



Συχνές Ερωτήσεις και Απαντήσεις για την ασφαλή χρήση του Διαδικτύου



Συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση
Διευκόλυνση «Συνδέοντας την Ευρώπη»



«FAQ – Συχνές ερωτήσεις και απαντήσεις για την ασφαλή χρήση του Διαδικτύου»
3η έκδοση - Μάρτιος 2015

Δικαιούχος πνευματικής ιδιοκτησίας γραφικών παραστάσεων και λογοτύπου:
Safer Internet Hellas © 2010 - 2015

Δικαιούχος πνευματικής ιδιοκτησίας κειμένων: Safer Internet Hellas © 2008 - 2015

ISBN 978-960-99061- 0 - 4

Το έργο αυτό της Δράσης Ενημέρωσης Saferinternet.gr του Ελληνικού Κέντρου
Ασφαλούς Διαδικτύου βρίσκεται υπό άδεια Creative Commons
Αναφορά - Μη Εμπορική Χρήση - Όχι Παράγωγα Έργα 4.0 Διεθνές



Επιτρέπεται η χρήση του έργου ως έχει και στο σύνολό του με αντιγραφή, διανομή και μετάδοση υπό τους εξής όρους:

1. Απαγορεύεται η χρήση του έργου μέσα στα πλαίσια σκοπού άμεσα ή έμμεσα κερδοσκοπικού.
2. Απαγορεύεται η διασκευή, η προσαρμογή ή η οποιαδήποτε άλλη μετατροπή, η αποσπασματική χρήση του έργου ή η δημιουργία παράγωγου έργου.
3. Απαγορεύεται η χρήση του έργου χωρίς αναφορά του δικαιούχου πνευματικής ιδιοκτησίας καθώς και των όρων που διέπουν την παρούσα άδεια.

Η παρούσα άδεια σε καμία περίπτωση δεν αναιρεί ή περιορίζει το ηθικό δικαίωμα του δικαιούχου πνευματικής ιδιοκτησίας.
Για οιαδήποτε άλλη χρήση πέραν αυτής που προβλέπεται από τη συγκεκριμένη άδεια, απαιτείται γραπτή άδεια από τον δικαιούχο της πνευματικής ιδιοκτησίας.

Για να δείτε αντίγραφο της άδειας, επισκεφθείτε:
<https://creativecommons.org/licenses/by-nc-nd/4.0/>

Την αποκλειστική ευθύνη της παρούσας έκδοσης φέρει ο συγγραφέας της.
Η Ευρωπαϊκή Ένωση δεν φέρει καμία ευθύνη για οποιαδήποτε χρήση των περιεχομένων σ' αυτήν πληροφοριών.

Η Δράση Saferinternet.gr του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου συγχρηματοδοτείται από το πλαίσιο του τομέα Τηλεπικοινωνιών του Μηχανισμού «Συνδέοντας την Ευρώπη» ("Connecting Europe Facility - CEF Telecom") της Ευρωπαϊκής Ένωσης.

Αποτελεί κοινή παραδοχή ότι τα νέα διαδραστικά μέσα, όπως το Διαδίκτυο και το κινητό τηλέφωνο, αποτελούν καταπληκτικά χρηστικά εργαλεία επικοινωνίας, μάθησης, δημιουργίας, διασκέδασης και εργασίας. Είναι επίσης αδιαμφισβήτητο ότι τα παιδιά και οι νέοι γνωρίζουν πολύ περισσότερα από τους μεγαλύτερους για αυτές τις τεχνολογίες.

Όμως, ο αχανής αυτός ιδεατός κόσμος, όπως άλλωστε και ο πραγματικός κόσμος στον οποίο ζούμε, έχει και τις σκοτεινές πλευρές του. Ένας ενήλικας είναι σε θέση να κρίνει και να αποφύγει τους κινδύνους που θα συναντήσει, για ένα παιδί, όμως, τα πράγματα είναι εντελώς διαφορετικά. Η ευθύνη της προστασίας του, λοιπόν, βρίσκεται, όπως και στον φυσικό κόσμο, στα χέρια των γονέων του.

Ωστόσο, η προστασία των ανηλίκων δεν είναι μια απλή διαδικασία. Το επιθυμητό δεν είναι ούτε η πλήρης απαγόρευση της πρόσβασης στους διαδραστικούς κόσμους, που στερεί το παιδί από ανεκτίμητα εργαλεία, ούτε φυσικά η παντελής απουσία επιτήρησης και κατά συνέπεια η στροφή προς τις ευχές...για να μη συμβεί τίποτα κακό.

Έχει φτάσει λοιπόν η ώρα να αφήσουμε στην άκρη την άγνοια για τα νέα μέσα και να γίνουμε μέλη του ψηφιακού κόσμου. Δεν μπορούμε εμείς οι μεγάλοι να αντιμετωπίζουμε την Κοινωνία της Πληροφορίας με φόβο και καχυποψία. Πρέπει να ανοίξουμε τις πόρτες της τεχνολογίας και να γίνουμε γνώστες αυτής. Αν χρειαστεί, ας ζητήσουμε από τα παιδιά μας να μας βοηθήσουν στον δρόμο της γνώσης. Μόνο έτσι θα μπορέσουμε να αντιληφθούμε τους κινδύνους που εγκυμονούν, και να βοηθήσουμε αποτελεσματικά τα παιδιά μέσα από επικοινωνία και σαφείς κανόνες, να μάθουν πώς να χρησιμοποιούν τα νέα μέσα με σύνεση, με κριτική σκέψη και συνεπώς με ασφάλεια.

Για να γνωρίσετε λοιπόν το θαυμαστό κόσμο του Διαδικτύου και για να λύσετε τις απορίες σας γύρω από την ασφαλή χρήση των νέων τεχνολογιών, η Δράση Ενημέρωσης Saferinternet.gr του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου δημιούργησε αυτό το έντυπο συχνών ερωτήσεων – απαντήσεων. Τα θέματα με τα οποία ασχολούμαστε είναι: Spam, Ανταλλαγή Αρχείων, Blogging, Chat, e-Επιχειρείν, Κοινωνική Δικτύωση, Ιδιωτική Ζωή, Κινητά Τηλέφωνα, Ιοί και βλαβερό λογισμικό, Παιδική Πορνογραφία, Παιχνίδια και Τζόγος, Παρενόχληση, Ρατσισμός στο Διαδίκτυο, Φιλτράρισμα.

Ελπίζουμε το υλικό αυτό να σας φανεί χρήσιμο και να αποτελέσει οδηγό στον δρόμο της γνώσης.

Δρ. Βερόνικα Σαμαρά
Επικεφαλής Δράσης Saferinternet.gr
Ελληνικό Κέντρο Ασφαλούς Διαδικτύου



Το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου και η Δράση Ενημέρωσης Saferinternet.gr

Το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου και η Δράση Ενημέρωσης και Επαγρύπνησης Saferinternet.gr υλοποιούνται με τη συγχρηματοδότηση της Ευρωπαϊκής Επιτροπής και του προγράμματος πλαισίου Safer Internet.

Στόχος της δράσης Saferinternet.gr είναι να αφυπνίσει όλους τους Έλληνες και να τους ενημερώσει για τους τρόπους με τους οποίους μπορούν να προστατευθούν αλλά και να προστατεύσουν αποτελεσματικά τα παιδιά τους από τους κινδύνους που εγκυμονούν από τη μη ορθή χρήση των διαδικραστικών τεχνολογιών, όπως είναι το Διαδίκτυο και το κινητό τηλέφωνο. Αυτό επιτυγχάνεται με την υλοποίηση πλειάδας πολυμορφικών εκδηλώσεων και δράσεων που δρομολογούνται σε διετή βάση.

Οι δράσεις εναρμονίζονται με τα αποτελέσματα των ερευνών του Ευρωβαρόμετρου όπως και Εθνικών ερευνών που αφορούν στο Διαδίκτυο και στην κινητή τηλεφωνία, έτσι ώστε οι ενέργειες που υλοποιούνται να έχουν το μέγιστο αποτέλεσμα.

Η δράση Saferinternet.gr πιστεύει ότι η απάντηση στους πιθανούς κινδύνους του Διαδικτύου βρίσκεται τόσο στην εκπαίδευση, όσο και στην πρόληψη:

- Εκπαίδευση που συνεισφέρει στην απαραίτητη αλλαγή του τρόπου συμπεριφοράς, και που δημιουργεί μια υπεύθυνη στάση απέναντι στο Διαδίκτυο.
- Πρόληψη, έτσι ώστε να προωθηθούν οι θετικές πλευρές και τα οφέλη της χρήσης των διαδικραστικών τεχνολογιών.

Η δράση Saferinternet.gr πιστεύει επίσης ότι είναι ευθύνη όλων των κοινωνικών φορέων να λάβουν τα απαραίτητα μέτρα για την ασφαλή πλοήγηση των παιδιών στο Διαδίκτυο και την διασφάλιση των δικαιωμάτων τους στον κόσμο των διαδικραστικών τεχνολογιών και της κοινωνίας της πληροφορίας.

Η δράση Saferinternet.gr αποτελεί τον εθνικό εκπρόσωπο του Πανευρωπαϊκού Δικτύου Εθνικών Κέντρων Ενημέρωσης Insafe (www.saferinternet.org).

Spam.....	6
Ανταλλαγή Αρχείων.....	8
Blogging.....	12
Chat.....	16
e-Επιχειρείν.....	20
Κοινωνική Δικτύωση.....	24
Ιδιωτική Ζωή.....	28
Κινητό Τηλέφωνο.....	32
Ιοί – Βλαβερό Λογισμικό.....	36
Παιδική Πορνογραφία.....	40
Παιχνίδια – Τζόγος.....	44
Παρενόχληση.....	48
Ρατσισμός στο Διαδίκτυο.....	52
Φιλτράρισμα.....	56
Σημειώσεις.....	60
Χρήσιμες Ιστοσελίδες.....	62

1 Τι είναι Spam;

Τα Spam e-mail είναι ανεπιθύμητη αλληλογραφία που διανέμεται σε τεράστιο αριθμό παραληπτών.

Συνήθη παραδείγματα είναι τα spam με περιεχόμενο που σχετίζεται με την πορνογραφία, φαρμακευτικά προϊόντα ή αμφίβολης αξιοπιστίας οικονομικές συναλλαγές. Στις περισσότερες περιπτώσεις τα Spam αποστέλλονται με σκοπό την εξαπάτηση των παραληπτών.

Υπάρχουν βέβαια και περιπτώσεις όπου αξιόπιστες εταιρίες ή απλοί χρήστες στέλνουν μαζικά e-mails. Οι νόμοι έχουν ποικίλους ορισμούς σχετικά με το χαρακτηρισμό ενός e-mail ως Spam.

2 Τι μπορώ να κάνω για να αντιμετωπίσω το Spam;

Το καλύτερο εργαλείο για την αντιμετώπιση του spam είναι τα «φίλτρα spam». Μπορείτε να τα ενεργοποιήσετε στο πρόγραμμα για e-mail που χρησιμοποιείτε και συνήθως ο πάροχος ηλεκτρονικού ταχυδρομείου σας προσφέρει επιλογές κατά του spam. Επικοινωνήστε με τον πάροχό σας για περισσότερες πληροφορίες.

Να είστε προσεκτικοί: Τα φίλτρα spam δεν είναι πάντα απολύτως ακριβή. Μπορεί να χαρακτηρίσουν spam ακόμα και e-mails που είναι κάθε άλλο παρά ανεπιθύμητα. Μπορεί από την άλλη να μην αναγνωρίσουν ως spam μερικά ύποπτα μηνύματα.

Τα μέτρα προστασίας από το spam είναι πολύ σημαντικά. Δείτε και στο «Πώς μπορώ να αποτρέψω το Spam;». Πάντως, δυστυχώς δεν υπάρχει ολοκληρωμένος τρόπος αντιμετώπισης του φαινομένου.

3

Πώς μπορώ να αποτρέψω το Spam;

Γενικά να είστε πολύ προσεκτικοί όταν δημοσιεύετε την ηλεκτρονική σας διεύθυνση.

Χρησιμοποιήστε δύο e-mails. Το ένα θα πρέπει να το χρησιμοποιείτε αποκλειστικά για την επικοινωνία με τους φίλους σας, συναδέλφους κ.λπ. Η άλλη διεύθυνση θα χρησιμοποιείται για τα δημόσια forum, τα βιβλία επισκεπτών, τις εγγραφές σε υπηρεσίες κ.λπ. Αν λάβετε πάρα πολλά μηνύματα spam στην δευτερεύουσα διεύθυνσή σας, μπορείτε απλά να τη διαγράψετε και να δημιουργήσετε μια νέα. Για το σκοπό αυτό μπορείτε να χρησιμοποιήσετε δωρεάν υπηρεσίες μηνυμάτων, όπως το Hotmail ή το Yahoo.

Ποτέ μην απαντάτε σε spam (π.χ. για να διαμαρτυρηθείτε) γιατί αυτό επιβεβαιώνει ότι η διεύθυνσή σας είναι ενεργή. Μπορείτε επίσης να «καλύψετε» τη διεύθυνσή σας στις ιστοσελίδες ώστε να μην τις εντοπίζουν τα προγράμματα αναζήτησης e-mail που χρησιμοποιούν οι αποστολείς spam. Μπορείτε δηλαδή να κάνετε χρήση γραφικών αντί για απλό κείμενο, ή να γράψετε για παράδειγμα john dot public at xy dot com αντί για john.public@xy.com.

Να είστε επίσης προσεκτικοί με το πώς χρησιμοποιείτε τον αριθμό του κινητού σας τηλεφώνου. Δεν υπάρχει μόνο e-mail spam αλλά και sms spam.



1

Τι είναι η ανταλλαγή αρχείων;

Ανταλλαγή αρχείων (στα αγγλικά «file sharing») είναι η διαδικασία κατά την οποία άτομα που χρησιμοποιούν υπολογιστές συνδεδεμένους στο Διαδίκτυο στέλνουν μεταξύ τους αρχεία. Ο όρος καλύπτει το λεγόμενο «ανέβασμα» ενός αρχείου (uploading) και αντίστοιχα το «κατέβασμα» ενός αρχείου (downloading) από το Διαδίκτυο στον υπολογιστή. Σε γενικές γραμμές ο όρος υποδεικνύει ανταλλαγή οποιασδήποτε μορφής αρχείων όπως κείμενα, προγράμματα ηλεκτρονικού υπολογιστή, φωτογραφίες, μουσική και ταινίες. Δεν γίνεται διαχωρισμός μεταξύ της ανταλλαγής αρχείων που έχουν δημιουργηθεί από τον χρήστη που τα διακινεί, και της ανταλλαγής αρχείων που ανήκουν σε τρίτους.

2

Τι είναι copyright;

Η πνευματική ιδιοκτησία (Copyright) παρέχει αποκλειστικό δικαίωμα στους δημιουργούς ενός έργου να διανέμουν, να αναπαράγουν και να διαθέτουν το έργο αυτό στο ευρύ κοινό. Επιτρέπει έτσι στους δημιουργούς να βιοποριστούν από τη δημιουργικότητά τους και να ελέγχουν τη χρήση του έργου τους.

Υπάρχουν ορισμένες εξαιρέσεις στο αποκλειστικό δικαίωμα του δημιουργού που επιτρέπουν τη χρήση περιορισμένων αντιγράφων ενός έργου για κάποιες συγκεκριμένες χρήσεις, οι οποίες περιγράφονται λεπτομερώς στον Νόμο περί πνευματικής ιδιοκτησίας (Ν 2121/1993).

