Ασφάλεια στο διαδίκτυο

Διονύσης Πολίζος
Γυμνάσιο Οινουσσών σχολικό έτος 2020-2021

Περιεχόμενα

1. Τι είναι το διαδίκτυο..... 3
2. Ασφάλεια στο διαδίκτυο..... 3
3. Ασφάλεια προσωπικών δεδομένων 5
4. Κίνδυνοι διαδυκτίου..... 6
5. Κίνδυνος ανεπιθύμιτων μηνυμάτων..... 9
6.αντιμετώπιση προβλημάτων 9
7.Από πού μπορώ να ζητήσω βοήθεια.....10

1. Τι είναι το διαδίκτυο

Το Διαδίκτυο είναι παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι χρησιμοποιούν καθιερωμένη ομάδα πρωτοκόλλων, η οποία συχνά αποκαλείται "TCP/IP" (αν και αυτή δεν χρησιμοποιείται από όλες τις υπηρεσίες του Διαδικτύου) για να εξυπηρετεί δισεκατομμύρια χρήστες καθημερινά σε ολόκληρο τον κόσμο. Οι διασυνδεδεμένοι ηλεκτρονικοί υπολογιστές ανά τον κόσμο, οι οποίοι βρίσκονται σε ένα κοινό δίκτυο επικοινωνίας, ανταλλάσσουν μηνύματα (πακέτα) με τη χρήση διαφόρων πρωτοκόλλων (τυποποιημένοι κανόνες επικοινωνίας), τα οποία υλοποιούνται σε επίπεδο υλικού και λογισμικού. Το κοινό αυτό δίκτυο καλείται Διαδίκτυο.

2. Ασφάλεια στο διαδίκτυο

Η ασφάλεια στο Διαδίκτυο ή η διαδικτυακή ασφάλεια είναι η γνώση των κινδύνων προσωπικής ασφάλειας και ασφάλειας του χρήστη σε ιδιωτικές πληροφορίες και περιουσίες που σχετίζονται με τη χρήση του Διαδικτύου και την αυτοπροστασία από το ηλεκτρονικό έγκλημα.

Δεδομένου ότι ο αριθμός των χρηστών του Διαδικτύου συνεχίζει να αυξάνεται παγκοσμίως, διαδικτυακοί οργανισμοί, κυβερνήσεις και οι οργανισμοί εξέφρασαν ανησυχίες για την ασφάλεια των παιδιών που χρησιμοποιούν το Διαδίκτυο.

- Προσωπική Ασφάλεια

Η ανάπτυξη του Διαδικτύου δημιούργησε πολλές σημαντικές υπηρεσίες προσβάσιμες σε οποιονδήποτε συνδέεται. Μία από αυτές τις σημαντικές υπηρεσίες είναι η ψηφιακή επικοινωνία . Ενώ η υπηρεσία αυτή επέτρεπε την επικοινωνία με άλλους μέσω του Διαδικτύου, επιτρέπει επίσης την επικοινωνία με κακόβουλους χρήστες. Ενώ οι κακόβουλοι χρήστες συχνά χρησιμοποιούν το διαδίκτυο για προσωπικό κέρδος, αυτό μπορεί να μην περιορίζεται σε οικονομικό / υλικό κέρδος. Αυτό είναι ιδιαίτερα ανησυχητικό για τους γονείς και τα παιδιά, καθώς τα παιδιά

αποτελούν συχνά στόχους αυτών των κακόβουλων χρηστών. Οι κοινές απειλές για την προσωπική ασφάλεια περιλαμβάνουν: phishing, ηλεκτρονικές απάτες, κακόβουλο λογισμικό, cyberstalking, ηλεκτρονική παρενόχληση, online προσθήκες και σεξουαλικότητα.

- Ηλεκτρονική παρενόχληση

Η ηλεκτρονική παρενόχληση είναι η επίθεση εναντίον ενός ατόμου ή μιας ομάδας μέσω της χρήσης ηλεκτρονικών μέσων όπως η άμεση ανταλλαγή μηνυμάτων, τα κοινωνικά δίκτυα, το ηλεκτρονικό ταχυδρομείο και άλλες μορφές ηλεκτρονικής επικοινωνίας με σκοπό την κατάχρηση, τον εκφοβισμό ή την υπερνίκηση.

