Ηλεκτρονικό Ταχυδρομείο (Email)

Μάθημα 4

Κατηγορία: Ασφάλεια Ηλεκτρονικού Ταχυδρομείου (Email)

Περιγραφή Δραστηριότητας:

Επαφές (Contacts)

Στόχοι:

Στο τέλος του μαθήματος θα μπορούμε να:

- Κατανοούμε τους κινδύνους που μπορούν να προκύψουν από τη χρήση του ηλεκτρονικού ταχυδρομείου και να προτείνουμε τρόπους για την αντιμετώπισή τους.

Ψηφιακές δεξιότητες:

- Αξιολόγηση δεδομένων, πληροφοριών και ψηφιακού περιεχομένου.
- Προστασία προσωπικών δεδομένων και ιδιωτικότητας.

Τι θα χρειαστούμε;

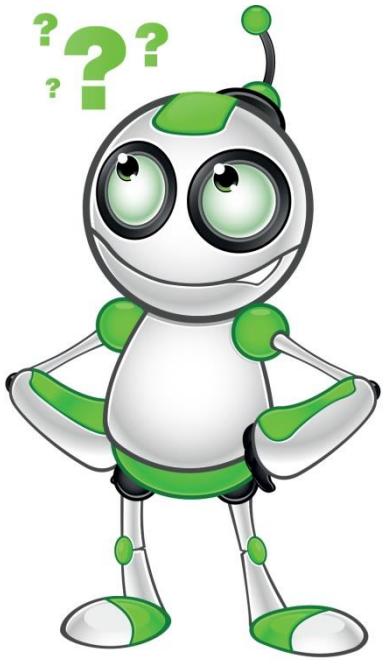
Υλικός Εξοπλισμός (Hardware):

- Ηλεκτρονικό υπολογιστή φορητό ή όχι, ή έξυπνη συσκευή.

- Πρόσβαση στο διαδίκτυο.
- Διεύθυνση Ηλεκτρονικού Ταχυδρομείου.

Λογισμικό(Software):

- Πρόγραμμα πλοήγησης



Ακροατήριο: 16 ετών και άνω

Χρονική Διάρκεια: 10 λεπτά

Επίπεδο δυσκολίας: **1**

Πριν αρχίσουμε βεβαιωνόμαστε ότι ο χρήστης έχει:

- την δυνατότητα να χειρίζεται βασικές λειτουργίες ενός Η/Υ ή μιας έξυπνης συσκευής
- βασικές δεξιότητες πλοήγησης στο Διαδίκτυο
- Διεύθυνση Ηλεκτρονικού Ταχυδρομείου.

Διαδικτυακές πλατφόρμες για ηλεκτρονικές αγορές με παρόμοια χρήση:

- www.yahoo.com
- www.outlook.com

Ας προχωρήσουμε ….

(1) Εισαγωγή

Αναμφισβήτητα, το ηλεκτρονικό ταχυδρομείο παρουσιάζει πληθώρα θετικών στοιχείων και για αυτό το λόγο αποτελεί αναπόσπαστο μέρος της ζωής μας.
Παρόλα αυτά η χρήση του εγκυμονεί αρκετούς κινδύνους . Οι συνήθεις κίνδυνοι που μπορεί να προκύψουν με τη χρήση του ηλεκτρονικού ταχυδρομείου είναι:

- Ιοί
- Ανεπιθύμητη Αλληλογραφία (spam)
- Μηνύματα οικονομικής εξαπάτησης (phishing)

(2) Κίνδυνοι που προκύπτουν από τη χρήση του ηλεκτρονικού ταχυδρομείου

Ιοί: Η μετάδοση ιών μέσω του ηλεκτρονικού ταχυδρομείου είναι ο πιο συνηθισμένος τρόπος μετάδοσής τους. Οι ιοί βρίσκονται στα συνημμένα αρχεία των μηνυμάτων. Οι χρήστες του ηλεκτρονικού ταχυδρομείου θα πρέπει να αποφεύγουν να ανοίγουν μηνύματα τα οποία προέρχονται από άγνωστο αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα αρχεία (συνήθως με κατάληξη .exe , .com, .vbs, .dll, .bat κ.ά.) ενώ υπάρχει πιθανότητα να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής .html) που ενεργοποιείται αυτόματα με την ανάγνωση του e-mail.
Θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με κάπως περίεργο θέμα.
Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντι-ιικό (antivirus) πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς.