Πριν την εμφάνιση του Διαδικτύου, η δημιουργία αντιγράφων σελίδων ενός βιβλίου για προσωπική χρήση θεωρούνταν στις περισσότερες χώρες νόμιμη. Όμως, μέσα στο ψηφιακό περιβάλλον τίθεται εκ νέου το θέμα νομιμότητας της δημιουργίας προσωπικών αρχείων και ανταλλαγής αυτών με φίλους ή με άλλους χρήστες του Διαδικτύου.

3

Είναι η ανταλλαγή αρχείων παράνομη;

Ο διαχωρισμός μεταξύ αρχείων για τα οποία κατέχετε τα πνευματικά δικαιώματα επειδή τα δημιουργήσατε εσείς, και αρχείων, τα δικαιώματα των οποίων ανήκουν σε άλλους, είναι απαραίτητος, γιατί η νομοθεσία περί πνευματικής ιδιοκτησίας δίνει διαφορετικά δικαιώματα στους δημιουργούς και στους χρήστες αρχείων τρίτων.



Έτσι, η ανταλλαγή αρχείων δεν είναι παράνομη αν αφορά αποκλειστικά ανταλλαγή δικών σας αρχείων ή αρχείων που δεν υπόκεινται σε νόμο περί πνευματικής ιδιοκτησίας. Μπορείτε να ανταλλάξετε φωτογραφίες από τις διακοπές σας με τους φίλους σας, αλλά το να ανεβάζετε και να κατεβάζετε μουσική και ταινίες χωρίς την έγγραφη άδεια από τον κάτοχο των πνευματικών δικαιωμάτων είναι παράνομο στις περισσότερες χώρες της Ευρωπαϊκής Ένωσης.

Επιστούμε την ιδιαίτερη προσοχή σας σε αυτό, καθώς τα περισσότερα αρχεία που διακινούνται αφορούν μουσική ή ταινίες.

4 Υπάρχει ενδεχόμενο φυλάκισης λόγω παράνομης ανταλλαγής αρχείων;

Όταν η παράνομη ανταλλαγή αρχείων αφορά μια μεμονωμένη περίπτωση, όπου για παράδειγμα ο δράστης ανταλλάσει μια χολλυγουντιανή ταινία ή μια μουσική επιτυχία με τους φίλους του, η πιο πιθανή ποινή θα είναι χρηματική, ανάλογα με το υπολογιζόμενο κόστος της παράβασης που θα αποφασίσουν τα δικαστήρια. Η εκτεταμένη όμως παράνομη ανταλλαγή αρχείων μπορεί να οδηγήσει σε ποινικές δίωξεις και σε φυλάκιση, ανάλογα με τον όγκο των αρχείων που διακινήθηκαν, το κίνητρο για κέρδος κ.α.

Οι νόμοι περί πνευματικής ιδιοκτησίας διαφέρουν από χώρα σε χώρα. Αντίστοιχα διαφέρουν και οι συνέπειες των παραβάσεων. Ακόμη και στην Ευρωπαϊκή Ένωση όπου τα πνευματικά δικαιώματα και η επιβολή τους είναι εναρμονισμένα ως ένα βαθμό, οι παραβάσεις δεν αντιμετωπίζονται απαραίτητα με τον ίδιο τρόπο σε όλες τις χώρες-μέλη.

5 Τι μπορώ να προτείνω στα παιδιά μου;

Συμβουλέψτε τα παιδιά σας να χρησιμοποιούν κάποια από τις πολλές νόμιμες υπηρεσίες που διαθέτουν μουσική και ταινίες προς κατέβασμα έναντι αντιτίμου. Σε καμία περίπτωση πάντως δεν θα πρέπει τα παιδιά να ανταλλάσσουν τα αρχεία αυτά με άλλους εκτός αν το επιτρέπει ρητά ο κάτοχος των πνευματικών δικαιωμάτων.

6

Η ανταλλαγή αρχείων ταυτίζεται με τα δίκτυα peer-to-peer;

Ένα δίκτυο peer-to-peer (P2P) είναι μια τεχνολογία που επιτρέπει σε όσους είναι συνδεδεμένοι σε αυτό να ανταλλάσσουν αρχεία. Είναι ένας από τους πολλούς τρόπους με τους οποίους γίνεται ανταλλαγή αρχείων στο Διαδίκτυο. Όμως, χάρη στην ανωνυμία που προσφέρουν, αυτά τα δίκτυα έχουν συχνά συσχετισθεί με την παράνομη ανταλλαγή αρχείων. Οι υπηρεσίες και η τεχνολογία peer-to-peer χρησιμοποιούνται όλο και περισσότερο από τη βιομηχανία του θεάματος για την παροχή νόμιμων υπηρεσιών περιεχομένου μέσω του Διαδικτύου.

7

Πού μπορώ να μάθω περισσότερα για την ανταλλαγή αρχείων και για τα πνευματικά δικαιώματα;

Πολλοί οργανισμοί παρέχουν εκτενή πληροφόρηση για τα πνευματικά δικαιώματα και την ανταλλαγή αρχείων. Σας παραθέτουμε μια ενδεικτική λίστα με οργανισμούς και ιστοσελίδες που παρέχουν χρήσιμες πληροφορίες:

- Ελληνική Εταιρεία Προστασίας της Πνευματικής Ιδιοκτησίας ΑΕΠΙ:
<http://www.aepi.gr>
- Ένωση Ελλήνων Παραγωγών Ηχογραφημάτων IFPI:
<http://www.ifpi.gr>
- Ευρωπαϊκή Επιτροπή:
http://ec.europa.eu/internal_market/
- World Intellectual Property Organisation WIPO:
<http://www.wipo.int/enforcement/en/>
- Motion Picture Association of America MPAA:
<http://www.mpa.org>

1 Τι είναι τα weblogs ή blogs;

Η λέξη «weblog» προέρχεται από το συνδυασμό δύο λέξεων: «web» που σημαίνει Διαδίκτυο και «log» που σημαίνει καταχώρηση. Συνήθως χρησιμοποιείται η σύντμηση «blog». Blogging ονομάζεται η διαδικασία δημιουργίας και φόρτωσης πληροφοριών σε ένα blog, ενώ ο δημιουργός λέγεται blogger.

Τα blogs ή ιστολόγια, όπως λέγονται στα Ελληνικά, είναι εικονικά ημερολόγια που αποθηκεύονται στο Διαδίκτυο και μπορούν να δημιουργηθούν πολύ εύκολα από οποιονδήποτε καθώς δεν χρειάζονται ειδικές τεχνικές γνώσεις για τη δημιουργία τους. Τα blogs αποτελούνται γενικά από κείμενο και εικόνες και μπορεί να έχουν μορφή ημερολογίου.

Vlog είναι το blog στο οποίο οι χρήστες δημοσιεύουν και βίντεο εκτός από γραπτά σχόλια. Τα Moblog ή Mobile Logs χρησιμοποιούν δυνατότητες δημοσίευσης υλικού στο Διαδίκτυο μέσω του κινητού τηλεφώνου.

2 Διατρέχω κάποιον κίνδυνο αν δημιουργήσω το δικό μου blog;

Ένας από τους μεγαλύτερους κινδύνους στα blogs είναι το να μπει κανείς στον πειρασμό να αποκαλύψει προσωπικές πληροφορίες που μπορεί να διαδοθούν σε όλο τον κόσμο και να χρησιμοποιηθούν εις βάρος του (π.χ. κλοπή ταυτότητας). Μπορείτε να χρησιμοποιήσετε κάποιο ψευδώνυμο για να προστατεύσετε την ταυτότητά σας. Να θυμάστε ότι όλοι έχουν δικαίωμα να προστατεύσουν την ιδιωτική τους ζωή. Αν σκοπεύετε να δημοσιεύσετε πληροφορίες και εικόνες για τρίτους, πρέπει πρώτα να πάρετε την άδειά τους.

Ένας ακόμη κίνδυνος είναι η καταπάτηση των πνευματικών δικαιωμάτων. Δεν πρέπει να χρησιμοποιείτε υλικό (π.χ. κείμενο, εικόνα, ήχο, βίντεο) ή σχέδιο blog από ιστοσελίδες άλλων ατόμων χωρίς την άδειά τους. Επίσης, ποτέ μη δημοσιεύετε προσβλητικό (π.χ. ρατσιστικό) ή παράνομο (τζόγος, πορνογραφία κ.α.) υλικό.

3

Πώς μπορώ να δημιουργήσω το δικό μου blog;

Πολλές ιστοσελίδες προσφέρουν εργαλεία για τη δημιουργία και τη δημοσίευση υλικού, όπως είναι τα blogs. Μπορείτε να συμβουλευτείτε π.χ. το <http://www.blogger.com/start> το οποίο παρέχει εργαλεία για blogging και moblogging ή το <http://www.schoolblogs.net>. Και οι δύο ιστοχώροι προσφέρουν οδηγίες βήμα προς βήμα για να σας βοηθήσουν να δημιουργήσετε ένα λογαριασμό, να ονομάσετε το blog σας και να επιλέξετε ένα κατάλληλο πρότυπο για να ξεκινήσετε. Τότε μπορείτε να συνθέσετε, να προσθέσετε ή να επεξεργαστείτε το περιεχόμενο από μια κεντρική ιστοσελίδα που παρέχει φιλικά προς το χρήστη εργαλεία. Οι εικόνες και οι σύνδεσμοι θα κάνουν το blog σας ακόμη πιο ενδιαφέρον.

Αν θέλετε το weblog σας να είναι διαδραστικό, βεβαιωθείτε ότι έχετε επιλέξει εργαλεία που σας επιτρέπουν τη δημοσίευση σχολίων έτσι ώστε να μπορείτε να προσκαλείτε άλλους χρήστες να σχολιάσουν τις δημοσιεύσεις σας. Οι επισκέπτες του blog μπορούν να σχολιάζουν επί του περιεχομένου που δημοσιεύετε πατώντας τον αντίστοιχο σύνδεσμο στο τέλος κάθε δημοσίευσης.

4

Τι να κάνω αν βρω προσωπικά μου στοιχεία, δημοσιευμένα σε blog άλλου ατόμου;

Η δημοσίευση προσωπικών πληροφοριών τρίτων είναι παραβίαση της ιδιωτικής τους ζωής. Αν οποιοσδήποτε δημοσιεύσει τα δικά σας προσωπικά στοιχεία στο ιστολόγιό του, επικοινωνήστε άμεσα μαζί του μέσω e-mail ζητώντας του να αφαιρέσει το υλικό που σας αφορά. Οι ιστοσελίδες που φιλοξενούν blogs συνήθως δίνουν στοιχεία επικοινωνίας, αν όχι επικοινωνήστε με την ιστοσελίδα που το φιλοξενεί και ζητήστε από τους υπεύθυνους να λάβουν τα απαραίτητα μέτρα.

Μη δημοσιεύετε κάποιο σχόλιο για το υλικό που σας αφορά παρά μόνο αν είναι η έσχατη λύση στο πρόβλημά σας, γιατί έτσι προσελκύετε περισσότερη προσοχή στα στοιχεία που θέλετε να προφυλάξετε. Εάν εσείς σκοπεύετε να δημοσιεύσετε τέτοιου είδους στοιχεία για τρίτα άτομα, πρέπει πάντα να τα έχετε ενημερώσει πρώτα για το υλικό που θα δημοσιεύσετε και να έχετε πάρει την άδειά τους.

5

Τι να κάνω με τις ανεπιθύμητες και παράνομες δημοσιεύσεις στο blog μου;

Όταν επιλέξετε το λογισμικό blog που θα χρησιμοποιήσετε, βεβαιωθείτε ότι θα σας επιτρέπεται η διαγραφή σχολίων τα οποία θεωρείτε ακατάλληλα. Αν κάποιος επιμένει να δημοσιεύει προσβλητικά σχόλια, επικοινωνήστε με την υπηρεσία φιλοξενίας blog που χρησιμοποιείτε.

Ορισμένα λογισμικά blog στέλνουν στον ιδιοκτήτη ένα e-mail κάθε φορά που δημοσιεύεται ένα σχόλιο. Αν ελέγχετε συχνά τα εισερχόμενά σας μηνύματα, αυτός είναι ένας πολύ πρακτικός τρόπος ειδοποίησης που σας επιτρέπει να απαλλαχθείτε άμεσα από ανεπιθύμητα σχόλια.

Αν κάποιος σας πληροφορήσει ότι έχετε προσωπικά ή προσβλητικά στοιχεία στο ιστολόγιό σας, ελέγξτε το αμέσως και λάβετε τα απαραίτητα μέτρα (π.χ. διαγράψτε τα δεδομένα). Δεν θέλετε, φυσικά, να κατηγορηθείτε για καταπάτηση πνευματικών δικαιωμάτων.

6

Πώς μπορώ να περιορίσω την πρόσβαση στο blog μου;

Πολλοί πάροχοι λογισμικού blog σας επιτρέπουν να κάνετε μέρη του ή ακόμη και ολόκληρο το blog προσβάσιμο μόνο από άτομα που έχουν τον κωδικό πρόσβασης σε αυτό, τα άτομα δηλαδή που εσείς θα υποδείξετε.

Οι bloggers που επιθυμούν να ανταλλάξουν πιο προσωπικές πληροφορίες (π.χ. οικογενειακές φωτογραφίες) στο blog τους θα ήταν καλό να αναζητήσουν αυτή την υπηρεσία κατά το στήσιμο του blog τους.

Μπορείτε να αποφύγετε την εμφάνιση του blog σας στα αποτελέσματα μεγάλων μηχανών αναζήτησης δημιουργώντας ένα ειδικό αρχείο που δίνει την εντολή στις μηχανές αναζήτησης να αγνοούν την ιστοσελίδα σας.

7

Πού μπορώ να βρω περισσότερες πληροφορίες;

Οι πάροχοι λογισμικού blog δίνουν αρκετές συμβουλές. Μπορείτε να δείτε την ιστοσελίδα του παρόχου σας για γενικές συμβουλές, και για να ανακαλύψετε τι εργαλεία σας προσφέρουν.

Το Electronic Frontiers Foundation (www EFF .org), ένας μη κερδοσκοπικός οργανισμός που εδρεύει στις ΗΠΑ, παρέχει έναν ηλεκτρονικό οδηγό για τη διατήρηση της ανωνυμίας σε ιστολόγια. Σας παραθέτουμε ορισμένες συμβουλές για ανώνυμο blogging:

- Χρησιμοποιήστε ψευδώνυμα και μην ανακαλύπτετε προσωπικά δεδομένα.
- Περιορίστε την πρόσβαση στο blog σας.
- Χρησιμοποιήστε τεχνολογία που σας προσφέρει ανωνυμία και δεν εμφανίζει το blog σας στα αποτελέσματα μηχανών αναζήτησης.
- Κατοχυρώστε την ηλεκτρονική σας διεύθυνση ανώνυμα.



