

Ασφάλεια στο διαδίκτυο

Κουκούμιαλου Φραντζέσκα
Σχολικό έτος 2020-2021

Table of Contents

Ασφάλεια στο διαδίκτυο.....	1
1. Τι είναι το Διαδίκτυο	3
2. Ασφάλεια στο Διαδίκτυο	3
3. Προστασία από το Διαδίκτυο.....	3
4. Κίνδυνοι στο Διαδίκτυο	5
5. Κανόνες ασφαλούς πλοήγησής.....	8
6. 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 (τυποποιημένο 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 ιδιωτικών πληροφοριών και περιουσίας του χρήστη, που σχετίζονται με τη χρήση του Διαδικτύου και την αυτοπροστασία από το ηλεκτρονικό έγκλημα.

3. Προστασία από το Διαδίκτυο

Το «ηλεκτρονικό ψέμα» είναι ένας τύπος απάτης στον οποίο οι απατεώνες εμφανίζονται με ψεύτικα στοιχεία για την απόκτηση ιδιωτικών πληροφοριών, όπως κωδικών πρόσβασης, πληροφοριών πιστωτικών καρτών κ.λπ. μέσω του διαδικτύου. Το ηλεκτρονικό "ψάρεμα" (phishing) 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 συχνά σχεδιασμένες ώστε να φαίνονται όμοιοι με τους νόμιμους ομολόγους τους, για να αποφεύγεται η υποψία από τον χρήστη.

Διαδικτυακές απάτες

Πρόκειται για προγράμματα που εξαπατούν τον χρήστη με διάφορους τρόπους, προσπαθώντας να εκμεταλλευτούν πληροφορίες του χρήστη. Οι απάτες στο Διαδίκτυο προσπαθούν να εξαπατήσουν το θύμα με πράγματα της προσωπικής ιδιοκτησίας παρά με προσωπικές πληροφορίες μέσω ψευδών υποσχέσεων, τεχνάσματα εμπιστοσύνης και πολλά άλλα.

Το κακόβουλο λογισμικό , ιδιαίτερα το λογισμικό υποκλοπής spyware , είναι κακόβουλο λογισμικό που μεταμφιέζεται ως λογισμικό που έχει σχεδιαστεί για τη 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.

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. Σε μια μελέτη του 2012 με περισσότερους από 11.925 φοιτητές στις Ηνωμένες Πολιτείες, αναφέρθηκε ότι το 23% των εφήβων ανέφερε ότι ήταν θύμα της παρενόχλησης στον κυβερνοχώρο, το 30% των οποίων ανέφερε ότι αντιμετώπιζε αυτοκτονική συμπεριφορά.

Αστείο/προσβλητικό περιεχόμενο

Διάφοροι ιστότοποι στο Διαδίκτυο περιέχουν υλικό που κάποιοι θεωρούν προσβλητικό, δυσάρεστο ή ρητό, το οποίο συχνά δεν μπορεί να είναι από τις προτιμήσεις του χρήστη. Τέτοιες ιστοσελίδες μπορεί να περιλαμβάνουν το διαδίκτυο , ιστοσελίδες σοκ , ομιλία μίσους ή άλλο φλεγμονώδες περιεχόμενο. Ένα τέτοιο περιεχόμενο μπορεί να εκδηλωθεί με πολλούς τρόπους, όπως οι αναδυόμενες διαφημίσεις και οι ανυποψίαστοι σύνδεσμοι.



4. Κίνδυνοι στο Διαδίκτυο

Το διαδίκτυο αποτελεί πραγματικά ένα καταπληκτικό εργαλείο, το οποίο προσφέρει αμέτρητες δυνατότητες σε όσους το χρησιμοποιούν σωστά και μεθοδικά. Άλλωστε, κάθε τι στη ζωή θέλει μέτρο και εννοείται πως το διαδίκτυο δεν θα μπορούσε να αποτελεί εξαίρεση. Όλοι μας βρισκόμαστε μόλις μερικά κλικ μακριά κυριολεκτικά από τα πάντα. Στο διαδίκτυο έχουμε τη δυνατότητα να κάνουμε τόσες και τόσες δραστηριότητες με πιο χαρακτηριστικά και συνηθισμένα παραδείγματα να είναι τα παιχνίδια, η λήψη γνώσεων, η συνομιλία, η αναζήτηση πληροφοριών, οι ηλεκτρονικές αγορές, οι κάθε είδους συναλλαγές και η εργασία εξ' αποστάσεως.

