

Σόφισμα για γονείς

Φροντίζοντας για την ασφάλεια των παιδιών στο Διαδίκτυο



s@ferinternet.gr

ins@fe

Με τη στήριξη της:



upc

ΠΕΡΙΕΧΟΜΕΝΑ

Α. Πώς να χρησιμοποιήσετε τον οδηγό για γονείς σελ. 4



Β. Οδηγίες για γονείς και κηδεμόνες σελ. 5



1. Η ασφάλεια φέρνει σιγουριά σελ. 6

2. Επικοινωνία σελ. 10

3. Ηλεκτρονική παρενόχληση σελ. 15

4. Διασκέδαση και κατέβαση αρχείων σελ. 17

Γ. Προτεινόμενες λύσεις των δραστηριοτήτων σελ. 21



1. Η ασφάλεια φέρνει σιγουριά σελ. 21

2. Επικοινωνία σελ. 24

3. Ηλεκτρονική παρενόχληση σελ. 26

4. Διασκέδαση και κατέβαση αρχείων σελ. 27

Δ. Γλωσσάρι σελ. 29



Ε. Χρήσιμες διαδικτυακές διευθύνσεις σελ. 39





A: Πώς να χρησιμοποιήσετε τον οδηγό για γονείς

*Αν κάνετε σχέδια για ένα χρόνο, φυτέψτε ρύζι
Αν κάνετε σχέδια για δέκα χρόνια, φυτέψτε ένα δέντρο
Αν κάνετε σχέδια για μια ζωή, εκπαιδέυστε τα παιδιά σας*

Κινέζικη παροιμία

Αγαπητοί γονείς/κηδεμόνες,

Κρατάτε στα χέρια σας τον οικογενειακό οδηγό ασφάλειας στο Διαδίκτυο που δημιουργήθηκε για οικογένειες με παιδιά ηλικίας μεταξύ 6 και 12 ετών. Πρόκειται για εκπαιδευτικό υλικό, φτιαγμένο με την πεποίθηση ότι οι νέες τεχνολογίες δεν θα πρέπει να διχάζουν τις γενιές, αλλά αντιθέτως να τις ενώνουν. Ο οικογενειακός οδηγός είναι αποτέλεσμα της γνώσης του Πανευρωπαϊκού Δικτύου Εθνικών Κέντρων Ενημέρωσης και Επαγρύπνησης για ένα Ασφαλέστερο Διαδίκτυο, Insafe, με την υποστήριξη της εταιρείας UPC.

Όπως το παιχνίδι στην παιδική χαρά ή η διέλευση του δρόμου μπορεί να ενέχουν κινδύνους εάν δεν προσέχουμε, έτσι και η χρήση του Διαδικτύου και των κινητών τεχνολογιών χρειάζεται προσοχή. Ευτυχώς, υπάρχουν εργαλεία που μπορούν να εξοπλίσουν τους χρήστες του Διαδικτύου με γνώση γύρω από τους τρόπους ορθής πλοήγησης, τα οφέλη και τους κινδύνους του Διαδικτύου.



Χρησιμοποιήστε τον νέο σας οδηγό για να βοηθήσετε τα παιδιά σας να μάθουν να χρησιμοποιούν το Διαδίκτυο με ασφάλεια και αποτελεσματικότητα. Ο οδηγός σας προσφέρει επάνω από πενήντα συμβουλές και δραστηριότητες, που θα σας βοηθήσουν να διδάξετε στα παιδιά σας την ασφάλεια στο Διαδίκτυο με διασκεδαστικό τρόπο. Ο οδηγός περιλαμβάνει:

- Δύο βιβλιαράκια ασφάλειας στο Διαδίκτυο: το διασκεδαστικό οδηγό για όλη την οικογένεια και τον οδηγό για γονείς
- Χρυσούς κανόνες για όλη την οικογένεια
- Ένα οικογενειακό πιστοποιητικό
- Αυτοκόλλητα
- 12 κάρτες περιπτώσεων, τις οποίες μπορούν να κόψουν τα παιδιά

Οι δύο οδηγοί είναι κωδικοποιημένοι χρωματικά για να αναδείξουν τέσσερα βασικά θέματα ασφάλειας: **Ασφάλεια**, **Επικοινωνία**, **Ηλεκτρονική παρενόχληση** και **Διασκέδαση και κατέβασμα αρχείων**. Ο οδηγός για τους γονείς χρησιμεύει ως σημείο αναφοράς για τη χρήση του διασκεδαστικού οδηγού για όλη την οικογένεια: περιέχει γενικές πληροφορίες, σημειώσεις σχετικά με τις δραστηριότητες, καθώς και προτεινόμενες λύσεις για τις δραστηριότητες και τις κάρτες περιπτώσεων.

Ο διασκεδαστικός οδηγός είναι φτιαγμένος για όλη την οικογένεια. Τα τέσσερα βασικά θέματα του οδηγού προσεγγίζονται μέσα από την ιστορία δύο παιδιών, του Αλέξη και της Ζέτας, των γονιών τους και της Αθηνάς, που είναι ξεφτέρι στους υπολογιστές. Κάθε κεφάλαιο περιλαμβάνει εκπαιδευτικές δραστηριότητες, μαζί με κουίζ, χρυσούς κανόνες και χρήσιμες διαδικτυακές διευθύνσεις.

Διαβάστε την ιστορία δυνατά με τα παιδιά σας και ασχοληθείτε με τις δραστηριότητες που προτείνουμε. Στο τέλος κάθε κεφαλαίου, μπορείτε να χρησιμοποιήσετε τις αντίστοιχες κάρτες περιπτώσεων για να ξεκινήσετε διάλογο με τα παιδιά σας, με στόχο την καλύτερη κατανόηση του περιεχομένου του οδηγού.

Όταν τα παιδιά έχουν ολοκληρώσει με επιτυχία τα τέσσερα κεφάλαια του οδηγού, ανταμείψτε τα συμφωνώντας μαζί σε μια σειρά χρυσών κανόνων και υπογράψτε το οικογενειακό πιστοποιητικό όλοι μαζί. Τέλος, τα παιδιά μπορούν να διακοσμήσουν τους οδηγούς με τα αυτοκόλλητα.

Τα σχόλιά σας μας είναι πολύτιμα. Επικοινωνήστε μαζί μας για τυχόν ερωτήσεις ή σχόλια. Ευχόμαστε σε εσάς και την οικογένειά σας καλή διασκέδαση στην «εξημέρωση» του Διαδικτύου!

Με ευχές για ασφαλή πλοήγηση,



Β. Οδηγίες για γονείς και κηδεμόνες

1. Η ασφάλεια φέρνει σιγουριά



ΕΝΑΣ ΥΠΟΛΟΓΙΣΤΗΣ ΣΤΟ ΣΠΙΤΙ

Ένας υπολογιστής στο σπίτι μπορεί να είναι πηγή γνώσης και ψυχαγωγίας για όλη την οικογένεια. Τοποθετώντας τον υπολογιστή σε κοινόχρηστο χώρο του σπιτιού και θέτοντας συγκεκριμένους κανόνες σχετικά με τη χρήση του, βοηθάτε τα νέα μέλη της οικογένειάς σας να παραμείνουν ασφαλή.

Να θυμάστε ότι τα παιδιά σας μπορούν να χρησιμοποιήσουν το **Διαδίκτυο** σε 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.

ΘΩΡΑΚΙΖΟΝΤΑΣ ΤΟΝ ΥΠΟΛΟΓΙΣΤΗ ΣΑΣ

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** ή **CD-ROM**, το άνοιγμα **συνημμένων** αρχείων και το **κατέβασμα** προγραμμάτων από το Διαδίκτυο, μπορεί να ενέχουν

κινδύνους. Οι κίνδυνοι αυτοί αφορούν κυρίως τη **διάδοση προγραμμάτων κακόβουλου λογισμικού**, φτιαγμένων με στόχο να βλάψουν τον υπολογιστή σας, να υποκλέψουν προσωπικά δεδομένα, ή να σας βομβαρδίσουν με ανεπιθύμητο διαφημιστικό υλικό.

Στο κεφάλαιο αυτό, τα παιδιά ενημερώνονται για διάφορους τύπους κακόβουλου λογισμικού όπως οι «**ιοί**», τα «**ακουλήκια**», οι «**Δούρειοι Ίπποι**» και τα «**λογισμικά κατασκοπείας**». Επίσης, διδάσκονται να αναγνωρίζουν τα συμπτώματα ενός μολυσμένου υπολογιστή και πώς να αποφεύγουν μολύνσεις από κακόβουλα λογισμικά, φροντίζοντας πάντα να έχουν πρόσβαση στο Διαδίκτυο από υπολογιστή που προστατεύεται από ενημερωμένα προγράμματα “**antivirus**” και “**antispyware**”. Μαθαίνουν, επίσης, να προσέχουν όταν ανοίγουν συνημμένα αρχεία που λαμβάνουν μέσω **ηλεκτρονικών μηνυμάτων** από άγνωστους αποστολείς, όταν κατεβάζουν προγράμματα από το Διαδίκτυο, ή όταν χρησιμοποιούν συσκευές αποθήκευσης USB ή CD-ROMs.

ΚΑΤΑΠΟΛΕΜΩΝΤΑΣ ΤΑ ΑΝΕΠΙΘΥΜΗΤΑ ΜΗΝΥΜΑΤΑ

Το 80% των ηλεκτρονικών μηνυμάτων που κυκλοφορούν στο Διαδίκτυο είναι ανεπιθύμητα, **spam**, που μπορούν εύκολα να επηρεάσουν τα παιδιά σας. Η αλόγιστη δημοσίευση της **ηλεκτρονικής σας διεύθυνσης** στο **Διαδίκτυο** σε ιστοχώρους συνομιλίας **τσατ**, σε δημόσια **φόρουμ**, σε **ηλεκτρονικές φόρμες**, ή σε υπηρεσίες **κοινωνικής δικτύωσης**, μπορεί να έχει ως αποτέλεσμα την αποστολή spam. Αυτό συμβαίνει επειδή υπάρχουν ειδικά **λογισμικά** που μπορούν να συλλέξουν αυτόματα διευθύνσεις ηλεκτρονικού ταχυδρομείου από το Διαδίκτυο για τη μαζική αποστολή ανεπιθύμητων μηνυμάτων.

Οι εταιρείες που εμπλέκονται σε αυτές τις δραστηριότητες έχουν συνήθως την έδρα τους σε χώρες όπου δεν υπάρχει κατάλληλη νομοθεσία που να εμποδίζει την αποστολή ανεπιθύμητων ηλεκτρονικών μηνυμάτων!

Τα μηνύματα spam σχετίζονται συνήθως με πορνογραφία, φαρμακευτικά προϊόντα, αμφιλεγόμενες οικονομικές συναλλαγές κλπ. Επίσης, τα spam συχνά μεταφέρουν κακόβουλο λογισμικό, όπως ιούς. Παρακάτω ακολουθούν κάποιες συμβουλές που θα σας βοηθήσουν να προστατέψετε την οικογένειά σας:

- Χρησιμοποιήστε «**φίλτρα spam**». Ο πάροχος σύνδεσης στο Διαδίκτυο που χρησιμοποιείτε σας προσφέρει συνήθως ανάλογες επιλογές τις οποίες μπορείτε να ενεργοποιήσετε. Επικοινωνήστε με τον πάροχό σας για περισσότερες πληροφορίες. Ελέγχετε τακτικά τον **φάκελο «ανεπιθύμητη αλληλογραφία (junk ή spam)»** για να σιγουρευτείτε ότι δεν έχουν καταλήξει εκεί αθώα μηνύματα που θα έπρεπε να έχετε λάβει χωρίς πρόβλημα. Η τεχνολογία δεν είναι αλάνθαστη.
- Μάθετε στα παιδιά σας να μην ανοίγουν μηνύματα που προέρχονται από αγνώστους. Τα μηνύματα spam περιέχουν σχεδόν πάντα δελεαστικές προσφορές και συνημμένα αρχεία. Δείτε τους πώς να αποκλείουν τον αποστολέα ενός ηλεκτρονικού μηνύματος, ή απλά ζητήστε τους να διαγράψουν οποιοδήποτε ύποπτο μήνυμα.

ΣΕΡΦΑΡΟΝΤΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Ακόμη και τα πολύ μικρά παιδιά μπορούν να επωφεληθούν από την πλοήγηση στο Διαδίκτυο σε **ιστοσελίδες** που προσφέρονται για ψυχαγωγικούς ή εκπαιδευτικούς σκοπούς. Ωστόσο, στο Διαδίκτυο υπάρχει κάθε λογής περιεχόμενο που δεν είναι πάντα κατάλληλο για την ηλικία τους.

Οι μηχανές αναζήτησης διευκολύνουν τον εντοπισμό περιεχομένου στο Διαδίκτυο. Ωστόσο, επειδή η αναζήτηση εξαρτάται από την επιλογή κατάλληλων λέξεων-κλειδίων, είναι εύκολο να πέσει κανείς επάνω σε ανεπιθύμητο περιεχόμενο. Μια αθώα λέξη-κλειδί μπορεί να οδηγήσει σε μια όχι και τόσο αθώα ιστοσελίδα που τυχαίνει να περιέχει την εν λόγω λέξη-κλειδί. Παρακάτω ακολουθούν μερικές συμβουλές για να μπορούν τα παιδιά σας να σερφάρουν με μεγαλύτερη ασφάλεια στο Διαδίκτυο:

- Δημιουργήστε ξεχωριστό λογαριασμό χρήστη για το παιδί σας μέσω του **λειτουργικού σας συστήματος** (π.χ. Windows, Linux, Mac OS), στον οποίο μπορείτε να ενεργοποιήσετε επιλογές **γονικού ελέγχου**.
- Εξετάστε τις επιλογές γονικού ελέγχου του **πλοηγού** (browser) και της μηχανής αναζήτησης που χρησιμοποιείτε. Βεβαιωθείτε ότι γνωρίζετε τις επιλογές που σας παρέχουν οι **οικογενειακές ρυθμίσεις** αυτών των προγραμμάτων.
- Προτείνετε στα παιδιά σας **μηχανές αναζήτησης** φιλικές για παιδιά, όπως π.χ. <http://kids.yahoo.com>
- Φυλάξτε τις αγαπημένες ιστοσελίδες των παιδιών σας στον φάκελο των **αγαπημένων** τους (μια επιλογή του πλοηγού). Με αυτόν τον τρόπο μπορούν να χρησιμοποιούν τις αγαπημένες τους σελίδες ξανά και ξανά χωρίς να χρειάζεται να περάσουν μέσα από μηχανές αναζήτησης.

Εκτός της ενεργοποίησης των λειτουργιών γονικού ελέγχου στον πλοηγό σας και τη μηχανή αναζήτησης, μπορείτε να χρησιμοποιήσετε ένα πρόσθετο φίλτρο - λογισμικό που στοχεύει στην προστασία των ανήλικων χρηστών από ακατάλληλο περιεχόμενο. Ρωτήστε στην αγορά, ή αναζητήστε δοκιμαστικές εκδόσεις τέτοιων φίλτρων στο Διαδίκτυο. Να θυμάστε ότι κανένα πρόγραμμα δεν μπορεί να αντικαταστήσει την καθοδήγηση και παρουσία σας ως γονείς και κηδεμόνες. Τα τεχνικά μέσα δεν είναι πανάκεια και ορισμένες φορές μπορούν να δημιουργήσουν μια ψευδή αίσθηση ασφάλειας εάν δεν συνδυαστούν με την κοινή λογική.

Τα φίλτρα μπορεί να είναι τόσο περιοριστικά ώστε να μπλοκάρουν αθώο περιεχόμενο. Θα μπορούσαν π.χ. να μπλοκάρουν την έρευνα για την ιστορία του Δεύτερου Παγκόσμιου Πολέμου, επειδή η αναζήτηση πιθανότατα να οδηγήσει σε σελίδες με περιγραφές βίας. Επιπλέον, οποιοδήποτε φίλτρο μπορεί να ενεργοποιηθεί, μπορεί και να απενεργοποιηθεί από έξυπνους νεαρούς χρήστες, που συχνά είναι ειδικοί στο να καλύπτουν τα ίχνη τους. Μόνο εάν ξέρετε πώς να χειρίζεστε τον υπολογιστή σας και τα προγράμματα που περιέχει, θα μπορείτε να εντοπίζετε τέτοιου είδους ενέργειες.

Επισκεφθείτε την ιστοσελίδα του **SIP-Bench** (βλ. Χρήσιμες διαδικτυακές διευθύνσεις), όπου θα βρείτε τα αποτελέσματα μιας μελέτης των πιο διαδεδομένων προγραμμάτων γονικού ελέγχου και φίλτρων. Η συγκριτική αυτή μελέτη πραγματοποιήθηκε με την υποστήριξη της Ευρωπαϊκής Επιτροπής. Στόχος ήταν η αξιολόγηση των προγραμμάτων αυτών ως προς την προστασία των παιδιών από **επιβλαβές περιεχόμενο** σε διάφορες υπηρεσίες και εφαρμογές του Διαδικτύου: **πλοήγηση** σε ιστοσελίδες, ηλεκτρονική αλληλογραφία, **μεταφορά αρχείων**, **συνομιλίες** μέσω Διαδικτύου.

Πέρα από την αποφυγή **επιβλαβούς περιεχομένου**, θα πρέπει να διδάξετε στα παιδιά σας να μη πιστεύουν σιδηρήτε βλέπουν ή διαβάζουν στο Διαδίκτυο. Στον οικογενειακό οδηγό προτείνουμε στα παιδιά, όταν αναζητούν κάτι στο Διαδίκτυο, πάντα να επισκέπτονται τουλάχιστον 3 ιστοσελίδες για να συγκρίνουν τις πληροφορίες που αυτές παρέχουν. Συνιστούμε, επίσης, να αναφέρουν συστηματικά τις πηγές των πληροφοριών που χρησιμοποιούν ως βάση για τις σχολικές τους εργασίες.

ΧΡΥΣΟΙ ΚΑΝΟΝΕΣ ΓΙΑ ΓΟΝΕΙΣ ΠΑΙΔΙΩΝ ΠΟΥ ΠΛΗΗΓΟΥΝΤΑΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

- Βεβαιωθείτε ότι ο υπολογιστής σας προστατεύεται από **λογισμικό ασφαλείας “fire-wall”** καθώς και από ενημερωμένα λογισμικά για την καταπολέμηση των ιών (antivirus) και των προγραμμάτων κατασκοπείας (antispyware). Ρωτήστε τον πάροχο της σύνδεσής στο Διαδίκτυο για τέτοιου είδους προγράμματα. Λαμβάνετε υπόψη σας τις προειδοποιήσεις που σας στέλνουν τα προγράμματα αυτά.
- Ενεργοποιήστε τα φίλτρα κατά των spam στο πρόγραμμα ηλεκτρονικού ταχυδρομείου που χρησιμοποιείτε και διατηρείτε την ηλεκτρονική σας διεύθυνση όσο πιο ιδιωτική γίνεται. Μη τη δημοσιεύετε αλόγιστα στο Διαδίκτυο. Αποφεύγετε μηνύματα από αγνώστους αποστολείς και φροντίστε να σαρώσετε τα συνημμένα αρχεία πριν τα ανοίξετε.
- Χρησιμοποιείτε στο έπακρο τις επιλογές γονικού ελέγχου που προσφέρουν το λειτουργικό σύστημα του υπολογιστή σας, ο πλοηγός, η μηχανή αναζήτησης και το πρόγραμμα ηλεκτρονικού ταχυδρομείου σας. Δημιουργήστε ξεχωριστούς λογαριασμούς χρήστη για τα παιδιά σας και βεβαιωθείτε ότι οι **επιλογές απορρήτου** είναι ενεργοποιημένες (επισκεφθείτε το μενού “Options” του πλοηγού σας).
- Εξετάστε τη χρήση συμπληρωματικού λογισμικού φίλτραρίσματος.
- Σε περίπτωση που ο υπολογιστής σας συμπεριφέρεται παράξενα, μη διστάσετε να επικοινωνήσετε με κάποιον ειδικό ή με τον πάροχο σύνδεσής στο Διαδίκτυο, διότι υπάρχει περίπτωση να είναι μολυσμένος. Επίσης, ο πάροχός σας θα πρέπει να μπορεί να σας προσφέρει ειδικές συμβουλές για γονείς.
- Εάν πέσει στην αντίληψή σας ανεπιθύμητο περιεχόμενο στο Διαδίκτυο, αναφέρετέ το στην Ανοιχτή Γραμμή Καταγγελιών Safeline (βλ. Χρήσιμες διαδικτυακές διευθύνσεις).
- Όποτε μπορείτε, κάνετε παρέα στα παιδιά σας όταν χρησιμοποιούν το Διαδίκτυο. Είναι ένας εξαιρετικός τρόπος να συζητήσετε άμεσα οποιοδήποτε θέμα προκύψει και να καλλιεργήσετε την εμπιστοσύνη μεταξύ σας. Το να μαθαίνετε μαζί είναι μια ευχάριστη πρόκληση.
- Θυμηθείτε ότι αυτές οι συμβουλές αφορούν και εσάς και τα παιδιά σας. Ενθαρρυνετέ τα να σας αναφέρουν οτιδήποτε τους φαίνεται παράξενο.

ΧΡΗΣΙΜΕΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΔΙΕΥΘΥΝΣΕΙΣ

Η γνώση αποτελεί το κλειδί για την ασφαλή και διασκεδαστική πλοήγηση στο Διαδίκτυο. Επισκεφθείτε τον ιστοχώρο www.saferinternet.gr για να βρείτε πλειάδα πληροφοριών γύρω από την ασφαλή πλοήγηση στο Διαδίκτυο, για εσάς και τα παιδιά σας.

<http://www.saferinternet.gr>

Αν βρείτε παράνομο περιεχόμενο καταγγείλτε το στην Ανοιχτή Γραμμή Καταγγελιών Safeline:

<http://www.safeline.gr>

Στη μελέτη του SIP-Bench θα βρείτε συγκριτική αξιολόγηση γονικών εργαλείων και φίλτρων:

<http://www.yprt.eu/sip/>

2. ΕΠΙΚΟΙΝΩΝΙΑ



ΤΑ ΚΟΜΜΑΤΙΑ ΤΟΥ ΠΑΖΛ

Θυμάστε πόσο σημαντική ήταν η επαφή με τους φίλους σας όταν μεγαλώνατε; Το Διαδίκτυο προσφέρει πολλές νέες ευκαιρίες έκφρασης και κοινωνικοποίησης μέσω ηλεκτρονικού ταχυδρομείου, **ανταλλαγής αρχείων**, **blogging**, **ιστοσελίδων κοινωνικής δικτύωσης** (π.χ. Facebook, Twitter) κλπ. Οι έφηβοι σήμερα χρησιμοποιούν την τεχνολογία για να δοκιμάσουν καινούρια πράγματα και κοινωνικοποιούνται σε ένα χώρο που αισθάνονται ιδιωτικό και απαλλαγμένο από τη γονική επιτήρηση.