Spam: Αναφέρεται σε μεγάλο αριθμό μηνυμάτων με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Τα μηνύματα αυτά έχουν σαν στόχο την διαφήμιση κάποιων προϊόντων ή υπηρεσιών και καταλήγουν στην ηλεκτρονική θυρίδα των παραληπτών χωρίς αυτοί να το επιθυμούν και χωρίς να έχουν συνειδητά προκαλέσει την αλληλογραφία με τον εν λόγω αποστολέα. Η ανεπιθύμητη αλληλογραφία δεν περιορίζεται μόνο στα μηνύματα με εμπορικό περιεχόμενο καθώς πολλές φορές διευκολύνει απάτες, προσφέρει πορνογραφικό υλικό ή περιέχει επικίνδυνα αρχεία, επιφυλάσσοντας έτσι κινδύνους για τους χρήστες.
Καθένας από εμάς, θα πρέπει να προσέχει ιδιαίτερα να μην απαντάει σε μηνύματα τέτοιου είδους, ούτε σε αυτά με την ένδειξη "remove me from the mailing list".
Μπορούμε επίσης, να χρησιμοποιήσουμε τα φίλτρα που του προσφέρουν τα περισσότερα web mail για να διαγράφουμε τα μηνύματα αυτά, ή να ρυθμίσουμε κατάλληλα το πρόγραμμα διαχείρισης αλληλογραφίας του υπολογιστή μας.
Επίσης, στο Διαδίκτυο υπάρχουν προγράμματα καταπολέμησης των spam, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη μας.

Phishing: είναι ένας τρόπος οικονομικής εξαπάτησης ανυποψίαστων πελατών, οι οποίοι λαμβάνουν μηνύματα από «αξιόπιστες» πηγές (τράπεζες, εταιρείες κ.λπ.) που τους ζητούν προσωπικά τους στοιχεία (συνήθως αριθμούς πιστωτικών καρτών, αριθμούς λογαριασμών τραπέζης, κωδικούς πρόσβασης κ.α.), προκειμένου να διεκπεραιώσουν συναλλαγή.
Παρόλο που οι περισσότεροι browsers έχουν ήδη αναπτύξει τεχνολογία anti-phishing προκειμένου να ανιχνεύουν τις σελίδες που ανοίγει ο χρήστης και να τον ειδοποιούν για το αν βρίσκεται σε σελίδα phishing, τα θύματα από τέτοιες επιθέσεις αυξάνονται ανησυχητικά σε όλον τον κόσμο. Ο χρήστης πρέπει να είναι ιδιαίτερα καχύποπτος απέναντι σε τέτοια μηνύματα και να επαληθεύει το περιεχόμενό τους επικοινωνώντας με την εταιρεία ή την τράπεζα που το έστειλε, όχι μέσω του μηνύματος, αλλά με τον τρόπο που χρησιμοποιούσε ως τώρα. Γενικά, οι αξιόπιστες εταιρείες και τράπεζες δεν καταφεύγουν σε γενικόλογα μηνύματα προκειμένου να εξυπηρετήσουν τους πελάτες τους, ούτε τους ζητούν να αποκαλύψουν τους κωδικούς τους. Σήμερα κυκλοφορούν αρκετά προγράμματα anti-phishing, τα οποία είτε ελέγχουν το περιεχόμενο των ιστοσελίδων που διατρέχει ο χρήστης, είτε το περιεχόμενο των e-mail.

Φτάσαμε ήδη στο τέλος του 4ου μαθήματος!!!

Αξιολόγηση του μαθήματος

Στόχος	Κυκλώστε
1. Έχουμε κατανοήσει τους κίνδυνους που προκύπτουν από τη χρήση του ηλεκτρονικού ταχυδρομείου?	ΝΑΙ/ΟΧΙ