Κυβερνοασφάλεια (Cybersecurity)
Τρόποι Προστασίας και Μέτρα Ασφάλειας

Αναμφίβολα, η **ραγδαία ανάπτυξη της ψηφιακής τεχνολογίας** έχει αποφέρει πολλά **οφέλη** στην καθημερινότητά μας, αλλά επίσης και **σημαντικές προκλήσεις**, όπως για παράδειγμα η ανάγκη διασφάλισης της ασφάλειας και της προστασίας των προσωπικών μας δεδομένων.

Επομένως, το θέμα της **Κυβερνοασφάλειας και της προστασίας των δεδομένων φαίνεται να είναι πιο κρίσιμο από ποτέ**.

Πώς μπορούμε όμως, να παραμείνουμε προστατευμένοι, καθώς συνεχίζουμε να απολαμβάνουμε τα οφέλη της ψηφιακής τεχνολογίας και ειδικά των τεχνολογιών που σχετίζονται με το διαδίκτυο και τις συναφείς του υπηρεσίες;

[i]Οι ακόλουθες συμβουλές για την προσωπική ασφάλεια στον κυβερνοχώρο παρέχονται για να σας βοηθήσουν να βελτιώσετε την προστασία σας από τις διαρκώς εξελισσόμενες τακτικές των χάκερ, σε ένα περιβάλλον γεμάτο προκλήσεις και δυνητικές απειλές.

- **Χρήση Ισχυρών Κωδικών Πρόσβασης**:
  - Το **μήκος του κωδικού πρόσβασης** πρέπει να είναι μεγαλύτερο από 8 χαρακτήρες.
  - Θα πρέπει **να αποφεύγεται η χρήση του ίδιου κωδικού πρόσβασης σε πέραν της μιας υπηρεσίας / ιστοτόπου**.
  - Χρησιμοποιήστε τουλάχιστον ένα κεφαλαίο γράμμα, ένα πεζό γράμμα, έναν αριθμό και ένα σύμβολο κ.λπ.
  - Διαλέξτε κωδικούς πρόσβασης που είναι εύκολο να θυμάστε και αποφύγετε να δίνετε υποδείξεις ή πληροφορίες για να είστε ασφαλείς.
  - Για να διατηρείτε τον κωδικό πρόσβασής σας σε ισχύ, επαναφέρετέ τον συχνά.

- **Χρήση Τείχους Προστασίας (Firewall) και Λογισμικού Προστασίας από Ιούς**:

  Η πιο δημοφιλής μορφή ασφάλειας έναντι επιβλαβών επιθέσεων είναι το λογισμικό προστασίας από ιούς (Antivirus). Η ασφάλεια που προσφέρει το λογισμικό προστασίας από ιούς εμποδίζει το κακόβουλο λογισμικό και άλλους καταστροφικούς ιούς να διεισδύσουν στη συσκευή σας ή να θέσουν σε κίνδυνο τα δεδομένα σας. **Στον υπολογιστή σας, θα πρέπει να έχετε ταυτόχρονα σε λειτουργία μόνο ένα λογισμικό προστασίας από ιούς. Επιπλέον, η χρήση ενός τείχους προστασίας (Firewall) είναι απαραίτητη για την προστασία των δεδομένων σας από επιζήμιες επιθέσεις**. Ένα τείχος προστασίας περιλαμβάνεται σε κάθε έκδοση των Windows και του Mac OS X, με την ονομασία Windows Firewall και Mac Firewall, αντίστοιχα.

- **Προστατευτείτε από τις απάτες phishing!**

  Σε αυτές τις περιπτώσεις αναμένονται συνήθως επιθέσεις Ransomware. Η ταυτότητα του αποστολέα χρησιμοποιείται από τον επιτιθέμενο για να ξεγελάσει τον παραλήπτη ώστε να αποκαλύψει διαπιστευτήρια, να κάνει κλικ σε έναν επιβλαβή σύνδεσμο ή να κατεβάσει ένα συνημμένο αρχείο, τα οποία θα μολύνουν το σύστημα του χρήστη με κακόβουλο λογισμικό.

  - Ποτέ μην ανοίγετε επισυναπτόμενα αρχεία από μηνύματα ηλεκτρονικού ταχυδρομείου που σας έχουν σταλθεί από αποστολείς που δεν γνωρίζετε.
  - Περάστε με το ποντίκι πάνω από τους συνδέσμους για να δείτε ποιοι είναι ασφαλείς και ποιοι όχι.
  - **Θα πρέπει να είστε καχύποπτοι απέναντι στα μηνύματα ηλεκτρονικού ταχυδρομείου που λαμβάνετε**, γι' αυτό φροντίστε να αναζητήσετε γραμματικά λάθη και να μάθετε από πού προέρχονται.
  - Είναι πιθανό φίλοι σας που έχουν επηρεαστεί παρόμοια να σας στείλουν κακόβουλους συνδέσμους. Επομένως, να είστε ιδιαίτερα προσεκτικοί.

