3ο ΓΥΜΝΑΣΙΟ ΥΜΗΤΤΟΥ **ΣΧ. ΕΤΟΣ: 2020-2021**

ΠΛΗΡΟΦΟΡΙΚΗ Α' ΓΥΜΝΑΣΙΟΥ

Διαδίκτυο:
Ένα ασφαλές εργαλείο
ή
μια επικίνδυνη εφεύρεση;

Μυρτώ Κομίνη-Αλτάνη

Τμήμα: Α1(α)

Ημ/νία παράδοσης: 24 Απριλίου 2021

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος

Η εργασία αυτή πραγματοποιήθηκε στο πλαίσιο του μαθήματος της πληροφορικής και αναφέρεται στους κινδύνους του διαδικτύου και στις πρακτικές προστασίας μας από αυτούς. Στην εποχή μας, όλοι σχεδόν έχουμε κάποια συσκευή με πρόσβαση στο Διαδίκτυο. Πλοηγούμαστε σε αυτό καθημερινά, ειδικά με την κατάσταση που επικρατεί αυτή τη στιγμή, λόγω της πανδημίας του covid-19. Αρκετοί υποστηρίζουν πως το Διαδίκτυο μόνο ωφελεί ή μόνο βλάπτει, αλλά πρέπει να παραδεχτούμε πως, όπως όλα τα πράγματα, έχει και οφέλη αλλά και κινδύνους. Οι κίνδυνοι αυτοί χωρίζονται σε δύο κατηγορίες: κίνδυνοι από τη λανθασμένη χρήση του αλλά και από διαδικτυακές απάτες. Είναι πολύ εύκολο να αντιμετωπίσουμε και τα δύο αυτά είδη κινδύνων, έχοντας υπόψη μας ποιοι είναι οι πιο συνηθισμένοι και εφαρμόζοντας κάποιες βασικές και απλές τεχνικές που θα δούμε παρακάτω.

1. Ιστορία και Ανάπτυξη του Διαδικτύου

1.1 Τι είναι το Διαδίκτυο;

Το **Διαδίκτυο** (Internet) είναι ένα παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι ανταλλάσσουν δεδομένα με σκοπό την εξυπηρέτηση δισεκατομμυρίων χρηστών καθημερινά σε ολόκληρο τον κόσμο. Το σύνολο των διασυνδεδεμένων ηλεκτρονικών υπολογιστών ανά τον κόσμο, σχηματίζουν ένα κοινό δίκτυο επικοινωνίας και ανταλλάσσουν μηνύματα (πακέτα δεδομένων) με τη χρήση διαφόρων τυποποιημένων κανόνων επικοινωνίας (πρωτόκολλα), τα οποία υλοποιούνται σε επίπεδο υλικού και λογισμικού. Η χρήση του Διαδικτύου αφορά κυρίως την ενημέρωση (ειδήσεις), την επικοινωνία (ανταλλαγή μηνυμάτων, κοινωνικά δίκτυα) την ψυχαγωγία (μουσική, ταινίες) καθώς και την πραγματοποίηση ηλεκτρονικών οικονομικών συναλλαγών (αγορές, πληρωμές λογαριασμών).

1.2 Ιστορία και ανάπτυξη του Διαδικτύου

Το Διαδίκτυο αναπτύχθηκε και εξελίχθηκε με ταχύτατους ρυθμούς μέσα σε λίγα χρόνια κατέχοντας κυρίαρχη θέση στην καθημερινότητα εκατομμυρίων ανθρώπων σε όλο τον κόσμο. Είναι λοιπόν, αξιοσημείωτο να αναφέρουμε το πως ξεκίνησε. Το Διαδίκτυο όπως το γνωρίζουμε σήμερα αποτελεί την εξέλιξη ενός πειραματικού δικτύου από τις ΗΠΑ κατά τη διάρκεια του ψυχρού πολέμου, που ονομαζόταν Arpanet. Ήταν ένα ερευνητικό πρόγραμμα της κυβέρνησης των ΗΠΑ, επιχορηγούμενο από την Advanced Research Projects Agency (ARPA).

Αρχικός στόχος της ARPA ήταν η διασύνδεση των υπολογιστικών δικτύων, ώστε να υπάρχει η δυνατότητα χρήσης υπολογιστών σε ευρύτερες περιοχές. Σκοπός των Αμερικανών στρατιωτικών ήταν η κατασκευή ενός δικτύου, το οποίο δεν θα κατέρρεε σε περίπτωση καταστροφής μερικών κόμβων του, κάτι που επιτυγχάνεται και την σημερινή δομή του Internet. Εγκαταστάθηκε και λειτούργησε για πρώτη φορά το 1969.

Το Internet αναπτύχθηκε γρήγορα στις δεκαετίες του 1980 και 1990. Η μεγάλη άνθιση του Διαδικτύου ξεκίνησε με την εφαρμογή της υπηρεσίας του Παγκόσμιου Ιστού στο ερευνητικό ίδρυμα CERN στην Ελβετία το 1989.