Ασφαλές Διαδίκτυο

Έργο της μαθήτριας
Δημοτικού:
Α.Ιωαννίδου

1

Τι είναι ένα chat room;

Ένα δωμάτιο ανοιχτής επικοινωνίας, γνωστό στην γλώσσα του Διαδικτύου ως chat room, προσφέρει άμεση (συγχρονισμένη) επικοινωνία σε πραγματικό χρόνο. Τα chat rooms είναι εικονικά μέρη, όπου άνθρωποι από όλο τον κόσμο έχουν τη δυνατότητα να «συναντηθούν» και να «συνομιλήσουν» μέσω μηνυμάτων που γράφουν με το πληκτρολόγιό τους. Όπως αποκαλύπτει και η λέξη «συγχρονισμένη», για να κάνει κανείς chat με άλλα άτομα πρέπει να τα «συναντήσει» την ίδια ώρα σε ένα chat room.

Πολύ δημοφιλή είναι τα αποκαλούμενα «Instant Messenger Programs» (Προγράμματα Άμεσων Μηνυμάτων), μέσω των οποίων μπορεί κανείς να πληροφορηθεί τότε οι φίλοι του είναι συνδεδεμένοι στο Διαδίκτυο. Τότε μπορεί να τους καλέσει σε συνομιλία, να τους στείλει μηνύματα, αρχεία, κ.λπ. τα οποία θα λάβουν και μπορούν να διαβάσουν άμεσα.

2

Πώς μπορώ να συνομιλώ με ασφάλεια;

Είναι εύκολο να συνομιλήσετε με ασφάλεια, ακολουθώντας μερικούς απλούς κανόνες:

1. Οι εικονικοί φίλοι μπορεί να είναι διαφορετικοί από αυτό που δείχνουν.
2. Μη δίνετε ποτέ προσωπικές πληροφορίες, όπως τη διεύθυνση ηλεκτρονικού ταχυδρομείου, τη διεύθυνση του σπιτιού σας ή τον αριθμό του κινητού σας τηλεφώνου.
3. Ποτέ μη δίνετε πληροφορίες για την οικογένειά σας, τους φίλους σας και τρίτους.
4. Αν νιώθετε ότι κάποιος σας παρενοχλεί, θυμηθείτε: μπορείτε να βγείτε από το chat room με ένα απλό «κλικ».

3

Πώς οι άγνωστοι προσεγγίζουν τα νεαρά άτομα στα chat rooms και ποιοί είναι οι κίνδυνοι;

Τις περισσότερες φορές οι άγνωστοι χρησιμοποιούν ψευδείς πληροφορίες για να προσεγγίσουν νεαρά άτομα. Δίνουν π.χ. πλαστό όνομα, ηλικία, ενδιαφέροντα. Τότε με δόλιες μεθόδους αρχίζουν επικοινωνία με τα νεαρά άτομα και με τον καιρό κερδίζουν την εμπιστοσύνη τους.

Έτσι οι νέοι (σκεπτόμενοι ότι τα chat rooms είναι ασφαλή) αρχίζουν να αποκαλύπτουν προσωπικές τους πληροφορίες, στοιχεία φίλων τους και της οικογένειάς τους, το όνομα του σχολείου τους, αριθμούς τηλεφώνου, κ.λπ.

Οι άγνωστοι που έχουν κακές προθέσεις είναι πολύ υπομονετικοί και περιμένουν αρκετό καιρό μέχρι να συλλέξουν αρκετές πληροφορίες για το υποψήφιο θύμα. Κάποια στιγμή δε αρχίζουν να ρωτάνε τα νεαρά άτομα για τις σεξουαλικές τους εμπειρίες.

Τότε η συζήτηση μπορεί να οδηγηθεί σε σεξουαλικά θέματα και ενδέχεται το νεαρό θύμα να γίνει παραλήπτης πορνογραφικού υλικού στο οποίο συμμετέχουν ανήλικοι, με σκοπό να πιστέψει ότι τέτοιου είδους δραστηριότητες δεν είναι κακές ή για να το φέρουν σε δύσκολη θέση, ώστε να μην αναφέρει το περιστατικό στους γονείς του. Αυτές οι ενέργειες έχουν ως σκοπό την αποδυνάμωση των υποψήφιων θυμάτων και την μετέπειτα συμμετοχή τους σε σεξουαλικές πράξεις.

Επιπλέον, πολλοί άγνωστοι ζητούν κατ' ιδίαν συναντήσεις όταν πιστεύουν ότι έχουν κερδίσει την εμπιστοσύνη του νέου. Τέτοιες συναντήσεις μπορεί να αποδειχθούν πολύ επικίνδυνες και να οδηγήσουν σε σεξουαλική κακοποίηση, ακόμα και σε απαγωγή με ολέθριες συνέπειες.

4

Τι να κάνω αν με παρενοχλούν;

Πρέπει πάντα να θυμάστε ότι έχετε τον έλεγχο. Εάν κάνετε chat και αισθανθείτε ότι κάποιος σας ενοχλεί, μπορείτε απλά να σταματήσετε την συνομιλία με ένα κλικ. Εάν κάποιος συνεχίσει να σας παρενοχλεί χρησιμοποιώντας το ηλεκτρονικό σας ταχυδρομείο, τότε το καλύτερο που μπορείτε να κάνετε είναι να μπλοκάρετε τα μηνύματα αυτά, έτσι ώστε να μην φτάνουν στον υπολογιστή σας. Τέλος, μπορείτε να αλλάξετε την ηλεκτρονική σας διεύθυνση.

Μην ξεχνάτε ποτέ, ότι οι άνθρωποι που γνωρίσατε μέσα από το Διαδίκτυο δεν είναι πάντοτε αυτοί που σας λένε. Πολλές φορές λένε ψέματα για την ηλικία τους, και ενώ συστήνονται ως συνομήλικοί σας, μπορεί να είναι στην πραγματικότητα πολύ μεγαλύτεροί σας. Μην ξεχνάτε ποτέ, ότι τέτοιοι άνθρωποι είναι πολύ υπομονετικοί και δεν έχουν κανένα πρόβλημα να περιμένουν πολλούς μήνες μέχρι να σας πείσουν να τους εμπιστευτείτε και τελικά να τους συναντήσετε σε κάποιο μέρος που θα σας προτείνουν αυτοί, με πρόθεση να σας βλάψουν.

Τακτικές για
ασφαλές Διαδίκτυο

Έργο του μαθητή
Δημοτικού:
Α.Αγαπητού



5

Πώς μπορώ να σώσω τις συνομιλίες;

Η αποθήκευση των συζητήσεων είναι ένας πολύ σημαντικός τρόπος για να συλλέξετε στοιχεία για οποιαδήποτε άσχημη συμπεριφορά. Υπάρχουν τρεις τρόποι με τους οποίους μπορείτε να αποθηκεύσετε μία συζήτηση. Η μέθοδος που θα χρησιμοποιήσετε θα εξαρτηθεί από το πρόγραμμα που χρησιμοποιείτε.

Μέθοδος 1 - Αποθηκεύστε τη συζήτηση

1. Πηγαίνετε στο Μενού "Φάκελος". Εάν έχετε αγγλικό μενού, τότε κάντε κλικ στο «File».
2. Επιλέξτε «Αποθήκευση ως». Εάν έχετε αγγλικό μενού, επιλέξτε «Save as».

Μέθοδος 2 – Αντιγράψτε τη συζήτηση

1. Επιλέξτε με το ποντίκι σας το κείμενο της συζήτησης και πατήστε συγχρόνως τα πλήκτρα CTRL + C.
2. Πηγαίνετε σε ένα πρόγραμμα επεξεργασίας κειμένου (π.χ.

Word), και δημιουργήστε ένα νέο αρχείο.

3. Πατήστε συγχρόνως τα πλήκτρα CTRL + V για να αντιγράψετε τη συζήτηση.
4. Σώστε το αρχείο που δημιουργήσατε ή εκτυπώστε το για να το χρησιμοποιήσετε σε περίπτωση καταγγελίας ή για να το δείξετε στους γονείς σας αν είστε ανήλικοι.

Μέθοδος 3 – Εκτυπώστε την οθόνη

1. Πατήστε το πλήκτρο «PrtScn» στο πληκτρολόγιό σας (δηλαδή «Print Screen»). Το πλήκτρο αυτό βρίσκεται συνήθως δεξιά επάνω στο πληκτρολόγιό σας.
2. Ανοίξτε ένα πρόγραμμα επεξεργασίας κειμένου ή επεξεργασίας γραφικών και εικόνων.
3. Πατήστε συγχρόνως CTRL + V για να αντιγράψετε την οθόνη.
4. Σώστε το αρχείο που μόλις δημιουργήσατε ή εκτυπώστε το.

1

Τι είναι οι ύποπτες εμπορικές σελίδες;

Μη αξιόπιστες ιστοσελίδες ενδέχεται:

- Να μην εκτελούν τα καθήκοντά τους προς τους πελάτες τους, π.χ. μπορεί να μην παραδώσουν προϊόντα που έχουν αγοραστεί.
- Να κάνουν κακή χρήση προσωπικών δεδομένων.
- Να κάνουν κακή χρήση των πληροφοριών πληρωμής (στοιχεία πιστωτικής κάρτας).
- Τέτοιοι εμπορικοί ιστοχώροι μπορεί ακόμη να προσφέρουν ανεπιθύμητες ή παράνομες υπηρεσίες σε παιδιά (τζόγος, πορνογραφικό υλικό κ.α.)
- Συνήθως, τέτοιες ιστοσελίδες έχουν δημιουργηθεί σε χώρες όπου δεν υπάρχει αντίστοιχο νομοθετικό πλαίσιο που να απαγορεύει τέτοιου είδους δραστηριότητες.

2

Πώς μπορώ να αναγνωρίσω τις ασφαλείς μεθόδους συναλλαγών;

Οι αξιόπιστες εμπορικές ιστοσελίδες παρέχουν συναλλαγές μόνο μέσω μεθόδων «ασφαλών ηλεκτρονικών συναλλαγών» (secure electronic transaction). Έτσι είναι πολύ σημαντικό, όταν καταχωρείτε πληροφορίες πληρωμής (π.χ. δεδομένα της πιστωτικής κάρτας), να ελέγχετε πάντα αν η διεύθυνση της ιστοσελίδας που έχετε επισκεφθεί ξεκινά με "https://" και όχι με "http://". Με αυτό τον τρόπο, θα γνωρίζετε αν η ιστοσελίδα προσφέρει ασφαλείς συναλλαγές ή όχι.

3

Πώς μπορώ να αναγνωρίσω τις αξιόπιστες εμπορικές ιστοσελίδες;

Πρώτα απ' όλα, οι γνωστές και εδραιωμένες εταιρίες είναι πιθανότατα το ίδιο αξιόπιστες στο Διαδίκτυο όσο και στην πραγματική ζωή.

Άλλα κριτήρια που μας βοηθούν να αναγνωρίσουμε τις αξιόπιστες εμπορικές σελίδες:

- Ξεκάθαρος προσδιορισμός της εταιρίας με το όνομά της, τη διεύθυνση, τον αριθμό τηλεφώνου, στοιχεία επικοινωνίας κ.λπ.
- Οι όροι των συμβάσεων είναι εύκολα προσβάσιμοι και διαφανείς.
- Τα χαρακτηριστικά του προϊόντος και οι όροι της εγγύησης είναι σαφή και εύκολα προσβάσιμα.
- Η τιμή του προϊόντος περιλαμβάνει όλες τις τυχόν χρεώσεις.
- Ο ιστοχώρος παρέχει ασφαλή τρόπο πληρωμής.
- Οι παραγγελίες επιβεβαιώνονται με e-mail.
- Οι καταναλωτές έχουν ένα σαφώς καθορισμένο δικαίωμα ανάκλησης της παραγγελίας.
- Η ώρα της παράδοσης είναι προκαθορισμένη.

Σε περίπτωση που υπάρξουν προβλήματα σε κάποια ηλεκτρονική συναλλαγή, τότε είναι ευκολότερη η αντιμετώπισή τους αν η συναλλαγή έχει γίνει με κάποιο ηλεκτρονικό κατάστημα που εδρεύει στην ίδια χώρα με αυτή του πελάτη.

4

Τι είναι η κλοπή ταυτότητας ;

Μιλάμε για κλοπή ταυτότητας, όταν προσωπικές πληροφορίες έχουν κλαπεί και χρησιμοποιούνται παράνομα. Στις περισσότερες περιπτώσεις η κλοπή ταυτότητας γίνεται μέσω του phishing και του pharming (Βλ. επόμενη σελίδα).

5

Πώς μπορώ να αποφύγω τους κινδύνους στις online δημοπρασίες;

Το βασικό πρόβλημα με τις ηλεκτρονικές δημοπρασίες είναι οι προκαταβολές. Αν οι συμβαλλόμενοι σας παραλάβουν χρήματα και τελικά δεν γίνει η παράδοση του προϊόντος που πλειοδοτήθηκε, είναι πολύ δύσκολο να πάρει κανείς πίσω τα λεφτά της συναλλαγής.

Η καλύτερη λύση είναι η χρήση υπηρεσιών εμπιστοσύνης που προσφέρονται από πλατφόρμες ηλεκτρονικών δημοπρασιών.

6

Τι είναι το Pharming;

Το Pharming είναι μια μορφή απάτης της ηλεκτρονικής διεύθυνσης (domain name) που έχει ως αποτέλεσμα να πιστεύουν οι χρήστες ότι βρίσκονται σε μια γνήσια ιστοσελίδα με το σωστό URL. Ωστόσο, στην πραγματικότητα έχουν παραπεμφθεί σε μια ψεύτικη.

Εκμεταλλευόμενοι κάποια κενά στην ασφάλεια μιας ιστοσελίδας στην οποία οι χρήστες μπαίνουν για να πραγματοποιήσουν διάφορες συναλλαγές, οι απατεώνες καταφέρνουν να εκτρέψουν την ροή των επισκεπτών σε άλλο ιστοχώρο όπου τα στοιχεία των συναλλαγών που καταχωρούνται χρησιμοποιούνται για την οικονομική εξαπάτηση των επισκεπτών.

Για να διαπιστώσετε αν οι συναλλαγές που κάνετε είναι ασφαλείς, δείτε στο πεδίο της διεύθυνσης αν υπάρχει η ένδειξη **https://** αντί για το συμβατικό **http://**.

7

Τι είναι το Phishing;

Το Phishing είναι η πρακτική της παραπλάνησης ενός χρήστη κάνοντάς τον να δώσει προσωπικές του πληροφορίες σε μια ψεύτικη φόρμα στο Διαδίκτυο. Μια τέτοιου είδους δραστηριότητα θα επιτρέψει σε έναν cracker να κλέψει ή να πλαστογραφήσει τα στοιχεία του θύματος ή/και να κερδίσει παράνομη πρόσβαση στα δεδομένα του/της, όπως προσωπικούς λογαριασμούς, συνδρομές, e-mail, κωδικούς PIN, κωδικούς TAN, κ.λπ.

Για παράδειγμα, ο χρήστης λαμβάνει ένα e-mail που μοιάζει ότι έχει σταλεί από την τράπεζά του και στο οποίο πληροφορείται για κάποια «κενά» ασφαλείας στο τραπεζικό σύστημα, και του ζητείται ευγενικά να συνδεθεί σε μια ειδική ιστοσελίδα (η οποία επίσης μοιάζει να προέρχεται από την τράπεζα αυτή) για να καταχωρήσει εκεί το όνομα χρήστη, κωδικούς του, προσωπικές πληροφορίες λογαριασμών, κ.λπ. Είναι σημαντικό να θυμάται κανείς ότι καμία τράπεζα δεν θα ζητάγε ποτέ προσωπικές πληροφορίες των πελατών της μέσω e-mail ή διαδικτυακών υπηρεσιών.