Ωστόσο, οι ανήλικοι κάνουν όλα τα παραπάνω, συνήθως, χωρίς επίβλεψη και έχοντας μία πρωτόγνωρη ελευθερία, η οποία δεν υφίσταται στην πραγματική ζωή. Επομένως, στην προκειμένη περίπτωση, το μείζον ζήτημα έχει να κάνει με το πόσο γνωρίζουν τα παιδιά και οι έφηβοι να χρησιμοποιούν το διαδίκτυο σωστά και να αποφεύγουν τους πολλούς-δυστυχώς-κινδύνους που κρύβονται.

Πρόκειται για μία ψυχοπαθολογική ασθένεια του ατόμου, η οποία είναι εξαιρετικά δύσκολο να διαγνωστεί. Παρόλα αυτά, η αντιμετώπιση της είναι κάτι παραπάνω από αναγκαία. Δημιουργεί πλήθος αρνητικών συνεπειών, όπως η συναισθηματική

ανισορροπία, η αδυναμία εκτίμησης των πραγμάτων που αξίζουν στη ζωή, χάσιμο επαφής με τη πραγματικότητα και οικονομική καταστροφή. Τα παιδιά και οι νέοι που βιώνουν εθισμό στο διαδίκτυο, δημιουργούν προβλήματα, εκτός από τον εαυτό τους, και στα άτομα του κύκλου τους.

Ο εθισμός περιλαμβάνει:

- Υπερβολική ενασχόληση με κοινωνικά μέσα δικτύωσης (social media) και συνομιλία με άλλους χρήστες
- Εμμονή με ιστοσελίδες ερωτικού περιεχομένου
- Διάφορες μορφές τζόγου
- Ηλεκτρονικές αγορές και υπερκαταναλωτισμός

Η διαδικτυακή παρενόχληση έχει να κάνει με τον εκφοβισμό, την απειλή, την ταπείνωση και γενικά την παρενόχληση παιδιών και εφήβων από συνομήλικους τους όταν χρησιμοποιούν γενικά το διαδίκτυο και ειδικότερα τα social media και τα κινητά τους τηλέφωνα.

Ο εκφοβισμός στα social media είναι ένα φαινόμενο που, δυστυχώς, έχει πάρει μεγάλες διαστάσεις και στην χώρα μας. Δημοφιλείς πλατφόρμες κοινωνικής δικτύωσης, όπως το Facebook και το Instagram προσφέρονται άθελα τους για εκφοβισμό και παρενόχληση μεταξύ των χρηστών τους που διατηρούν προσωπικό λογαριασμό.



Μορφές διαδικτυακής παρενόχλησης:

- Επαναλαμβανόμενη αποστολή μηνυμάτων είτε ηλεκτρονικών είτε στο κινητό τηλέφωνο
- Παρέμβαση και παρενόχληση οποιασδήποτε διαδικτυακής δραστηριότητας του ατόμου
- Δημιουργία ψεύτικων προφίλ στα social media
- Είσοδος σε προσωπικούς λογαριασμούς social media του ατόμου
- Αποστολή φωτογραφιών ή και άλλου είδους μαγνητοσκοπημένου υλικού του ατόμου σε τρίτους
- Αποστολή προσωπικών πληροφοριών του ατόμου σε τρίτους
- Αποστολή απειλητικών μηνυμάτων σε άλλα άτομα υποκρινόμενοι το άτομο που εκφοβίζεται
- Υποκίνηση τρίτων για διαδικτυακή παρακολούθηση και παρενόχληση του ατόμου

Λόγοι άσκησης διαδικτυακής παρενόχλησης:

- Νιώθει ανίσχυρος
- Χαμηλή αυτοεκτίμηση
- Επιδίωξη της προσοχής και του θαυμασμού από φίλους
- Φοβάται το αίσθημα του να μην ανήκει πουθενά, σε καμία κοινωνική ομάδα
- Παρορμητικότητα και αδυναμία ελέγχου του θυμού
- Ανεπτυγμένο το στοιχείο της επιθετικότητας και του εκφοβισμού
- Μίμηση
- Έλλειψη επίγνωσης και συνείδησης των συγκεκριμένων πράξεων
- Υπήρξε το ίδιο το άτομο θύμα εκφοβισμού κατά το παρελθόν

Το διαδίκτυο κρύβει πολλούς κινδύνους, ειδικά για τα ανήλικα παιδιά και τους εφήβους και από την πλευρά τους τα μέσα κοινωνικής δικτύωσης έχουν αποδειχθεί αδύναμα να προστατεύσουν τους ανήλικους από κρούσματα παρενόχλησης. Γι' αυτόν τον λόγο, οι γονείς πρέπει να είναι ιδιαίτερα προσεκτικοί προκειμένου να εξασφαλίσουν την ασφάλεια του παιδιού τους.

Η έγκαιρη και ουσιαστική βοήθεια για το παιδί ή τον έφηβο μπορούν πραγματικά να κάνουν τη διαφορά. Σχετικές έρευνες δείχνουν ότι όσο πιο νωρίς πάρουν βοήθεια τα θύματα διαδικτυακής παρενόχλησης, τόσο περισσότερες είναι οι πιθανότητες να προλάβουμε άσχημες καταστάσεις. Δυστυχώς, η σεξουαλική παρενόχληση στο διαδίκτυο είναι ένα φαινόμενο, το οποίο έχει πάρει ανησυχητικές διαστάσεις. Πλέον, δεν πρόκειται για έναν αριθμό μεμονωμένων περιστατικών, αλλά για μία τραγική πραγματικότητα που βιώνουν άνδρες και γυναίκες και ειδικά παιδιά και έφηβοι. Ένα στατιστικό στοιχείο που δείχνει την σοβαρότητα της κατάστασης είναι το γεγονός πως ένας στους πέντε ανηλίκους έχουν δεχθεί σεξουαλική παρενόχληση στο διαδίκτυο.

Στη πλειοψηφία των περιπτώσεων, άτομα με ψεύτικη ταυτότητα και προφίλ προσεγγίζουν και παρασύρουν παιδιά και έφηβους λέγοντας τους ότι έχουν την ίδια ηλικία και ότι τους ενώνουν κοινά χόμπι και ασχολίες. Επιπλέον, η διαδικτυακή σεξουαλική παρενόχληση πολλές φορές οδηγεί και σε πρακτική σεξουαλική παρενόχληση του θύματος. Είναι ζωτικής σημασίας οι γονείς να αναλάβουν δράσεις και να συμβουλευθούν κάποιον ειδικό σε περίπτωση που παρατηρήσουν κάποια απότομη αλλαγή στη συμπεριφορά του παιδιού.

Εθισμός στα διαδικτυακά παιχνίδια, όπου δημιουργείται μια εικονική κοινότητα μεταξύ φαντασίας και πραγματικότητας σε έναν κόσμο στον οποίο αίρονται οι αναστολές, καθώς υπάρχει ανωνυμία και αορατότητα.

5. Κανόνες ασφαλούς πλοήγησής

Με βάση όλα τα παραπάνω και τους κινδύνους που υπάρχουν στο διαδίκτυο, το τελικό συμπέρασμα, στο οποίο καταλήγει κανείς είναι ότι η ασφάλεια στο διαδίκτυο γίνεται ολοένα και πιο σημαντική, διότι στην σημερινή εποχή τα παιδιά αποκτούν πρόσβαση στο διαδίκτυο από πολύ μικρή ηλικία. Γι' αυτόν ακριβώς τον λόγο, παρακάτω θα παρουσιάσουμε κάποιους τρόπους με τους οποίους η πλοήγηση στο διαδίκτυο γίνεται ασφαλέστερη

Τοποθετώντας τον υπολογιστή σε κοινόχρηστο χώρο του σπιτιού και θέτοντας συγκεκριμένους κανόνες σχετικά με τη χρήση του, βοηθάτε τα παιδιά σας να

παραμείνουν ασφαλή. Να θυμάστε ότι τα παιδιά σας μπορούν να χρησιμοποιήσουν το διαδίκτυο και αλλού, όπως σπίτια φίλων, σε Ίντερνετ καφέ κλπ. Για αυτό, είναι σημαντικό να δημιουργήσετε μαζί έναν κώδικα ασφαλούς συμπεριφοράς που να μπορούν να τον εφαρμόζουν ανά πάσα στιγμή, οπουδήποτε και αν βρίσκονται.

