από προεπιλογή.

Επικίνδυνοι τύποι αρχείων στα downloads

Πέρα από τα εκτελέσιμα, υπάρχουν τύποι αρχείων που φαίνονται αθώοι αλλά αποτελούν κοινό φορέα επίθεσης.

🗜️ ZIP με κωδικό πρόσβασης

Τα password-protected ZIPs χρησιμοποιούνται για να παρακάμψουν τους antivirus scanners. Ο κωδικός δίνεται στο email, αλλά το περιεχόμενο είναι malware. Μην αποσυμπιέζετε χωρίς να γνωρίζετε την πηγή.

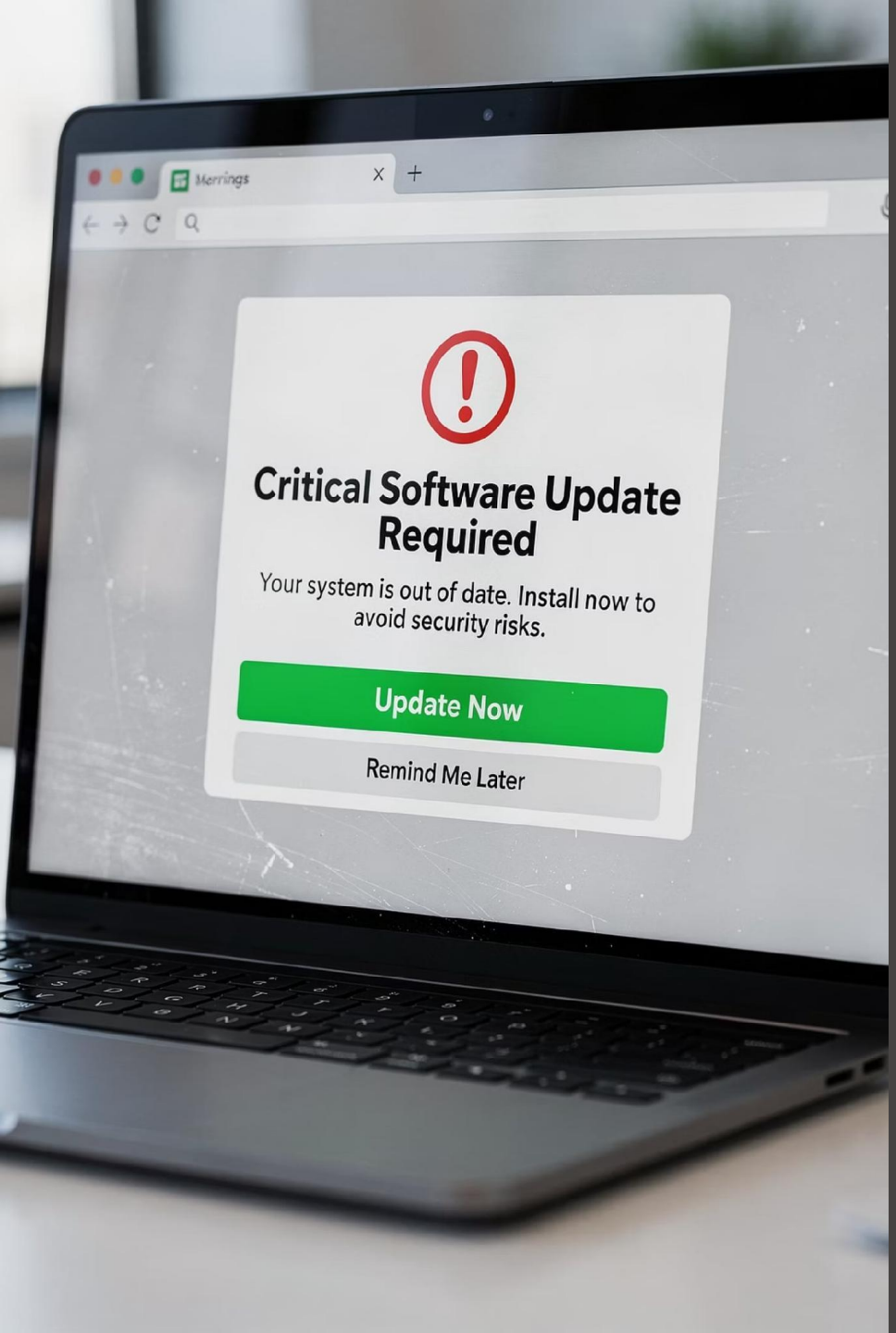
💿 ISO / IMG αρχεία

Εικόνες δίσκων που μπορούν να εκτελεστούν απευθείας στα Windows 10/11. Χρησιμοποιούνται για bypass του Mark-of-the-Web (MOTW) protection του Defender.