Internet: a powerful tool or a big trap?

Έργο των μαθητών Λυκείου:

Α.Αραμπατζή, Π.Βεζυρόπουλου, Α.Γκατσιούδη, Ε.Δημοσχάκη, Π.Δόβρη, Χ.Καδγιαννοπούλου, Ο.Κανέλλου, Χ.Κιτσικούδη, Π.Κοπούκη, Χ.Κουμανούδη, Μ.Μίχου, Γ.Μούλλα, Γ.Μπροντίδη, Μ.Πάλλα, Ε.Παπαβασιλείου, Μ.Παπαδούδη, Χ.Μουχαμέρ, Α.Φουντούκη

1 Τι είναι η κοινωνική δικτύωση;

Οι ιστοσελίδες κοινωνικής δικτύωσης (social networking) αποτελούν εικονικές κοινότητες όπου οι χρήστες του Διαδικτύου έχουν τη δυνατότητα να δημιουργήσουν εικονικά προφίλ και να αναπτύξουν ένα δίκτυο επαφών με τις οποίες μπορούν να επικοινωνούν μέσω της ιστοσελίδας. Οι πιο διαδεδομένες πλατφόρμες κοινωνικής δικτύωσης παγκοσμίως αυτή τη στιγμή είναι το Myspace και το Facebook.

Netiquette-Decalogue

Έργο των μαθητών
Γυμνασίου:
Μ.Βρύκου, Χ.Γκαβανούδη,
Α.Γρηγορούδη, Δ.Μήλη,
Ε.Μητσιάρα, Γ.Κουλουμπή,
Α.Παπακαρμύξη, Ν.Τερζή,
Χ.Χαλκίδη, Π.Χατζηδάκη



2

Τι προβλήματα ενδέχεται να προκύψουν στις ιστοσελίδες κοινωνικής δικτύωσης;

Σας παραθέτουμε τα πιο σημαντικά προβλήματα που αφορούν τους ανηλίκους:

Κακή χρήση προσωπικών δεδομένων. Τα παιδιά δεν πρέπει να δίνουν στα στοιχεία του προφίλ τους τηλέφωνα, διευθύνσεις, στοιχεία της οικογένειας ή οποιαδήποτε άλλη πληροφορία που μπορεί να οδηγήσει στον εντοπισμό τους στον φυσικό κόσμο. Ιδιαίτερη προσοχή πρέπει να δίνεται στη δημοσίευση φωτογραφιών καθώς είναι ιδιαίτερα εύκολο να παραπονηθούν και να κυκλοφορήσουν αλλαγμένες στο Διαδίκτυο.

Grooming. Παιδόφιλοι εμφανίζονται ως ανήλικοι για να προσεγγίσουν παιδιά στο Διαδίκτυο. Θα ήταν καλό να αποφεύγονται οι προσωπικές συναντήσεις με εικονικούς φίλους χωρίς τη συνοδεία κάποιου ενηλίκου. Το παιδιά θα πρέπει να σταματούν συζητήσεις που τα φέρνουν σε δύσκολη θέση και να αποκλείουν την επικοινωνία με άτομα που τα παρενοχλούν.

Παρενόχληση. Η ανωνυμία που προσφέρεται σε αυτούς τους ιστοχώρους δίνει τη δυνατότητα σε πολλούς επιτήδειους να εκτοξεύουν απειλές και να παρενοχλούν συστηματικά ορισμένα άτομα. Οι γονείς πρέπει να συζητούν με τα παιδιά για τις διαδικτυακές τους γνωριμίες έτσι ώστε αν αντιληφθούν κάποιο πολύ σοβαρό περιστατικό να το καταγγείλουν.

Αξιοπιστία περιεχομένου. Η δυνατότητα που διανοίγεται στον καθένα να παρεμβαίνει και να επεξεργάζεται το περιεχόμενο ορισμένων ιστοχώρων είναι καταπληκτική, ωστόσο πολλές πληροφορίες ενδέχεται να είναι παραπλανητικές ή λανθασμένες. Στοιχεία που έχουν αντληθεί από τέτοιου είδους ιστοχώρους είναι καλό να διασταυρώνονται προτού χρησιμοποιηθούν αλλού.

3

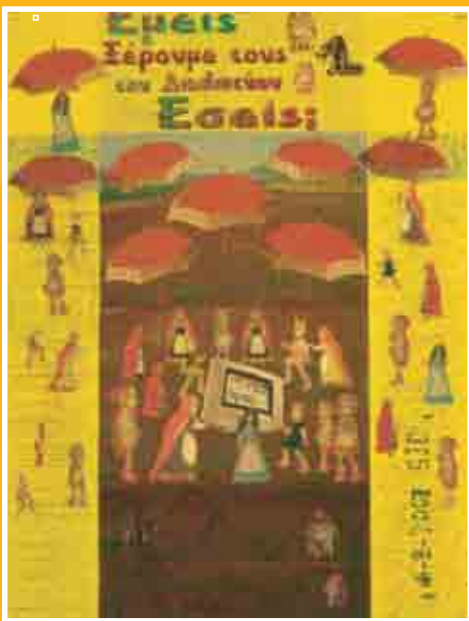
Τι θα πρέπει να προσέχω στις φωτογραφίες που αναρτώ στο προφίλ μου;

Μην ανεβάζετε στο προφίλ σας φωτογραφίες όπου φαίνεται καθαρά η τοποθεσία στην οποία βρίσκεστε, ειδικότερα αν πρόκειται για το σπίτι σας, το σχολείο ή μέρη που συχνάζετε. Έτσι θα μειώσετε τις πιθανότητες εντοπισμού σας στον φυσικό κόσμο.

Να έχετε πάντα υπόψη σας ότι οι πληροφορίες που δημοσιεύετε στις ιστοσελίδες κοινωνικής δικτύωσης είναι δημόσια προσπελάσιμες, επομένως, καλό θα ήταν να μη δημοσιεύετε στοιχεία και φωτογραφίες που θα σας έφερναν σε δύσκολη θέση. Ακόμα και όταν διαγράψετε το προφίλ σας, πολλές πληροφορίες που σας αφορούν δεν αφαιρούνται και ενδέχεται να τις συναντήσετε και αλλού στο Διαδίκτυο.

Η κοκκινোসκουφίτσα και τα 3 γουρουνάκια στο Διαδίκτυο

Έργο των μαθητριών Λυκείου:
Μ.Σταυροπούλου,
Α.Σίσκογλου,
Κ.Παπαδέα,
Σ.Χατζηθεοδωρίδη,
Κ.Σταφυλάτου,
Α.Πανοπούλου,
Α.Βέρδη



4

Πώς μπορώ να διαφυλάξω προσωπικά δεδομένα που εμφανίζονται στο προφίλ μου;

Από τη στιγμή που δημιουργείτε το εικονικό σας προφίλ σας συμβουλευόμαστε να επισκεφθείτε το μενού των ρυθμίσεων για τη διαχείριση των προσωπικών σας δεδομένων (συνηθέστερα θα το βρείτε στα αγγλικά ως *privacy settings*) και να αλλάξετε τις προεπιλεγμένες ρυθμίσεις. Στο μενού αυτό μπορείτε μεταξύ άλλων:

- Να επιλέξετε αν οι επισκέπτες του προφίλ σας μπορούν να δουν αν είστε online ή όχι.
- Να καθορίσετε ποιοι θα μπορούν να βλέπουν το εικονικό σας προφίλ ή συγκεκριμένα στοιχεία που περιλαμβάνονται σε αυτό (ημερομηνία γέννησης, φωτογραφία κ.α.)
- Να μπλοκάρτε την πρόσβαση συγκεκριμένων ατόμων στο προφίλ σας.
- Να ρυθμίσετε από ποιους χρήστες μπορείτε να λαμβάνετε προσωπικά μηνύματα και σχόλια.
- Να ρυθμίσετε αν θα εμφανίζεται το προφίλ σας στα αποτελέσματα αναζήτησης μέσω της ιστοσελίδας καθώς και τη μορφή που θα έχει (αν θα φαίνεται η φωτογραφία, τα στοιχεία επικοινωνίας κ.α.)
- Καθώς κάθε ιστοσελίδα κοινωνικής δικτύωσης έχει διαφορετική πολιτική διαχείρισης των δεδομένων σας, διαβάστε προσεκτικά τη δήλωση απορρήτου και δράστε ανάλογα.

1

Πώς μπορώ να προστατεύσω την ιδιωτική μου ζωή στο Διαδίκτυο;

Μπορείτε εύκολα να προστατεύσετε την ιδιωτική σας ζωή με το να μη δημοσιεύετε ποτέ προσωπικά σας δεδομένα, όπως το πραγματικό σας όνομα, τη διεύθυνσή σας, τον αριθμό τηλεφώνου, το όνομα του σχολείου σας (αν είστε ανήλικος) ή στοιχεία που αφορούν φίλους και οικογένεια.

Όταν κάνετε chat, χρησιμοποιήστε ψευδώνυμο και αποφύγετε να μπαίνετε σε προσωπικές λεπτομέρειες, αν δεν γνωρίζετε προσωπικά το άτομο με το οποίο συνομιλείτε.

Όταν επισκέπτεστε ιστοσελίδες που ζητούν τις προσωπικές σας πληροφορίες, σιγουρευτείτε ότι η σελίδα είναι αξιόπιστη και πριν καταχωρήσετε τα στοιχεία σας, ρωτήστε για ποιο λόγο τα χρειάζονται. Πάντα να συμβουλευέστε τους όρους και προϋποθέσεις (terms and conditions) και την πολιτική απορρήτου (privacy statement) της εταιρίας που διαχειρίζεται τον ιστοχώρο.

2

Αν κάποιος φίλος ζητήσει τον κωδικό της σύνδεσής μου στο Διαδίκτυο, να του τον δώσω;

Μη δίνετε τον κωδικό σας γιατί εσείς θα είστε υπεύθυνος/η για ότι δραστηριότητα κάνει ο φίλος ή η φίλη σας στο Διαδίκτυο. Γενικά δεν πρέπει ποτέ να αποκαλύπτετε τον κωδικό σας. Αν πιστεύετε ότι κάποιος ανακάλυψε τον κωδικό σας πρέπει να τον αλλάξετε άμεσα. Να χρησιμοποιείτε πάντα κωδικούς πρόσβασης που είναι δύσκολο να φανταστεί κανείς. Για παράδειγμα, να αποφεύγετε να χρησιμοποιείτε το όνομά σας, το επίθετό σας ή ονόματα φίλων, κατοικίδιων και ημερομηνίες γενεθλίων.

3

Είμαι ορατός στο Διαδίκτυο;

Όλοι οι χρήστες του Διαδικτύου, αφήνουν πάντα ηλεκτρονικά ίχνη, τα αποκαλούμενα «cybertrails» όταν είναι συνδεδεμένοι σε αυτό.

Αυτό στην πραγματικότητα είναι καλό: αν κάποιος διαπράττει εγκλήματα στο Διαδίκτυο, η αστυνομία και άλλες αρχές μπορούν να εντοπίσουν τα αποδεικτικά στοιχεία και να τους πιάσουν.



Internet: Δίκτυο να επικοινωνούμε ή δίκτυο για να μπλεχτούμε;

*Έργο του μαθητή Δημοτικού:
Δ.Καβάζη*

4

Μπορώ να ανεβάσω στο Διαδίκτυο φωτογραφίες φίλων μου;

Αν θέλετε να βγάλετε μια φωτογραφία ενός φίλου, ενός μέλους της οικογένειας, ενός συμμαθητή κ.λπ., πρώτα πρέπει να ζητήσετε την άδεια του ατόμου αυτού.

Σε κάθε περίπτωση, μην ανεβάζετε τη φωτογραφία στο Διαδίκτυο, αλλά κρατήστε τη σε ασφαλές μέρος, μόνο για προσωπική σας χρήση. Να θυμάστε ότι από τη στιγμή που στέλνετε μια φωτογραφία στο Διαδίκτυο παύει να είναι για ιδιωτική χρήση και δεν μπορείτε να ελέγξετε το που θα καταλήξει.

5

Τι να κάνω αν κάποια εμπορική εταιρία ζητήσει τα στοιχεία μου για να μου στέλνει διαφημιστικό υλικό ή για να συμμετάσχω σε μια κλήρωση;

Πρώτα απ' όλα σιγουρευτείτε ότι η εταιρία είναι αξιόπιστη. Δεν υπάρχει κάτι μεμπτό στο να λαμβάνει κανείς διαφημιστικό υλικό ή στη συμμετοχή σε μια ηλεκτρονική κλήρωση ή διαγωνισμό, εφόσον το επιθυμεί.

Αλλά προτού στείλετε τα προσωπικά σας δεδομένα, ελέγξτε την πολιτική απορρήτου (privacy policy) της εταιρίας, π.χ. το πως πρόκειται να χρησιμοποιήσει τα στοιχεία σας, και αν δηλώνει ρητά ότι τα προσωπικά σας στοιχεία θα κρατηθούν εμπιστευτικά και δεν θα δοθούν σε τρίτους.

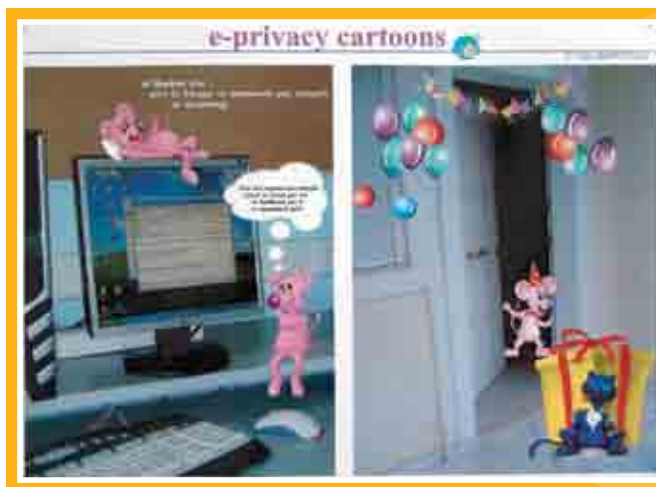
Αν είστε ανήλικος, πρώτα ρωτήστε τους γονείς σας αν σας επιτρέπουν να δώσετε τα στοιχεία σας, και μόνο αν σας το επιτρέπουν κάντε το.

6

Ένας ηλεκτρονικός φίλος μου ζήτησε να του στείλω μια φωτογραφία μου. Τι να κάνω;

Το να στέλνετε φωτογραφίες σε ηλεκτρονικούς φίλους δεν είναι και τόσο καλή ιδέα. Έτσι, λοιπόν αποφύγετε να στέλνετε δικές σας φωτογραφίες σε άτομα που γνωρίσατε μέσω Διαδικτύου και δεν γνωρίζετε προσωπικά.

Μια δική σας φωτογραφία θα κάνει πιο εύκολο τον εντοπισμό σας στον πραγματικό κόσμο. Επίσης να θυμάστε ότι μια ψηφιακή φωτογραφία σας μπορεί να υπάρχει για πάντα και αν κάποιος ηλεκτρονικός σας φίλος την έχει κρατήσει, μπορεί κάποια μέρα να συναντήσετε τη φωτογραφία αυτή στο Διαδίκτυο και υπάρχει περίπτωση να μη μοιάζει καθόλου με το πρωτότυπο, καθότι η επεξεργασία μιας φωτογραφίας είναι με τα σημερινά μέσα απίστευτα εύκολη. Να θυμάστε πάντα ότι από τη στιγμή που ανεβάσετε μια φωτογραφία σας στο Διαδίκτυο, παύει πια να είναι προσωπική και δεν μπορείτε να ελέγξετε που θα δημοσιευθεί και από ποιον θα χρησιμοποιηθεί.