Το κεφάλαιο «Επικοινωνία» εισάγει τους γονείς και τα παιδιά στην έννοια των **προσωπικών δεδομένων**, του **απορρήτου**, της θετικής επικοινωνίας και της διαχείρισης πιθανών κινδύνων, όπως η επαφή με αγνώστους. Η έννοια του απορρήτου συνδέεται πολύ στενά με τους **λογαριασμούς** και τα **προφίλ χρηστών** που δημιουργούμε για να χρησιμοποιήσουμε τις διάφορες υπηρεσίες που μας προσφέρει το Διαδίκτυο.

Στην καθημερινή σας ζωή, η κάρτα του λεωφορείου, ή η κάρτα μέλους του γυμναστηρίου σας περιέχουν προσωπικές πληροφορίες. Το ίδιο συμβαίνει στις υπηρεσίες του Διαδικτύου. Για να έχετε πρόσβαση σε μια υπηρεσία, πρέπει να δώσετε ορισμένες προσωπικές πληροφορίες για τη δημιουργία ενός **“προφίλ χρήστη”**. Είναι σημαντικό ότι μπορείτε να επιλέξετε τόσο το είδος των πληροφοριών που θέλετε να δημοσιοποιήσετε για τον εαυτό σας, όσο και με ποιους θέλετε να μοιραστείτε τις πληροφορίες αυτές.

Η προστασία των προσωπικών δεδομένων σημαίνει τη σωστή διαχείρισή τους και όχι ψευδή παρουσίαση της ταυτότητάς σας. Οι νέοι επικοινωνούν με ενθουσιασμό με τους φίλους τους σε απευθείας σύνδεση και δημιουργούν τη διαδικτυακή εικόνα τους. Ωστόσο, δεν συνειδητοποιούν πάντα τον αντίκτυπο που μπορεί να έχει η δημοσίευση προσωπικών στοιχείων σε ένα δημόσιο χώρο, όπως το Διαδίκτυο.

ΔΗΜΙΟΥΡΓΙΑ ΠΡΟΦΙΛ

Το πρώτο βήμα για την προστασία των προσωπικών δεδομένων είναι η δημιουργία ενός ασφαλούς προφίλ με ενεργοποιημένες τις ρυθμίσεις απορρήτου. Σκεφτείτε προσεκτικά τις πληροφορίες που θα δημοσιεύσετε.

Σας συνιστούμε να φτιάξετε διαφορετικούς λογαριασμούς ηλεκτρονικού ταχυδρομείου για διαφορετικές χρήσεις: ενθαρρύνετε το παιδί σας να χρησιμοποιεί μια ουδέτερη διεύθυνση ηλεκτρονικού ταχυδρομείου και **όνομα χρήστη** που να μην αποκαλύπτουν το πλήρες όνομά του, όταν χρησιμοποιεί διάφορες υπηρεσίες στο Διαδίκτυο (chat, blog, κλπ.).

Να κρατάτε πάντα μυστικούς τους **κωδικούς πρόσβασης** σας. Βεβαιωθείτε ότι τα παιδιά σας αντιλαμβάνονται πως δεν θα πρέπει να μοιράζονται τους προσωπικούς τους λογαριασμούς

με φίλους τους που μπορεί να κάνουν κατάχρηση της εμπιστοσύνης τους. Από την άλλη, ίσως να θέλετε να γνωρίζετε τους κωδικούς πρόσβασης των παιδιών σας, ώστε να μπορείτε να παρακολουθείτε το λογαριασμό τους – συζητήστε το με τα παιδιά σας.

Μην ξεχάσετε να προσαρμόσετε τις **ρυθμίσεις απορρήτου** του προφίλ σας / λογαριασμού σας, ώστε τα στοιχεία σας να είναι ιδιωτικά και όχι δημόσια. Ένα ιδιωτικό προφίλ σας δίνει τη δυνατότητα να ελέγχετε σε ποιους είναι ορατό και με ποιος μπορείτε να έρχεστε σε επαφή. Ένα ιδιωτικό προφίλ σημαίνει ότι μπορείτε να διαχειριστείτε τη **λίστα των επαφών** σας. Διδάξτε στα παιδιά σας να αποδέχονται μόνο επαφές από άτομα που ήδη γνωρίζουν από κοντά.

Αν τα παιδιά σας χρησιμοποιούν **δωμάτια επικοινωνίας τσατ** (chat rooms), ελέγξτε τα εξής:

- Υπάρχουν επιτηρητές; Η έλλειψη επιτηρητών σημαίνει έλλειψη ασφάλειας.
- Υπάρχουν ρυθμίσεις για τον αποκλεισμό ανεπιθύμητων επαφών;
- Υπάρχει υπηρεσία βοήθειας και **αναφοράς** σε περίπτωση προβλήματος;
- Οι κανόνες χρήσης είναι σαφείς και ευδιάκριτοι;

ΦΩΤΟΓΡΑΦΙΕΣ ΚΑΙ ΚΑΜΕΡΕΣ

Τα παιδιά θα πρέπει να αντιληφθούν ότι η εικόνα τους είναι αναπόσπαστο κομμάτι της ιδιωτικότητάς τους και ότι οι ψηφιακές φωτογραφίες έχουν μεγάλη δύναμη. Πολύ εύκολα μπορεί να κυκλοφορήσουν ευρέως, αλλά και να **παραποιηθούν**. Επίσης, από τη στιγμή που θα αποσταλούν μέσω ενός υπολογιστή ή κινητού τηλεφώνου, είναι πολύ δύσκολο να εξαλειφθούν – μπορούν να μείνουν στο Διαδίκτυο για πάντα!

Οι **κάμερες του υπολογιστή** μας (webcam) θα πρέπει να χρησιμοποιούνται με σύνεση. Τα παιδιά δεν ενδείκνυται να τις χρησιμοποιούν χωρίς επιτήρηση. Η χρήση τσατ με κάμερες ενέχει κινδύνους. Θα πρέπει και εσείς και τα παιδιά σας να μοιράζετε τις προσωπικές σας φωτογραφίες μόνον με άτομα που γνωρίζετε και εμπιστεύεστε. Ακόμη, πάντα να ζητάτε την άδεια πριν δημοσιεύσετε τη φωτογραφία κάποιου και φροντίστε τα παιδιά σας να μη χρησιμοποιούν την κάμερα και τον υπολογιστή μόνον στο δωμάτιο τους.

ΕΠΙΚΟΙΝΩΝΙΑ ΜΕ ΑΓΝΩΣΤΟΥΣ


Οι άνθρωποι που γνωρίζετε στο Διαδίκτυο δεν είναι πάντα απαραίτητα αυτοί που λένε ότι είναι. Μάθετε στα παιδιά σας να προστατεύουν τα προσωπικά τους δεδομένα στο Διαδίκτυο, όπως θα έκαναν και στην καθημερινή τους ζωή. Μαθαίνετε στα παιδιά σας να μη μιλούν με ξένους στον πραγματικό κόσμο, γιατί δεν θα πρέπει να τηρούν τον ίδιο κανόνα και στο Διαδίκτυο;

Τα παιδιά σας μπορεί να αναπτύξουν στενή σχέση με άτομα με τα οποία επικοινωνούν μέσω Διαδικτύου. Εύκολα μπορούν να εμπιστευτούν κάποιον που τους δείχνει ενδιαφέρον και κατανόηση, ακόμη και αν τους είναι άγνωστος. Συνεπώς, πιθανώς να μπουν στον πειρασμό να συναντήσουν αυτούς τους φίλους χωρίς να σας ενημερώσουν. Συχνά, τα παιδιά δεν αντιλαμβάνονται τους πιθανούς κινδύνους μιας τέτοιας συνάντησης. Το γεγονός αυτό τα καθιστά εύκολα θύματα **προσέλκυσης για γενετήσιους λόγους (grooming)**. Μελέτες δείχνουν ότι πολλά παιδιά πηγαίνουν σε συναντήσεις με άγνωστους ουσιαστικά “φίλους” ασυνόδευτα και χωρίς να ενημερώσουν τους γονείς τους. Μιλήστε στα παιδιά σας για αυτό το θέμα, ώστε να μη βρεθούν σε αυτή τη θέση. Η επικοινωνία είναι το παν.

ΚΑΝΟΝΕΣ ΣΥΜΠΕΡΙΦΟΡΑΣ (ΕΤΙΚΕΤΑ) ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Οι **κανόνες συμπεριφοράς** (ετικέτας) στο Διαδίκτυο αναφέρονται στους καλούς τρόπους στο Διαδίκτυο και στο σεβασμό των άλλων: συμπεριφερόμαστε στους άλλους χρήστες του Διαδικτύου, όπως θα θέλαμε να μας συμπεριφέρονται αυτοί. Τα παιδιά δεν συνειδητοποιούν πάντα ότι μπορεί άθελα τους να προσβάλουν ή να πληγώσουν κάποιον επικοινωνώντας μέσω Διαδικτύου. Δυστυχώς, κάποιοι άνθρωποι χρησιμοποιούν το Διαδίκτυο ή/και τα κινητά τηλέφωνα για να ενοχλήσουν ή να αναστατώσουν άλλους ανθρώπους. Αυτό λέγεται ηλεκτρονική παρενόχληση και αγγίζει μέχρι και ένα στα τέσσερα παιδιά (ανατρέξτε στο σχετικό κεφάλαιο για περισσότερες πληροφορίες).

Η ΓΛΩΣΣΑ ΤΟΥ ΤΣΑΤ

Όταν οι νέοι συνομιλούν μέσω του Διαδικτύου, χρησιμοποιούν μια μοναδική γλώσσα, γεμάτη **emoticons** και **ακρωνύμια!** Ρίξτε μια ματιά στον παρακάτω ενδεικτικό πίνακα για να εξοικειωθείτε με τους κώδικες και τις συντομογραφίες του τσατ 

Ενδεικτικός πίνακας ακρωνυμίων, για περισσότερες πληροφορίες δείτε τις χρήσιμες διαδικτυακές διευθύνσεις:

AFK: Away from keyboard
(δεν είμαι κοντά σε πληκτρολόγιο)

B/c: Because (επειδή)

B4N: Bye for now (χαίρετώ για την ώρα)

BBL: Be back later (θα γυρίσω αργότερα)

BRB: Be right back (γυρίζω αμέσως)

BTW: By the way (παρεμπιπτόντως)

C: See? (βλέπεις;)

Comp: Computer (υπολογιστής)

CU: See you (τα λέμε)

CUL: See you later (τα λέμε αργότερα)

F2F: Face to Face (πρόσωπο με πρόσωπο)

FAQ: Frequently asked questions
(συχνές ερωτήσεις)

JJ: Just joking (αστειεύομαι)

GL: Good luck (καλή τύχη)

GM: Good morning (καλημέρα)

GNT: Ginete (γίνεται)

GT: Giati (γιατί)

G2G / GTG: Got to go (πρέπει να φύγω)

IC: Ise (είσαι)

IDK: I don't know (δεν ξέρω)

L8R: Later (αργότερα)

LMIRL: Let's meet in real life (ας συναντηθούμε)

LOL: Laugh out loud (γελάω δυνατά)

LY4E: Love you forever
(σ' αγαπώ για πάντα)

MLM: Milame (μιλάμε)

MR: Moro (μωρό)

MT: Meta (μετά)

THLS: Thelis (θέλεις)

MZ: Mazi (μαζί)

THNX: Thanks (ευχαριστώ)

NA GN: Na gini (να γίνει)

TLK: Telika (τελικά)

NMZ: Nomizo (νομίζω)

TPT: Tipota (τίποτα)

NP: No problem (κανένα πρόβλημα)

TR: Tora (τώρα)

PAL: Parents are listening
(ακούνε οι γονείς μου)

TTYL: Talk to you later (τα λέμε αργότερα)

PAW: Parents are watching
(με παρακολουθούν οι γονείς μου)

