

Συμβουλές για Ασφαλή Πλοήγηση στο Διαδίκτυο

Ασφάλεια Λογαριασμών & Κωδικών

- Χρησιμοποιήστε διαχειριστή κωδικών πρόσβασης (π.χ. Bitwarden, 1Password) για τη δημιουργία και αποθήκευση μοναδικών κωδικών.
- Χρησιμοποιήστε δύο Παράγοντες αυθεντικοποίησης (**2FA**) (κατά προτίμηση μέσω εφαρμογών όπως το Authy ή με φυσικά κλειδιά όπως το YubiKey).
- Μην επαναχρησιμοποιείτε κωδικούς πρόσβασης σε διαφορετικές υπηρεσίες.

Ασφάλεια Δικτύου

- Χρησιμοποιήστε **VPN** όταν συνδέεστε σε δημόσια Wi-Fi.
- Αποφύγετε τη σύνδεση σε μη αξιόπιστα δίκτυα (όπως δωρεάν Wi-Fi σε αεροδρόμια).
- Ασφαλίστε το οικιακό σας **Wi-Fi** (αλλάξτε τα προεπιλεγμένα διαπιστευτήρια του router, χρησιμοποιήστε WPA3/WPA2).



Ασφάλεια Συσκευών & Λογισμικού

- Διατηρείτε το λειτουργικό σύστημα, τον περιηγητή και το λογισμικό σας ενημερωμένα.
- Ενεργοποιήστε την κρυπτογράφηση πλήρους δίσκου σε φορητούς υπολογιστές και smartphones.
- Χρησιμοποιήστε λογισμικό προστασίας από ιούς (π.χ. Windows Defender).



Ασφάλεια Περιήγησης & Email

- Ελέγχετε τις διευθύνσεις **URL** πριν κάνετε κλικ (περάστε τον δείκτη πάνω από τους συνδέσμους, αποφύγετε συντομευμένες διευθύνσεις URL).
- Μην κατεβάζετε συνημμένα από άγνωστους αποστολείς.
- Να είστε επιφυλακτικοί με **emails/SMS** που ζητούν διαπιστευτήρια.
- Χρησιμοποιήστε επεκτάσεις περιηγητή όπως το **uBlock Origin & HTTPS Everywhere**.

Προστασία Ιδιωτικότητας & Δεδομένων

- Περιορίστε τις προσωπικές πληροφορίες που κοινοποιείτε στο διαδίκτυο (αποφύγετε την υπερβολική κοινοποίηση στα κοινωνικά μέσα).
- Χρησιμοποιήστε εφαρμογές κρυπτογραφημένων μηνυμάτων (π.χ. Signal, Telegram με μυστικές συνομιλίες).
- Απενεργοποιήστε την παρακολούθηση στους περιηγητές (χρησιμοποιήστε Firefox, Brave ή Chrome με ρυθμίσεις ιδιωτικότητας προσαρμοσμένες).



Ασφάλεια Οικονομικών Συναλλαγών

- Χρησιμοποιήστε εικονικές κάρτες για online αγορές.
- Παρακολουθείτε τις τραπεζικές σας καταστάσεις για μη εξουσιοδοτημένες συναλλαγές.
- Να είστε προσεκτικοί με **phishing** απάτες που προσποιούνται τράπεζες ή υπηρεσίες.



Γενική Επαγρύπνηση & Καλές Πρακτικές

- Σκεφτείτε πριν κάνετε κλικ—η κοινωνική μηχανική είναι μεγαλύτερη απειλή από το hacking.
- Ελέγχετε τακτικά το **haveibeenpwned.com** για να δείτε αν το email σας έχει διαρρεύσει.
- Δημιουργήστε αντίγραφα ασφαλείας σημαντικών δεδομένων (τόσο offline όσο και στο cloud).

Συμπέρασμα

Η ασφάλεια είναι συνήθεια—παραμείνετε σε εγρήγορση! Χρειάζεστε συγκεκριμένες συμβουλές για κάτι;