Σήμερα, το Διαδίκτυο έχει πολύ γενικότερη χρήση, διατηρώντας τα χαρακτηριστικά σταθερότητας με βάση τα οποία σχεδιάστηκε από την αρχή αλλά και πολλά περισσότερα. Στο Σχήμα 1, παρουσιάζονται επιγραμματικά μερικά σημεία-σταθμοί στην ανάπτυξη του Διαδικτύου.

Σχήμα 1: Σημεία-σταθμοί στην ανάπτυξη του Διαδικτύου.
Πηγή: Broadband search, Who Invented the Internet – A Full History
(Μετάφραση: Μ. Κομίνη-Αλτάνη)

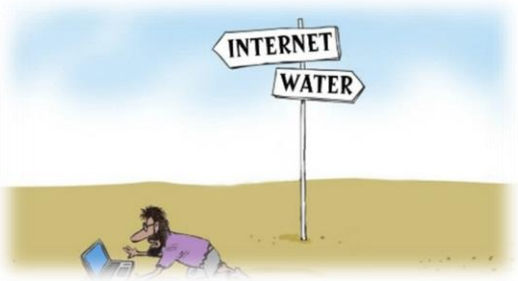
2. Κίνδυνοι και Απάτες στο Διαδίκτυο

Οι κίνδυνοι από την χρήση του Διαδικτύου, σχετίζονται τόσο με λανθασμένες πρακτικές και συνήθειες όσο και με κακόβουλες ενέργειες με σκοπό την εξαπάτηση.

2.1 Κίνδυνοι από λανθασμένες πρακτικές και συνήθειες στην χρήση του Διαδικτύου

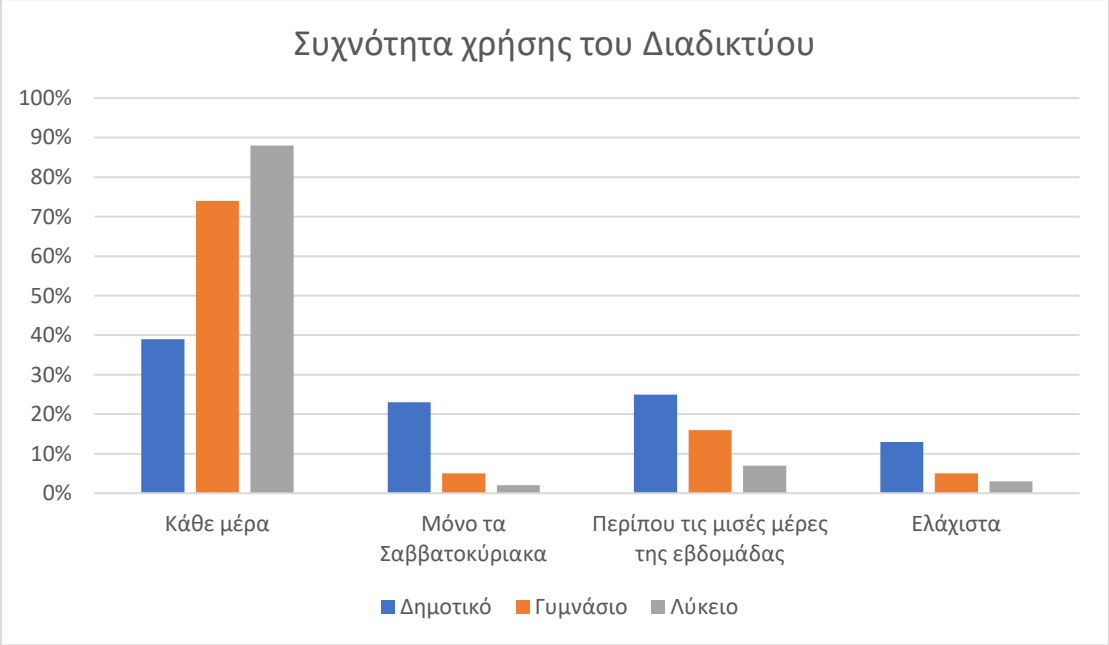
1. Εθισμός

Εθισμός στο Διαδίκτυο μπορεί να προκύψει με την πολύωρη ενασχόληση ατόμων σε διαδικτυακές δραστηριότητες όπως είναι τα παιχνίδια, δωμάτια συζητήσεων, ηλεκτρονικός τζόγος και άλλα. Ένα άτομο είναι εθισμένο όταν χαρακτηρίζεται από τουλάχιστο τρία από τα πιο κάτω:



- Χρήση του Διαδικτύου για μεγαλύτερο χρονικό διάστημα από το προτιθέμενο.
- Κατανάλωση υπερβολικού χρόνου ή/και χρήματος σε δραστηριότητες σχετικές με το Διαδίκτυο.
- Συμπτώματα συνδρόμου εξάρτησης, όπως για παράδειγμα άγχος, έμμονη σκέψη για το Διαδίκτυο, όνειρα για το Διαδίκτυο.
- Μείωση λειτουργικότητας του ατόμου. Συνήθως τα άτομα παραμελούν την προσωπική τους υγεία, γευματίζουν ανθυγιεινά, σταματούν τα αγαπημένα τους ενδιαφέροντα, εγκαταλείπουν το σχολείο, συγκρούονται έντονα στο σπίτι με τους γονείς τους, έχουν μεγάλη ένταση και θυμό που οδηγεί ακόμα και στη βία.
- Συνέχιση χρήσης του Διαδικτύου παρά τη γνώση της παραπάνω δυσλειτουργίας.

