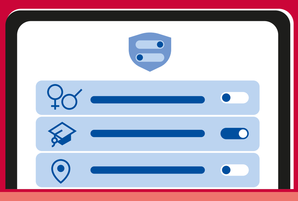
Χρήσιμες συμβουλές για την προστασία σας στο διαδίκτυο

Η σύνδεση στο διαδίκτυο σας βοηθά να παραμείνετε σε επαφή με την οικογένεια και τους φίλους σας, σας ενημερώνει για τις ειδήσεις, σας δίνει πρόσβαση στη μάθηση μέσω διαδικτύου και παρέχει πολλά ακόμη πλεονεκτήματα. Ωστόσο, είναι πάντοτε καλό να έχετε στον νου σας την ασφάλεια και υπάρχουν πολλά πράγματα που μπορείτε να κάνετε για να προστατεύσετε τον εαυτό σας.



1. Προσέχετε ποιες πληροφορίες μοιράζεστε

Όταν συμπληρώνετε το προφίλ ενός λογαριασμού, δίνετε μόνο τις πληροφορίες που είναι απαραίτητες και που αισθάνεστε άνετα να δώσετε.

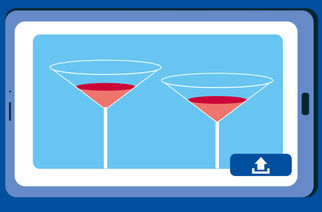
Χρησιμοποιείτε τις ρυθμίσεις απορρήτου και ασφάλειας και απενεργοποιήστε τυχόν χαρακτηριστικά που δεν χρειάζεστε.

Εάν δεν αισθάνεστε ασφαλείς, σκεφτείτε εάν σας ενδιαφέρει πραγματικά να δημιουργήσετε προφίλ στην εν λόγω εταιρεία.

2. Σκεφτείτε προτού κοινοποιήσετε

Η ανάρτηση πληροφοριών υπό καθεστώς έντονης συναισθηματικής φόρτισης δεν είναι πάντα καλή ιδέα. Οτιδήποτε αναρτάτε στο διαδίκτυο παραμένει εκεί για πάντα. Ακόμη και αν το διαγράψετε αργότερα, κάποιος μπορεί να το έχει αποθηκεύσει ή προωθήσει.

Περιμένετε μέχρι να ανακτήσετε την ψυχραιμία σας, και τότε ξανασκεφτείτε αν είστε βέβαιος/-η ότι θέλετε πραγματικά να αναρτήσετε αυτό το σχόλιο.



3. Αναλογιστείτε τις συνέπειες

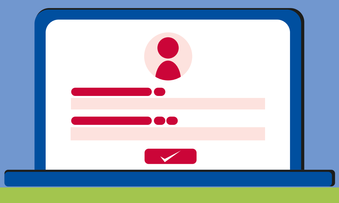
Πριν αναρτήσετε μια φωτογραφία, αναλογιστήκατε αν όλοι οι εικονιζόμενοι στη φωτογραφία συναινούν στη δημοσίευσή της; Ενδέχεται να αποκαλύπτετε πληροφορίες, όπως σχετικά με το πού ζείτε.

Και η ανάρτηση φωτογραφιών από τις εκπληκτικές διακοπές σας δίνει στους διαρρήκτες την πληροφορία πως δεν βρίσκεστε στο σπίτι!

4. Σκεφτείτε πριν παίξετε

Προτού λάβετε μέρος σε κάποιο διασκεδαστικό παιχνίδι που έχει γίνει ανάρπαστο στα μέσα κοινωνικής δικτύωσης, αναλογιστείτε τι σας ζητούν — το όνομα του πρώτου ζώου συντροφιάς σας, το πατρικό όνομα της μητέρας σας;

Πρόκειται για τις ίδιες ερωτήσεις που χρησιμοποιούνται για θέματα ασφάλειας, για παράδειγμα από την τράπεζα, και, ως εκ τούτου, απαντώντας σε αυτές ενδεχομένως να δίνετε σημαντικές πληροφορίες σε χάκερ.



5. Βεβαιωθείτε ότι γνωρίζετε με ποιον επικοινωνείτε

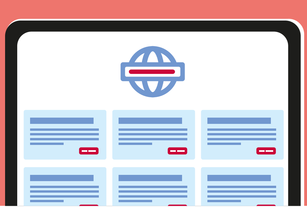
Έχετε υπόψη ότι οι απατεώνες χρησιμοποιούν κοινωνικά δίκτυα και δικτυακούς τόπους, και στέλνουν μηνύματα στο τηλέφωνό σας για να κλέψουν τις πληροφορίες, τα χρήματα ή την ταυτότητά σας.

Μπορείτε να προστατεύσετε τον εαυτό σας με το να μην δίνετε προσωπικά στοιχεία, χρήματα ή στοιχεία λογαριασμού, εκτός εάν μπορείτε να επαληθεύσετε με άλλα μέσα επικοινωνίας με ποιον/ποιαν τα μοιράζεστε.

6. Παρακολουθείτε τις νεότερες εξελίξεις για την κυβερνοασφάλεια

Παρακολουθώντας τις νεότερες εξελίξεις και ρωτώντας την οικογένεια και τους φίλους σας για να ενημερωθείτε σχετικά με τις απάτες που κυκλοφορούν, π.χ. απάτες ηλεκτρονικού «ψαρέματος», κακόβουλο λογισμικό (όπως το Flubot) και ψεύτικοι ιστότοποι, μπορείτε να παραμείνετε ασφαλείς στο διαδίκτυο.

Για άλλες πηγές πληροφοριών σχετικά με τη χώρα σας, επισκεφθείτε την ηλεκτρονική διεύθυνση https://cybersecuritymonth.eu/cyber-first-aid
Μην εφησυχάζετε!



SaferInternet4Kids.gr

Εθνική Αρχή Κυβερνοασφάλειας ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth

#ThinkB4UClick