E-privacy cartoons

Έργο των μαθητών ΤΕΕ:
Χ. Αναστασόπουλου,
Π. Μάρκου

1

Τι μπορώ να κάνω για να περιορίσω τις χρεώσεις του κινητού τηλεφώνου;

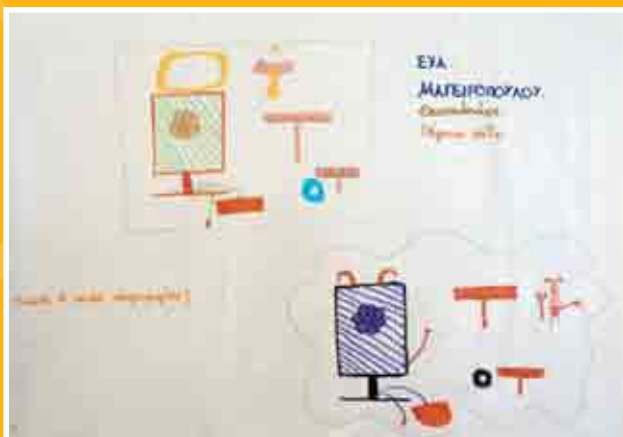
Χρησιμοποιήστε καρτο-κινητά ή άλλου είδους υπηρεσίες που προσφέρουν οι πάροχοι ώστε να μην ξεπερνάτε κάποια προκαθορισμένη χρέωση μηνιαίως.

Να έχετε υπόψη ότι οι υπηρεσίες προστιθέμενης αξίας (premium services) φωνής και SMS έχουν πιο μεγάλη χρέωση από τις βασικές υπηρεσίες (απλή κλήση φωνής ή αποστολή SMS σε φίλο). Οι προορισμοί πρόσθετης χρέωσης αρχίζουν από συγκεκριμένους αριθμούς (ενδεικτικά 90X XXX XXXX, 14XXX, 54XXX, 190XX, 195XX.) Όταν χρησιμοποιείτε τους παραπάνω προορισμούς να είστε προσεκτικοί και να βλέπετε την αναγραφόμενη χρέωση που πρέπει να αναφέρεται καθαρά και ευκρινώς.

Μόνο σε ειδικές περιστάσεις μπορείτε να επιτρέπετε τη χρήση του τηλεφώνου σας από άλλους και μόνο όταν είστε παρών. Ποτέ μην αφήνετε το κινητό σας εκτός της προσοχής σας.

Κακές ή καλές
πληροφορίες;

Έργο της μαθήτριας
Δημοτικού:
Ε.Μαγειροπούλου



2

Τι πρέπει να λάβω υπόψη μου σχετικά με τη χρήση της φωτογραφικής μηχανής του κινητού μου τηλεφώνου;

Σε ότι αφορά στη δημοσίευση των φωτογραφιών πρέπει να γνωρίζετε τα παρακάτω:

- **Ιδιωτική ζωή:** Δεν έχετε υπό τον έλεγχό σας τις φωτογραφίες που διακινήσατε μέσω κινητού τηλεφώνου. Τις φωτογραφίες που δημοσιεύονται στο Διαδίκτυο μπορεί να τις δει οποιοσδήποτε στον κόσμο. Αναλογισθείτε για τις πιθανές συνέπειες, π.χ. οι φωτογραφίες καθιστούν ευκολότερο τον εντοπισμό σας στον πραγματικό κόσμο και πιθανότατα δεν θα θέλατε να σας δουν όλοι σε συγκεκριμένες στιγμές.
- Σεβαστείτε τα δικαιώματα της προσωπικότητας (που είναι εξαιρετικής σημασίας αν οι φωτογραφίες δείχνουν άτομα σε ένα ακατάλληλο περιβάλλον) και τα δικαιώματα πνευματικής ιδιοκτησίας (αν οι φωτογραφίες ή τα βίντεο ενσωματώνουν τέτοια δικαιώματα και διακινούνται χωρίς τη συναίνεση των δημιουργών). Για να αποφύγετε τέτοιου είδους προβλήματα: αν θέλετε να βγάξετε φωτογραφίες άλλων ατόμων ζητήστε πρώτα την άδειά τους.
- Από τη στιγμή που οι φωτογραφίες δημοσιεύονται στο Διαδίκτυο, μπορεί να μείνουν αποθηκευμένες εκεί για πάντα ακόμη και να αλλοιωθούν.



4

Ποιες είναι οι συνέπειες σε σχέση με την ασφάλεια, από τη χρήση κινητών τηλεφώνων με πλήρη πρόσβαση στο Διαδίκτυο;

Όλο και περισσότερα κινητά τηλέφωνα έχουν πλήρη πρόσβαση στο Διαδίκτυο. Για το λόγο αυτό είναι σημαντικό κατά τη χρήση τους, να τηρούνται τα ίδια μέτρα ασφαλείας που ισχύουν για το σερφάρισμα μέσω υπολογιστή (προστασία προσωπικών δεδομένων, βλαβερό περιεχόμενο, προστασία του καταναλωτή, κ.λπ.)

Το κινητό τηλέφωνο είναι πανταχού παρόν. Για το λόγο αυτό οι γονείς πρέπει να είναι ενημερωμένοι και να ελέγχουν τις συνήθειες χρήσης των κινητών από τα παιδιά τους. Επικοινωνήστε με την εταιρία κινητής τηλεφωνίας για να ρωτήσετε αν προσφέρει συστήματα ελέγχου ηλικίας και φίλτρα.

5

Συμβουλές προς τα παιδιά

- Προληπτικό μέτρο: Μην δημοσιεύετε ευαίσθητα προσωπικά δεδομένα όπως φωτογραφίες, ονοματεπώνυμο, διεύθυνση, ηλικία κ.λπ.
- Αποθηκεύστε τα αποδεικτικά στοιχεία.
- Αγνοήστε όσους σας παρενοχλούν ηλεκτρονικά.
- Σε περίπτωση παρενόχλησης, μιλήστε στους γονείς σας ή σε κάποιο άτομο της εμπιστοσύνης σας, μην υποφέρετε μόνοι.
- Μην δέχεστε οποιεσδήποτε εφαρμογές σας στέλνουν μέσω Bluetooth ή με άλλο τρόπο και μην τις αποθηκεύετε στο κινητό σας τηλέφωνο, γιατί μπορεί να περιέχουν ιούς.

6

Συμβουλές προς τους γονείς

- Συζητήστε με το παιδί για την ηλεκτρονική παρενόχληση.
- Να είστε σε επαγρύπνηση για ενδείξεις ότι το παιδί σας είναι θύμα παρενόχλησης (π.χ. συναισθηματική ανησυχία, αποφυγή φίλων, σχολείου, δραστηριοτήτων, επιδείνωση βαθμών, σχόλια που μαρτυρούν διαταραγμένες σχέσεις ηλεκτρονικές ή μη).
- Μιλήστε με το σχολικό σύμβουλο, τους γονείς του παιδιού που παρενοχλεί, την εταιρία κινητής τηλεφωνίας ή, αν η παρενόχληση φτάνει στο σημείο να θεωρηθεί παράνομη, επικοινωνήστε με την αστυνομία.
- Αλλάξτε τον αριθμό τηλεφώνου του παιδιού σας.

7

Συμβουλές σχετικά με το grooming

Το grooming περιγράφει τη συμπεριφορά ατόμων με σεξουαλικό ενδιαφέρον προς τα παιδιά κάνοντας χρήση κινητών και διαδικτυακών τεχνολογιών για να αναγνωρίσουν και να στοχοποιήσουν πιθανά θύματα.

Για την αποφυγή τέτοιου είδους περιστατικών:

- Μην δίνετε προσωπικά στοιχεία επικοινωνίας.
- Σε περίπτωση που αντιληφθείτε ύποπτη συμπεριφορά, αποθηκεύστε αντίγραφο της συνομιλίας, αν είναι δυνατόν.
- Συγκρατηθείτε όταν προκύψουν ερωτήσεις σεξουαλικής φύσης και σταματήστε άβολες συζητήσεις.
- Πείτε όχι σε συναντήσεις πρόσωπο με πρόσωπο αν κάτι σας φαίνεται ύποπτο. Αν αποφασίσετε τελικά να συναντήσετε κάποιον, κανονίστε μια τέτοια συνάντηση μόνο σε δημόσιο χώρο. Αν δε είστε ανήλικος, φροντίστε να συνοδεύεστε από ένα γονέα σας.

1

Τι είναι Malware;

Είναι βλαβερό λογισμικό που περιλαμβάνει, μεταξύ άλλων, τους ιούς (viruses), τα σκουλήκια (worms) και τους δούρειους ίππους (trojan horses).

2

Τι είναι ένα Σκουλήκι (Worm);

Είναι ένας ιός που αναπαράγεται δημιουργώντας αντίγραφα του εαυτού του διαμέσου των δικτύων ηλεκτρονικών υπολογιστών. Ένα σκουλήκι μπορεί να βλάψει ένα δίκτυο και μπορεί να μειώσει κατά πολύ την ταχύτητα της σύνδεσής σας στο Διαδίκτυο καταναλώνοντας όλους τους πόρους του υπολογιστή και να οδηγήσει ακόμη και σε κλείσιμο του υπολογιστή.

3

Τι είναι ένας Δούρειος Ίππος (Trojan horse);

Είναι πρόγραμμα που, ενώ φαίνεται πως δουλεύει σωστά και με νόμιμο τρόπο, στην πραγματικότητα μπορεί να προκαλέσει αρκετές βλάβες. Ονομάζεται έτσι, γιατί (όπως και ο Δούρειος Ίππος της Τροίας) μπορεί να μπει στον υπολογιστή σας μέσω διαδικασιών που θεωρούνται ακίνδυνες, όπως για παράδειγμα μέσω ενός παιχνιδιού ή μέσω ενός προγράμματος ανίχνευσης ιών και έτσι να σας ξεγελάσει κρύβοντας την παρασκηνιακή του δραστηριότητα. Γενικά οι δούρειοι ίπποι δεν μπορούν να πολλαπλασιαστούν όπως οι ιοί.

Ένας δούρειος ίππος μπορεί να δράσει και ως κατάσκοπος, δηλαδή να ξεκινήσει να καταγράφει οτιδήποτε πληκτρολογείτε στο πληκτρολόγιό σας. Έτσι θα συλλέξει πληροφορίες κωδικών πρόσβασης, λογαριασμών, πιθανών τραπεζικών συναλλαγών και άλλα προσωπικά σας δεδομένα.

4

Τι είναι οι Hackers;

Hackers είναι τα άτομα, που χωρίς εξουσιοδότηση αποκτούν παράνομη πρόσβαση σε κάποιο σύστημα υπολογιστών και στα δεδομένα του, χωρίς ωστόσο να έχουν πρόθεση να προκαλέσουν ζημιά.

5

Τι είναι οι Crackers;

Crackers ονομάζονται τα άτομα που χωρίς εξουσιοδότηση, αποκτούν παράνομη πρόσβαση σε ένα σύστημα υπολογιστών και στα δεδομένα του, με σκοπό την πρόκληση οικονομικής ή άλλου είδους ζημιάς και την κλοπή πληροφοριών.

6

Τι είναι Spyware;

Είναι ένα πρόγραμμα που μπορεί να προσκολληθεί κρυφά σε αρχεία που κατεβάζετε από το Διαδίκτυο. Μόλις κατέβει, αυτοεγκαθίσταται στον υπολογιστή σας και ξεκινά την παρακολούθηση της διαδικτυακής σας δραστηριότητας. Οι πληροφορίες που καταγράφει αποστέλλονται τότε σε τρίτους, που τις περισσότερες φορές είναι εταιρίες που ενδιαφέρονται να δημιουργήσουν το δικό σας προφίλ και να ξεκινήσουν να σας στέλνουν διαφημιστικό ή άλλο υλικό ανάλογα με τα ενδιαφέροντά σας.

7

Πώς αποτρέπω την είσοδο βλαβερού λογισμικού στον υπολογιστή μου;

Είναι σημαντικό να μην ανοίγετε τα e-mails που λαμβάνετε από άγνωστο αποστολέα. Πολλά από αυτά έχουν τίτλους που προσελκύουν την προσοχή, όπως «Κερδίσατε στην κλήρωση!» ή «Χρόνια Πολλά, Σου έχω ένα δώρο» κ.ο.κ. Μην ανοίγετε ποτέ τα συνημμένα σε τέτοιου είδους e-mails αρχεία, γιατί είναι εξαιρετικά πιθανόν, κάποιο από αυτά να εγκαταστήσει ιό ή σκουλήκι στον υπολογιστή σας.

Εγκαταστήστε λογισμικό antivirus στον υπολογιστή σας. Αυτό θα σας προστατεύσει από ιούς, βλαβερό λογισμικό και άλλου είδους απειλές. Μπορείτε ακόμη να εγκαταστήσετε ένα firewall (τείχος προστασίας), το οποίο θα ελέγχει όλα τα αρχεία που μπαίνουν ή βγαίνουν από τον υπολογιστή σας.

Προσπαθήστε να αποφύγετε ύποπτες ιστοσελίδες και αν μπειτε σε κάποια από αυτές κατά λάθος και σας φαίνεται περίεργη, φύγετε αμέσως. Αν εμφανιστούν παράθυρα που σας ζητούν να συμφωνήσετε σε οτιδήποτε, κλείστε τα αμέσως και ποτέ μην πατάτε κουμπιά που βρίσκονται μέσα σε αυτά.

8

Τι είναι το λογισμικό antivirus;

Πρόκειται για λογισμικό που χρησιμοποιείται για την προστασία του υπολογιστή από τους ιούς, αλλά και από άλλο βλαβερό υλικό. Τα προγράμματα αυτά εγκαθίστανται στον υπολογιστή σας και ελέγχουν όλα τα αρχεία που βρίσκονται σε αυτόν αλλά και τα συνημμένα σε e-mail αρχεία.

Αν εντοπιστούν ιοί, το πρόγραμμα σας ενημερώνει αμέσως και στις περισσότερες περιπτώσεις, απομονώνει ή επιδιορθώνει τα αρχεία που έχουν προσβληθεί από τον ιό. Ένα πρόγραμμα antivirus πρέπει να ενημερώνεται συνεχώς και μπορεί επίσης να χρησιμοποιηθεί για φιλτράρισμα ιστοσελίδων.

9

Τι είναι ο dialer;

Ο dialer είναι ένα πρόγραμμα, το οποίο χωρίς να το γνωρίζετε σταματά τη σύνδεση στο Διαδίκτυο μέσω του παρόχου σας και εκτρέπει τη σύνδεση σε μια διεθνή γραμμή, κάτι που τις περισσότερες φορές έχει ως αποτέλεσμα υπέρογκους λογαριασμούς τηλεφώνου. Αυτό συμβαίνει συνήθως όταν ο χρήστης επισκεφθεί μια ιστοσελίδα με ύποπτο ή πορνογραφικό περιεχόμενο, ή αναξιόπιστες ιστοσελίδες. Ένας dialer μπορεί επίσης να εισέλθει στον υπολογιστή σας μέσω spam.