W8: Wait (περίμενε)

PLS: Please (παρακαλώ)

WB: Welcome back (καλώς ήλθες πίσω)

POS: Parent Over Shouler
(γονέας από πίσω μου)

WTGP: Want to go private?
(θέλεις να μιλήσουμε σε ιδιωτικό χώρο;)

S^, S'UP: What's up? (τι γίνεται;)

WYCM: Will you call me?
(Θα μου τηλεφωνήσεις;)

SRY: Sorry (συγγνώμη)

Μπορείτε να δημιουργήσετε emoticons συνδυάζοντας σημεία στίξης και γράμματα, σύμφωνα με τα παρακάτω παραδείγματα:

Χαμογελαστό πρόσωπο (με ή χωρίς μύτη)

:) ή :-)

άνω και κάτω τελεία, (παύλα), παρένθεση

Λυπημένο πρόσωπο (με ή χωρίς μύτη) :

:(ή :-(

άνω και κάτω τελεία, (παύλα), παρένθεση

Κλείνοντας το μάτι (με ή χωρίς μύτη)

;) ή ;-)

ερωτηματικό, (παύλα), παρένθεση

Έκπληξη (με ή χωρίς μύτη)

: o ή :-o

άνω και κάτω τελεία, (παύλα), μικρό όμικρον

Μεγάλο χαμόγελο (με ή χωρίς μύτη)

:-D ή :D

άνω και κάτω τελεία, (παύλα), κεφαλαίο D (λατινικό)

Γλώσσα έξω (με ή χωρίς μύτη)

: p ή :-p

άνω και κάτω τελεία, (παύλα), μικρό p (λατινικό)

ΧΡΥΣΟΙ ΚΑΝΟΝΕΣ

- Βρείτε το χρόνο να ανακαλύψετε πώς περνούν τα παιδιά σας το χρόνο τους και πώς επικοινωνούν με φίλους τους στο Διαδίκτυο.
- Διδάξτε τα πώς να προστατεύουν την ιδιωτική τους ζωή:
 - Δημιουργώντας ασφαλή προφίλ με ενεργοποιημένες ρυθμίσεις απορρήτου.
 - Προστατεύοντας τους κωδικούς πρόσβασής τους.
 - Επικοινωνώντας μόνο με ανθρώπους που γνωρίζουν στον πραγματικό κόσμο.
 - Ζητώντας τη συγκατάθεσή σας πριν δημοσιεύσουν φωτογραφίες του εαυτού τους ή της οικογένειάς σας, του σπιτιού, του σχολείου τους, κλπ.
 - Δίνοντας προσωπικά στοιχεία, όπως τον αριθμό του τηλεφώνου τους, τη διεύθυνσή τους, το όνομα του σχολείου τους, κλπ. μόνο σε ανθρώπους που γνωρίζουν καλά στον πραγματικό κόσμο.
- Τοποθετήστε τον υπολογιστή σας σε κοινόχρηστο χώρο του σπιτιού, ώστε να μπορείτε να παρακολουθείτε τις δραστηριότητές τους.
- Βεβαιωθείτε ότι όλοι σας γνωρίζετε:
 - Πώς να αρνείστε ή να αποκλείετε μια επαφή από τη λίστα επαφών σας.
 - Τις δικλίδες ασφαλείας και τις λειτουργίες αναφοράς που σας προσφέρουν οι ιστότοποι που χρησιμοποιείτε.
- Καλλιεργήστε δεσμούς εμπιστοσύνης με τα παιδιά σας διαβεβαιώνοντας τα ότι μπορούν να σας μιλήσουν ακόμη και για τα λάθη τους, ώστε να αναζητήσετε μαζί τις κατάλληλες λύσεις! Τα λάθη είναι αναπόφευκτο κομμάτι της μάθησης.

ΧΡΗΣΙΜΕΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΔΙΕΥΘΥΝΣΕΙΣ

Ενημερωθείτε για την υπεύθυνη και ασφαλή χρήση του Διαδικτύου στην ιστοσελίδα της δράσης [Saferinternet.gr](http://www.saferinternet.gr) του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου:

<http://www.saferinternet.gr>

Αναφέρετε ύποπτο / παράνομο περιεχόμενο ή ύποπτη /παράνομη συμπεριφορά στο Διαδίκτυο στην Ανοιχτή Γραμμή Καταγγελιών [Safeline](http://www.safeline.gr) του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου:

<http://www.safeline.gr>

Αν το Διαδίκτυο δυσκολεύει τη ζωή του παιδιού σας ζητείτε βοήθεια από τη Γραμμή Βοήθειας Υποστηρίξω στη Μονάδα Εφηβικής Υγείας, Β' Παιδιατρική Κλινική Πανεπιστημίου Αθηνών:

<http://www.saferinternet.gr/helpline>

Διαβάστε για τη συγκριτική μελέτη εργαλείων γονικού ελέγχου και φίλτρων στη διεύθυνση:

<http://www.yprt.eu/sip/>

3. Ηλεκτρονική παρενόχληση



ΜΙΑ ΠΕΡΙΠΤΩΣΗ ΗΛΕΚΤΡΟΝΙΚΗΣ ΠΑΡΕΝΟΧΛΗΣΗΣ

Η επικοινωνία μέσω του Διαδικτύου και των κινητών τηλεφώνων έχει πολλά εξαιρετικά πλεονεκτήματα. Δυστυχώς, όμως, το Διαδίκτυο μπορεί να προσφέρει και δυσάρεστες εμπειρίες. Τα παιδιά μπορεί να λάβουν ή να στείλουν μηνύματα με περιεχόμενο που μπορεί να βλάψει τα συναισθήματά τους ή τα συναισθήματα άλλων. Είναι σημαντικό να μάθετε στα παιδιά σας να συμπεριφέρονται με κοινωνικά αποδεκτό τρόπο. Θυμηθείτε ότι ακόμη και τα ίδια σας τα παιδιά δεν είναι πάντα αγγελούδια ;-)

Η **ηλεκτρονική παρενόχληση** αφορά στη χρήση των νέων τεχνολογιών πληροφόρησης και επικοινωνίας για τον εκφοβισμό ή την παρενόχληση ενός ατόμου ή μιας ομάδας μέσω ηλεκτρονικού ταχυδρομείου, τσατ, κινητών τηλεφώνων κτλ. Στα διαδικτυακά περιβάλλοντα παιχνιδιών, η παρενόχληση μπορεί να σημαίνει ότι κάποιος παίκτης επιτίθενται στο εικονίδιο **"avatar"** που αντικατοπτρίζει τον εικονικό εαυτό του παιδιού σας στο παιχνίδι, π.χ. πυροβολώντας το, κλέβοντας **εικονικές κτήσεις**, ή αναγκάζοντας το avatar να συμπεριφερθεί με ανεπιθύμητο τρόπο.

Συχνά, τα παιδιά αναφέρουν προβλήματα που σχετίζονται με την αποκάλυψη ιδιωτικών πληροφοριών σε δημόσιους χώρους, π.χ. την ανάρτηση προσωπικών φωτογραφιών ή πληροφοριών σε κάποια ιστοσελίδα ή δημόσιο φόρουμ. Η **παρενόχληση**, είτε γίνεται με ηλεκτρονικά μέσα είτε στην αυλή του σχολείου και την παιδική χαρά, αποτελεί κοινωνικά μη αποδεκτή συμπεριφορά. Γονείς, εκπαιδευτικοί και παιδιά πρέπει να είναι ευαισθητοποιημένοι και έτοιμοι να αντιδράσουν. Σε αντίθεση με την παραδοσιακή παρενόχληση, η ηλεκτρονική παρενόχληση έχει την ιδιαιτερότητα ότι μπορεί να επηρεάσει το παιδί σας ακόμη και όταν δεν βρίσκεται στον ίδιο χώρο με τον θύτη. Για παράδειγμα, ο θύτης μπορεί να στείλει εκφοβιστικό μήνυμα στο ηλεκτρονικό ταχυδρομείο του παιδιού ή στο κινητό του τηλέφωνο οποιαδήποτε ώρα της ημέρας ή της νύχτας.

Ως γονείς και κηδεμόνες, μπορείτε να προωθήσετε ένα περιβάλλον που δεν ανέχεται την παρενόχληση. Διδάξτε στα παιδιά σας ότι ανωνυμία στο Διαδίκτυο δεν σημαίνει ανεύθυνη συμπεριφορά. Τα παιδιά πρέπει να γνωρίζουν τα δικαιώματά και τις υποχρεώσεις τους και πώς να σέβονται τα δικαιώματα των άλλων. Διατηρείτε συνεχώς ανοικτό διάλογο μαζί με τα παιδιά σας, ώστε να σας εμπιστεύονται τις όποιες ανησυχίες τους. Οι διαδραστικές τεχνολογίες, όπως το Διαδίκτυο και η κινητή τηλεφωνία, μπορούν να σας προσφέρουν εξαιρετικές ευκαιρίες για συζήτηση και προβληματισμό!

ΧΡΥΣΟΙ ΚΑΝΟΝΕΣ

- Αποφύγετε τις αρνητικές εμπειρίες, φροντίζοντας τα παιδιά σας να γνωρίζουν πώς να προστατεύουν την ιδιωτική τους ζωή καθώς και να σέβονται την προσωπική ζωή και των άλλων.

- Διδάξτε στα παιδιά σας να μην απαντούν σε ενοχλητικά μηνύματα.
- Βοηθήστε τα παιδιά σας να καταλάβουν τι είδους μηνύματα και συμπεριφορές μπορούν να πληγώσουν τους άλλους και πώς να τις αποφύγουν.
- Σιγουρευτείτε ότι τα παιδιά σας ξέρουν πώς να μπλοκάρουν επαφές από τη λίστα επαφών τους.
- Φυλάξτε τα ενοχλητικά μηνύματα εάν προκύψουν, διότι μπορεί να χρειαστούν ως απόδειξη.
- Ενημερωθείτε για τη στρατηγική που ακολουθεί το σχολείο των παιδιών σας σε περιπτώσεις παρενόχλησης. Συνεργαστείτε με άλλους γονείς και εκπαιδευτικούς για την πρόληψη της παρενόχλησης, σε οποιαδήποτε μορφή της.
- Εξοικειωθείτε με το περιβάλλον των παιδιών σας και γνωρίστε τους φίλους τους, τους γονείς των φίλων τους, τους δασκάλους και τους συμμαθητές τους.
- Ενθαρρύνετε τα παιδιά σας να σας ενημερώνουν για οτιδήποτε τους ανησυχεί, τόσο στον πραγματικό κόσμο όσο και στο Διαδίκτυο. Ακόμη και αν κάνουν κάποια απροσεξία, θα πρέπει να ξέρουν ότι τα στηρίζετε και ότι μαζί θα βρείτε λύσεις!
- Βεβαιωθείτε ότι τα παιδιά σας κατανοούν, πως, αν πέσουν θύματα παρενόχλησης, δεν είναι ποτέ δικό τους λάθος.

ΧΡΗΣΙΜΕΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΔΙΕΥΘΥΝΣΕΙΣ

Στην ιστοσελίδα "stop bullying" (σταμάτησε τη παρενόχληση) θα βρείτε κινούμενα σχέδια με θέμα την παρενόχληση, μαζί με προτεινόμενες δραστηριότητες αναφορικά με το πώς να αντιμετωπίσετε και να σταματήσετε την παρενόχληση:

<http://www.stopbullying.org>

Η ιστοσελίδα της δράσης *Saferinternet.gr* του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου παρέχει πολλές πληροφορίες για γονείς και παιδιά γύρω από την ηλεκτρονική παρενόχληση: <http://www.saferinternet.gr>

Η Γραμμή Βοηθείας ΥποΣΤΗΡΙΖΩ του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου παρέχει υποστήριξη σε παιδιά, εφήβους και τις οικογένειές τους μέσω του δωρεάν τηλεφώνου 800 11 800 15 και μέσω email στην ηλεκτρονική διεύθυνση: help@saferinternet.gr

4. Διασκέδαση και κατέβασμα αρχείων



ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΟΤΙ ΛΑΜΠΕΙ ΔΕΝ ΕΙΝΑΙ ΧΡΥΣΟΣ

Το Διαδίκτυο προσφέρεται για πολλές δραστηριότητες, μεταξύ άλλων και εμπορικές. Αν δεν αφήνετε τα παιδιά σας να αποκοτούν όσα βλέπουν να διαφημίζονται στην τηλεόραση, ή που τους κάνουν εντύπωση στα καταστήματα, τότε θα πρέπει επίσης να τα μάθετε να μη ζητούν ή να πιστεύουν οτιδήποτε διαφημίζεται στο Διαδίκτυο, όπως μουσική, παιχνίδια, **μελωδίες κλήσης** για το κινητό, άλλα αξεσουάρ ή υπηρεσίες.

Περνώντας χρόνο με τα παιδιά σας στο Διαδίκτυο, σας δίνεται την ευκαιρία να τους εξηγήσετε ότι προϊόντα όπως οι μελωδίες κλήσης, τα **φόντα επιφάνειας εργασίας**, τα **MP3s**, τα εικονίδια κλπ. σπάνια είναι δωρεάν. Όποτε πέσουν στην αντίληψή σας ανάλογες μορφές διαφήμισης, δείξτε τους τα ψιλά γράμματα για να τους αποδείξετε ότι δεν πρέπει να θεωρούν τα πάντα στο Διαδίκτυο ως δεδομένα.

Για να εγγραφείτε σε οποιαδήποτε διαδικτυακή υπηρεσία (δωρεάν ή μη), θα πρέπει να συμπληρώσετε κάποια **ηλεκτρονική φόρμα** με σχετικές προσωπικές πληροφορίες. Συμπληρώστε τα στοιχεία σας μόνο όταν ξέρετε πώς αυτά θα χρησιμοποιηθούν. Αντίστοιχα, αποθαρρύνετε τα παιδιά σας από τη χρήση αυτών των φορμών, εκτός και αν τις συμπληρώσετε μαζί.

Τα **αναδυόμενα παράθυρα** χρησιμοποιούνται συχνά για πώληση προϊόντων και προώθηση υπηρεσιών. Αυτό δεν είναι πάντα κακό - εξαρτάται από το αν προέρχονται από μια αξιόπιστη ιστοσελίδα ή όχι. Σε γενικές γραμμές, αν εμπιστεύεστε την ιστοσελίδα μπορείτε να εμπιστευθείτε και τα αναδυόμενα παράθυρα που εμφανίζονται. Ωστόσο, ορισμένα αναδυόμενα παράθυρα χρησιμοποιούνται για την εμπορία αναξιόπιστων προϊόντων ή οδηγούν σε ηλεκτρονικά ερωτηματολόγια για τη συλλογή δεδομένων προσωπικού χαρακτήρα. Διδάξτε στα παιδιά σας να κλείνουν αναξιόπιστα παράθυρα κάνοντας κλικ στο κόκκινο «X» της επάνω δεξιάς γωνίας.

ΠΑΙΖΟΝΤΑΣ ΠΑΙΧΝΙΔΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Τα **διαδικτυακά παιχνίδια** διαφέρουν από παλαιότερα ψηφιακά παιχνίδια, επειδή απαιτούν ζωντανή **σύνδεση δικτύου**. Τα παιδιά μπορούν να παίξουν παιχνίδια χρησιμοποιώντας

ένα CD / DVD σε ιστοσελίδες, κονσόλες παιχνιδιών, κινητά τηλέφωνα και άλλες φορητές συσκευές.

Τα διαδικτυακά παιχνίδια ποικίλουν από απλά, γνωστά παιχνίδια όπως το Pacman και το Tetris έως παιχνίδια εικονικής πραγματικότητας, στα οποία πολλοί παίκτες παίζουν μεταξύ τους σε απευθείας σύνδεση, δημιουργώντας περιεχόμενο και ιστορίες από κοινού. Πολλά παιχνίδια με **πολλαπλούς παίκτες** υποστηρίζουν εικονικές κοινότητες παικτών, γεγονός που μπορεί να εκθέσει τα παιδιά σε κινδύνους σχετικούς με την επαφή με αγνώστους (βλ. κεφάλαιο «Επικοινωνία»).

Τα παιχνίδια διαδραματίζουν σημαντικό ρόλο στην ανάπτυξη των παιδιών, καθώς συνεισφέρουν στην ανάπτυξη κοινωνικών δεξιοτήτων και στρατηγικής σκέψης μέσα σε ένα περιβάλλον που οριοθετείται από κανόνες. Πολλά ψηφιακά παιχνίδια είναι ελκυστικά και διαδραστικά και χρησιμοποιούνται για εκπαιδευτικούς σκοπούς.

Ωστόσο, δεν είναι όλα τα ψηφιακά παιχνίδια καλής ποιότητας. Θα πρέπει να αποφασίσετε τι είδους παιχνίδια είναι τα πιο κατάλληλα για τα παιδιά σας και επιπλέον, θέτοντας κανόνες, να εξασφαλίσετε ότι ο χρόνος που τα παιδιά σας θα καταναλώνουν σε διαδικτυακά παιχνίδια δεν θα δρα εις βάρος άλλων δραστηριοτήτων.



Το πανευρωπαϊκό σύστημα PEGI online κατατάσσει τα διαδικτυακά παιχνίδια ανάλογα με το περιεχόμενό τους και την ηλικία των παικτών. Το σύστημα υποστηρίζεται από διάφορους μεγάλους κατασκευαστές (συμπεριλαμβανομένων των PlayStation, Xbox και Nintendo) όπως και από εκδότες και σχεδιαστές διαδραστικών παιχνιδιών σε όλη την Ευρώπη.

Αναζητήστε και συμβουλευτείτε τις επικέτες PEGI στο οπισθόφυλλο κάθε ηλεκτρονικού παιχνιδιού, χωρίς όμως να ξεχνάτε ότι κάθε παιδί μιας συγκεκριμένης ηλικίας είναι διαφορετικό.

ΚΑΤΕΒΑΣΜΑ ΑΡΧΕΙΩΝ ΚΑΙ ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ

Τα νέα παιδιά αντιμετωπίζουν το Διαδίκτυο ως ένα θησαυρό ταινιών, μουσικής και παιχνιδιών, που μπορούν να κατεβάσουν στον υπολογιστή τους, να παρακολουθήσουν, να ακούσουν και να παίξουν αντίστοιχα. Συχνά κατεβάζουν ή ανεβάζουν υλικό χρησιμοποιώντας **ισότιμα δίκτυα** (peer networks), δίχως να αντιλαμβάνονται ότι το γνήσιο έργο ενός καλλιτέχνη ή άλλων δημιουργών / συγγραφέων προστατεύεται από το νόμο περί πνευματικής ιδιοκτησίας. Τέτοια έργα είναι π.χ. ταινίες, τραγούδια, βιβλία, λογισμικό ή φωτογραφίες.

Είναι παράνομο;

Η ανταλλαγή αρχείων δεν είναι παράνομη, εφόσον αφορά στην ανταλλαγή των αρχείων που έχετε εσείς δημιουργήσει. Σε γενικές γραμμές, το ανέβασμα και το κατέβασμα μουσικής και ταινιών χωρίς την άδεια του κατόχου της πνευματικής ιδιοκτησίας είναι παράνομο σε όλο τον κόσμο (εάν και κάθε κράτος έχει τη δική του νομοθεσία περί πνευματικής

ιδιοκτησίας). Ως κανόνα, θεωρείστε την ανταλλαγή ταινιών και μουσικής παράνομη και να είστε προσεχτικοί με εφαρμογές ισότιμων δικτύων (peer-to-peer).

Είναι ριψοκίνδυνο;

Η **ανταλλαγή αρχείων** θέτει τον υπολογιστή σας σε κινδύνους, καθώς ανοίγει πόρτες μέσω των οποίων μπορούν να εισβάλλουν κακόβουλα λογισμικά, οδηγώντας τον υπολογιστή σας σε βλάβες λειτουργίας. Επίσης, είναι πιθανό τρίτα άτομα να αποκτήσουν πρόσβαση σε προσωπικά σας δεδομένα ή να χρησιμοποιήσουν τον υπολογιστή σας για να αποστείλουν παράνομο περιεχόμενο.

Πού μπορώ να βρω νόμιμη μουσική;

Εκατοντάδες ιστοσελίδες σε όλο τον κόσμο παρέχουν την αγορά αρχείων μουσικής με νόμιμο τρόπο (βλ. Χρήσιμες διαδικτυακές διευθύνσεις), κάποιες, δε, παρέχουν μουσική δωρεάν! Παραδείγματα αποτελούν ιστοσελίδες, όπου μουσικοί δημοσιεύσουν δείγματα της δουλειάς τους για τους θαυμαστές τους, και προωθούν τις εμφανίσεις και τα άλμπουμ τους.

ΧΡΥΣΟΙ ΚΑΝΟΝΕΣ

- Ενθαρρύνετε τα παιδιά σας να χρησιμοποιούν ιστοσελίδες με νόμιμο περιεχόμενο και εξηγήστε τους ότι καμιά φορά τα φαινόμενα απατούν στο Διαδίκτυο.
- Εξηγήστε τους ότι το κατέβασμα υλικού από το Διαδίκτυο μπορεί να είναι επικίνδυνο και για αυτό χρειάζεται προσοχή.
- Βεβαιωθείτε ότι ο υπολογιστής σας είναι θωρακισμένος και ότι διαθέτει ενημερωμένο λογισμικό "antivirus".
- Μάθετε στα παιδιά σας να σώζουν τα αρχεία που έχουν κατεβάσει νόμιμα από το Διαδίκτυο στον σκληρό δίσκο του υπολογιστή και να τα σαρώνουν πριν τα ανοίξουν.
- Πάντοτε ελέγχετε την πολιτική απορρήτου και τους όρους χρήσης πριν να εγκαταστήσετε κάποιο πρόγραμμα. Μπορείτε να κάνετε μια έρευνα (στο Διαδίκτυο) για να δείτε αν το πρόγραμμα που θέλετε να κατεβάσετε είναι αξιόπιστο.
- Κλείνετε τα ύποπτα αναδυόμενα παράθυρα κάνοντας κλικ στον κόκκινο Χ της επάνω δεξιάς γωνίας. Ποτέ μην κάνετε κλικ στο εσωτερικό τους.

ΠΑΙΔΙΑ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΑ ΠΑΙΧΝΙΔΙΑ

- Θέστε κανόνες σχετικά με τον χρόνο που θα μπορεί το παιδί σας να παίζει ηλεκτρονικά παιχνίδια.

- Φροντίστε να παίζουν σε έναν οικογενειακό χώρο ώστε να μπορείτε να τα παρακολουθείτε.
- Παρακολουθείτε τις συνήθειες του παιδιού σας όταν παίζει. Όπως το παρακολουθείτε στην παιδική χαρά, γιατί να μην κάνετε το ίδιο όταν παίζει στο Διαδίκτυο;
- Συζητήστε το περιεχόμενο των παιχνιδιών. Ποια στοιχεία μοιάζουν με την πραγματικότητα, ποια όχι και τι τους αρέσει ιδιαίτερα;
- Πριν αγοράσετε κάποιο παιχνίδι, βεβαιωθείτε ότι το περιεχόμενό του είναι κατάλληλο για την ηλικία του παιδιού σας (βλ. Πανευρωπαϊκό σύστημα PEGI).