Σύμφωνα με στατιστικά στοιχεία της Μονάδας Εφηβικής Υγείας (Μ.Ε.Υ.) στην Ελλάδα, το φαινόμενο είναι συχνότερο σε αγόρια, σε δυσλειτουργικές οικογένειες και σε παιδιά με καταθλιπτικά συναισθήματα ή σύνδρομο υπερκινητικότητας. Στο Διάγραμμα 1, αναφέρονται στοιχεία για την συχνότητα χρήσης του Διαδικτύου από μαθητές.

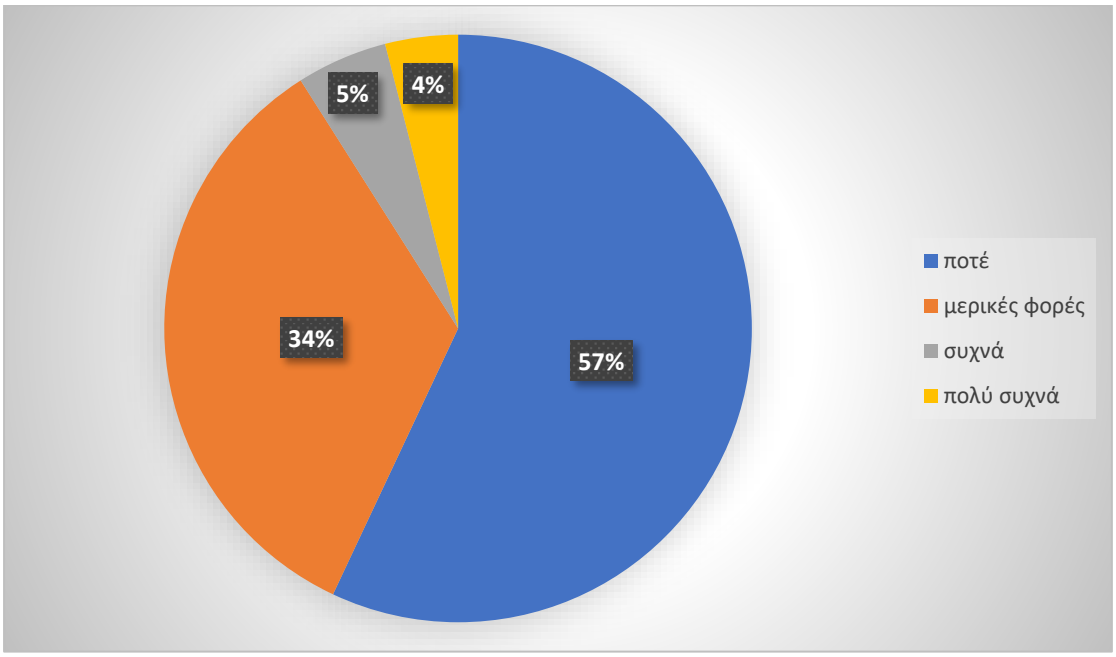


Διάγραμμα 1: Συχνότητα χρήσης του Διαδικτύου από μαθητές Δημοτικού, Γυμνασίου και Λυκείου.
Πηγή: Έρευνα σε 14.000 μαθητές ηλικίας 10-17 ετών για τις διαδικτυακές συνήθειες, Ελληνικό Κέντρο Ασφαλούς Διαδικτύου.

2. Αποξένωση από τον πραγματικό κόσμο

Αρκετοί άνθρωποι 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, εφόσον επιτρέπει στους ανθρώπους να ψυχαγωγούνται ή να επικοινωνούν χωρίς τα πλεονεκτήματα και τα μειονεκτήματα της προσωπικής επαφής. Αρκετοί είναι αυτοί για παράδειγμα οι οποίοι αναπτύσσουν διαδικτυακές (online) σχέσεις χωρίς να εγκαταλείπουν τα σπίτια τους.

Όλα αυτά γίνονται σε βάρος του χρόνου που διαφορετικά μπορούν να έχουν διαθέσιμο για τη συμμετοχή σε άλλες δραστηριότητες με φίλους, γείτονες ή ομάδες ανθρώπων με κοινά ενδιαφέροντα. Στο Διάγραμμα 2, αναφέρονται σχετικά στοιχεία για μαθητές.



Διάγραμμα 2: Συχνότητα παραμέλησης δραστηριοτήτων λόγω ενασχόλησης με το Διαδίκτυο από μαθητές Δημοτικού, Γυμνασίου και Λυκείου.
Πηγή: Έρευνα σε 14.000 μαθητές ηλικίας 10-17 ετών για τις διαδικτυακές συνήθειες, Ελληνικό Κέντρο Ασφαλούς Διαδικτύου.

