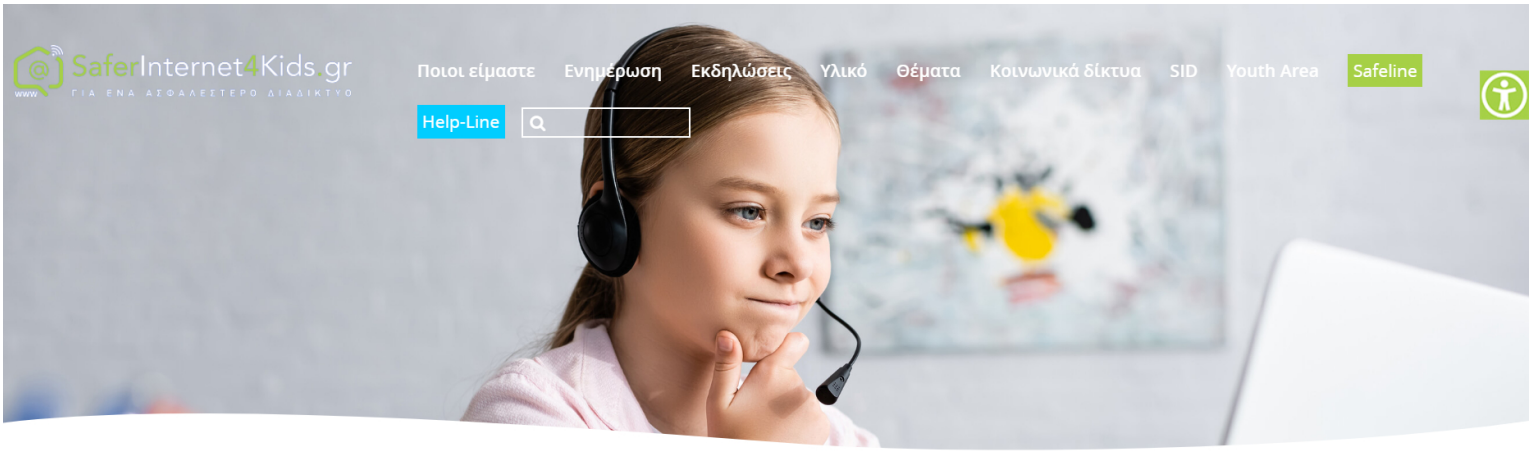

Πώς μπορούμε να προστατέψουμε την ψηφιακή μας ταυτότητα

Ακούστε αυτό το άρθρο
00:00 / 06:04

Η κλασική έννοια της ταυτότητας ορίζεται μέσω των εξωτερικών γνωρισμάτων μας όπως είναι τα βιομετρικά χαρακτηριστικά μας (χρώμα ματιών, δακτυλικά αποτυπώματα κ.α), το όνομά μας, την ημερομηνία γέννησής μας, την υπογραφή μας. Η διαδικτυακή μας ταυτότητα έχει πιο δυναμικό χαρακτήρα και προκύπτει κυρίως από τα ψηφιακά μας αποτυπώματα: τους διαδικτυακούς φίλους μας, το τι κοινοποιούμε, την εικόνα που προβάλλουμε για τον εαυτό μας. Αν κάποιος υποκλέψει τους κωδικούς μας αυτομάτως μπορεί να γίνει «εμείς» οπότε η προστασία της ψηφιακής μας ταυτότητας είναι βαρύνουσας σημασίας στο διαδίκτυο.

Ακολουθούν βασικές συμβουλές προστασίας της ψηφιακής μας ταυτότητας:

Ισχυροί κωδικοί πρόσβασης παντού:

Η δημιουργία ισχυρών κωδικών πρόσβασης, **διαφορετικό για κάθε λογαριασμό που χρησιμοποιείτε** είναι ένα πολύ σημαντικό βήμα. Ένας ισχυρός κωδικός πρόσβασης περιλαμβάνει τουλάχιστον 8 χαρακτήρες γράμματα, αριθμούς και σύμβολα, είναι εύκολος στο να τον θυμάστε εσείς και δύσκολος για τους άλλους να τον μαντέψουν. Για ακόμα μεγαλύτερη προστασία μπορείτε να χρησιμοποιήσετε έλεγχο ταυτότητας πολλαπλών παραγόντων (2 Factor Authentication) ο οποίος θα ενισχύσει τους διαδικτυακούς λογαριασμούς σας ενεργοποιώντας τα ισχυρότερα διαθέσιμα εργαλεία ελέγχου ταυτότητας όπως βιομετρικά στοιχεία ή έναν κωδικό μιας χρήσης που αποστέλλεται στο τηλέφωνό σας. Έναν αναλυτικό οδηγό μπορείτε να διαβάσετε **εδώ**.

Για να δημιουργήσετε και να θυμηθείτε διαφορετικούς, σύνθετους κωδικούς πρόσβασης για κάθε έναν από τους λογαριασμούς σας μπορείτε να χρησιμοποιήσετε password manager. Αυτή η λύση ενδείκνυται κυρίως για προχωρημένους χρήστες που έχουν να διαχειριστούν πολλούς διαφορετικούς κωδικούς και έχουν διαδικτυακή δραστηριότητα που μπορεί να προσελκύσει χάκερς.

Διατηρήστε τη συσκευή σας «καθαρή»:

Εγκαταστήστε antivirus σε όλες τις συσκευές σας και φροντίστε να το ανανεώνεται τακτικά με τις νεότερες εκδόσεις. Με αυτόν τον τρόπο προστατεύεστε από τον συχνότερο κίνδυνο που υπάρχει, να προσβληθεί η συσκευή σας από κάποιο κακόβουλο λογισμικό. Τα διάφορα antivirus διαφέρουν σε ότι αφορά τις μεθόδους τους, ωστόσο όλα έχουν τον ίδιο στόχο: να προστατέψουν τις συσκευές σας.

Το antivirus εκτελεί τακτικές σαρώσεις και ελέγχους στις συσκευές σας, παρακολουθώντας τα αρχεία, τα προγράμματα και τις ιστοσελίδες για πιθανές απειλές. Το antivirus ανιχνεύει οποιαδήποτε κακόβουλη ή απειλητική συμπεριφορά θα μπορούσε να θεωρηθεί ως μορφή κακόβουλου λογισμικού, αφαιρώντας το από τη συσκευή σας όσο το δυνατόν γρηγορότερα, ενώ εργάζεται για να αποτρέψει μελλοντικές επιθέσεις.

Ρυθμίστε τις παραμέτρους των συσκευών σας ώστε να ενημερώνονται αυτόματα ή να σας ειδοποιούν όταν είναι διαθέσιμη μια ενημέρωση στο antivirus που έχετε εγκαταστήσει.

Περισσότερα για το πως να εγκαταστήσετε ένα antivirus μπορείτε να δείτε **εδώ**.

Μάθετε περισσότερα σχετικά με τα wifi hotspot:

Τα δημόσια ασύρματα δίκτυα δεν είναι ασφαλή. Οποιοσδήποτε θα μπορούσε ενδεχομένως να δει τι κάνετε στον φορητό υπολογιστή ή το smartphone σας ενώ είστε συνδεδεμένοι σε ένα τέτοιο δίκτυο. Περιορίστε τι κάνετε στο δημόσιο WiFi και αποφύγετε τη σύνδεση σε βασικούς λογαριασμούς όπως email και τραπεζικούς λογαριασμούς. Εξετάστε το ενδεχόμενο να χρησιμοποιήσετε ένα εικονικό ιδιωτικό δίκτυο (VPN) ή να συνδεθείτε μόνο με δεδομένα εάν χρειάζεστε μια πιο ασφαλή σύνδεση.

Σκεφτείτε πριν ανοίξετε οποιοδήποτε link σας έχει αποσταλεί:

Εάν λάβετε μια δελεαστική προσφορά μέσω ηλεκτρονικού ταχυδρομείου ή μέσω μηνύματος, μη βιαστείτε να ανοίξετε το σύνδεσμο. Οι επιτιθέμενοι συχνά στέλνουν απατηλά μηνύματα ηλεκτρονικού ταχυδρομείου και κειμένου, που αναφέρονται ως ηλεκτρονικό ψάρεμα (phishing), προκειμένου να εξαπατήσουν τα άτομα να παρέχουν πληροφορίες όπως ονόματα χρήστη και κωδικούς πρόσβασης ή να κατεβάσουν κακόβουλο λογισμικό.