Όταν τα παιδιά σας παίζουν ηλεκτρονικά παιχνίδια για πολλαπλούς χρήστες:

- Επιλέξτε ιστοχώρους με αυστηρούς κανόνες και επιτηρητές.
- Μάθετε στα παιδιά σας να μη δίνουν προσωπικές πληροφορίες σε άλλους παίκτες.
- Μάθετε στα παιδιά σας να μη δεχτούν συνάντηση στο φυσικό κόσμο με άλλους παίκτες, εκτός και αν τα συνοδεύσετε.
- Ενθαρρύνετε τα να σας αναφέρουν παρενόχληση, εκφοβισμό, χρήση ανάρμοστης γλώσσας, δημοσίευση δυσάρεστου περιεχομένου ή προσκλήσεις για συναντήσεις εκτός παιχνιδιού.
- Απομακρύνετε τα παιδιά σας από το παιχνίδι ή αλλάξτε την ταυτότητά τους, εάν το παιχνίδι ή ο τρόπος που εξελίσσεται σαν κάνει να αισθάνεστε άβολα.

ΧΡΗΣΙΜΕΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΔΙΕΥΘΥΝΣΕΙΣ

Μάθετε περισσότερα για τα διαδικτυακά βιντεοπαιχνίδια και για το σύστημα PEGI:

<http://www.pegi.info/gr/>

<http://www.pegionline.eu/el/>

Ενημερωθείτε για νέα και πληροφορίες σχετικά με τη νόμιμη προσφορά μουσικής στο Διαδίκτυο:

<http://www.pro-music.org>

Βρείτε την άκρη της γλώσσας του chat από τις παρακάτω σελίδες:

<http://www.transl8it.com>

<http://www.netlingo.com>



Γ. Προτεινόμενες λύσεις για τις δραστηριότητες

1. Η ασφάλεια φέρνει σιγουριά



ΣΗΜΕΙΩΣΕΙΣ ΓΙΑ ΤΙΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Αντιστοίχισε τις εικόνες με τις λέξεις: πύργος, mouse pad, οθόνη, ηχεία, κάμερα, εκτυπωτής, συσκευή αποθήκευσης USB, ποντίκι, CD-ROM.

Μια άσκηση ζέσταμα για να εξοικειωθούν τα παιδιά σας με τα διαφορετικά μέρη του υπολογιστή και άλλων σχετικών εξαρτημάτων του συστήματος. Μπορείτε να συνεχίσετε την άσκηση όπως σας φαίνεται κατάλληλο.

Ζήτησε από τους γονείς σου να σου στείλουν ένα ηλεκτρονικό μήνυμα με ένα **συνημμένο αρχείο** ή στείλε στον εαυτό σου ένα. Εξασκήσου στο παρακάτω: κάνε δεξί κλικ επάνω στο αρχείο για να το σώσεις επάνω στην επιφάνεια εργασίας. Πήγαινε στην επιφάνεια εργασίας για να βρεις ξανά το αρχείο, κάνε δεξί κλικ επάνω του και επέλεξε **σάρωση** για να το σαρώσεις για ιούς. Όταν βεβαιωθείς ότι το αρχείο είναι ασφαλές, μπορείς να το ανοίξεις. Θυμήσου: Δεξί κλικ – ΦΥΛΑΞΕ, Δεξί κλικ – ΣΑΡΩΣΕ, Δεξί κλικ – ΑΝΟΙΞΕ.

*Στείλτε ένα μήνυμα στη διεύθυνση του παιδιού σας ή στη δική σας με ένα **συνημμένο αρχείο**. Αφήστε το παιδί σας να ακολουθήσει τις οδηγίες της άσκησης και να σώσει το αρχείο κάνοντας δεξί κλικ επάνω του χωρίς να το ανοίξει. Αφού σώσει το αρχείο στην επιφάνεια εργασίας ή σε ένα φάκελο στον υπολογιστή, δείξτε του πώς να κάνει ακόμη μια φορά δεξί κλικ επάνω στο αρχείο για να το σαρώσει πριν να το ανοίξει. Το παιδί σας θα αποκτήσει έτσι ασφαλείς συνήθειες.*

Ακολούθησε τη συμβουλή της Αθηνάς και μάθε πώς να περιγράψεις τη διεύθυνσή σου όποτε χρειαστεί να τη δημοσιεύσεις. Έτσι θα αποφύγεις τη συλλογή της διεύθυνσής σου από μηχανές και τη μετέπειτα αποστολή πολλών ανεπιθύμητων μηνυμάτων.

Παράδειγμα: marios.gatos@mymail.gr = marios τελεία gatos παπάκι mymail τελεία gr

Για να εξασκηθείς, γράψε με τον παραπάνω τρόπο τις ηλεκτρονικές διευθύνσεις της οικογένειάς σου: τη δική σου, την οικογενειακή, της μητέρας σου, του πατέρα σου.

Για να αποφύγετε την αυτόματη συλλογή της δημόσιας ηλεκτρονικής σας διεύθυνσης από λογισμικά με σκοπό την αποστολή ανεπιθύμητων μηνυμάτων, περιγράψτε την αντί να την αποδώσετε κατά λέξη, όποτε χρειαστείτε να τη δημοσιεύσετε. Αφήστε το παιδί σας να εξασκηθεί στην τεχνική αυτή. Σε κάθε περίπτωση, όμως, να έχετε πάντα στο μυαλό σας ότι το παιδί σας θα πρέπει να αποφεύγει τη δημοσίευση της διεύθυνσής του στο Διαδίκτυο. Ωστόσο, αν είναι αναγκαίο, θα πρέπει να χρησιμοποιεί κάποια ηλεκτρονική διεύθυνση που δεν αποκαλύπτει το ονοματεπώνυμό του (βλ. κεφάλαιο «Επικοινωνία»).

Για να βοηθήσεις τη Ζέτα να καταλάβει καλύτερα τι γίνεται πριν να συνεχίσει η Αθηνά, κοίταξε τις πιο κάτω δραστηριότητες και κύκλωσε αυτές που μπορείς να κάνεις μόνο όταν είσαι συνδεδεμένος/η στο Διαδίκτυο.

Τα πολύ μικρά παιδιά δεν ξέρουν πάντα ποιες δραστηριότητες απαιτούν σύνδεση στο Διαδίκτυο και ποιες όχι. Η γραφή κειμένου δεν απαιτεί σύνδεση, το τσατ όμως, απαιτεί. Μπορεί κανείς να ακούσει μουσική στον υπολογιστή χρησιμοποιώντας ένα CD, ένα αρχείο MP3 ή παρόμοιο, μπορεί, όμως, να ακούσει μουσική και απευθείας από το Διαδίκτυο. Εδώ ζητάμε από τα παιδιά να σημειώσουν μόνο τις δραστηριότητες εκείνες για τις οποίες η σύνδεση στο Διαδίκτυο είναι απολύτως απαραίτητη.

Μαζί με τους γονείς σου, πληκτρολόγησε <http://kids.yahoo.com> στον πλοηγό (browser) του υπολογιστή σου. Ψάξε πληροφορίες για τον Τυραννόσαυρο Ρεξ και προσπάθησε να βρεις πότε έζησε στον πλανήτη Γη. Προσπάθησε, επίσης, να βρεις μια καλή εικόνα για τον Τυραννόσαυρο. Μην ξεχάσεις να συγκρίνεις τουλάχιστον τρεις διαφορετικές ιστοσελίδες.

Μάθετε στα παιδιά σας καλές συνήθειες στην αναζήτηση πληροφοριών θυμίζοντάς τα να μην εμπιστεύονται οτιδήποτε βλέπουν στο Διαδίκτυο. Μάθετέ τα να ψάχνουν και να συγκρίνουν πληροφορίες σε τουλάχιστον 3 ιστοσελίδες και να αναφέρουν πάντα τις πηγές τους όταν γράφουν σχολική εργασία.

Μαζί με τους γονείς σου άνοιξε έναν πλοηγό και πήγαινε στη σελίδα <http://kids.yahoo.com>. Ψάξε μαζί τους για ένα θέμα, όπως για παράδειγμα για τον Τυραννόσαυρο Ρεξ, και φύλαξε τις τρεις καλύτερες ιστοσελίδες στα αγαπημένα σου, από το μενού «Αγαπημένα» (Favorites / Bookmarks) που θα βρεις στην μπάρα εργαλείων του πλοηγού σου. Αν θέλεις, φτιάξε εκεί δικό σου φάκελο.

Σώστε και οργανώστε ενδιαφέρουσες ιστοσελίδες στο φάκελο «Αγαπημένα». Είναι ένας καλός τρόπος να μειώσετε την ανάγκη των παιδιών σας να αναζητούν πληροφορίες στο Διαδίκτυο.

ΤΑ ΚΑΤΑΛΑΒΕΣ ΣΩΣΤΑ;

1: (προστατευμένος) 2: (ιό), (άγνωστος), (κατεβάζοντας), (μολυσμένα), (απροστάτευτο) 3: (παράξενα) 4: (γνωρίζεις), (συνημμένα αρχεία), (τίτλους), (spam) 5: (μοναδική), (ανεπιθύμητων μηνυμάτων / spam) 6: (πρώτη), (τρεις), (σύγκρινε), (οποιοσδήποτε), (δημοσιεύσει) 7: («antivirus»), («antispyware») 8: (μίλησε), (γονείς).

ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ ΓΙΑ ΤΙΣ ΚΑΡΤΕΣ ΠΕΡΙΠΤΩΣΕΩΝ

ΠΕΡΙΠΤΩΣΗ 1. Ποτέ μη χρησιμοποιείτε το Διαδίκτυο εάν ο υπολογιστής σας δεν προστατεύεται από ενημερωμένα προγράμματα προστασίας “antivirus” και “anti-spyware”. Είναι σαν να έχετε σύνορα χωρίς φύλακες. Ο υπολογιστής σας μπορεί να μολυνθεί από βλαβερά προγράμματα, όπως ιούς, δούρειους ίππους, σκουλήκια ή προγράμματα κατασκοπείας

ΠΕΡΙΠΤΩΣΗ 2. Κρατάτε τα μάτια σας ανοιχτά για ηλεκτρονικά μηνύματα που λαμβάνετε από αγνώστους και που περιέχουν συνημμένα αρχεία ή τάζουν λαγούς με πετραχήλια: πολύ πιθανό να πρόκειται για spam! Τα μηνύματα spam μπορούν να μολύνουν τον υπολογιστή σας με βλαβερά προγράμματα όπως ιούς, δούρειους ίππους, σκουλήκια ή προγράμματα κατασκοπείας. Μην ανοίγετε αυτά τα μηνύματα. Αποκλείστε τον αποστολέα κάνοντας δεξί κλικ στο μήνυμα ή απλά σβήστε τα.

ΠΕΡΙΠΤΩΣΗ 3. Όταν ψάχνετε πληροφορίες στο Διαδίκτυο, μην εμπιστεύεστε την πρώτη καλή σελίδα που θα βρείτε. Ελέγξτε τουλάχιστον τρεις διαφορετικές πηγές και συγκρίνετε τις πληροφορίες. Να θυμάστε ότι οποιοσδήποτε με πρόσβαση στο Διαδίκτυο μπορεί να δημιουργήσει και να δημοσιεύσει υλικό. Όταν κάνετε κάποια εργασία, πρέπει πάντα να αναφέρετε τις πηγές σας, δηλαδή πού βρήκατε τις πληροφορίες και τις φωτογραφίες που χρησιμοποιήσατε. Αυτό θα έκανε και ένας αληθινός επιστήμονας.