3. Ηλεκτρονικός τζόγος

Πρόκειται για δραστηριότητα κατά την οποία δύο ή περισσότερα άτομα συναντώνται διαδικτυακά με σκοπό την ανταλλαγή στοιχημάτων. Μια τέτοια δραστηριότητα περιλαμβάνει το ρίσκο της πραγματικής οικονομικής απώλειας ή του κέρδους. Ένα από τα βασικότερα προβλήματα του τζόγου είναι η απώλεια χρημάτων. Κάποιος μπορεί να χάσει τις οικονομίες του, το σπίτι του, την περιουσία του ακόμη και τον/την σύζυγό της/του, λόγω των συνεπαγόμενων προβλημάτων στην σχέση τους. Πολλοί είναι αυτοί που εθίζονται και δεν μπορούν να σταματήσουν πιστεύοντας πως στον επόμενο γύρο θα πάρουν τα χρήματά τους πίσω. Η ευκολία πρόσβασης σε ιστοσελίδες ηλεκτρονικού τζόγου

αυξάνει τους κινδύνους εμπλοκής παιδιών και εφήβων σε τέτοιες δραστηριότητες.

4. Παραποίηση γλώσσας

Η ανάγκη για γρήγορη και εύκολη επικοινωνία, μια συνήθεια που την αποκτήσαμε με την είσοδο της κινητής τηλεφωνίας και του Διαδικτύου στη ζωή μας, άρχισε να οδηγεί στην παραποίηση της γλώσσας μας. Αντί για ελληνικά χρησιμοποιούνται τα «greeklish», δηλαδή, ελληνικά γραμμένα με λατινικούς χαρακτήρες, στα οποία ο τονισμός και η ορθογραφία δεν είναι σημαντικά. Για παράδειγμα η φράση «θα σε δω σε λίγο» αποδίδεται εσφαλμένα «tha se do se ligo».

Αυτό ξεκίνησε, επειδή η χρήση του ελληνικού αλφαβήτου στην τεχνολογία ήταν είτε αδύνατη, είτε δύσκολη. Παρόλο που τα τελευταία χρόνια πολλοί υπολογιστές και προγράμματα χρησιμοποιούν την ελληνική γλώσσα, πάρα πολλοί δεν επικοινωνούν στα ελληνικά αλλά σε greeklish, όταν στέλνουν μηνύματα στο κινητό ή όταν χρησιμοποιούν το Διαδίκτυο. Υπάρχουν επίσης ιστοσελίδες, όπου η γλώσσα που χρησιμοποιείται δεν είναι τα Ελληνικά αλλά τα greeklish. Όλα αυτά μπορούν να οδηγήσουν όχι μόνο στη παραποίηση της γλώσσας μας αλλά, όπως κάποιοι υποστηρίζουν, και στην αλλοίωση της πολιτιστικής μας ταυτότητας.

2.2 Κακόβουλες ενέργειες και κίνδυνοι εξαπάτησης στο Διαδίκτυο

1. Παραπληροφόρηση

Αν και τα πλεονεκτήματα της γρήγορης και εύκολης πρόσβασης στην πληροφορία μέσω του Διαδικτύου είναι τεράστια, υπάρχει παράλληλα και ο κίνδυνος να εκτεθούμε σε πληροφορίες, οι οποίες δεν ανταποκρίνονται στην πραγματικότητα, είναι ελλιπείς ή είναι τροποποιημένες, με πιθανό σκοπό την παραπλάνησή μας.

Διαδικτυακά καταστήματα	18,12%
Διαδικτυακές πύλες (portals)	15,94%
Τράπεζες	10,72%
Κοινωνικά δίκτυα και blogs	10,02%
Συστήματα ηλεκτρονικών πληρωμών	8,41%
Υπηρεσίες μηνυμάτων (IMS)	6,09%
Εταιρείες τηλεπικοινωνιών	4,14%
Εταιρείες πληροφορικής (IT)	1,93%
Οικονομικές υπηρεσίες	1,29%
Εταιρείες μεταφορών (delivery)	0,97%
Άλλο	22,38%

Πίνακας 1: Κατανομή οργανισμών που στοχοποιούνται για την υποκλοπή στοιχείων μέσω phishing.
Πηγή: Spam and phishing in 2020 (report), www.securelist.com
(Μετάφραση: Μ. Κομίνη-Αλτάνη)

2. Υποκλοπή προσωπικών δεδομένων

Η υποκλοπή προσωπικών δεδομένων στο Διαδίκτυο είναι πράξη εξαπάτησης ενός χρήστη με σκοπό την απόσπαση προσωπικών πληροφοριών (π.χ. διεύθυνση, αριθμό ταυτότητας, αριθμό διαβατηρίου, αριθμούς τραπεζικών λογαριασμών, πιστωτικών καρτών κ.λπ.).