Για να μην πέσετε θύμα των dialers, αν χρησιμοποιείτε modem για τη σύνδεσή σας, επικοινωνήστε με τον τηλεπικοινωνιακό πάροχό σας και ζητήστε φραγή διεθνών κλήσεων. Ο πάροχός σας θα σας δώσει έναν κωδικό, τον οποίο θα πρέπει να καλείτε πριν από κάθε άλλον διεθνή κωδικό. Με αυτόν τον τρόπο, ο dialer δεν θα μπορεί να εκτρέψει τη σύνδεσή σας στο εξωτερικό, καθώς το τηλεφώνό σας θα φράζει την εξερχόμενη κλήση.

10 Τι είναι ένας ιός (Virus);

Πρόκειται για πρόγραμμα το οποίο είναι έτσι σχεδιασμένο ώστε να «εισβάλλει» στον υπολογιστή σας και να δημιουργεί ανεπιθύμητες παρενέργειες, όπως αδυναμία έναρξης του υπολογιστή σας, μη σωστή λειτουργία των εφαρμογών που χρησιμοποιείτε ή ξαφνική εμφάνιση διάφορων χαρακτήρων και αριθμών στην οθόνη σας. Ένα ιός μπορεί όμως να προκαλέσει και σοβαρές ή ανεπανόρθωτες βλάβες (όπως την καταστροφή των αρχείων σας από τον σκληρό δίσκο).

11 Τι είναι ένα firewall (τείχος προστασίας);

Πρόκειται για μία συσκευή ή ένα λογισμικό που αναλαμβάνει να αποτρέψει ή να σταματήσει μη εξουσιοδοτημένα άτομα να αποκτήσουν πρόσβαση στον υπολογιστή σας.

Το «τείχος προστασίας» firewall ελέγχει όλα τα αρχεία που μπαίνουν ή βγαίνουν από τον υπολογιστή σας. Αν υπάρχει κάποιο ύποπτο αρχείο θα το αναλάβει και ο υπολογιστής σας θα είναι ασφαλής.

12 Ποιες μεθόδους ακολουθούν οι Crackers;

Οι crackers συνήθως βάζουν ιούς και άλλου είδους προγράμματα που περιέχουν ειδικό κώδικα στα συστήματα στόχους, με σκοπό να προκαλέσουν σοβαρή ζημιά. Στις περισσότερες περιπτώσεις αυτοί οι κώδικες είναι:

- Ένας δούρειος ίππος, κρυμμένος σε άλλα προγράμματα που φαινομενικά δεν είναι βλαβερά.
- Ένα σκουλήκι, το οποίο δεν είναι κρυμμένο σε άλλα αρχεία, αλλά αποστέλλεται εκμεταλλευόμενο τα κενά στην ασφάλεια των δικτύων που έχουν εντοπίσει οι crackers.
- Μια «λογική βόμβα», που υποδηλώνει ανενεργό κώδικα τοποθετημένο μέσα σε ένα πρόγραμμα λογισμικού και ο οποίος ενεργοποιείται σε συγκεκριμένη ημερομηνία ή συμβάν.

1

Τι είναι παιδική πορνογραφία;

Η παιδική πορνογραφία ορίζεται διαφορετικά από τη νομοθεσία της κάθε χώρας. Ο κοινός παρανομαστής είναι οι αναπαραστάσεις 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 ή και καρτούν.

Είναι ευρέως γνωστό ότι η παιδική πορνογραφία είναι παράνομη και υπόκειται σε ποινικές κυρώσεις. Επιπλέον υπάρχουν σημαντικές διαφορές στην αντιμετώπιση της παιδικής πορνογραφίας από χώρα σε χώρα. Στην Ελλάδα, ακόμη και η εν γνώση κατοχή παιδικής πορνογραφίας είναι έγκλημα.

Σύμφωνα με τη Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης η παιδική πορνογραφία έχει τις εξής μορφές:

- α.** Ένας ανήλικος που συμμετέχει σε σεξουαλική δραστηριότητα.
- β.** Ένα άτομο που συμμετέχει σε σεξουαλική δραστηριότητα προσποιούμενο ότι είναι ανήλικο.
- γ.** Ρεαλιστικές εικόνες που αναπαριστούν ένα ανήλικο να συμμετέχει σε σεξουαλικές δραστηριότητες.

2

Τι είναι τα κυκλώματα παιδοφιλίας;

Ένα κύκλωμα παιδοφιλίας είναι μια ομάδα ανθρώπων που εργάζονται μαζί μέσω Διαδικτύου σε διαφορετικές χώρες και υπό διαφορετικά νομοθετικά πλαίσια, με σκοπό τη συλλογή και διανομή πορνογραφικού υλικού για τη δική τους ικανοποίηση.

Μπορεί επίσης να γίνεται και ανταλλαγή εμπειριών και γνώσεων ως προς την αποφυγή ανίχνευσης και το σχεδιασμό εγκληματικών ενεργειών εις βάρος παιδιών.

3

Πώς τα κυκλώματα παιδοφιλίας χρησιμοποιούν το Διαδίκτυο;

Υπάρχει μια ισχυρή εντύπωση ότι το Διαδίκτυο έχει γίνει ένας ισχυρός παράγων στην εξέλιξη των παιδοφιλικών κυκλωμάτων παγκοσμίως. Πολλές πρόσφατες καταδίκες στις Ηνωμένες Πολιτείες Αμερικής και στο Ηνωμένο Βασίλειο απέδειξαν ότι το Διαδίκτυο χρησιμοποιείται ευρέως από τα μέλη τέτοιων κυκλωμάτων, τόσο για να την ανταλλαγή εμπειριών όσο και για την διακίνηση φωτογραφιών παιδικής πορνογραφίας.

Η διάδοση της παιδικής πορνογραφίας προκαλεί μεγάλη ανησυχία στους διεθνείς φορείς που ασχολούνται με την προστασία των ανηλίκων. Ανεξάρτητα από τους τρόπους που χρησιμοποιούνται για την διακίνηση φωτογραφιών παιδικής πορνογραφίας στο Διαδίκτυο, το πρόβλημα εξακολουθεί να είναι σοβαρό στη δυτική Ευρώπη, όπου αποκαλύφθηκαν σημαντικά κυκλώματα παιδικής πορνογραφίας στη Δανία, την Ισπανία, τη Γερμανία, την Ιταλία, την Ολλανδία, τη Σουηδία και το Ηνωμένο Βασίλειο.

Καθώς αυτά τα δίκτυα χρησιμοποιούν εξελιγμένες τεχνολογίες τηλεπικοινωνιών, κάνοντας χρήση κρυπτογράφησης και κωδικών ονομασιών, γίνεται συνεχώς δυσκολότερη η ανακάλυψή τους από τις αρχές.



Ασφαλές Internet,
ήσυχοι όλοι!!!

Έργο της μαθήτριας
Δημοτικού:
Δ.Αθανασιάδου

4

Τι σημαίνει ο όρος grooming;

Το grooming είναι η διαδικασία κατά την οποία, παιδόφιλοι, προσποιούμενοι ότι είναι έφηβοι, χρησιμοποιούν τα chat rooms για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν. Τα chat rooms φιλοξενούνται στο Διαδίκτυο και σε αυτά μπορεί να έχει πρόσβαση οποιοσδήποτε από οποιοδήποτε σημείο στον κόσμο. Συχνά θεωρούνται από τα παιδιά ασφαλείς τόποι συνομιλίας στο Διαδίκτυο, τόσο εξαιτίας της δημόσιας φύσης της συζήτησης αλλά και της λανθασμένης εκτίμησης των παιδιών ότι διατηρείται η ανωνυμία τους.

Οι παιδόφιλοι ξεκινούν συζητήσεις με τα πιθανά θύματα με σκοπό να αναπτύξουν φιλική σχέση με αυτά και να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, τα ενδιαφέροντα, τα χόμπι και τις σεξουαλικές τους εμπειρίες.

Μέσα από την σχέση αυτή προκαλούν σιγά σιγά συζητήσεις σεξουαλικής φύσεως και πολλές φορές οι παιδόφιλοι στέλνουν στα υποψήφια θύματα φωτογραφίες παιδικής πορνογραφίας αλλά και πορνογραφίας ενηλίκων για να δώσουν την αίσθηση ότι αυτό είναι κάτι το αποδεκτό και φυσιολογικό. Η τακτική αυτή χρησιμοποιείται για να υπονομεύσει την απροθυμία των παιδιών στο να λάβουν μέρος σε σεξουαλική επαφή. Χρησιμοποιείται επίσης για να αποτρέψει το θύμα από το να ζητήσει προστασία από τους γονείς και τους δασκάλους του, αφού καταλήγει να νιώθει ένοχο που έχει ανταλλάξει τέτοιου είδους φωτογραφίες.

5

Πού μπορώ να καταγγείλω ύποπτες σελίδες;

Εάν πιστεύετε ότι βρήκατε μια ιστοσελίδα στην οποία υπάρχει παράνομο υλικό, τότε σας προτρέπουμε να έρθετε σε επαφή με την Ελληνική Ανοιχτή Γραμμή SafeLine (www.safeline.gr).

Η SafeLine δέχεται καταγγελίες για ιστοχώρους (websites) ή υπηρεσίες νέων (newsgroups) που περιέχουν:

- Εικόνες κακομεταχείρισης των παιδιών, οπουδήποτε στον κόσμο.
- Ρατσιστικό και ξενοφοβικό περιεχόμενο που, κατά την άποψή σας, παραβαίνει την Ελληνική νομοθεσία.
- Άλλο περιεχόμενο, παράνομο, κατά την άποψή σας.

Τηλέφωνο Καταγγελιών:

2811 391615 καθημερινά από 9:00 π.μ. έως 16:00 μ.μ.

Ηλεκτρονικές Καταγγελίες:

μέσω της ιστοσελίδας www.safeline.gr ή στο report@safeline.gr.

Η SafeLine συνεργάζεται με τους Φορείς Παροχής Υπηρεσιών Διαδικτύου (ISP), το Ακαδημαϊκό Δίκτυο ΕΔΕΤ και το Σχολικό Δίκτυο, Ερευνητικά και Πολιτιστικά Ιδρύματα, Ενώσεις Καταναλωτών και την Ελληνική Αστυνομία για τον περιορισμό της ροής του παράνομου περιεχομένου στο Διαδίκτυο.

Η SafeLine είναι σε στενή επαφή με όλες τις Ευρωπαϊκές ανοιχτές γραμμές επικοινωνίας, ως μέλος της Ευρωπαϊκής Ένωσης των hotlines INHOPE.

1

Τι σημαίνει ο όρος gaming;

Gaming είναι ένας συγκεντρωτικός όρος για τη «δραστηριότητα του να παίζει κανείς ηλεκτρονικά παιχνίδια». Χρησιμοποιείται κυρίως για να υποδείξει ένα ενδιαφέρον πάνω από το μέσο όρο.

2

Τι σημαίνει ο όρος gambling;

Ο όρος gambling υποδεικνύει μια δραστηριότητα αρκετών χιλιάδων ετών, τον γνωστό σε όλους τζόγο. Κάποιος στοιχηματίζει χρήματα στο αποτέλεσμα κάποιου συμβάντος, το οποίο μπορεί να ελέγχεται από αυτόν που στοιχηματίζει ή να εξαρτάται από εξωγενείς παράγοντες.

3

Τι είναι online gaming;

Σε μερικά ηλεκτρονικά παιχνίδια μπορούν να παίξουν παραπάνω από ένας παίχτες που μοιράζονται την ίδια περιοχή του παιχνιδιού (τα λεγόμενα multiplayer παιχνίδια). Οι παίχτες μπορούν είτε να δημιουργήσουν ομάδες που παίζουν μεταξύ τους είτε απλά να βλέπουν ποιος μεμονωμένος παίχτης είναι ο καλύτερος. Μπορεί κανείς να παίξει multiplayer παιχνίδια μέσω υπολογιστών συνδεδεμένων σε τοπικό δίκτυο ή μέσω Διαδικτύου. Δημοφιλής κατηγορία παιχνιδιών online είναι τα παιχνίδια δράσης, τα παιχνίδια ρόλων και τα παιχνίδια στρατηγικής.

Για παράδειγμα παίζονται στοιχήματα, για το ποιος θα κερδίσει σε έναν αγώνα ποδοσφαίρου, μια κούρσα ιπποδρομίας ή για το ποιος θα κερδίσει σε μια παρτίδα τάβλι. Αν αφαιρεθεί το οικονομικό ενδιαφέρον, η δραστηριότητα μετατρέπεται σε απλό παιχνίδι.

4

Τι είναι online gambling;

Ο συστηματικός τζόγος περιλαμβάνει τη συνάντηση δύο ή περισσότερων ατόμων με σκοπό την ανταλλαγή στοιχημάτων ή/και την ίδια την δραστηριότητα για την οποία γίνονται τα στοιχήματα, αν αυτό είναι δυνατό. Αυτό γίνεται είτε με φυσική παρουσία είτε με μεσάζοντες όπως τα παραδοσιακά γραφεία στοιχημάτων. Το Διαδίκτυο έχει κάνει τη συνάντηση αυτών των τζογαδόρων πολύ πιο εύκολη, είτε πρόκειται για απλό στοίχημα είτε για πόκερ, τάβλι, και σκάκι. Δεν είναι απαραίτητο να συναντήσει κανείς τους υπόλοιπους παίκτες. Για παράδειγμα, στο πόκερ οι παίκτες παίζουν σε πραγματικό χρόνο σε ένα κοινό ηλεκτρονικό περιβάλλον το οποίο ο κάθε παίκτης βλέπει στην οθόνη του.

5

Ποιες είναι οι διαφορές ανάμεσα στα παιχνίδια και τον τζόγο;

Τα παιχνίδια και ο τζόγος είναι δύο εντελώς διαφορετικοί όροι. Ενώ το παιχνίδι έχει μια μη πραγματική προσέγγιση με μόνο φανταστικούς δεσμούς με τον φυσικό κόσμο, ο τζόγος περιλαμβάνει το ρίσκο της πραγματικής οικονομικής απώλειας ή του κέρδους.

Ψυχολογικά, αυτό οδηγεί σε δυο πολύ διαφορετικούς τρόπους παιχνιδιού: Αν κάποιος χάσει ένα γύρο στο αγαπημένο του παιχνίδι, μπορεί πάντα να θεωρήσει ότι είχε «απλά μια κακή ημέρα» και να επιστρέψει για ρεβάνς την επομένη, ενώ ο φόβος του να χάσει κανείς τα χρήματά του εξαιτίας μιας λανθασμένης κρίσης σε ένα γύρο πόκερ ξυπνά ένα εντελώς διαφορετικό είδος συναισθημάτων.