📊 Office με macros

Αρχεία .docm, .xlsm, .pptm που ζητούν «Ενεργοποίηση περιεχομένου» για macros. Αυτό εκτελεί κώδικα VBA που μπορεί να κατεβάσει και να εγκαταστήσει malware.

⊗ Κανόνας: Αν ένα αρχείο σας ζητά να «ενεργοποιήσετε» κάτι για να λειτουργήσει, είναι ύποπτο.



Fake updates – Ψεύτικες ενημερώσεις

Μια από τις πιο διαδεδομένες τακτικές κοινωνικής μηχανικής: ψεύτικα αναδυόμενα μηνύματα που σας πείθουν να «ενημερώσετε» λογισμικό που δεν χρειάζεται ενημέρωση.

🟢 Πώς να προστατευτείτε

- Ενημερώνετε τον browser **μόνο μέσα από τις επίσημες ρυθμίσεις** του (Chrome: Βοήθεια → Σχετικά με τον Chrome).
- Το Flash Player **δεν υπάρχει πλέον** — οποιαδήποτε σελίδα που ζητά ενημέρωση Flash είναι κατ' ευθείαν απάτη.
- Κλείστε αμέσως τη σελίδα που εμφανίζει τέτοιο μήνυμα χωρίς να κάνετε κλικ οπουδήποτε.

🔴 Χαρακτηριστικά ψεύτικων updates

- Αναδύονται ενώ περιηγείστε σε άσχετη ιστοσελίδα.
- Δημιουργούν αίσθηση επείγοντος: «Ο browser σας είναι ξεπερασμένος! Ενημερώστε τώρα!»
- Μιμούνται την εμφάνιση των Windows system dialogs ή γνωστών browsers.
- Το αρχείο λήψης δεν έχει ψηφιακή υπογραφή από γνωστό εκδότη.

Notification scams – παραπλανητικές ειδοποιήσεις

Ένα από τα πιο επίμονα προβλήματα: ιστοσελίδες που εξαπατούν τους χρήστες να αποδεχθούν browser notifications, στη συνέχεια τους βομβαρδίζουν με spam ή scam ειδοποιήσεις.

🔔 «Click Allow» απάτη

Σελίδα ζητά να πατήσετε «Allow» ισχυριζόμενη ότι πρόκειται για αποδοχή όρων, επαλήθευση ηλικίας ή πρόσβαση σε περιεχόμενο. Στην πραγματικότητα δίνετε άδεια για ειδοποιήσεις.