Μια συνήθης τεχνική υποκλοπής είναι το ηλεκτρονικό "ψάρεμα" (phishing), το οποίο συμβαίνει συχνά μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου και άμεσων μηνυμάτων και μπορεί να περιέχει συνδέσμους σε ιστότοπους που

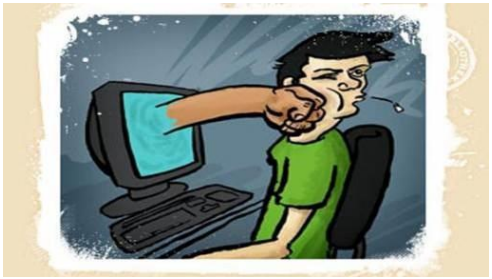
κατευθύνουν τον χρήστη να εισαγάγει τις προσωπικές του πληροφορίες. Αυτές οι ψεύτικες ιστοσελίδες είναι προσεκτικά σχεδιασμένες ώστε να είναι αληθοφανείς ώστε να αποφεύγεται η υποψία από τον χρήστη. Μια τέτοιου είδους δραστηριότητα επιτρέπει σε έναν απατεώνα να κλέψει ή να πλαστογραφήσει τα στοιχεία του θύματος ή/και να κερδίσει παράνομη πρόσβαση στα δεδομένα του, όπως προσωπικούς λογαριασμούς, συνδρομές, email, κωδικούς, κ.λπ.

3. Αποπλάνηση

Αποπλάνηση συμβαίνει, όταν άγνωστοι εκμεταλλεύονται κακόβουλα το στοιχείο της ανωνυμίας στο Διαδίκτυο, για να προσεγγίσουν ανήλικα παιδιά με στόχο τη σεξουαλική παρενόχληση. Στο Διαδίκτυο ποτέ δεν μπορούμε να είμαστε σίγουροι για την πραγματική ταυτότητα του συνομιλητή μας στις ηλεκτρονικές μας επικοινωνίες, ακόμα και αν βλέπουμε τη φωτογραφία του ή αν χρησιμοποιούμε κάμερα. Έτσι, πολλοί επιτήδειοι εκμεταλλεύονται το γεγονός αυτό, δίνουν ψεύτικα στοιχεία (κυρίως για την ηλικία τους) και ξεκινούν συζητήσεις με τα πιθανά θύματά τους με στόχο να αναπτύξουν φιλική με αυτά σχέση και να αποσπάσουν όσο το δυνατό περισσότερες πληροφορίες (π.χ. τόπο διαμονής, τα ενδιαφέροντά τους, τα χόμπι τους, τις σεξουαλικές τους εμπειρίες κ.λ.π.).

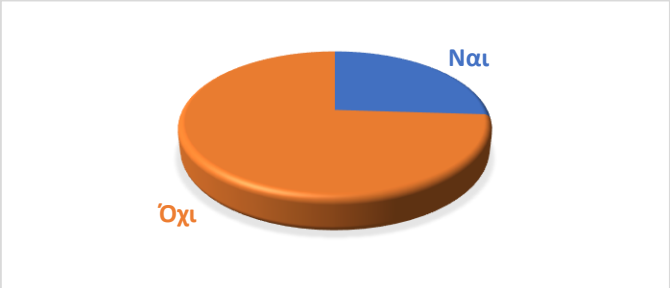
Τα δωμάτια επικοινωνίας (chat rooms) είναι ένας δημοφιλής τρόπος επικοινωνίας μεταξύ των νέων αλλά και δημοφιλές μέσο αποπλάνησης. Αυτά είναι εικονικά μέρη όπου άνθρωποι από όλο τον κόσμο μπορούν να «συναντηθούν» και να «συνομιλήσουν» μέσω μηνυμάτων. Πρέπει να γνωρίζουμε, όμως, ότι οποιοσδήποτε μπορεί, χρησιμοποιώντας απλά ένα ψευδώνυμο, να παρακολουθεί ή να συμμετέχει σε συζητήσεις μας.

4. Εκφοβισμός



Εκφοβισμός είναι δυνατό να συμβεί μέσω του Διαδικτύου και περιλαμβάνει εσκεμμένη, επαναλαμβανόμενη και εχθρική συμπεριφορά απέναντι σε άτομο ή ομάδα ατόμων με σκοπό την πρόκληση συναισθηματικής και ψυχολογικής βλάβης. Ο διαδικτυακός εκφοβισμός συνήθως έχει τη μορφή ενός εκφοβιστικού, ρατσιστικού, προσβλητικού ή πρόστυχου ηλεκτρονικού μηνύματος, φωτογραφίας ή βίντεο. Κάποιες φορές ο εκφοβισμός μπορεί να οδηγήσει στο να περιθωριοποιηθούν και να αποκλειστούν ένα η περισσότερα άτομα από μια ομάδα ή κοινότητα. Στο Διάγραμμα 3 αναφέρονται στοιχεία για το ποσοστό παιδιών/εφήβων που έχουν υποστεί σχετική ενόχληση στο Διαδίκτυο.

Ο διαδικτυακός εκφοβισμός διαφέρει από τα άλλα είδη εκφοβισμού, αφού επεμβαίνει στον προσωπικό χώρο του θύματος. Ο εκφοβισμός αυτός είναι δύσκολο να περιοριστεί, αφού δεν υπάρχει περιορισμός ούτε των μηνυμάτων που διανέμονται ηλεκτρονικά, ούτε του αριθμού των παραληπτών που μπορούν να γίνουν αποδέκτες αυτών των μηνυμάτων. Η σύγχρονη έρευνα έχει δείξει ότι το σχολείο, όταν υπάρχει πληροφόρηση και ενημέρωση του προσωπικού, μπορεί να αντιμετωπιστεί το πρόβλημα.