6

Υπάρχουν προβλήματα με τα online παιχνίδια;

- Πρόσφατα έχουν γίνει πολλές έρευνες για να βρεθούν τυχόν δεσμοί μεταξύ των ηλεκτρονικών παιχνιδιών και της βίαιης συμπεριφοράς. Δεν έχει εδραιωθεί ακόμα επιστημονικά η ύπαρξη μιας τέτοιας σχέσης, ούτε αναμένεται ότι κάτι τέτοιο θα γίνει ποτέ, παρά τις αναφορές που κάνουν λόγο για το αντίθετο. Άλλοι κοινωνικοί παράγοντες έχουν πολύ μεγαλύτερη επιρροή στις πράξεις του ατόμου.
- Τα παιχνίδια προκαλούν την έκκριση αδρεναλίνης και αυτό το αυξημένο επίπεδο ορμονών μπορεί να δημιουργήσει μια βραχυχρόνια αλλαγή συμπεριφοράς, που υπολογίζεται στη μία ώρα. Είναι επομένως σημαντικό να δίνουμε λίγο χρόνο στον εαυτό μας για να ηρεμήσουμε μετά από ένα παιχνίδι.
- Υπάρχουν ενδείξεις ότι ο εθισμός στα online παιχνίδια μπορεί να αποτελέσει πρόβλημα για ορισμένους. Η έρευνα ωστόσο έχει αποδείξει ότι αυτό σπάνια έχει να κάνει με το ίδιο το παιχνίδι αλλά με το online κοινωνικό δίκτυο που υπάρχει στο παιχνίδι. Για αυτούς που δεν είναι ικανοί να διαμορφώσουν τακτικούς κοινωνικούς δεσμούς στην δική τους πραγματική κοινότητα, αυτές οι διαδικτυακές κοινότητες μπορούν να δώσουν ώθηση στην αυτοπεποίθησή τους και να τους επιτρέψουν κατ' επέκταση να δημιουργήσουν σχέσεις με τους γύρω τους. Από την άλλη, υπάρχει ο πραγματικός κίνδυνος της υπερβολικής ενασχόλησης των παικτών με ένα παιχνίδι, για ώρες καθημερινά, με αποτέλεσμα το υπόλοιπο της ζωής τους να επηρεάζεται σοβαρά.
- Όπως συμβαίνει με όλα τα μέσα προσφοράς περιεχομένου, κάποιος μπορεί να θεωρήσει το περιεχόμενο και τις απεικονίσεις ενός παιχνιδιού προβληματικές ή ακόμα και προσβλητικές. Επίσης, πρέπει να σημειωθεί ότι εφόσον όλα τα online παιχνίδια περιλαμβάνουν κάποια μορφή επικοινωνίας μεταξύ των παιχτών, μερικοί (αν όχι όλοι) από τους κινδύνους που αφορούν τα συμβατικά ανοιχτά δωμάτια επικοινωνίας, γνωστά ως chat rooms, ισχύουν και στα παιχνίδια. Μεγάλης σημασίας είναι και τα θέματα που αφορούν τη λεκτική βία και την προστασία της ιδιωτικής ζωής.

7

Ποια είναι τα προβλήματα με τον online τζόγο;

Το βασικό πρόβλημα με τον τζόγο στο Διαδίκτυο είναι ο κίνδυνος χρηματικής απώλειας. Είναι εξαιρετικά πιθανό να χάσει κανείς με αυτό τον τρόπο τις οικονομίες του, το σπίτι του, ακόμα και την περιουσία του. Αυτό συνδέεται ως ένα βαθμό με τον εθισμό στον τζόγο, μια κατάσταση στην οποία δεν μπορεί κανείς να σταματήσει να στοιχηματίζει με την ελπίδα ότι με ένα ακόμα γύρο θα πάρει πίσω τα χαμένα.

Σε αντίθεση με τα παιχνίδια όπου ο σκοπός είναι η διασκέδαση, στον τζόγο όλα έχουν να κάνουν με το χρήμα. Ο εθισμός στον τζόγο είναι ένα γνωστό ψυχολογικό φαινόμενο για το οποίο υπάρχουν θεραπευτικά προγράμματα σε πολλές χώρες.

Επιπλέον, όσοι ασχολούνται με τον ηλεκτρονικό τζόγο, διατρέχουν κινδύνους δίνοντας τα στοιχεία των πιστωτικών τους καρτών, πέραν των θεμάτων υγείας που συνδέονται με την πολύωρη παραμονή μπροστά στον ηλεκτρονικό υπολογιστή.

8

Τι είναι ο χαρακτηρισμός παιχνιδιών PEGI;

Το σύστημα του Πανευρωπαϊκού οργανισμού «PEGI - Pan European Game Information» έχει σχεδιαστεί για να παρέχει βοήθεια στους αγοραστές των βιντεοπαιχνιδιών (ειδικά τους γονείς) σχετικά με το εάν ένα παιχνίδι είναι κατάλληλο για ένα παιδί ή ένα νεότερο έφηβο. Το σύστημα αποτελείται από δύο μέρη: την κατάταξη του παιχνιδιού σε ηλικιακές ομάδες (3+, 7+, 12+, 16+, 18+) και τον χαρακτηρισμό του περιεχόμενου (βία, τζόγος, φόβος, σεξ, ναρκωτικά, ρατσισμός, χυδαία γλώσσα). Για περισσότερες πληροφορίες συμβουλευτείτε την ιστοσελίδα <http://www.pegi.info/gr/>

1 Τι είναι παρενόχληση;

Παρενόχληση (bullying) είναι η επιθετική συμπεριφορά από πρόθεση, που επαναλαμβάνεται με τον καιρό, και περιλαμβάνει μια ανισορροπία δύναμης και εξουσίας. Τα παιδιά που γίνονται αντικείμενο παρενόχλησης αντιμετωπίζουν δυσκολίες στο να υπερασπιστούν τον εαυτό τους.

Παρενόχληση είναι όταν κάποιος συνεχίζει να κάνει ή να λέει πράγματα για να έχει δύναμη πάνω σε κάποιο άλλο άτομο. Μερικοί τρόποι να φοβηρίσει κανείς τους άλλους είναι με το να τους βρίζει, να λέει ή να γράφει δυσάρεστα πράγματα για αυτούς, να τους αφήνει έξω από δραστηριότητες, να μην τους μιλάει, να τους απειλεί, να τους κάνει να νιώθουν άβολα ή φοβισμένοι, να παίρνει ή να καταστρέφει τα πράγματά τους, να τους χτυπά ή να τους κλωτσά ή να τους ωθεί να κάνουν πράγματα παρά τη θέλησή τους.

2 Πώς εκδηλώνεται;

Περιστατικά παρενόχλησης μεταξύ παιδιών και εφήβων μπορούν να συμβούν με πολύ διαφορετικές μορφές. Δεν εκδηλώνονται μόνο μέσω καυγάδων και επιθετικότητας, αλλά και μέσω διαφορετικών τύπων εκφοβισμού που αφήνουν το θύμα εκτεθειμένο. Αυτοί μπορεί να είναι:

- Λεκτικοί εκφοβισμοί (προσβολές, βρισιές, διάδοση φημών...).
- Ψυχολογικοί εκφοβισμοί (απειλές με σκοπό την πρόκληση φόβου στο θύμα, την απόσπαση χρημάτων και άλλων αντικειμένων ή απλά τον εξαναγκασμό του θύματος να κάνει πράγματα που δεν επιθυμεί).
- Σωματική επιθετικότητα (καυγάδες και ξύλο), καταστροφή προσωπικών αντικειμένων και μικροκλοπές.
- Κοινωνική απομόνωση, είτε με την αποτροπή της συμμετοχής του ατόμου σε ορισμένες δραστηριότητες είτε με αγνόηση της παρουσίας του.

3

Η παρενόχληση είναι μέρος της ανάπτυξης;

Μερικοί άνθρωποι θέλουν να πιστεύουν ότι η παρενόχληση είναι απλά μέρος της ανάπτυξης και ότι είναι ένας τρόπος να μάθουν τα παιδιά και οι νέοι να υπερασπίζονται τον εαυτό τους. Ωστόσο, η παρενόχληση μπορεί να κάνει τα νέα άτομα να νιώθουν μοναχικά, δυστυχή και φοβισμένα, να αισθάνονται ανασφαλή και να πιστεύουν ότι κάτι δεν πάει καλά με αυτά. Χάνεται η εμπιστοσύνη στον εαυτό τους και μπορεί να μην θέλουν να ξαναπάνε στο σχολείο. Αυτό μπορεί να οδηγήσει σε εκπαιδευτική αποτυχία, ανάμεσα σε άλλα προβλήματα. Επιπλέον, συνεχής, επίμονη και έντονη παρενόχληση έχει οδηγήσει σε τρομερές συνέπειες όπως η αυτοκτονία παιδιών σε πολλές Ευρωπαϊκές χώρες.

4

Τι είναι η ρατσιστική παρενόχληση;

Ρατσιστική παρενόχληση προκύπτει όταν άτομα παρενοχλούνται εξαιτίας της φυλής τους, της κουλτούρας ή της θρησκευτικής τους πίστης. Τα θύματα αυτού του τύπου παρενόχλησης είναι πολιτισμικές, φυλετικές ή θρησκευτικές μειονότητες. Σε αυτές τις περιπτώσεις οι ρατσιστικές βρισιές και η χρήση στερεοτυπικών εκφράσεων είναι πολύ διαδεδομένη.



Προσβλέποντας
σ' ένα
ασφαλέστερο
Διαδίκτυο

Έργο των
μαθητριών
Λυκείου:
Μ.Σταυροπούλου,
Α.Σίσκογλου,
Κ.Παπαδέα,
Σ.Χατζηθεοδωρίδη,
Κ.Σταφυλάτου,
Α.Πανοπούλου,
Α.Βέρδη

5

Τι είναι η παρενόχληση στον κυβερνοχώρο;

Η παρενόχληση στον κυβερνοχώρο προκύπτει όταν παιδιά ή έφηβοι παρενοχλούνται μεταξύ τους μέσω του Διαδικτύου ή μέσω κινητών τηλεφώνων και άλλων ηλεκτρονικών τεχνολογιών. Πρόκειται δε για μια εξελισσόμενη μέθοδο. Οι συμπεριφορές που μπορεί να προκύψουν περιλαμβάνουν:

- Αποστολή κειμένων, e-mail, ή άμεσων μηνυμάτων με κακό περιεχόμενο.
- Η δημοσίευση δυσάρεστων φωτογραφιών ή μηνυμάτων για άλλους σε ιστολόγια (blogs) ή άλλες ιστοσελίδες.
- Χρήση του ονόματος ξένου χρήστη με σκοπό τη διάδοση φημών και ψευμάτων για κάποιον τρίτο (κλοπή ταυτότητας).
- Νεκρές κλήσεις.
- Προσβλητικά προφορικά μηνύματα.

Μερικές φορές προσβλητικά γραπτά μηνύματα προς κινητά τηλέφωνα στέλνονται μέσω ιστοσελίδων χρησιμοποιώντας ονόματα και τηλέφωνα ανθρώπων που δεν έχουν καμία σχέση με το μήνυμα αυτό, αλλά καταλήγουν να κατηγορούνται ότι το έστειλαν οι ίδιοι.

Μια άλλη τεχνική που χρησιμοποιείται από όσους παρενοχλούν ηλεκτρονικά είναι η δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας άλλους να δημοσιεύσουν μηνύματα μίσους.

6

Πού μπορούν να ζητήσουν βοήθεια οι γονείς και τα παιδιά;

Το δίκτυο γραμμών βοήθειας INHOPE, επικεντρώνεται στον εντοπισμό παράνομου περιεχομένου στο Διαδίκτυο. Σε πολλές χώρες το ρατσιστικό και ξενοφοβικό υλικό θεωρείται παράνομο και κατά συνέπεια καταγγέλλεται σε αυτές τις γραμμές. Επιπλέον, το δίκτυο INHOPE έχει θεμελιώσει νόμιμες και επίσημες διαδικασίες για την καταγγελία των εν λόγω περιστατικών στους αρμόδιους κυβερνητικούς φορείς.

Στην Ελλάδα η ανοιχτή γραμμή επικοινωνίας για καταγγελίες τέτοιων προβλημάτων είναι η Safeline (www.safeline.gr).

Η SafeLine δέχεται καταγγελίες για ιστοχώρους (websites) ή υπηρεσίες νέων (newsgroups) που περιέχουν:

- Εικόνες κακομεταχείρισης των παιδιών, οπουδήποτε στον κόσμο.
- Ρατσιστικό και ξενοφοβικό περιεχόμενο που, κατά την άποψή σας, παραβαίνει την Ελληνική νομοθεσία.
- Άλλο περιεχόμενο, παράνομο, κατά την άποψή σας.

Τηλέφωνο Καταγγελιών:

2811 391615 καθημερινά από 9:00 π.μ. έως 16:00 μ.μ.

Ηλεκτρονικές Καταγγελίες:

μέσω της ιστοσελίδας www.safeline.gr ή στο report@safeline.gr.

Επίσης, υπάρχει και το Διεθνές Δίκτυο κατά του Διαδικτυακού Μίσους (INCHACH) που επίσης δέχεται καταγγελίες μέσω e-mail στο complaints@inach.net ή μέσω της ιστοσελίδας <http://www.inach.net>.

1

Ποιοι είναι οι νομικοί λόγοι που υπαγορεύουν την εξάλειψη του ρατσισμού στην Ευρώπη;

Σύμφωνα με το άρθρο 14 της Ευρωπαϊκής Σύμβασης για την Προάσπιση των Ανθρωπίνων Δικαιωμάτων και των Θεμελιωδών Ελευθεριών του Ανθρώπου, η απόλαυση των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών που αναφέρονται στη σύμβαση δεν μπορεί να είναι αντικείμενο καμίας διάκρισης σε κανένα τομέα, όπως φύλο, φυλή, χρώμα, γλώσσα, θρησκεία, κ.λπ.

Άρθρο 14 . Απαγόρευση των διακρίσεων

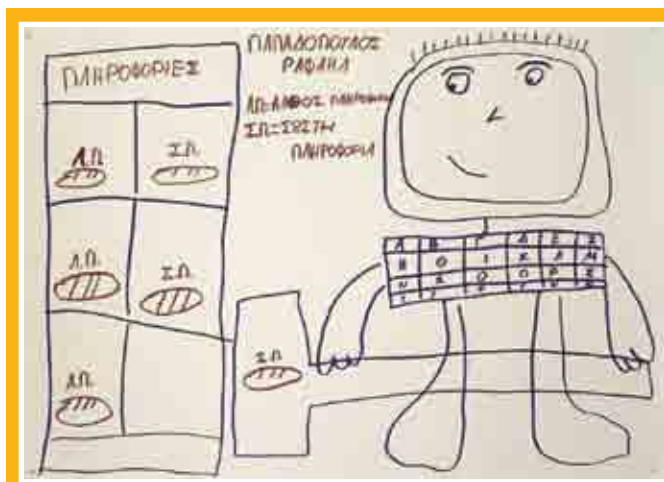
«Η χρήσις των αναγνωριζομένων εν τη παρούση Συμβάσει δικαιωμάτων και ελευθεριών δέον να εξασφαλισθή ασχέτως διακρίσεως φύλου, φυλής, χρώματος, γλώσσης, θρησκείας, πολιτικών ή άλλων πεποιθήσεων, εθνικής ή κοινωνικής προελεύσεως, συμμετοχής εις εθνικήν μειονότητα, περιουσίας, γεννήσεως ή άλλης καταστάσεως.»

