ΟΔΗΓΟΣ **ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ**

ΓΙΑ ΤΟΥΣ ΠΟΛΙΤΕΣ

Παρακάτω θα βρείτε βέλτιστες πρακτικές πρόληψης για την καλύτερη προστασία των προσωπικών σας πληροφοριών, υπολογιστών και συσκευών

1. Χρησιμοποιείτε ισχυρούς κωδικούς πρόσβασης

Όλοι έχουμε ακούσει ότι είναι σημαντικό να έχουμε ισχυρό κωδικό πρόσβασης, αλλά τι χαρακτηρίζεται ως ισχυρός κωδικός πρόσβασης;

Ισχυρός κωδικός πρόσβασης:
- Θα πρέπει να αποτελείται από τουλάχιστον 16 χαρακτήρες και συστήνεται να μην είναι οι ίδιοι χαρακτήρες σε ακολουθία.
- Να περιέχει και να συνδυάζει γράμματα, σύμβολα, αριθμούς και ειδικούς χαρακτήρες.
- Να μην περιέχει ποτέ στοιχεία προσωπικής ταυτοποίησης.
- Να μην επαναχρησιμοποιείται.
- Να μην χρησιμοποιείται ο ίδιος κωδικός σε συστήματα και ιστοσελίδες.
  Η χρήση μιας εφαρμογής διαχείρισης κωδικών πρόσβασης για την αποθήκευση και τη διαχείριση διαφορετικών κωδικών πρόσβασης μπορεί να σας βοηθήσει να οργανωθείτε με ασφάλεια.

2. Χρησιμοποιήστε τη μέθοδο «SLAM» για να εντοπίσετε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου:

Οι επιθέσεις «ηλεκτρονικού ψαρέματος» είναι ένα τεράστιο μέρος των σύγχρονων επιθέσεων στον κυβερνοχώρο. Ορισμένες είναι εξαιρετικά εξατομικευμένες και μπορεί να περιέχουν αναφορές σε συναδέλφους σας, μέλη της οικογένειάς σας, χόμπι σας κ.ά. Ο καλύτερος τρόπος για να μετριαστεί αυτό είναι η ευαισθητοποίηση και η διαρκής ενημέρωση. Χρησιμοποιήστε τη μέθοδο «SLAM» για να βοηθήσετε στον εντοπισμό επιθέσεων ηλεκτρονικού ψαρέματος:

- **S**ender: Ελέγξτε την ηλεκτρονική διεύθυνση (email) του αποστολέα.
- **L**inks: Τοποθετήστε το δείκτη του ποντικιού και ελέγξτε τυχόν συνδέσμους πριν κάνετε κάποιο κλικ.
- **A**ttachment: Μην ανοίγετε συνημμένα από κάποιον που δεν γνωρίζετε ή συνημμένα που δεν περιμένετε.
- **M**essage: Ελέγξτε το περιεχόμενο του μηνύματος και προσέξτε για κακή γραμματική ή ορθογραφικά λάθη.

3. Δημιουργήστε αντίγραφα ασφαλείας των δεδομένων σας

Η δημιουργία αντιγράφων ασφαλείας των δεδομένων στις συσκευές σας σε ξεχωριστή τοποθεσία είναι ένα από τα πιο σημαντικά πράγματα που θα πρέπει να κάνετε. Εάν στοχοποιηθείτε από κάποια κυβερνοεπίθεση, ενδέχεται να μην μπορείτε να αποκτήσετε πρόσβαση ή να χρησιμοποιήσετε τον υπολογιστή, το τηλέφωνο ή οποιαδήποτε άλλη συσκευή σας. Ωστόσο, εάν έχετε δημιουργήσει αντίγραφα ασφαλείας των δεδομένων σας, δεν θα χάσετε τίποτα από αυτά, ανεξάρτητα από το τι θα συμβεί στη συσκευή σας.

4. Διατηρήστε τις συσκευές και τις εφαρμογές σας ενημερωμένες

Μην αγνοείτε τις ειδοποιήσεις που λαμβάνετε για ενημερώσεις που είτε αφορούν τη συσκευή σας ή μια από τις εφαρμογές σας. Εγκαταστήστε τις ενημερώσεις αυτές άμεσα. Οι ενημερώσεις δεν αφορούν μόνο την προσθήκη νέων λειτουργιών, αλλά αφορούν τη διόρθωση ευπαθειών σε μια συσκευή ή μια εφαρμογή που θα μπορούσαν να βρουν και να χρησιμοποιήσουν οι επιτιθέμενοι για να αποκτήσουν πρόσβαση στο σύστημά σας. Εάν η συσκευή σας δεν μπορεί πλέον να λαμβάνει ενημερώσεις, συνιστούμε να προγραμματίσετε την αναβάθμιση σε νεότερο μοντέλο.

5. Ενεργοποιήστε τον έλεγχο ταυτότητας δύο παραγόντων

Ο έλεγχος ταυτότητας δύο παραγόντων (two-factor authentication — 2FA) είναι ένας επιπλέον τρόπος με τον οποίο μπορείτε να βοηθήσετε στην προστασία των διαδικτυακών λογαριασμών σας. Μπορείτε να επιλέξετε να αποσταλεί ή να δημιουργηθεί ένας κωδικός στη συσκευή σας, όπως το τηλέφωνό σας, τον οποίο μπορείτε να χρησιμοποιείτε για να επαληθεύετε ποιοι είστε κάθε φορά που συνδέεστε. Με αυτόν τον τρόπο, ακόμα κι αν κάποιος αποκτήσει πρόσβαση στον κωδικό πρόσβασης του λογαριασμού, εάν δεν λάβει κωδικό για επαλήθευση, δεν θα μπορεί να συνδεθεί στο λογαριασμό σας.