Η γνώση των πιθανών κινδύνων και των μέσων αποφυγής τους αποτελεί βασικό στοιχείο ασφάλειας. Τα μέσα αυτά περιλαμβάνουν χρήσιμα τεχνολογικά εργαλεία καθώς και την κοινή λογική. Όπως σε όλους τους τομείς, έτσι και η κοινή λογική αναπτύσσεται με την ηλικία και την εμπειρία. Καθημερινές ενέργειες, όπως η χρήση συσκευών αποθήκευσης USB, το άνοιγμα συνημμένων αρχείων και το κατέβασμα προγραμμάτων από το διαδίκτυο, μπορεί να εμπεριέχουν κινδύνους. Οι κίνδυνοι αυτοί αφορούν κυρίως τη διάδοση προγραμμάτων κακόβουλου λογισμικού, φτιαγμένων με στόχο να βλάψουν τον υπολογιστή σας ή να υποκλέψουν προσωπικά δεδομένα.

Το 80% των ηλεκτρονικών μηνυμάτων που κυκλοφορούν στο διαδίκτυο είναι ανεπιθύμητα, spam, που μπορούν εύκολα να επηρεάσουν τα παιδιά σας. Η αλόγιστη χρήση και δημοσίευση της ηλεκτρονικής σας διεύθυνσης στο διαδίκτυο μπορεί να έχει ως αποτέλεσμα την αποστολή ανεπιθύμητων μηνυμάτων. Αυτό συμβαίνει επειδή υπάρχουν ειδικά λογισμικά που μπορούν να συλλέξουν αυτόματα διευθύνσεις ηλεκτρονικού ταχυδρομείου από το διαδίκτυο για τη μαζική αποστολή ανεπιθύμητων μηνυμάτων.

1. Ποτέ δεν επικοινωνούμε με άγνωστα άτομα στο διαδίκτυο. Δεν μπορούμε να είμαστε σίγουροι με ποιόν επικοινωνούμε.
2. Ποτέ δεν δίνουμε προσωπικά στοιχεία σε άγνωστα άτομα.
3. Ποτέ μα ποτέ δεν συναντούμε κάποιον που γνωρίσαμε στο διαδίκτυο.
4. Να θυμόμαστε πάντα ότι αυτοί που θέλουν να μας ξεγελάσουν θα δίνουν πάντα ψεύτικα στοιχεία.
5. Ποτέ δεν απαντούμε σε ανώνυμα ή προσβλητικά μηνύματα.
6. Προσπαθούμε να μην παραμένουμε πολλή ώρα συνδεδεμένοι στον υπολογιστή μας.
7. Κλείνουμε τη σύνδεση αν δούμε ή διαβάσουμε κάτι που μας ενόχλησε.
8. Προσπαθούμε να μην κατεβάζουμε οποιαδήποτε αρχεία στον υπολογιστή μας.