Σύμβαση για το Έγκλημα στον Κυβερνοχώρο του Συμβουλίου της Ευρώπης - Πρόσθετο Πρωτόκολλο

Το πρόσθετο Πρωτόκολλο στη Σύμβαση για το Έγκλημα στον Κυβερνοχώρο αφορά στην ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσεως, οι οποίες έχουν διαπραχθεί μέσω ηλεκτρονικών υπολογιστών. Ομιλία μίσους ορίζεται το: «ρατσιστικό και ξενοφοβικό υλικό». Ρατσιστικό και ξενοφοβικό υλικό προσδιορίζεται κάθε είδους γραπτό κείμενο, εικόνα ή άλλη αναπαράσταση ιδεών και θεωριών που συνηγορεί, προωθεί ή προκαλεί έχθρα, διακρίσεις ή βία εις βάρος κάποιου ατόμου ή ομάδας ατόμων, χρησιμοποιώντας ως πρόφαση για οποιαδήποτε από τις παραπάνω πράξεις τη φυλή, το χρώμα, την καταγωγή, την εθνική προέλευση και την θρησκεία.

Οδηγία του Ευρωπαϊκού Συμβουλίου της 29ης Ιουνίου 2000

Εκτός από τον σκοπό να εφαρμοστεί η αρχή της ίσης μεταχείρισης στην Ευρωπαϊκή Ένωση ανεξάρτητα από την φυλετική και εθνική προέλευση του ατόμου, υιοθετήθηκε και η οδηγία του Ευρωπαϊκού Συμβουλίου της 29ης Ιουνίου 2000. Η οδηγία καταπολεμά τις διακρίσεις που βασίζονται στην φυλετική και εθνική καταγωγή. Συμπληρώνει και ενισχύει τις ολοκληρωμένες εθνικές νομοθεσίες δίνοντας κοινό ορισμό των παράνομων διακρίσεων. Αυτή η οδηγία απαγορεύει όλες τις διακρίσεις για λόγους φυλής και εθνικότητας. Τέτοιου είδους διακρίσεις μπορούν να εκφραστούν με αρνητική συμπεριφορά προς το πρόσωπο στο οποίο απευθύνονται ή με οποιαδήποτε άλλη διάθεση, κριτήρια ή πρακτικές που μπορεί να είναι ουδέτερες αρχικά αλλά μπορεί να οδηγήσουν σε ανεπιθύμητες συνέπειες για ένα αποφασισμένο άτομο ή ομάδα ανθρώπων. Έτσι τα κράτη μέλη υποχρεώνονται να εγγυηθούν ισότητα στην πρόσβαση στην εργασία, την κατάρτιση, την εκπαίδευση, τις συνθήκες εργασίας, τη συμμετοχή σε επαγγελματικές οργανώσεις, την προστασία και την κοινωνική ασφάλεια, την πρόσβαση σε αγαθά και υπηρεσίες και την παροχή τους.



Σωστή και Λάθος
Πληροφορία

Έργο του μαθητή
Δημοτικού:
Ρ. Παπαδόπουλου

2

Ποια είναι η επίδραση του ρατσιστικού και ξενοφοβικού περιεχομένου;

Η χρήση του Διαδικτύου με σκοπό τη διάδοση ρατσιστικής, αντισημιτικής και άλλου είδους προπαγάνδας αυξάνεται σε όλο τον κόσμο. Οι στόχοι του μίσους μπορεί να ποικίλουν από τόπο σε τόπο, αλλά καμία χώρα δεν έχει ανοσία στο πρόβλημα και συχνά τα πράγματα γίνονται πιο περίπλοκα αφού η διαχείριση ορισμένων ιστοσελίδων γίνεται από πολλές χώρες.

Υπάρχει η συνεχώς αυξανόμενη ανησυχία ότι το διαδικτυακό μίσος μπορεί να προκαλέσει βία και να οδηγήσει σε κανονικά εγκλήματα μίσους. Ακόμα και αν είναι δύσκολο να εδραιωθεί ένας αιτιολογικός δεσμός, δεν υπάρχει αμφιβολία ότι το Διαδίκτυο μπορεί να χρησιμοποιηθεί ώστε να ενισχύσει το εχθρικό κλίμα εναντίον συγκεκριμένων ομάδων, όπως άλλωστε και για τη συγκέντρωση χρημάτων και την προσέλκυση συμπαθούντων.

Η διάσωση του
υπολογιστή

Έργο της
μαθήτριας
Δημοτικού:
Σ.Λαζοπούλου



3

Πού να καταγγείλω τέτοιου είδους περιεχόμενο;

Το δίκτυο γραμμών βοήθειας INHOPE, επικεντρώνεται στον εντοπισμό παράνομου περιεχομένου στο Διαδίκτυο. Σε πολλές χώρες ρατσιστικό και ξενοφοβικό υλικό θεωρείται παράνομο και κατά συνέπεια καταγγέλλεται σε αυτές τις γραμμές. Επιπλέον, το δίκτυο INHOPE έχει θεμελιώσει νόμιμες και επίσημες διαδικασίες για την καταγγελία των εν λόγω περιστατικών στους αρμόδιους κυβερνητικούς φορείς.

Στην Ελλάδα η ανοιχτή γραμμή επικοινωνίας για καταγγελίες τέτοιων προβλημάτων είναι η Safeline. Ακόμη, υπάρχει και το Διεθνές Δίκτυο Κατά του Διαδικτυακού Μίσους (INCHACH) που επίσης δέχεται καταγγελίες μέσω e-mail στο complaints@inach.net ή μέσω του website <http://www.inach.net>.

Η Safeline δέχεται καταγγελίες για ιστοχώρους (websites) ή υπηρεσίες νέων (newsgroups) που περιέχουν:

1. Εικόνες κακομεταχείρισης των παιδιών, οπουδήποτε στον κόσμο.
2. Ρατσιστικό και ξενοφοβικό περιεχόμενο που, κατά την άποψή σας, παραβαίνει την Ελληνική νομοθεσία.
3. Άλλο περιεχόμενο, παράνομο, κατά την άποψή σας.

Σε περίπτωση που πιστεύετε ότι έχετε βρει μια τέτοια ιστοσελίδα, μπορείτε να επικοινωνείτε με την Safeline με τους παρακάτω τρόπους:

Τηλέφωνο Καταγγελιών:

2811 391615 καθημερινά από 9:00 π.μ. έως 16:00 μ.μ.

Ηλεκτρονικές Καταγγελίες:

μέσω της ιστοσελίδας www.safeline.gr ή στο report@safeline.gr.

1 Τι είναι το φίλτρο;

Τα συστήματα φιλτραρίσματος ή απλά φίλτρα ρυθμίζουν την πρόσβαση σε πληροφορίες ή υπηρεσίες στο Διαδίκτυο σύμφωνα με καθορισμένα κριτήρια. Μπορούν να εγκατασταθούν στον υπολογιστή του χρήστη, σε ένα κεντρικό υπολογιστή που ανήκει σε κάποιο φορέα (π.χ. proxy server σε ένα σχολείο) ή τους υπολογιστές ενός παρόχου υπηρεσιών Διαδικτύου και μπορούν να αντιδράσουν ποικιλοτρόπως: μπορούν να προειδοποιήσουν για προβληματικές ιστοσελίδες, να καταγράψουν λεπτομερώς τις κινήσεις ενός χρήστη στο Διαδίκτυο, να μπλοκάρουν ύποπτους ιστοχώρους, ακόμα και να κλείσουν τελείως τον υπολογιστή.

2 Ποιος είναι ο βασικός στόχος ενός φίλτρου;

Ο βασικός στόχος των φίλτρων για την προστασία των ανηλίκων είναι η παροχή ενός αξιόπιστου φράγματος που αποτρέπει την πρόσβαση σε μη αποδεκτό περιεχόμενο, σε περιεχόμενο που θεωρείται επικίνδυνο ή σε περιεχόμενο που μπορεί να προκαλέσει ηθικές βλάβες στην ανάπτυξη των παιδιών. Ταυτόχρονα, το κατάλληλο για παιδιά και για νέους περιεχόμενο δεν θα πρέπει να μπλοκάρεται.

Σε ότι αφορά τον γονικό έλεγχο, τα φίλτρα ασχολούνται και με τα δεδομένα που εξέρχονται από τον υπολογιστή, π.χ. για την αποφυγή δημοσίευσης προσωπικών στοιχείων από τα παιδιά, όπως ονόματα, διευθύνσεις σπιτιού ή σχολείου, στοιχεία πιστωτικών καρτών, κ.λπ. Αυτός ο τύπος φιλτραρίσματος είναι πολύ σημαντικός για την προστασία των νεαρών χρηστών και υπάρχουν λογισμικά προγράμματα που διατίθενται δωρεάν στο Διαδίκτυο για τον συγκεκριμένο σκοπό.

3

Το φιλτράρισμα του περιεχομένου αρκεί;

Τα φίλτρα μπορούν να αποδειχτούν πολύτιμα εργαλεία στην προστασία των ανηλίκων από επιβλαβές περιεχόμενο. Όμως, πρέπει να κατανοήσουμε ότι μπορούν να δράσουν μόνο συμπληρωματικά και πιθανώς μόνο σε μικρότερες ηλικίες. Η εκπαιδευτική επίβλεψη στο σπίτι, σε αντιστοιχία με αυτή που γίνεται στα σχολεία, μαζί με την επικοινωνία μέσα στην οικογένεια και την γνώση των κινδύνων, είναι προτιμότερη από τα τεχνολογικά φράγματα, καθώς συμβάλλει στη σωστή εκπαίδευση των ανηλίκων, στην κατανόηση των προβλημάτων και στην ανάπτυξη κριτικής σκέψης για την αντιμετώπιση αυτών.



*Σώστε το Internet
ΟΧΙ στα
ακατάλληλα sites*

Έργο του μαθητή
Δημοτικού:
Ρ.Χαντάκη

4

Τι είδους φίλτρα διατίθενται;

Περιφραγμένες τοποθεσίες

Οι λεγόμενες «περιφραγμένες τοποθεσίες» (walled gardens) ή «λευκές λίστες» (white lists) είναι λίστες απο ιστοσελίδες που είναι κατάλληλες για ανηλίκους και επιτρέπουν στον χρήστη να έχει πρόσβαση αποκλειστικά σε αυτές.

Λίστες «Όχι»

Συντάσσεται μία λίστα «Όχι» από ιστοσελίδες που πρέπει να αποφευχθούν (π.χ. με προσβλητικό, βίαιο ή ρατσιστικό περιεχόμενο) και αν το παιδί σας προσπαθήσει να μπει σε κάποια από αυτές, τότε μπλοκάρεται η πρόσβασή του/της. Ορισμένα προγράμματα λειτουργούν και με λίστες απαγορευμένων λέξεων. Μόλις βρεθεί κάποια από αυτές τις λέξεις σε κάποια ηλεκτρονική διεύθυνση ή στην ίδια την ιστοσελίδα, τότε μπλοκάρεται η πρόσβαση. Το πρόβλημα με τις λίστες τύπου «Όχι» είναι ότι πρέπει να αναβαθμίζονται συνεχώς.

Μπλοκάρισμα ιστοσελίδων με απαγορευμένες λέξεις

Τα πιο απλά φίλτρα της αγοράς μπλοκάρουν περιεχόμενο στο Διαδίκτυο, χρησιμοποιώντας λίστα με απαγορευμένες λέξεις. Αυτές οι λέξεις – κλειδιά δημιουργούνται και μπορούν να ανανεώνονται εύκολα και γρήγορα.

Φιλτράρισμα βάσει αυτόματης ταξινόμησης του περιεχομένου

Τα συστήματα αυτόματης ταξινόμησης αξιολογούν ολόκληρο το κείμενο που υπάρχει σε μια ιστοσελίδα. Χρησιμοποιούν για αυτό γνώστες στατιστικές μεθόδους, όπως αυτές που εφαρμόζουν τα φίλτρα ανεπιθύμητης αλληλογραφίας.

Αυτοαξιολόγηση ιστοσελίδων

Οι πάροχοι της διαδικτυακής πληροφορίας τοποθετούν εθελοντικά στον αντίστοιχο ιστοχώρο μια ετικέτα, η οποία δείχνει αν και σε ποιο βαθμό η ιστοσελίδα αυτή περιέχει συγκεκριμένο υλικό (π.χ. βία, γυμνό, τυχερά παιχνίδια, περιεχόμενο για ενήλικους, κ.λπ.). Οι ετικέτες και οι κατηγορίες έχουν δημιουργηθεί από την Ένωση Αξιολόγησης Περιεχομένου του Διαδικτύου ICRA. Το φίλτρο διαβάζει αυτές τις ετικέτες και αποφασίζει αν θα επιτρέψει την πρόσβαση, σύμφωνα με αυτά που οι γονείς επέλεξαν να επιτρέψουν στα παιδιά τους να δουν. Το πρόβλημα με αυτό το σύστημα είναι ότι εξαρτάται από το αν οι ιδιοκτήτες των ιστοσελίδων θα αξιολογήσουν εθελοντικά τις ιστοσελίδες τους, και μέχρι στιγμής, δεν είναι πολλοί αυτοί που το κάνουν.

Συνδυασμός μεθόδων φιλτραρίσματος

Οι βασικές προσεγγίσεις στο φιλτράρισμα συνδυάζονται σήμερα με πολλούς τρόπους με σκοπό να αυξηθεί η αποτελεσματικότητα, αλλά και για να διαφοροποιείται η προσβασιμότητα ανάλογα με την ηλικία.

[illegible]

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

- <http://www.saferinternet.gr>
**Δράση Ενημέρωσης & Επαγρύπνησης
Ελληνικού Κέντρου Ασφαλούς Διαδικτύου**
- <http://www.help-line.gr>
**Γραμμή Βοηθείας Ελληνικού Κέντρου
Ασφαλούς Διαδικτύου**
- <http://www.safeline.gr>
**Ανοικτή Γραμμή Καταγγελιών παράνομου περιεχομένου
στο Διαδίκτυο - Ελληνικό Κέντρο Ασφαλούς Διαδικτύου**
- <http://www.saferinternet.org>
**Πανευρωπαϊκό Δίκτυο Εθνικών Κέντρων
Ενημέρωσης & Επαγρύπνησης Insafe**
- <http://internet-safety.sch.gr>
**Ενημερωτικός κόμβος «Ασφάλεια στο Διαδίκτυο»
του Πανελλήνιου Σχολικού Δικτύου**
- <http://www.sch.gr>
Πανελλήνιο Σχολικό Δίκτυο
- <http://www.pegi.info/gr/>
Πανευρωπαϊκό Σύστημα Πληροφόρησης για τα Ηλεκτρονικά Παιχνίδια (PEGI)
- <http://www.e-yliko.gr>
**Δικτυακή Εκπαιδευτική Πύλη του Υπουργείου Παιδείας
και Θρησκευμάτων**
- <http://www.dpa.gr>
Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- <http://www.opi.gr>
Οργανισμός Πνευματικής Ιδιοκτησίας
- <http://ec.europa.eu/saferinternet>
Πρόγραμμα Safer Internet της Ευρωπαϊκής Επιτροπής

s@ferinternet.gr



Ελληνικό Κέντρο Ασφαλούς Διαδικτύου

Δράση Ενημέρωσης Saferinternet.gr

Τηλ. / Fax: 210 62 12 365
Email: info@saferinternet.gr
URL: www.saferinternet.gr

Γραμμή Βοηθείας



210 6007686

Εάν το Διαδίκτυο
δυσκολεύει τη ζωή του παιδιού σας
ζητήστε βοήθεια



Καταγγείλετε
παράνομο περιεχόμενο
στο Διαδίκτυο

Ελληνικό Κέντρο Ασφαλούς Διαδικτύου
Δράση Ενημέρωσης

s@ferinternet.gr
για ένα ασφαλέστερο διαδίκτυο



ISBN 978-960-99061-0-4



9 789609 906104 >