2. Επικοινωνία LoL ;-D



ΣΗΜΕΙΩΣΕΙΣ ΓΙΑ ΤΙΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Σημείωσε πόσο **προσωπικά** είναι τα παρακάτω για σένα: το τηλέφωνό σου, το χρώμα των μαλλιών σου, το όνομά σου, η χώρα που μένεις, το σχολείο σου, η διεύθυνσή σου, το όνομα του κατοικίδιού σου, τα επαγγέλματα των γονιών σου, η ηλεκτρονική σου διεύθυνση, οι φωτογραφίες σου, η ηλικία σου.

Έχουν τα παιδιά σας την ίδια αίσθηση της ιδιωτικότητας όπως εσείς; Τα τρία χρώματα συμβολίζουν τις πολύ προσωπικές (κόκκινο), τις αρκετά προσωπικές (πορτοκαλί) και τις όχι και τόσο προσωπικές πληροφορίες (πράσινο).

Βοήθησε τη Ζέτα να φτιάξει έναν ασφαλή κωδικό πρόσβασης ακολουθώντας τις συμβουλές της Αθηνάς.

Οι καλοί κωδικοί θα πρέπει να αποτελούνται από έναν τυχαίο συνδυασμό χαρακτήρων (αριθμών, γραμμάτων και σημείων στίξης) και θα πρέπει πάντα να μένουν μυστικοί.

Ακολούθησε το παράδειγμα της Ζέτας και φτιάξε ένα ασφαλές προφίλ. Έπειτα φτιάξε ένα παράδειγμα μη ασφαλούς προφίλ.

Αφήστε το παιδί σας να φτιάξει αρχικά ένα ασφαλές προφίλ και ακολούθως ένα λιγότερο ασφαλές που αποκαλύπτει προσωπικά στοιχεία. Θυμίστε στο παιδί σας ότι ένα ασφαλές προφίλ δεν είναι αρκετό για την προστασία του, εάν δεν προστατεύει την προσωπική του ζωή όταν επικοινωνεί μέσω του Διαδικτύου.

Παρατήρησε αυτήν την εικόνα και σημείωσε τι μπορείς να πεις για αυτό το άτομο.

Τι είδους προσωπικές πληροφορίες μπορεί κανείς να αντλήσει από μια φωτογραφία; Τα παιδιά δεν αντιλαμβάνονται πάντα τη δύναμη των φωτογραφιών.

Ακολούθησε την ιδέα της Ζέτας και σκέψου 3 συμβουλές που θα έδινε η Αθηνά στον «Αλέξη κοκκίνοσκουφίτσο» για να φυλάγεται από τους λύκους του Διαδικτύου.

Ελέγξτε εάν τα παιδιά σας έχουν καταλάβει ότι η επικοινωνία με αγνώστους στο Διαδίκτυο μπορεί να ενέχει κινδύνους.

Πώς θα ήθελες να σου συμπεριφέρονται οι άλλοι στο Διαδίκτυο (1..... 2..... 3.....);

Βεβαιωθείτε ότι τα παιδιά σας καταλαβαίνουν πως θα πρέπει να συμπεριφέρονται στους άλλους όπως θα επιθυμούσαν να τους συμπεριφέρονται αυτοί.

ΣΠΑΣΕ ΤΟΝ ΚΩΔΙΚΑ: Ανακάλυψε τι σημαίνουν τα πιο δημοφιλή ακρωνύμια, ενώνοντάς τα με τη σωστή εξήγηση στη δεύτερη στήλη.

Βελτιώστε τη γνώση σας σχετικά με τα ακρωνύμια που χρησιμοποιούνται στο τσατ ανατρέχοντας στο κεφάλαιο «Επικοινωνία - Κανόνες Συμπεριφοράς (Ετικέτα) στο Διαδίκτυο, η Γλώσσα του τσατ».

Χρησιμοποίησε συνδυασμούς στο πληκτρολόγιό σου για να συμβολίσεις τα παρακάτω emoticons: Χαμογελαστό πρόσωπο – Λυπημένο πρόσωπο – Κλείνοντας το μάτι – Έκπληξη – Μεγάλο χαμόγελο – Γλώσσα έξω.

Ανατρέξτε στο κεφάλαιο «Επικοινωνία - Κανόνες Συμπεριφοράς (Ετικέτα) στο Διαδίκτυο, η Γλώσσα του τσατ» για περισσότερες πληροφορίες.

ΤΑ ΚΑΤΑΛΑΒΕΣ ΣΩΣΤΑ;

1: (προφίλ) 2: (ιδιωτικής ζωής), (υπεύθυνοι) 3: (αγνώστους), (ενημερώνεις) 4: (Ετικέτα), (φέρονται) 5: (emoticon) 6: (κωδικός πρόσβασης) 7: (κρυφός) 8: (αρνούμαι) 9: (γνωρίζω)

ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ ΓΙΑ ΤΙΣ ΚΑΡΤΕΣ ΠΕΡΙΠΤΩΣΕΩΝ

ΠΕΡΙΠΤΩΣΗ 4. Όταν χρησιμοποιείτε το Διαδίκτυο, οι πληροφορίες που δίνετε για τον εαυτό σας, στο προφίλ σας για παράδειγμα, μπορούν να φτάσουν σε δεκάδες, εκατοντάδες, χιλιάδες ή ακόμη εκατομμύρια ανθρώπων. Για αυτό, θα πρέπει να επιλέγετε με προσοχή τις πληροφορίες που μοιράζεστε. Φροντίστε να μοιράζεστε προσωπικά σας στοιχεία μόνο με άτομα που ξέρετε καλά και εμπιστεύεστε εκτός Διαδικτύου.

ΠΕΡΙΠΤΩΣΗ 5. Ο Μιχάλης μάλλον μοιράστηκε τον κωδικό του ηλεκτρονικού του ταχυδρομείου με τον φίλο του που αποφάσισε να τον εκδικηθεί, στέλνοντας μηνύματα εκ μέρους του. Για αυτό, είναι σημαντικό να κρατάτε τους κωδικούς σας μυστικούς, εκτός και αν δεν σας ενοχλεί να μπορούν τρίτοι να διαβάζουν τα προσωπικά σας μηνύματα, ή να προσποιούνται ότι είναι εσείς και να λένε πράγματα για λογαριασμό σας που ποτέ δεν θα λέγατε!

ΠΕΡΙΠΤΩΣΗ 6. Η συνάντηση με κάποιον άγνωστο δεν είναι πολύ καλή ιδέα. Αν όμως πραγματικά πιστεύετε ότι μπορείτε να εμπιστευτείτε κάποιον που γνωρίσατε στο Διαδίκτυο και που θέλει να σας γνωρίσει, μιλήστε στους γονείς σας για να σας συνοδεύσουν. Κανένας αληθινός φίλος με ειλικρινείς προθέσεις δεν θα είχε πρόβλημα με κάτι τέτοιο. Μόνο ένα άτομο που θέλει να κρύψει κάτι θα είχε πρόβλημα.

3. Ηλεκτρονική παρενόχληση



ΣΗΜΕΙΩΣΕΙΣ ΓΙΑ ΤΙΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Ζωγράφισε την πρόσκληση που έλαβε ο Αλέξης από το σχολείο του. Δημιούργησε το λογότυπο και το σύνθημα που χρησιμοποιεί το σχολείο για την «εβδομάδα κατά της παρενόχλησης».

Αφήστε τα παιδιά σας να δημιουργήσουν μέσα στο κενό πλαίσιο.

Ακολούθησε το παράδειγμα του Αλέξη και δώσε πέντε πιθανούς λόγους για τους οποίους θα έδινες “κόκκινη κάρτα” σε κάποιον.

Συζητήστε με τα παιδιά σας τι είδους συμπεριφορά θεωρούν απαράδεκτη.

ΤΑ ΚΑΤΑΛΑΒΕΣ ΣΩΣΤΑ;

1: (δίκαια), (Χαλάει) 2: (μιλάμε) 3: (καλός) 4: (Ηλεκτρονική παρενόχληση) 5:(Μπλοκάρω)
6: (γνωρίζω) 7: (απαντούσα)

ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ ΓΙΑ ΤΙΣ ΚΑΡΤΕΣ ΠΕΡΙΠΤΩΣΕΩΝ

ΠΕΡΙΠΤΩΣΗ 7. Αυτός ο τρόπος χρήσης του κινητού τηλεφώνου είναι ανεπίτρεπτος. Μην κυκλοφορείτε μηνύματα, εικόνες ή άλλο υλικό που θα μπορούσε να πληγώσει κάποιον. Να φέρεστε πάντα στους άλλους όπως θα θέλατε να σας φέρονται. Σε μια τέτοια περίπτωση, μιλήστε με τους γονείς σας ή με κάποιον άλλον ενήλικα εμπιστοσύνης.

ΠΕΡΙΠΤΩΣΗ 8. Ο Αλέξης θα πρέπει να πει στον φίλο του ότι δε φταίει αυτός για την παρενόχληση. Επίσης, ο Αλέξης πρέπει να συμβουλευτεί το φίλο του να μην απαντά στα μηνύματα αυτά, αλλά να τα κρατήσει σαν απόδειξη και να τα δείξει στους γονείς ή στους δασκάλους του. Ο Αλέξης θα πρέπει επίσης να μιλήσει και στους δικούς του γονείς, για να τον βοηθήσουν να στηρίξει τον φίλο του.

ΠΕΡΙΠΤΩΣΗ 9. Η Επικέτα του Διαδικτύου μας προτρέπει να συμπεριφερόμαστε στους άλλους όπως θα θέλαμε να μας φέρονται. Σίγουρα τώρα ξέρετε αρκετά για να βοηθήσετε τη Ζέτα.

4. Διασκέδαση και κατέβασμα αρχείων



ΣΗΜΕΙΩΣΕΙΣ ΓΙΑ ΤΙΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Άνοιξε την αγαπημένη σου μηχανή αναζήτησης. Πληκτρολόγησε “δωρεάν μελωδίες κλήσης” ή “δωρεάν παιχνίδια” και κοίταξε τα αποτελέσματα αναζήτησης. Έλεγξε μερικές από τις ιστοσελίδες που βρήκες. Μπορείς να εντοπίσεις παγίδες;

Εξασκηθείτε κάνοντας αναζήτηση με τις προτεινόμενες λέξεις-κλειδιά και ελέγξτε εάν μπορείτε να βρείτε τις διαφημιστικές παγίδες στις ιστοσελίδες των αποτελεσμάτων. Δείτε πώς οι πληροφορίες με ψιλά γράμματα δεν αναφέρονται στα διαφημιστικά αλόγκα.

Ποιο είναι το αγαπημένο σου ηλεκτρονικό παιχνίδι; Έλεγξε αν οι γονείς σου το γνωρίζουν και μπορούν να το περιγράψουν. Εάν δεν έχουν ιδέα, εξήγησέ τους το και στη συνέχεια ζήτησέ τους να σου γράψουν μια μικρή περιγραφή. Τι βαθμό τους δίνεις με άριστα το δέκα; .../10. Οι γονείς γράφουν περιλήψη για το αγαπημένο παιχνίδι του παιδιού τους, το παιδί ζωγραφίζει μια χαρακτηριστική εικόνα.

Γνωρίζετε πραγματικά τι είδους διαδικτυακά παιχνίδια παίζουν τα παιδιά σας; Γνωρίζετε ποιο παιχνίδι είναι το αγαπημένο τους; Αφήστε τα παιδιά σας να ελέγξουν τις γνώσεις σας!