🤖 Fake CAPTCHA

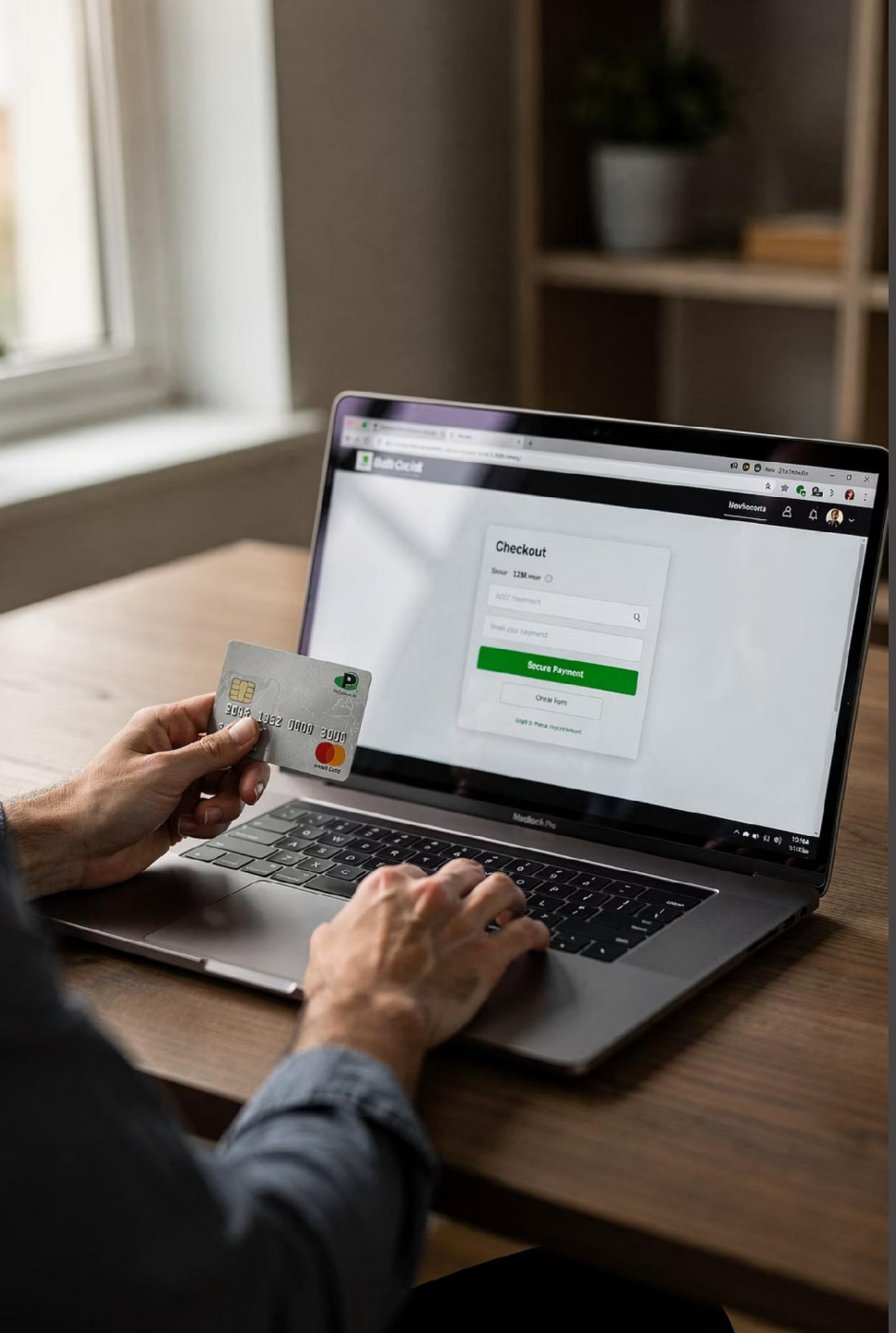
«Κάντε κλικ στο Allow για να αποδείξετε ότι δεν είστε ρομπότ» — ψεύτικο CAPTCHA που στην πραγματικότητα αιτείται δικαιώματα ειδοποιήσεων ή εκτελεί κακόβουλα scripts.

🟢 Λύση

Ρυθμίστε τον browser να **μπλοκάρει αυτόματα** αιτήματα ειδοποιήσεων. Ελέγξτε τις υπάρχουσες άδειες και αφαιρέστε άγνωστες ιστοσελίδες: Ρυθμίσεις → Δικαιώματα → Ειδοποιήσεις.

🔴 Τι να αποφύγετε

Να πατάτε «Allow» σε αναδυόμενα αιτήματα ειδοποιήσεων από άγνωστες σελίδες χωρίς να σκέφτεστε τι αποδέχεστε.



Safe online shopping – Ασφαλείς Online αγορές

Οι online αγορές προσφέρουν ευκολία, αλλά και σημαντικούς κινδύνους. Μια λανθασμένη κίνηση μπορεί να οδηγήσει σε οικονομική απώλεια ή κλοπή ταυτότητας.

1 HTTPS & ασφαλής σύνδεση

Βεβαιωθείτε για το λουκέτο και το HTTPS στη σελίδα πληρωμής. Ποτέ μην εισάγετε στοιχεία κάρτας σε HTTP σελίδες.

2 Έλεγχος αξιοπιστίας

Αναζητήστε κριτικές για το e-shop σε ανεξάρτητες πλατφόρμες (Trustpilot, Google Reviews). Ελέγξτε στοιχεία επικοινωνίας και φυσική διεύθυνση.