Το κινητό μας τηλέφωνο, το laptop ή ακόμα και τον υπολογιστή μας δεν τα αποχωριζόμαστε ούτε στην περίοδο των διακοπών. Δεδομένου ότι η πρόσβαση στο Internet μέσω Data συνεπάγεται συνήθως κάποιο έξτρα κόστος, υπερισχύει η πεποίθηση ότι η χρήση ενός δωρεάν Hotspot δεν μπορεί να είναι επιβλαβής και για το λόγο αυτό είναι προτιμότερη από τους χρήστες… Στην πραγματικότητα, δεν συμβαίνει κάτι τέτοιο… Με τη σύνδεση σας σε ένα ελεύθερο δίκτυο Wi-Fi, προκειμένου να ρίξετε μια ματιά στα εισερχόμενά σας ή στο timeline του Social λογαριασμού σας, κινδυνεύετε να απωλέσετε όχι μόνο κάποιους κωδικούς πρόσβασης, αλλά και κρίσιμα δεδομένα από τη συσκευή σας.

- Η σύνδεση σε ένα τυχαίο δίκτυο που βρέθηκε μπροστά σας μπορεί να θέσει σε κίνδυνο τα δεδομένα σας. Είναι μεγάλο λάθος να υποθέσετε ότι το δίκτυο το οποίο σας προσφέρουν είναι «νόμιμο» ή ελεγχόμενο από την εγκατάσταση (εστιατόριο, καφετέρια, ξενοδοχείο, κατάστημα γενικά) όπου βρίσκεστε. Ενδεχομένως να πρόκειται για κάποιο δίκτυο που έχει «δημιουργήσει» ένας εγκληματίας. Γενικός κανόνας είναι να μη συνδέεστε σε δίκτυα με την ένδειξη «Free Wi-Fi». Αν υπάρχει σχετική ένδειξη – πινακίδα στο χώρο, είναι πολύ πιθανό οι ιδιοκτήτες να θέλουν να σας αναγκάσουν να εγγραφείτε σε ένα newsletter ή να τους δώσετε το email σας για να σας στείλουν διαφημιστικά μηνύματα (αυτό δε σημαίνει απαραίτητα ότι το hotspot σχετίζεται με κάποιο κακόβουλο λογισμικό).

- Μην συνδέεστε στο mail σας ή στον τραπεζικό σας λογαριασμό.

- Αν θέλετε να διαβάσετε τα emails σας, τότε το καλύτερο που έχετε να κάνετε είναι να χρησιμοποιήσετε τον browser του υπολογιστή σας. Εκεί η σύνδεση στη θυρίδα ηλεκτρονικού ταχυδρομείου γίνεται μέσω ασφαλούς σύνδεσης: το εικονίδιο με το λουκέτο στη γραμμή διεύθυνσης είναι μια ένδειξη, ενώ ακόμα ένα σημάδι ότι τα δεδομένα μεταφέρονται κρυπτογραφημένα είναι η ύπαρξη του HTTPS (S από το Secure). Οι hackers, που ίσως «παρακολουθούν» το δίκτυο, περιμένουν από εσάς να πληκτρολογήσετε κωδικούς πρόσβασης σε θυρίδες ηλεκτρονικού ταχυδρομείου και σε λογαριασμούς σε ιστοσελίδες κοινωνικής δικτύωσης.

3. ***Ασφάλεια των προσωπικών δεδομένων***

- Στο σπίτι σας σίγουρα ο υπολογιστής ή το κινητό σας τηλέφωνο συνδέεται αυτόματα με άλλες συσκευές, όπως εκτυπωτές. Όταν είστε έξω καλό είναι να "κλείνετε" αυτή την λειτουργία, όπως και να απενεργοποιείτε το «network discovery», ώστε να μην εμφανίζεται η συσκευή σας.
- Προσοχή στις ιστοσελίδες που δεν είναι ασφαλείς.

- Εάν δεν είστε σίγουροι για μία ιστοσελίδα, μην μπείτε μέσα. Καλύτερα να είστε προσεκτικοί παρά να γεμίσετε με ιούς. Για να βεβαιωθείτε ότι μία ιστοσελίδα είναι ασφαλής, μπορείτε να δείτε στο url εάν υπάρχει ένα πράσινο εικονίδιο πριν από το «https» και ότι το «s» είναι στο τέλος του «http».
- Αποφύγετε να χρησιμοποιείτε εφαρμογές.

- Ακούγεται περίεργο αλλά όταν βρίσκεστε σε δημόσιο δίκτυο προτιμήστε να μπαίνετε κατευθείαν στην ιστοσελίδα από τον browser παρά μέσω της εφαρμογής. Ο λόγος είναι ότι οι ιστοσελίδες έχουν περισσότερη ασφάλεια σε σχέση με τις εφαρμογές.

- Μετά τη σύνδεσή σας σε ένα δίκτυο Wi-Fi και την απομάκρυνσή σας από το σημείο του hotspot, φροντίστε να διαγράψετε από τη μνήμη το δίκτυο, καθώς αν πλησιάσετε εκ νέου στο ίδιο σημείο, θα συνδεθείτε αυτόματα και μπορεί τα δεδομένα σας να περιέλθουν στην κατοχή ενός hacker – αν αυτός έχει παρέμβει στο δίκτυο.

4. Κίνδυνοι διαδικτύου

- **Εθισμός**

Μπορεί να προκύψει με την πολύωρη χρήση του διαδικτύου, όπως οι διάφορες διαδικτυακές δραστηριότητες (παιχνίδια, δωμάτια συζητήσεων, ηλεκτρονικός τζόγος και άλλα). Ένα άτομο που είναι εθισμένο συνήθως παραμελεί την προσωπική του υγεία, γευματίζει ανθυγιεινά, σταματά τα αγαπημένα του ενδιαφέροντα, εγκαταλείπει το σχολείο, συγκρούεται έντονα στο σπίτι με τους γονείς του, έχει μεγάλη ένταση και θυμό.

- **Υποκλοπή προσωπικών δεδομένων**

Είναι η πράξη της εξαπάτησης ενός χρήστη κάνοντας τον να δώσει προσωπικές πληροφορίες σε μια «πλαστή ιστοσελίδα» στο Διαδίκτυο (π.χ διεύθυνση, αριθμό ταυτότητας, αριθμούς τραπεζικών λογαριασμών κ.λπ). Μια τέτοιου είδους δραστηριότητα επιτρέπει σε κάποιον να κλέψει ή να πλαστογραφήσει τα στοιχεία του χρήστη και να κερδίσει παράνομη πρόσβαση στα δεδομένα του, όπως προσωπικούς λογαριασμούς, e-mail, κωδικούς, κ.λπ.

- **Παραπληροφόρηση**

Είναι δυνατό να συμβεί με την παρουσίαση διάφορων ψευδών ή τροποποιημένων πληροφοριών σε ιστοσελίδες, με πιθανό σκοπό την παραπλάνησή μας. Παραπληροφόρηση συμβαίνει και όταν οι πληροφορίες είναι ελλιπείς με αποτέλεσμα να οδηγήσουν σε λανθασμένα συμπεράσματα.

- **Συνομιλίες με αγνώστους**

Ποτέ δεν μπορούμε να είμαστε σίγουροι για το ποιος είναι ο συνομιλητής μας, ιδιαίτερα αν είναι κάποιος άγνωστος σε μας. Γι' αυτό δεν πρέπει να δίνουμε καμία προσωπική πληροφορία σε έναν άγνωστο. Πολλοί δίνουν ψεύτικα στοιχεία όπως φύλο, όνομα, ηλικία και έχουν σκοπό να αποσπάσουν πληροφορίες από τον χρήστη ή να τον βλάψουν.

- **Εκφοβισμός**

Είναι η συνεχόμενη, εχθρική συμπεριφορά απέναντι σε ένα άτομο με σκοπό να του προκαλέσει συναισθηματικά και ψυχολογικά προβλήματα. Ο εκφοβισμός μπορεί να αφορά άτομα διαφορετικής εθνικότητας, κιλών, ύψους, θρησκείας, αντιλήψεων και άλλα και εκφράζεται συνήθως με ηλεκτρονικά μηνύματα, φωτογραφίες ή βίντεο.

- **Ανεπιθύμητα μηνύματα**

Παραδείγματα ανεπιθύμητων μηνυμάτων είναι μηνύματα που περιέχουν διαφημιστικά προϊόντα, μηνύματα για ψεύτικα παιχνίδια, για ψεύτικες υπηρεσίες, για πορνογραφικό υλικό κτλ.

- **Αποξένωση από τον πραγματικό κόσμο**
  Αρκετοί είναι αυτοί οι οποίοι ξοδεύουν άπειρες ώρες μπροστά στον υπολογιστή παίζοντας διαδικτυακά παιχνίδια, σερφάροντας στο Διαδίκτυο ή ακόμα και επικοινωνώντας με φίλους τους μέσω του διαδικτύου. Η πολύωρη ενασχόληση με τα πιο πάνω, οδηγεί πολλές φορές στην αποξένωση από τον πραγματικό κόσμο και στην μείωση της επικοινωνίας με γονείς, με φίλους κλπ.

