ΕΘΝΙΚΗ
ΥΠΗΡΕΣΙΑ
ΠΛΗΡΟΦΟΡΙΩΝ

CERT

Π. Κανελλοπούλου 4
Αθήνα - ΤΚ: 10177
210 697 3121
cert@nis.gr

Καλές Πρακτικές

Ο εντοπισμός των ατόμων που έχουν τη δυνατότητα να αποκτήσουν απομακρυσμένη πρόσβαση στις συσκευές σας δεν είναι τόσο εύκολος όσο ο εντοπισμός των ατόμων που θα μπορούσαν να αποκτήσουν φυσική πρόσβαση σε αυτές. Όταν η συσκευή σας είναι συνδεδεμένη στο διαδίκτυο, υπάρχει ο κίνδυνος κάποιος να αποκτήσει πρόσβαση στις πληροφορίες σας. Μπορείτε να μειώσετε σημαντικά αυτό τον κίνδυνο, χρησιμοποιώντας ορισμένες καλές πρακτικές:

1. Βελτιώστε την ασφάλεια του κωδικού πρόσβασης (password) κάνοντας τα εξής:
   - α) Δημιουργήστε έναν μοναδικό ισχυρό κωδικό πρόσβασης για κάθε συσκευή ή λογαριασμό. Χρησιμοποιήστε κατά τη δημιουργία του κωδικού σας: αριθμούς, κεφαλαία και μικρά γράμματα και σύμβολα. Μην επαναχρησιμοποιείτε παλιούς κωδικούς και προσωπικές σας πληροφορίες κατά τη δημιουργία των κωδικών (π.χ. ημερομηνίες γενεθλίων, ονόματα συζύγων κλπ).
   - β) Εάν η συσκευή ή το λογισμικό σας δίνει τη δυνατότητα, χρησιμοποιήστε έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) που είναι σχετικά ασφαλής μέθοδος εξουσιοδότησης πρόσβασης. Συνδυάζει δύο από τους ακόλουθους τρεις τύπους διαπιστευτηρίων: κάτι που γνωρίζετε (π.χ. κωδικό πρόσβασης ή PIN), κάτι που έχετε (π.χ. διακριτικό ή ταυτότητα) και κάτι που είστε (π.χ. βιομετρικό δακτυλικό αποτύπωμα). Δεδομένου ότι ένα από τα απαιτούμενα διαπιστευτήρια απαιτεί φυσική παρουσία, αυτό το βήμα καθιστά πιο δύσκολο για έναν παράγοντα απειλής να θέσει σε κίνδυνο τη συσκευή σας.
   - γ) Σκεφτείτε να χρησιμοποιήσετε έναν διαχειριστή κωδικών πρόσβασης (password manager). Υπάρχουν πολλές διαφορετικές επιλογές, οπότε αναζητήστε μια εφαρμογή με πολλούς χρήστες και υψηλή βαθμολογία.
2. Χρησιμοποιήστε προσωπικές πληροφορίες που μόνο εσείς γνωρίζετε όσον αφορά τις ερωτήσεις ασφαλείας κατά τη δημιουργία λογαριασμού σε κάποιον ιστότοπο.
3. Να διατηρείτε ενημερωμένες τις συσκευές και τα λογισμικά που χρησιμοποιείτε. Οι κατασκευαστές εκδίδουν συνεχώς ενημερώσεις καθώς ανακαλύπτουν ευπάθειες στα προϊόντα τους. Οι περισσότερες συσκευές (υπολογιστές, τηλέφωνα, tablets και άλλες έξυπνες συσκευές) ενημερώνονται αυτόματα, αλλά σε κάποιες άλλες ίσως χρειαστεί να το κάνετε εσείς.
4. Προσοχή για μη αναμενόμενα μηνύματα ηλεκτρονικού ταχυδρομείου και μηνύματα στα κινητά σας τηλέφωνα. Τα μηνύματα ηλεκτρονικού "ψαρέματος" (phishing) είναι ο πιο διαδεδομένος κίνδυνος για τους χρήστες. Στόχος αυτών των μηνυμάτων είναι η κλοπή των χρημάτων σας, η απόκτηση πληροφοριών για εσάς ή η εγκατάσταση κακόβουλου λογισμικού στη συσκευή σας.
5. Επιλέξτε ασφαλή δίκτυα για να συνδεθείτε, ειδικά όταν πρόκειται για ασύρματα. Εάν επιλέξετε να συνδεθείτε σε ανοιχτά δίκτυα, βεβαιωθείτε ότι χρησιμοποιείτε λογισμικό προστασίας από ιούς (antivirus) και τείχος προστασίας (firewall) στη συσκευή σας.