Μερικές συμβουλές που μπορούν να σας βοηθήσουν να εντοπίσετε ένα μήνυμα "phising":

- Εάν ένα μήνυμα περιέχει γενικούς ή ανεπίσημους χαιρετισμούς ή στερείτε εξατομίκευσης (π.χ. "Αγαπητέ πελάτη"), τότε θα πρέπει να υποψιαστείτε ότι κάτι πάει στραβά. Το ίδιο ισχύει και αν χρησιμοποιούνται τυχαίοι ή ψευδείς αριθμοί αναφοράς.
- Αν περιέχεται ένα αίτημα για καταχώρηση προσωπικών πληροφοριών. Κανένα χρηματοπιστωτικό ίδρυμα δε θα σας ζητήσει προσωπικά στοιχεία μέσω email.

- Τα ορθογραφικά και συντακτικά λάθη συχνά υποδεικνύουν ένα ψεύτικο μήνυμα.
- Αίσθηση επείγουσας ανάγκης. Τα μηνύματα ηλεκτρονικού "ψαρέματος" προσπαθούν συχνά να προκαλέσουν ταχείες ενέργειες.
- Εάν το μήνυμα ακούγεται πολύ καλό για να είναι αλήθεια, είναι σχεδόν βέβαιο ότι δεν είναι.

Έχετε τον έλεγχο της παρουσίας σας στο διαδίκτυο

Κάθε φορά που κάνετε εγγραφή σε έναν νέο λογαριασμό ή κατεβάζετε μια νέα εφαρμογή ορίστε αμέσως τις ρυθμίσεις ασφαλείας και ιδιωτικότητας που επιθυμείτε (ιδανικά ιδιωτικό προφίλ). Ελέγχετε τακτικά αυτές τις ρυθμίσεις (τουλάχιστον μία φορά το εξάμηνο) για να βεβαιωθείτε ότι εξακολουθούν να είναι ρυθμισμένες με βάση την επιθυμία σας. Επίσης, όταν κατεβάζετε εφαρμογές να ελέγχετε πάντα τους όρους χρήσεις πριν τους κάνετε αποδεκτούς έτσι ώστε να γνωρίζετε που έχετε συναινέσει.

Κάθε έξι μήνες καλό είναι να ανατρέχετε στις εφαρμογές που έχετε κατεβάσει και αν δε σας είναι πλέον χρήσιμες να τις σβήνετε. Το ίδιο ισχύει και με τα προφίλ σε κοινωνικά δίκτυα που πλέον δε χρησιμοποιείτε. Έναν οδηγό για την προστασία της ιδιωτικότητας κατά τη χρήση εφαρμογών μπορείτε να διαβάσετε **εδώ.**

Μοιραστείτε με προσοχή:

Να σκέφτεστε διπλά πριν κοινοποιήσετε περιεχόμενο για τον εαυτό σας ή για τους άλλους στο διαδίκτυο. Εξετάστε τι αποκαλύπτει μια δημοσίευση, ποιος μπορεί να την δει και πώς μπορεί να επηρεάσει εσάς ή άλλους. Να θυμάστε ότι δεν έχετε δικαίωμα να κοινοποιείτε περιεχόμενο στο διαδίκτυο που αφορά άλλους χωρίς να έχετε την έγκρισή τους.

Οι προσωπικές πληροφορίες που είναι άμεσα διαθέσιμες στο διαδίκτυο μπορούν να χρησιμοποιηθούν από κακόβουλους για να κάνουν διάφορα πράγματα, όπως πλαστοπροσωπία και εικασία ονομάτων χρηστών και κωδικών πρόσβασης.

Περισσότερα για την Identity Management Day 2021 μπορείτε να διαβάσετε **εδώ**