- **Διατηρείτε πάντοτε ενημερωμένο το λογισμικό σας:**

  Μια βασική συμβουλή για την ασφάλεια στον κυβερνοχώρο ειδικά για την πρόληψη του ransomware είναι η επιδιόρθωση του ξεπερασμένου λογισμικού, συμπεριλαμβανομένων των λειτουργικών συστημάτων και των εφαρμογών.

  - **Ρυθμίστε τη συσκευή σας ώστε να λαμβάνει αυτόματα ενημερώσεις συστήματος**.
  - Οι ενημερώσεις ασφαλείας θα πρέπει να κατεβαίνουν και να εγκαθίστανται αυτόματα από το πρόγραμμα περιήγησης στο web της επιφάνειας εργασίας σας.

- **Θα πρέπει να χρησιμοποιείται έλεγχος ταυτότητας δύο ή τριών παραγόντων:**

  Η ασφάλεια ενός διαδικτυακού λογαριασμού μπορεί να αυξηθεί με τη χρήση ελέγχου ταυτότητας δύο ή πολλών παραγόντων εκτός από τον κωδικό πρόσβασης. **Ο έλεγχος ταυτότητας δύο παραγόντων μπορεί να απαιτεί τη χρήση του δακτυλικού σας αποτυπώματος, ενός προσωπικού κωδικού αναγνώρισης (PIC) ή ενός άλλου κωδικού πρόσβαση που πιθανόν να λαμβάνετε μέσω μηνύματος κειμένου στο κινητό σας τηλέφωνο**. Θα σας ζητηθεί να εισαγάγετε πρόσθετες μεθόδους ελέγχου ταυτότητας που χρησιμοποιούν τον έλεγχο ταυτότητας πολλαπλών παραγόντων, αφού εισαγάγετε τη σύνδεση και τον κωδικό πρόσβασής σας.

- **Βεβαιωθείτε ότι δημιουργείτε τακτικά αντίγραφα ασφαλείας των δεδομένων σας:**

  Μια ιδιαίτερα σημαντική πτυχή της προσωπικής ασφάλειας στο διαδίκτυο είναι **η τακτική δημιουργία αντιγράφων ασφαλείας δεδομένων** (backup). Αντίγραφα των δεδομένων σας μπορούν να αποθηκεύονται σε τοπικά μέσα (όπως ένας σκληρός δίσκος) ή και σε υπηρεσίες νέφους. Μπορείτε να ανακάμψετε από μόλυνση ή ransomware εάν έχετε ένα πρόσφατο αντίγραφο ασφαλείας δεδομένων!

- **Η χρήση της κοινωνικής δικτύωσης μπορεί να είναι επικίνδυνη:**

  Χάρη στην έλευση της σημερινής ψηφιακής εποχής, μπορούμε πλέον να μένουμε αβίαστα σε επαφή με τους αγαπημένους μας χρησιμοποιώντας πολλαπλές διαδικτυακές πλατφόρμες κοινωνικής δικτύωσης, όπως το Facebook, το WhatsApp και το Twitter. Θα πρέπει να είστε προσεκτικοί όταν μιλάτε μαζί τους στο διαδίκτυο για τη δική σας ασφάλεια. Οι χάκερ μπορεί να αποκτήσουν πρόσβαση σε πολλές προσωπικές πληροφορίες χρησιμοποιώντας τους λογαριασμούς και τους ιστότοπους των μέσων κοινωνικής δικτύωσης. Τα δεδομένα σας μπορεί να αποκτήσουν ταχεία πρόσβαση από χάκερ, γι' αυτό περιορίστε τον αριθμό των δεδομένων που μοιράζεστε στο διαδίκτυο. Τα αντίγραφα ασφαλείας αυτών των συζητήσεων δεν προστατεύονται πλήρως, επειδή διατηρούνται σε υπηρεσίες cloud, όπως το Google Drive ή το iCloud, γεγονός που τα καθιστά ευάλωτα στην ανάγνωση ή την αλλοίωση.

- **Πρέπει να χειρίζεστε τις κινητές συσκευές σας με ασφάλεια:**

  - Μην χρησιμοποιείτε την ημερομηνία γέννησής σας ή το τραπεζικό PIN ως κωδικό πρόσβασης για το κινητό σας.
  - Χρησιμοποιείτε μόνο εφαρμογές που έχετε κατεβάσει από αξιόπιστες πηγές
  - Θα πρέπει να αποφεύγεται η αποστολή γραπτών μηνυμάτων ή ηλεκτρονικού ταχυδρομείου με προσωπικές ή ευαίσθητες πληροφορίες.
  - Προς αξιοποίηση για την αποτροπή κλοπής ή απώλειας, χρησιμοποιήστε το Find My iPhone ή το Android Device Manager.
  - Δημιουργήστε τακτικά αντίγραφα ασφαλείας της κινητής συσκευής σας με το iCloud ή ενεργοποιήστε το Backup & Sync στη συσκευή Android.

[i] https://csirt.cy/security-news/top10-tips