9. Να θυμόμαστε πάντα πως, ότι ανεβεί στο διαδίκτυο, παύει να είναι πλέον προσωπικό στοιχείο.
10. Να ενημερώνω αμέσως τους γονείς μου ή τους δασκάλους μου σε περίπτωση που κάποιος με ενοχλήσει στο διαδίκτυο.
11. Υπολογιστής / Λογισμικό:
12. Να κρατάμε το λειτουργικό σύστημα του υπολογιστή μας, πάντοτε ενημερωμένο (updated).
13. Εγκαθιστούμε και χρησιμοποιούμε κάποιο πρόγραμμα προστασίας από ιούς, το οποίο και ενημερώνουμε συχνά, με όλες τις νέες εκδόσεις ιών που κυκλοφορούν. Ρυθμίζουμε το πρόγραμμα προστασίας από ιούς ώστε να ανιχνεύει όλα τα εισερχόμενα αρχεία και τα συνημμένα των ηλεκτρονικών μηνυμάτων πριν τα ανοίξουμε.
14. Εγκαθιστούμε και εκτελούμε ένα πρόγραμμα για τον εντοπισμό και την αφαίρεση λογισμικού υποκλοπής (anti-spyware).
15. Εγκαθιστούμε και χρησιμοποιούμε κάποιο τείχος προστασίας (firewall) στον υπολογιστή του σπιτιού μας. Οι νεότερες εκδόσεις των Windows προσφέρουν ενσωματωμένο πρόγραμμα firewall.
16. Κρατάμε backup των αρχείων του υπολογιστή σας, ώστε ακόμη και αν συμβεί κάτι στον υπολογιστή μας, να μπορούμε να ανακτήσουμε ξανά τα δεδομένα μας.
17. Χρησιμοποιούμε ένα φίλτρο ανεπιθύμητων μηνυμάτων (antispam).
18. Προστατεύουμε τους κωδικούς ασφαλείας μας. Δεν τους μοιραζόμαστε με κανέναν, ούτε και με τους φίλους μας ή το χειριστή του μηχανήματός μας.
19. Είμαστε πολύ προσεκτικοί με μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) ή ιστοσελίδες, που μας ζητούν να τους παραχωρήσετε προσωπικές πληροφορίες ή μας προτρέπουν να κατεβάσουμε κάποιο αρχείο.

6. Βοήθεια

Νούμερο 1 αρχή που πρέπει να θυμάσαι είναι ότι πρέπει να μιλάς και να συζητάς αυτό που σου συμβαίνει, και αυτό πρέπει να το καταλάβουν και οι μικρότεροι σε ηλικία, μόνο έτσι μπορούν να προληφθούν τα χειρότερα και μόνο έτσι μπορούν να δράσουν οι αρμόδιες αρχές.

Οι άνθρωποί σου, λοιπόν, σε περίπτωση ανάγκης βρίσκονται στους παρακάτω συνδέσμους:

- Στη **Δίωξη Ηλεκτρονικού Εγκλήματος**, όπου μπορείς να βρεις ενδιαφέρουσες πληροφορίες, οδηγίες, δράσεις ΔΙΔΗΕ και φυσικά το 11188 , το τηλέφωνο που σε βγάζει απευθείας στη γραμμή της αστυνομίας που ασχολείται με τις ηλεκτρονικά εγκλήματα και τις καταγγελίες.
- Στο **Cyber Alert**, από τη διεύθυνση δίωξης ηλεκτρονικού εγκλήματος, είναι ένας ιστότοπος που σε ενημερώνει για τις εξελίξεις γύρω από το ηλεκτρονικό έγκλημα τόσο σε επιχειρήσεις και ενήλικες, όσο και σε παιδιά, ενώ σε παραπέμπει για καταγγελίες στο 11188.
- Στη **Γραμμή Βοηθείας help-line 210 6007686**, η οποία απευθύνεται σε παιδιά & εφήβους και τις οικογένειές τους, παρέχοντας υποστήριξη και συμβουλές για θέματα που σχετίζονται με τη χρήση του Διαδικτύου, του κινητού τηλεφώνου και των ηλεκτρονικών παιχνιδιών. Επίσης στη help-line, για πρώτη φορά στα ελληνικά δεδομένα παρέχεται εξατομικευμένη και ανώνυμη υποστήριξη μέσω chat από εξειδικευμένο προσωπικό.
- Last but not least, στην **Ελληνική Ανοικτή Γραμμή για το παράνομο περιεχόμενο στο Διαδίκτυο**, η οποία δέχεται καταγγελίες για περιεχόμενο που εντοπίζεται στο Διαδίκτυο και περιέχει εικόνες κακοποίησης παιδιών σε οποιοδήποτε σημείο του κόσμου, ρατσιστικό και ξενοφοβικό υλικό που παραβαίνει την ελληνική νομοθεσία, οτιδήποτε άλλο θεωρείται ότι είναι παράνομο. Πρωταρχικό μέλημα της SafeLine είναι η εξάλειψη από το Διαδίκτυο περιεχομένου παιδικής πορνογραφίας. Σκοπός της είναι η καταπολέμηση κάθε είδους παράνομου περιεχομένου του Διαδικτύου.