3 Ασφαλείς μέθοδοι πληρωμής

Προτιμήστε virtual cards, PayPal ή 3D Secure. Αποφύγετε bank transfers σε άγνωστα shops. Ενεργοποιήστε SMS alerts για κάθε συναλλαγή.

Πριν συνδεθείτε – προκαταρκτικός έλεγχος

Τα δευτερόλεπτα πριν πατήσετε «Login» είναι κρίσιμα. Αυτές οι τρεις πρακτικές μειώνουν δραστικά τον κίνδυνο παραβίασης λογαριασμού.

Ελέγξτε το URL

Πριν πληκτρολογήσετε τα στοιχεία σας, ελέγξτε ότι βρίσκεστε στο σωστό domain. Phishing sites μιμούνται νόμιμες σελίδες pixel-perfect. Ελέγξτε: domain, TLD, πιστοποιητικό.

Password Manager

Χρησιμοποιήστε password manager (Bitwarden, 1Password, KeePass) για μοναδικούς, ισχυρούς κωδικούς σε κάθε υπηρεσία. Ο manager δεν συμπληρώνει αυτόματα σε phishing sites.

MFA – Πολυπαραγοντική αυθεντικοποίηση

Ενεργοποιήστε MFA (Google Authenticator, Microsoft Authenticator) σε όλες τις κρίσιμες υπηρεσίες. Ακόμη και αν κλαπεί ο κωδικός, ο λογαριασμός παραμένει ασφαλής.

VPN & δημόσιο Wi-Fi

Τα δημόσια δίκτυα Wi-Fi σε καφέ, αεροδρόμια και ξενοδοχεία είναι εξ ορισμού μη αξιόπιστα. Χωρίς προστασία, η κυκλοφορία σας είναι ορατή σε όσους βρίσκονται στο ίδιο δίκτυο.

🟢 VPN – Η σωστή επιλογή

- Ένα αξιόπιστο VPN (Mullvad, ProtonVPN, NordVPN) κρυπτογραφεί όλη την κυκλοφορία σας, ακόμα και σε δημόσια δίκτυα.
- Επιλέξτε παρόχους με πολιτική «no-logs» και ανεξάρτητους ελέγχους ασφαλείας.
- Ενεργοποιήστε το VPN **πριν** συνδεθείτε σε δημόσιο Wi-Fi, όχι μετά.

🔴 Τι να αποφύγετε σε δημόσιο Wi-Fi

- Online banking ή εισαγωγή κωδικών χωρίς VPN.
- Σύνδεση σε «Free Wi-Fi» hotspots χωρίς κωδικό πρόσβασης — μπορεί να είναι Evil Twin attacks.
- Αποστολή ευαίσθητων εγγράφων ή email με εμπιστευτικές πληροφορίες.

Browser security checklist

Ένας γρήγορος οδηγός επαλήθευσης για τον browser σας. Ελέγξτε κάθε σημείο τακτικά — ιδανικά μία φορά το μήνα.

Browser ενημερωμένος

Ελέγξτε αν χρησιμοποιείτε την τελευταία έκδοση. Οι παλαιές εκδόσεις έχουν γνωστές ευπάθειες που εκμεταλλεύονται ενεργά.

Safe browsing ενεργό

Βεβαιωθείτε ότι το Safe Browsing (Chrome/Edge) ή η Enhanced Tracking Protection (Firefox) είναι ενεργά και στο υψηλότερο επίπεδο.

Secure DNS ρυθμισμένο

Επαληθεύστε ότι χρησιμοποιείτε DNS-over-HTTPS με αξιόπιστο πάροχο. Αποτρέπει υποκλοπή DNS queries.

Extensions ελεγμένα

Αναθεωρήστε λίστα extensions — αφαιρέστε αχρησιμοποίητα και ελέγξτε δικαιώματα των υπολοίπων.

Case study: Phishing μέσω ψεύτικης ιστοσελίδας

Πραγματικό σενάριο επίθεσης που αποδεικνύει πώς ακόμα και έμπειροι χρήστες μπορούν να εξαπατηθούν.

Βήμα 1: Email

Ο χρήστης λαμβάνει email από «support@paypa1.gr» με θέμα «Επείγον: Επαλήθευση λογαριασμού».

1

Βήμα 2: Κλικ

Κάνει κλικ στον σύνδεσμο που οδηγεί σε **paypa1.gr/login** — ίδιο layout με το αληθινό PayPal.