- **Παραβίαση πνευματικών δικαιωμάτων**

Στο διαδίκτυο υπάρχουν εικόνες, κείμενα, βίντεο που μας προσφέρονται δωρεάν αλλά δεν μας ανήκουν γιατί δεν τα δημιουργήσαμε εμείς. Αυτός που τα δημιούργησε έχει τα πνευματικά δικαιώματα γι'αυτά, δηλαδή μόνο εκείνος έχει το δικαίωμα να λέει ότι τα δημιούργησε. Πολλοί χρησιμοποιούν υλικό που δεν είναι δικό τους και το παρουσιάζουν σαν δικό τους, με αποτέλεσμα να καταπατούν τα πνευματικά δικαιώματα του ιδιοκτήτη. Αν θέλουμε να χρησιμοποιήσουμε το υλικό, θα πρέπει να πάρουμε την άδεια του ιδιοκτήτη.

- **Αποπλάνηση**

Συμβαίνει όταν άγνωστοι εκμεταλλεύονται το στοιχείο της ανωνυμίας στο Διαδίκτυο για να προσεγγίσουν ανήλικα παιδιά με στόχο τη σεξουαλική παρενόχληση. Στο Διαδίκτυο ποτέ δεν μπορούμε να είμαστε σίγουροι ποιος είναι ο συνομιλητής, ακόμα και αν βλέπουμε τη φωτογραφία του ή αν χρησιμοποιούμε κάμερα. Πολλοί δίνουν ψεύτικα στοιχεία και ξεκινούν συζητήσεις με παιδιά, με στόχο να αναπτύξουν φιλία με αυτά και να αποσπάσουν περισσότερες πληροφορίες.

- **Ακατάλληλο περιεχόμενο**
  Συνήθως με τον όρο ακατάλληλο περιεχόμενο, αναφερόμαστε σε

περιεχόμενο, το οποίο μπορεί να περιλαμβάνει ρατσιστικό περιεχόμενο, προώθηση λάθος συμπεριφορών, προώθηση τυχερών παιχνιδιών, παρουσίαση πορνογραφικού υλικού, προώθηση βίας κ.λ.π. και μπορεί να προκαλέσει ψυχικές διαταραχές και να σοκάρει τον χρήστη

- **Παρακίνηση σε επιβλαβείς συμπεριφορές**
  Επειδή είναι αδύνατο να ελέγξει κανείς όλο το περιεχομένο του διαδικτύου, υπάρχουν πολλές ιστοσελίδες που παρακινούν σε επιβλαβείς συμπεριφορές, όπως ιστοσελίδες για τη βουλιμία, την ανορεξία, την αυτοκτονία, τον σατανισμό, τα τυχερά παιχνίδια και άλλα.

- **Παραβίαση ιδιωτικότητας**

Σε κάθε βήμα της γνωριμίας μας με το Διαδίκτυο "προσφέρουμε" προσωπικές πληροφορίες. Αυτές οι πληροφορίες είναι σαν ένα γρίφος που πρέπει να συμπληρωθεί για να αποκαλυφθεί η εικόνα μας. Πρέπει να γνωρίζουμε πως ότι και αν κάνουμε στο Διαδίκτυο αφήνει ίχνη. Αν δημοσιεύσουμε, δηλαδή, κάποια πληροφορία στο διαδίκτυο και μετά τη διαγράψουμε, τότε πρέπει να γνωρίζουμε ότι η πληροφορία δεν διαγράφεται οριστικά.

- **Ιοί**

Είναι κακόβουλο πρόγραμμα, το οποίο εγκαθίσταται στον υπολογιστή, συνήθως χωρίς να το γνωρίζει ο χρήστης, και ενεργοποιείται είτε μετά από κάποιο χρονικό διάστημα είτε ύστερα από κάποια συγκεκριμένη ενέργεια. Η ενεργοποίηση ενός ιού μπορεί να έχει επικίνδυνες συνέπειες, όπως το συνεχές άνοιγμα διαφόρων παραθύρων στην οθόνη, την καταστροφή αρχείων ή άλλες βλάβες. Ένας ιός ενσωματώνεται σε ηλεκτρονικά μηνύματα και προγράμματα, έτσι ώστε όταν ανοίξουμε τα μηνύματα αυτά ή εκτελέσουμε τα προγράμματα, ενεργοποιούμε άθελά μας και τον ιό.