Διάγραμμα 3: Ποσοστό παιδιών/εφήβων που έχουν υποστεί ενόχληση στο διαδίκτυο
Πηγή: Έρευνα σε 14.000 μαθητές ηλικίας 10-17 ετών για τις διαδικτυακές συνήθειες, Ελληνικό Κέντρο Ασφαλούς Διαδικτύου.

5. Παιδική πορνογραφία

Παιδική πορνογραφία ορίζεται ως η αναπαράσταση ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες. Μερικές φορές ο ορισμός περιλαμβάνει εικόνες που έχουν υποστεί επεξεργασία από ηλεκτρονικό υπολογιστή. Η εξάπλωση των κυκλωμάτων παιδοφιλίας είναι ανησυχητική. Τα κυκλώματα αυτά είναι ομάδες ατόμων, τα οποία εργάζονται μαζί μέσω του Διαδικτύου με στόχο τη συλλογή και διανομή πορνογραφικού υλικού για τη δική τους ικανοποίηση. Η παιδική πορνογραφία θεωρείται έγκλημα και υπόκειται σε ποινικές κυρώσεις.

6. Κακόβουλο λογισμικό

Ο Ιός είναι ένα είδος κακόβουλου προγράμματος, το οποίο εγκαθίσταται στον υπολογιστή, συνήθως εν αγνοία του χρήστη, και ενεργοποιείται είτε κάποια προκαθορισμένη χρονική στιγμή είτε ύστερα από κάποια συγκεκριμένη ενέργεια. Η ενεργοποίηση ενός ιού μπορεί να έχει ως αποτέλεσμα διάφορες συνέπειες, επικίνδυνες ή μη. Συγκεκριμένα, μπορεί να έχει ως αποτέλεσμα το συνεχές άνοιγμα διαφόρων παραθύρων στην οθόνη, μπορεί, όμως, και να προκαλέσει την καταστροφή δεδομένων σε αρχεία 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. Ένα άλλο είδος κακόβουλου λογισμικού είναι το λογισμικό υποκλοπής spyware το οποίο σχεδιάζεται για την συλλογή και τη μετάδοση ιδιωτικών πληροφοριών, όπως κωδικών πρόσβασης, χωρίς τη συγκατάθεση ή τη γνώση του χρήστη. Συχνά διανέμεται μέσω ηλεκτρονικού ταχυδρομείου, από ανεπίσημες τοποθεσίες. Το κακόβουλο λογισμικό είναι ένα από τα πιο διαδεδομένα προβλήματα ασφαλείας, καθώς συχνά είναι αδύνατο να προσδιοριστεί εάν ένα αρχείο έχει μολυνθεί, ακόμα και αν είναι ασφαλής η πηγή του αρχείου.

3. Κανόνες και Πρακτικές Ασφαλείας

Η ασφάλεια μας στην χρήση του Διαδικτύου προϋποθέτει τη γνώση των σχετικών κινδύνων και την επαγρύπνησή μας ως προς την τήρηση κάποιων βασικών κανόνων και πρακτικών ασφαλείας, όπως αναφέρεται στα παρακάτω:

1. Διαφύλαξη και προστασία των προσωπικών πληροφοριών

Είναι σημαντικό να μην εκθέτουμε καθαρά προσωπικές πληροφορίες σε ξένους και να μην τις δημοσιεύουμε στο Διαδίκτυο όπου θα είναι προσβάσιμες σε εκατομμύρια ανθρώπους. Για παράδειγμα, ακόμα και για επαγγελματικούς λόγους, οι πιθανοί εργοδότες ή οι πελάτες δεν χρειάζεται να γνωρίζουν τις προσωπικές μας σχέσεις ή τη διεύθυνση της κατοικίας μας. Τα μόνα που πρέπει να γνωρίζουν είναι η εμπειρία και το επαγγελματικό μας υπόβαθρο, καθώς και πώς να έρχονται σε επαφή μαζί μας.

2. Ενεργοποίηση των ρυθμίσεων απορρήτου

Οι άνθρωποι της διαφήμισης λατρεύουν να γνωρίζουν τα πάντα για εμάς, όπως άλλωστε και οι χάκερς. Και οι δύο μπορούν να μάθουν πολλά από την περιήγησή μας και την χρήση των κοινωνικών μέσων δικτύωσης. Ωστόσο, μπορούμε να προστατεύσουμε τα προσωπικά μας στοιχεία, αφού, τόσο τα προγράμματα περιήγησης ιστού, όσο και τα λειτουργικά συστήματα κινητής τηλεφωνίας διαθέτουν ρυθμίσεις διαθέσιμες για την προστασία του απορρήτου μας στο Διαδίκτυο. Σημαντικοί ιστότοποι όπως το Facebook έχουν επίσης διαθέσιμες ρυθμίσεις προστασίας της ιδιωτικότητάς μας. Αυτές οι ρυθμίσεις είναι μερικές

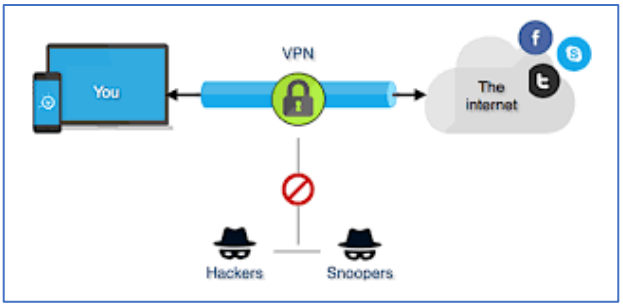
φορές (σκόπιμα) δύσκολο να βρεθούν, επειδή οι εταιρείες θέλουν τα προσωπικά μας στοιχεία για την αποστολή διαφημίσεων, που αφορούν τις διάφορες προτιμήσεις μας.