2

Βήμα 3: Credentials

Εισάγει email και κωδικό. Η ψεύτικη σελίδα στέλνει τα στοιχεία στον επιτιθέμενο και ανακατευθύνει στο αληθινό PayPal.

3

Βήμα 4: Παραβίαση

Ο λογαριασμός παραβιάζεται. Χωρίς MFA, ο επιτιθέμενος έχει πλήρη πρόσβαση σε λίγα λεπτά.

4

Πώς θα αποφεύγαμε: Έλεγχος URL (paypa**1**.gr vs paypa**l**.com), ενεργό MFA, password manager που δεν θα αυτοσυμπλήρωνε το phishing domain.

10 πρακτικές συμβουλές ασφαλούς περιήγησης

Εφαρμόστε αυτές τις συμβουλές σήμερα — δεν χρειάζονται τεχνικές γνώσεις, μόνο προσοχή και καλές συνήθειες.

- **Ενημερώνετε πάντα τον browser σας**

  Οι ενημερώσεις κλείνουν κρίσιμες ευπάθειες ασφαλείας που εκμεταλλεύονται ενεργά.

- **Ελέγχετε πάντα το URL πριν συνδεθείτε**

  Αφιερώστε 2 δευτερόλεπτα πριν εισάγετε οποιοδήποτε στοιχείο σε φόρμα σύνδεσης.

- **Χρησιμοποιείτε password manager**

  Μοναδικοί, ισχυροί κωδικοί για κάθε υπηρεσία — χωρίς την ανάγκη απομνημόνευσης.

- **Ενεργοποιήστε MFA παντού**

  Email, τράπεζες, κοινωνικά δίκτυα — το MFA είναι η πιο αποτελεσματική άμυνα κατά παραβίασης.

- **Αποφεύγετε δημόσιο Wi-Fi χωρίς VPN**

  Ή τουλάχιστον αποφύγετε ευαίσθητες ενέργειες όταν δεν χρησιμοποιείτε VPN.

Quiz – σενάρια προς συζήτηση

Ελέγξτε τις γνώσεις σας. Για κάθε σενάριο, σκεφτείτε ποια είναι η σωστή απόκριση πριν δείτε την απάντηση.

1

Σενάριο Α

Επισκέπτεστε μια ιστοσελίδα και εμφανίζεται μήνυμα: «Ο Chrome σας χρειάζεται ενημέρωση. Κατεβάστε τώρα!» Τι κάνετε;

Απάντηση: Κλείστε αμέσως τη σελίδα. Ενημερώστε μόνο μέσα από το μενού Βοήθεια του Chrome.

2

Σενάριο Β

Λαμβάνετε email από την «τράπεζά σας» με σύνδεσμο για επαλήθευση. Το URL είναι **alpha-bank-secure.net**. Τι κάνετε;

Απάντηση: ΜΗΝ κάνετε κλικ. Επισκεφτείτε απευθείας την επίσημη σελίδα της τράπεζας πληκτρολογώντας το URL.

3

Σενάριο Γ

Extension στο Chrome σας ζητά πρόσβαση «Να διαβάζει και να αλλάζει τα δεδομένα σε όλες τις ιστοσελίδες». Τι κάνετε;

Απάντηση: Αρνηθείτε. Αυτό το δικαίωμα είναι υπερβολικό για τα περισσότερα extensions — αποτελεί red flag.

Συμπεράσματα

Η ασφαλής περιήγηση ξεκινά από τον χρήστη.

Κανένα εργαλείο δεν μπορεί να σας προστατεύσει 100% αν δεν συνοδεύεται από επίγνωση και καλές συνήθειες. Η γνώση είναι η καλύτερη άμυνα.

🔑 Ρυθμίσεις

Ενεργοποιήστε Safe Browsing, HTTPS-Only και Secure DNS στον browser σας σήμερα.

🧠 Επίγνωση

Αναγνωρίστε phishing, fake updates και notification scams πριν γίνετε θύμα.

🛡️ Συνήθειες

Password manager, MFA, VPN σε δημόσιο Wi-Fi — τρεις συνήθειες που αλλάζουν τα πάντα.

✓ Εφαρμόστε έστω και μία σύσταση από σήμερα. Κάθε βήμα μετράει.