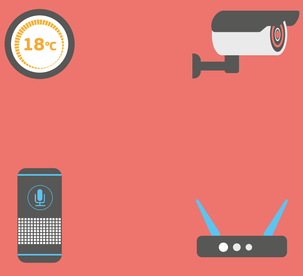
Χρήσιμες συμβουλές για την κυβερνοασφάλεια στο σπίτι σας

Το διαδίκτυο των πραγμάτων (στο εξής: IoT) είναι το δίκτυο όλων των συσκευών που μπορούν να συνδεθούν με το διαδίκτυο. Ο νους σας πηγαίνει αυτόματα στον φορητό υπολογιστή σας ή την έξυπνη τηλεόραση, αλλά το IoT περιλαμβάνει επίσης προϊόντα όπως κονσόλες παιχνιδιών, συσκευές οικιακής βοήθειας, τον οικιακό συναγερμό σας ή το σύστημα παρακολούθησης του βρέφους σας.

Και μολονότι οι συσκευές αυτές μπορεί να βελτιώνουν τον τρόπο ζωής και εργασίας μας, μην ξεχνάτε ότι οποιαδήποτε συσκευή συνδέεται με το διαδίκτυο μπορεί να είναι ευάλωτη σε επιθέσεις από χάκερ. Ας δούμε ορισμένα μέτρα που μπορείτε να λάβετε για να συμβάλετε στην προστασία του σπιτιού σας.



1. Ασφαλίστε όλες τις συσκευές σας

Βεβαιωθείτε ότι όλες οι συσκευές σας προστατεύονται με ισχυρούς κωδικούς πρόσβασης ή ενεργοποιήστε επαλήθευση δύο παραγόντων (2FA), η οποία είναι διαθέσιμη στις περισσότερες συσκευές IoT.

Θα πρέπει επίσης να αλλάξετε τον προεπιλεγμένο κωδικό πρόσβασης και το όνομα δικτύου.

Σας εφιστούμε την προσοχή στο ότι δεν πρέπει να συμπεριλάβετε στο όνομα του δικτύου σας οτιδήποτε παραπέμπει σε πληροφορίες σχετικά με την κατοικία ή την οικογένειά σας, για παράδειγμα το όνομα ή τη διεύθυνσή σας.

2. Ελέγξτε τις εφαρμογές σας

Η εγκατάσταση εφαρμογών απευθείας από το επίσημο κατάστημα εφαρμογών (Google Play, Apple App Store κ.λπ.) είναι ο ασφαλέστερος τρόπος απόκτησής τους. Η επιλογή τυχαίου συνδέσμου για την εγκατάσταση μιας εφαρμογής μπορεί να οδηγήσει σε μόλυνση της συσκευής σας.

Εξετάστε προσεκτικά τις πληροφορίες και τις άδειες που χορηγείτε πριν την εγκατάσταση. Ελέγχετε τακτικά τις εφαρμογές σας και καταργείτε όποια είναι περιττή.

3. Ελέγξτε τις ρυθμίσεις απορρήτου των λογαριασμών σας στα μέσα κοινωνικής δικτύωσης

Μεταβείτε στις ρυθμίσεις απορρήτου του λογαριασμού σας, όπου μπορείτε να επιλέξετε ρυθμίσεις με τις οποίες αισθάνεστε άνετα.

Σκεφτείτε προσεκτικά ποιες πληροφορίες πρέπει να συμπεριλάβετε στο προφίλ σας· οι πλατφόρμες ενίοτε ζητούν πληροφορίες που δεν είναι απαραίτητο να δώσετε.

4. Ενεργοποιήστε αυτόματες ενημερώσεις για όλες τις συσκευές και τηρείτε αντίγραφα ασφαλείας για τα δεδομένα σας

Οι συσκευές IoT είναι ευάλωτες σε επιθέσεις από χάκερ και, ως εκ τούτου, το να διαθέτετε τις πλέον πρόσφατες ενημερώσεις αποτελεί ζωτικό παράγοντα για τη διατήρηση της ασφάλειας των συσκευών σας. Ενεργοποιώντας τις αυτόματες ενημερώσεις δεν θα χρειάζεται να θυμάστε να το κάνετε ο/η ίδιος/-α.

Βεβαιωθείτε ότι έχετε αντίγραφα των σημαντικών πληροφοριών που έχετε αποθηκεύσει σε κάποιο σημείο εκτός διαδικτύου ή στο υπολογιστικό νέφος, για παράδειγμα τις φωτογραφίες σας ή τα στοιχεία επικοινωνίας σας.

5. Χρησιμοποιείτε άλλες συσκευές για την εργασία σας και άλλες για οικιακή χρήση

Σας προτείνουμε να έχετε χωριστές συσκευές για την εργασία και την οικιακή χρήση. Η συσκευή που χρησιμοποιείτε για την εργασία σας θα πρέπει να διατηρείται μόνο για σκοπούς εργασίας, γεγονός που θα σας βοηθήσει να ελαχιστοποιήσετε τις απώλειες σε περίπτωση που η συσκευή σας τεθεί σε κίνδυνο.

Εάν πρέπει να μοιραστείτε μια συσκευή, βεβαιωθείτε ότι κάθε χρήστης διαθέτει ξεχωριστό προφίλ χρήστη.

SaferInternet4Kids.gr
ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth
#ThinkB4UClick