3. Πρακτική ασφαλούς περιήγησης

Όπως δεν θα επιλέγαμε να περπατήσουμε σε μια επικίνδυνη γειτονιά έτσι λοιπόν θα πρέπει να μην επισκεπτόμαστε επικίνδυνες «γειτονιές» στο Διαδίκτυο. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν το δελεαστικό περιεχόμενο ως δόλωμα. Γνωρίζουν ότι οι άνθρωποι μερικές φορές μπαίνουν στον πειρασμό από περιεχόμενο που προκαλεί περιέργεια και έτσι μπορεί να πέσουν ευκολότερα θύματα εκμετάλλευσης.

4. Ασφάλεια σύνδεσης στο Διαδίκτυο με χρήση αξιόπιστου VPN

Όταν συνδεόμαστε σε δημόσιο δίκτυο, για παράδειγμα χρησιμοποιώντας μια δημόσια σύνδεση Wi-Fi, δεν έχουμε άμεσο έλεγχο της ασφάλειάς του. Οι εμπειρογνώμονες στον τομέα της ασφάλειας στον κυβερνοχώρο ανησυχούν για τα “endpoints”, τα μέρη όπου ένα ιδιωτικό δίκτυο συνδέεται με τον έξω κόσμο. Το ευάλωτο σημείο είναι η τοπική σύνδεση στο Διαδίκτυο. Πρέπει να βεβαιωνόμαστε ότι η συσκευή μας είναι ασφαλής και αν όχι, να μην συνδεόμαστε σε ανασφαλή σημεία πρόσβασης στο Διαδίκτυο διότι υπάρχει κίνδυνος ακόμα και υποκλοπής στοιχείων του τραπεζικού μας λογαριασμού.



Για την περαιτέρω βελτίωση της ασφάλεια της πλοήγησης μας στο Διαδίκτυο, μπορούμε να χρησιμοποιήσουμε μια ασφαλή σύνδεση VPN (Virtual Private Network - εικονικό ιδιωτικό δίκτυο). Το VPN επιτρέπει να έχουμε μια

ασφαλή σύνδεση μεταξύ της συσκευής μας και ενός διακομιστή Διαδικτύου που κανείς δεν μπορεί να παρακολουθεί ή να έχει πρόσβαση στα δεδομένα που ανταλλάσσονται μέσω αυτού.

5. Προσοχή στη λήψη περιεχομένου και αρχείων

Ένας κορυφαίος στόχος των εγκληματιών στον κυβερνοχώρο είναι να μας εξαπατήσουν με τη λήψη κακόβουλου λογισμικού με τη μορφή προγραμμάτων ή εφαρμογών που προσπαθούν να υποκλέψουν πληροφορίες. Αυτό το κακόβουλο λογισμικό μπορεί να συγκαλυφθεί ως εφαρμογή οποιαδήποτε μορφής όπως ένα δημοφιλές παιχνίδι ή μια εφαρμογή που ελέγχει την κυκλοφορία ή τον καιρό. Δεν πρέπει ποτέ να κατεβάζουμε εφαρμογές που φαίνονται ύποπτες ή προέρχονται από ιστότοπο που δεν εμπιστευόμαστε.

6. Επιλογή ισχυρών κωδικών πρόσβασης

Οι κωδικοί πρόσβασης είναι ένα από τα πιο αδύναμα σημεία σε ολόκληρη τη δομή ασφάλειας του Διαδικτύου. Το πρόβλημα με τους κωδικούς πρόσβασης είναι ότι οι άνθρωποι τείνουν να επιλέγουν εύκολους για να τους θυμούνται (όπως “password” και “123456”), οι οποίοι είναι επίσης εύκολο προσδιοριστούν από τους χάκερς. Επιλέγουμε λοιπόν δύσκολους και μεγάλους κωδικούς που να μην μπορεί κάποιος να τους μαντέψει. Το λογισμικό διαχείρισης κωδικών πρόσβασης μπορεί να μας βοηθήσει να διαχειριστούμε πολλούς κωδικούς πρόσβασης, ώστε να μην τους ξεχνάμε. Ένας ισχυρός κωδικός πρόσβασης είναι μοναδικός και περίπλοκος, με μήκος τουλάχιστον 15 χαρακτήρων, και περιλαμβάνει γράμματα, αριθμούς και ειδικούς χαρακτήρες.