6. Αποφύγετε ευαίσθητες συναλλαγές και χρήση προσωπικών λογαριασμών σε δωρεάν Wi-Fi

Είναι καλό να είστε προσεκτικοί σχετικά με την περιήγησή σας στο διαδίκτυο όταν χρησιμοποιείτε hotspot ή δωρεάν Wi-Fi, π.χ. εάν συνδέεστε σε μια καφετέρια, τις περισσότερες φορές αυτά τα δίκτυα δεν είναι ασφαλή. Όταν ένα δίκτυο δεν είναι ασφαλές, οποιοσδήποτε μπορεί να έχει πρόσβαση σε αυτό και να κρατήσει τα δεδομένα σας. Επομένως, είναι καλύτερα να προσπαθήσετε να περιορίσετε στο ελάχιστο τη χρήση πιο ευαίσθητων συναλλαγών, καθώς και τη χρήση των προσωπικών σας λογαριασμών σε χώρους με δωρεάν Wi-Fi. Προτιμήστε να χρησιμοποιείτε το πακέτο δεδομένων σας.

7. Εγκαταστήστε ένα λογισμικό πρόγραμμα προστασίας από ιούς και πραγματοποιείτε τακτική σάρωση για ιούς

Το λογισμικό προστασίας από ιούς (antivirus) μπορεί να σας βοηθήσει να εντοπίσετε και να αφαιρέσετε κακόβουλα λογισμικά και ιούς από τον υπολογιστή σας. Εάν δεν έχετε ήδη εγκατεστημένο πρόγραμμα προστασίας από ιούς, θα πρέπει να εγκαταστήσετε άμεσα. Προμηθευτείτε ένα νόμιμο πρόγραμμα προστασίας από ιούς από γνωστή και αξιόπιστη εταιρεία. Μην κατεβάζετε απλώς οποιοδήποτε δωρεάν λογισμικό προστασίας από ιούς στο διαδίκτυο, καθώς πολλά από αυτά που βλέπετε και διαφημίζονται δωρεάν είναι ψεύτικα. Θα μπορούσαν να κατεβάσουν κακόβουλο λογισμικό στον υπολογιστή σας αντί να σας βοηθήσουν να το εντοπίσετε και να το αφαιρέσετε.

8. Να γνωρίζετε ποιες πληροφορίες μοιράζεστε στα μέσα κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης μπορεί να είναι ένας πολύ καλός τρόπος για να μοιράζεστε πληροφορίες με την οικογένεια και τους φίλους σας, αλλά μοιράζεστε και πληροφορίες με τους εισβολείς. Οι απατεώνες και οι εισβολείς μπορούν να χρησιμοποιήσουν τις πληροφορίες που δημοσιεύετε στα μέσα κοινωνικής δικτύωσης για να αποκτήσουν δεδομένα και πληροφορίες για εσάς που μπορούν να χρησιμοποιηθούν εναντίον σας. Ελέγξτε τις ρυθμίσεις απορρήτου σας σε επαναλαμβανόμενη βάση, διαγράψτε παλιούς και αχρησιμοποίητους λογαριασμούς και ελέγξτε τις φωτογραφίες και τα βίντεο σας πριν τα δημοσιεύσετε, για να βεβαιωθείτε ότι δεν υπάρχει οτιδήποτε που αποκαλύπτει στοιχεία, τα οποία μπορούν να χρησιμοποιηθούν κακόβουλα.

9. Αποφύγετε την περιήγηση και τις συναλλαγές σε ιστοσελίδες που δεν είναι κρυπτογραφημένες (πρωτόκολλο HTTPS)

Το πρωτόκολλο μεταφοράς HTTPS είναι η ασφαλής επέκταση του πρωτοκόλλου HTTP. Βεβαιωθείτε ότι κάθε ιστοσελίδα μέσω της οποίας αποστέλλετε προσωπικές πληροφορίες (κωδικούς πρόσβασης, αριθμό πιστωτικής κάρτας, κ.ά.) λειτουργεί με το πρωτόκολλο HTTPS που χρησιμοποιείται για ασφαλή κρυπτογραφημένη επικοινωνία μεταξύ προγραμμάτων περιήγησης και διακομιστών ιστού. Να ελέγχετε ότι οι ηλεκτρονικές διευθύνσεις περιέχουν το ακρωνύμιο «https», καθώς «s» σημαίνει ασφάλεια (security).

10. Ελέγξτε τις κινήσεις του τραπεζικού λογαριασμού σας

Παρακολουθήστε τις τραπεζικές σας καταστάσεις για ύποπτη δραστηριότητα, όπως αγορές ή μεταφορές μεταξύ λογαριασμών που δεν περιμένετε. Εάν δείτε οποιαδήποτε ασυνήθιστη δραστηριότητα, επικοινωνήστε αμέσως με το τραπεζικό σας ίδρυμα.

ΥΦΥΠΟΥΡΓΕΙΟ ΕΡΕΥΝΑΣ, ΚΑΙΝΟΤΟΜΙΑΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ
ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ
Αρχή Ψηφιακής Ασφάλειας
ΓΡΑΦΕΙΟ ΤΥΠΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