- **Φυσικές παθήσεις**

Όταν κάνουμε υπερβολική χρήση του υπολογιστή, αυτό μπορεί να δημιουργήσει κινδύνους για την υγεία μας, όπως διαταραχές στην όρασή μας λόγω της ακτινοβολίας από την οθόνη, προβλήματα στον σκελετό και στο μυικό μας σύστημα επειδή καθόμαστε πολλές ώρες μπροστά από τον υπολογιστή, προβλήματα στον αυχένα, πόνους στους αγκώνες, τενοντίτιδα και άλλες παθήσεις.

5. *Κίνδυνοι ανεπιθύμητα μηνύματα*

Ανεπιθύμητα Μηνύματα θεωρούνται τα μηνύματα εκείνα που υπό κανονικές συνθήκες οι χρήστες δεν θα επέλεγαν να δουν και τα οποία διανέμονται σε μεγάλο αριθμό παραληπτών. Παραδείγματα ανεπιθύμητων μηνυμάτων είναι μηνύματα που περιέχουν διαφημιστικά για αμφίβολα προϊόντα, μηνύματα με περιεχόμενο που συσχετίζεται με ψευδοτυχερά παιχνίδια, ψευδονομικές υπηρεσίες κτλ. Πολύ συχνό φαινόμενο είναι και η λήψη αλυσιδωτών μηνυμάτων .Τα μηνύματα αυτά είναι, συνήθως, ανεπιθύμητα και ο αποστολέας ζητά από τον παραλήπτη να προωθήσει το μήνυμα σε άλλα άτομα, τα οποία γνωρίζει. Ο κίνδυνος εδώ, είναι ότι κάθε φορά που προωθούμε ένα μήνυμα, αν δεν είμαστε προσεχτικοί, μαζί με αυτό εμφανίζεται και η ηλεκτρονική διεύθυνση όλων των προηγούμενων ατόμων που προώθησαν το ίδιο μήνυμα. Έτσι δεν γνωρίζουμε ποιος θα παραλάβει το μήνυμα και τι θα κάνει με τις ηλεκτρονικές διευθύνσεις, οι οποίες θα εμφανίζονται σε αυτό.

6. *Αντιμετώπιση προβλημάτω*

Είμαστε προσεχτικοί όταν δίνουμε την ηλεκτρονική μας διεύθυνση. Ρυθμίζουμε την υπηρεσία φιλτραρίσματος του ηλεκτρονικού μας ταχυδρομείου, ώστε να σταματά ανεπιθύμητα μηνύματα.
Όταν το μήνυμα είναι από άγνωστο αποστολέα να μην παραπλανόμαστε ώστε να κάνουμε κλικ σε συνδέσμους, γιατί αυτό επιβεβαιώνει στον αποστολέα ότι η ηλεκτρονική διεύθυνσή μας είναι σωστή. Έτσι, ο αποστολέας θα συνεχίσει να την χρησιμοποιεί ή θα μπορέσει πιο εύκολα να την πουλήσει σε άλλους.
Είμαστε προσεχτικοί όταν δίνουμε τον αριθμό του κινητού μας τηλεφώνου. Ανεπιθύμητα μηνύματα μπορούμε να πάρουμε και στο κινητό. Χρησιμοποιούμε την κρυφή κοινοποίηση το ηλεκτρονικό ταχυδρομείο, εάν θέλουμε να προωθήσουμε κάποιο μήνυμα σε πολλούς παραλήπτες, ούτως ώστε να προστατεύσουμε τις ηλεκτρονικές διευθύνσεις των παραληπτών.
Όταν δεχόμαστε ανεπιθύμητα μηνύματα, τα διαγράφουμε χωρίς να τα διαβάζουμε. Έτσι, αν παίρνουμε πολλά ανεπιθύμητα μηνύματα στη δεύτερη διεύθυνση μπορούμε εύκολα να τη διαγράψουμε και να δημιουργήσουμε μια καινούρια. Μπορούμε να κρύψουμε την ηλεκτρονική μας διεύθυνση από προγράμματα ανίχνευσης ηλεκτρονικών διευθύνσεων.

7. Από πού μπορώ να ζητήσω βοήθεια

Αν κάποιος μας απειλή στο ίντερνετ μπορούμε να ζητήσουμε βοήθεια από κάποιον συγγενή από την αστυνομία στους εκπαιδευτικούς.