7. Πραγματοποίηση διαδικτυακών αγορών από ασφαλείς ιστότοπους

Κάθε φορά που πραγματοποιούμε μια αγορά στο Διαδίκτυο, καλούμαστε να παρέχουμε στοιχεία της πιστωτικής κάρτας ή του τραπεζικού λογαριασμού μας. Είναι σημαντικό να παρέχουμε αυτές τις πληροφορίες μόνο σε ιστότοπους που εκτελούν ασφαλείς και κρυπτογραφημένες συνδέσεις. Μπορούμε να προσδιορίσουμε τέτοιους ασφαλείς ιστότοπους αναζητώντας μια διεύθυνση που ξεκινά με https (το s σημαίνει ασφαλές - safe) και όχι απλώς http. Μπορούν επίσης να επισημανθούν από ένα εικονίδιο λουκέτου δίπλα στη γραμμή διευθύνσεων.

8. Προσοχή στις δημοσιεύσεις μας

Το Διαδίκτυο δεν έχει τρόπο διαγραφής. Οποιοδήποτε σχόλιο ή εικόνα που δημοσιεύεται στο Διαδίκτυο μπορεί να παραμείνει εκεί για πάντα, επειδή η αφαίρεση του πρωτότυπου (ας πούμε, από το Twitter) δεν αφαιρεί αντίγραφα από άλλα άτομα. Δεν υπάρχει τρόπος να "πάρουμε πίσω" μια παρατήρηση που δεν θα θέλαμε να έχουμε κάνει ή να απαλλαγούμε από μια ανεπιθύμητη πλέον φωτογραφία (π.χ. selfie).

9. Προσοχή στις διαδικτυακές γνωριμίες

Οι άνθρωποι που «συναντάμε» στο Διαδίκτυο δεν είναι πάντα αυτοί που ισχυρίζονται ότι είναι. Μπορεί να μην είναι καν αληθινοί ή να είναι άλλοι από αυτούς μας συστήνονται. Τα ψεύτικα προφίλ κοινωνικών μέσων είναι ένας δημοφιλής τρόπος για τους χάκερ να προσελκύσουν και να «χαλαρώσουν» τους απρόσεκτους χρήστες του Διαδικτύου ώστε να τους παρασύρουν και να τους εκμεταλλευτούν. Πρέπει να είμαστε τόσο προσεκτικοί και λογικοί στην διαδικτυακή κοινωνική μας ζωή όσο και στην πραγματική.

10. Διατήρηση και ενημέρωση των προγραμμάτων προστασίας από ιούς

Το λογισμικό ασφάλειας που χρησιμοποιούμε στο Διαδίκτυο δεν μπορεί να μας προστατεύσει από κάθε είδους απειλή, αλλά θα εντοπίσει και θα αφαιρέσει τα περισσότερα κακόβουλα προγράμματα, αν είναι πάντα ενημερωμένο. Πρέπει να φροντίζουμε για την τακτική αναβάθμισή του με τις τελευταίες διαθέσιμες ενημερώσεις ώστε να μας παρέχει ένα σημαντικό επίπεδο ασφάλειας.

4. Συμπεράσματα και προτάσεις

Συμπεραίνοντας λοιπόν, το Διαδίκτυο είναι ένα εργαλείο που έχει διευκολύνει πολύ τη σύγχρονη ζωή. Πρέπει όμως να είμαστε προσεκτικοί στην χρήση του. Όπως όλα τα πράγματα, έχει πολλά πλεονεκτήματα αλλά και κίνδυνους, τους οποίους μπορούμε να αποφύγουμε με μέτρο και προσοχή. Είναι εύκολο να πλοηγούμαστε σε αυτό παραμένοντας ασφαλείς, αρκεί να ακολουθούμε, σε καθημερινή βάση, τους βασικούς κανόνες που αναφέραμε σε αυτή την εργασία.

Βιβλιογραφία και Πηγές Πληροφόρησης

[1] Διαδίκτυο,Wikipedia, https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

[2] Διαδίκτυο, Ιστορική Αναδρομή, https://sites.google.com/site/chalellieirini/istorike-anadrome

[3] Broadband search, Who Invented the Internet – A Full History, https://www.broadbandsearch.net/blog/who-invented-the-internet-full-history#post-navigation-1

[4] Κίνδυνοι από τη χρήση του Διαδικτύου, 3ο Γυμνάσιο Άνω Λιοσίων, http://www.3gymanoliosia.gr/pupils/46-blogged/technology/83-dangers-of-internet-use

[5] Έρευνα σε 14.000 μαθητές ηλικίας 10-17 ετών για τις διαδικτυακές συνήθειες, Ελληνικό Κέντρο Ασφαλούς Διαδικτύου, Ελληνικό Κεντρο Ασφαλούς Διαδικτύου, www.SaferInternet4Kids.gr https://saferinternet4kids.gr/wp-content/uploads/2019/06/2019-%CE%B5%CF%81%CE%B5%CF%85%CE%BD%CE%B1-%CE%B3%CE%B5%CE%BD%CE%B9%CE%BA%CE%BF-GR.pdf

[6] Ασφάλεια στο διαδίκτυο, Wikipedia, https://el.wikipedia.org/wiki/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1_%CF%83%CF%84%CE%BF_%CE%B4%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

[7] A. Vasileiadis, 10 κανόνες για ασφαλή πλοήγηση στο διαδίκτυο, https://iguru.gr/2020/05/29/10-kanones-gia-asfali-ploigisi-sto-diadiktyo/