ΤΑ ΚΑΤΑΛΑΒΕΣ ΣΩΣΤΑ;

1: (δωρεάν) 2: (φόρμες) 3: (παγίδες). 4: (παράνομα) 5: (X) 6: (αγνοείς). 7: (προσωπικά δεδομένα) 8: (συμβουλευέσαι) 9: (κατεβάζεις)

ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΛΥΣΕΙΣ ΓΙΑ ΤΙΣ ΚΑΡΤΕΣ ΠΕΡΙΠΤΩΣΕΩΝ

ΠΕΡΙΠΤΩΣΗ 10. Τα ηλεκτρονικά ερωτηματολόγια μπορούν να είναι πολύ χρήσιμα για να αφουγκραστούν τη γνώμη μας. Παρόλα αυτά, εάν συλλέγονται προσωπικές πληροφορίες, θα πρέπει να αναγράφεται ευκρινώς ο σκοπός. Συμβουλευέστε τα παιδιά σας να συμπληρώνουν ηλεκτρονικές φόρμες μόνο όταν γνωρίζουν τον απώτερο σκοπό. Ακόμη και τότε, όμως, θα πρέπει να είναι πολύ προσεκτικά στη δημοσίευση προσωπικών στοιχείων (βλ. κεφάλαιο «Επικοινωνία»).

ΠΕΡΙΠΤΩΣΗ 11. Υπάρχουν δωρεάν υπηρεσίες στο Διαδίκτυο, ωστόσο, οι μελωδίες κλήσης, τα MP3s, τα φόντα επιφάνειας εργασίας, τα εικονίδια και άλλα συναφή σχεδόν ποτέ δεν είναι δωρεάν. Εάν ο Αλέξης ρίξει μια καλύτερη ματιά σε αυτή τη σελίδα, μάλλον θα ανακαλύψει κάποια ψιλά γράμματα που φανερώνουν το πραγματικό κόστος της υπηρεσίας. Οι μελωδίες κλήσης, τα κουίζ, τα παιχνίδια και τα συναφή ξεγελούν εύκολα κόσμο να εγγραφεί σε δήθεν δωρεάν υπηρεσίες που στην πραγματικότητα κοστίζουν χρήματα.

ΠΕΡΙΠΤΩΣΗ 12. Ο Αλέξης θα πρέπει να κρατά την ταυτότητά του απόρρητη όταν παίζει παιχνίδια στο Διαδίκτυο με παίκτες που δεν γνωρίζει εκτός Διαδικτύου. Δεν θα πρέπει να δίνει πληροφορίες όπως επώνυμο, διεύθυνση σπιτιού ή σχολείου, κτλ. Θα πρέπει, επίσης, να ενημερώνει τους γονείς του για τα παιχνίδια που παίζει και να μην κατεβάζει ποτέ παιχνίδια από το Διαδίκτυο χωρίς πρώτα να τους ενημερώσει. Πολλά από τα παιχνίδια που βρίσκονται στο Διαδίκτυο περιέχουν ιούς και άλλα κακόβουλα προγράμματα που μπορούν να βλάψουν τον υπολογιστή του.



Δ. Γλωσσάρι

Αγαπημένα: ένας φάκελος του πλοηγού σας (browser) όπου μπορείτε να αποθηκεύσετε ενδιαφέροντες συνδέσμους (ιστοσελίδες) ως «σελιδοδείκτες». Οι σελιδοδείκτες μπορούν να οργανωθούν σε υποφάκελους και να περιγραφούν με ηλεκτρονικές ετικέτες (tag) για καλύτερη οργάνωση και ευκολότερη αναζήτηση.

Ακρωνύμιο: συντομογραφία που αποτελείται από τα πρώτα γράμματα από κάθε λέξη μιας φράσης ή έκφρασης. Τα ακρωνύμια χρησιμοποιούνται συχνά στα τσάτ για ταχύτερη επικοινωνία (βλέπε κεφάλαιο «Επικοινωνία»).

Άμεσο Μήνυμα (Instant Messaging/IM): μια μορφή άμεσης και ταυτόχρονης ηλεκτρονικής επικοινωνίας μεταξύ δύο ή περισσότερων χρηστών. Το IM σας επιτρέπει να επικοινωνείτε με μια λίστα επαφών που καθορίζετε οι ίδιοι και να βλέπετε τότε οι άνθρωποι στη λίστα των επαφών σας είναι συνδεδεμένοι.

Αναδυόμενο παράθυρο (pop-up window): ένα παράθυρο που εμφανίζεται ξαφνικά, κατά την επίσκεψη σε μια ιστοσελίδα ή πατώντας ένα ειδικό πλήκτρο λειτουργίας. Συνήθως, τα παράθυρα αυτά περιλαμβάνουν ένα μενού εντολών και παραμένουν ανοιχτά μέχρι να επιλέξετε μια από τις εντολές ή να το κλείσετε κάνοντας κλικ στην επάνω δεξιά γωνία.

Αναφορά (report): λειτουργία που επιτρέπει στους χρήστες να αναφέρουν ένα πρόβλημα στους διαχειριστές του εκάστοτε διαδικτυακού χώρου, είτε αυτό είναι τεχνικό, είτε αφορά κακή συμπεριφορά άλλων χρηστών, παράνομο περιεχόμενο, κλπ.

Ανεπιθύμητη αλληλογραφία (spam ή junk): ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, συνήθως εμπορικού χαρακτήρα, που αποστέλλονται μαζικά. Η αποστολή spam είναι παράνομη και πολύ ενοχλητική, αποτελεί δε μια από τις πιο γνωστές παραβιάσεις που λαμβάνουν χώρα στο Διαδίκτυο. Παρόλα αυτά, δεδομένου ότι το Διαδίκτυο είναι δημόσιος χώρος, είναι δύσκολο να εξαλειφθεί η ανεπιθύμητη αλληλογραφία.

Ανταλλαγή αρχείων: απευθείας ανταλλαγή αρχείων μεταξύ χρηστών διαδικτυακών υπηρεσιών. Ο όρος αναφέρεται στην προσφορά αρχείων σε άλλους χρήστες (ανέβασμα/uploading) και την αντιγραφή διαθεσίμων αρχείων από το Διαδίκτυο σε έναν υπολογιστή (κατέβασμα/downloading). Συνήθως τα αρχεία ανταλλάσσονται μέσω δικτύων P2P (peer-to-peer).

Αρχείο (ηλεκτρονικό): αρχείο / συλλογή σχετικών πληροφοριών (εγγράφων, προγραμμάτων, κλπ.) τα οποία αποθηκεύονται σε υπολογιστή με ένα συγκεκριμένο όνομα. Τα ηλεκτρονικά αρχεία χρησιμοποιούνται για την οργάνωση πληροφοριών και μπορούν να θεωρηθούν ως το αντίστοιχο των έντυπων εγγράφων που φυλάσσονται στα γραφεία και τα αρχεία βιβλιοθηκών.

Αρχική σελίδα (homepage): είναι η ιστοσελίδα που φορτώνει αυτόματα κατά την εκκίνηση ενός πλοηγού. Ο όρος χρησιμοποιείται επίσης και για την αναφορά στην αρχική σελίδα ή την κύρια ιστοσελίδα ενός δικτυακού τόπου.

Γονικός έλεγχος: βλέπε οικογενειακές ρυθμίσεις.

Γραμμή αναφοράς (hotline): τηλεφωνική γραμμή ή ηλεκτρονική υπηρεσία (web-based), όπου μπορεί κανείς να αναφέρει πιθανό παράνομο περιεχόμενο ή / και παράνομη χρήση του Διαδικτύου. Οι γραμμές αναφοράς πρέπει να είναι αποτελεσματικές, με διαφανείς διαδικασίες για την εξέταση των καταγγελιών και να έχουν την υποστήριξη της κυβέρνησης, της βιομηχανίας, του νομικού συστήματος, καθώς και των χρηστών του Διαδικτύου στη χώρα λειτουργίας τους. Για την Ελλάδα η γραμμή αναφοράς είναι η Ανοιχτή Γραμμή Safeline.gr

Γραμμή βοήθειας (helpline): ηλεκτρονική ή/και τηλεφωνική υπηρεσία που παρέχεται σε πολλές χώρες από φορείς προστασίας των παιδιών και μέλη του δικτύου Insafe. Τα παιδιά μπορούν να αναφέρουν στη Γραμμή τις ανησυχίες τους σχετικά με παράνομο και επιβλαβές περιεχόμενο, ή σχετικά με δυσάρεστες / τρομακτικές εμπειρίες που σχετίζονται με τη χρήση του Διαδικτύου και των κινητών τηλεφώνων. Για την Ελλάδα, η Γραμμή Βοήθειας είναι η ΥποΣΤΗΡΙΖΩ: τηλ. 800 11 800 15 / email: help@safefinternet.gr. Η Γραμμή υλοποιείται από τη Μονάδα Εφηβικής Υγείας, της Β' Παιδιατρικής Κλινικής του Πανεπιστημίου Αθηνών.

Διαδίκτυο: ένα παγκόσμιο δίκτυο αποτελούμενο από υπο-δίκτυα υπολογιστών μέσω των οποίων πραγματοποιείται διαβίβαση και ανταλλαγή δεδομένων. Το Διαδίκτυο αποτελείται από μικρότερα δίκτυα, οικιακά, ακαδημαϊκά, επιχειρηματικά και κυβερνητικά τα οποία παρέχουν διάφορες υπηρεσίες, όπως πληροφόρηση, ηλεκτρονικό ταχυδρομείο, τσατ, μεταφορά αρχείων, κλπ.

Δίκτυο P2P: ένα δίκτυο υπολογιστών peer-to-peer (P2P) επιτρέπει σε όσους είναι συνδεδεμένοι με αυτό να ανταλλάσσουν αρχεία, ανεβάζοντας και κατεβάζοντάς τα (βλέπε ορισμό). Τα δίκτυα P2P είναι ένας από τους πολλούς τρόπους που υπάρχουν για διάθεση αρχείων για κοινή χρήση στο Διαδίκτυο. Ορισμένες υπηρεσίες κοινής χρήσης αρχείων P2P είναι παράνομες.

Δοκιμαστικό λογισμικό: λογισμικό που μπορείτε να δοκιμάσετε πριν το αγοράσετε. Οι δοκιμαστικές εκδόσεις ενός λογισμικού περιλαμβάνουν συνήθως όλες τις λειτουργίες της τακτικής έκδοσης, απλά η χρήση τους είναι χρονικά περιορισμένη.

Δούρειοι ίπποι: βλαβερά λογισμικά, τα οποία μπορούν να εισέλθουν στον υπολογιστή σας κρυμμένα πίσω από φαινομενικά αβλαβή προγράμματα, όπως παιχνίδια ή ακόμα και προγράμματα ανίχνευσης ιών. Οι δούρειοι ίπποι δεν πολλαπλασιάζονται από μόνοι τους. Συνήθως είναι σχεδιασμένοι για να αποκτήσουν πρόσβαση σε ή να καταστρέψουν ευαίσθητα δεδομένα, ακόμη και να διαγράψουν έναν σκληρό δίσκο ή να υποκλέψουν εμπιστευτικές πληροφορίες.

Εγγραφή: η εγγραφή σε μια ηλεκτρονική υπηρεσία (κοινωνικής δικτύωσης, φόρουμ, ηλεκτρονικό

ταχυδρομείου, τσατ, ηλεκτρονικού περιοδικού, κλπ.). Κανονικά, οι χρήστες θα πρέπει να έχουν τη δυνατότητα να απουσυνδεθούν ή να τερματίσουν την εγγραφή όποτε το θελήσουν.

Ειδοποίηση: ένα μικρό παράθυρο που εμφανίζεται στην οθόνη και παρέχει πληροφορίες ή προειδοποιήσεις σχετικά με ενδεχόμενες επιζήμιες λειτουργίες, π.χ. νέο μήνυμα ή την κατάσταση της προστασίας του συστήματος σας από ιούς.

Εικονική κτήση: ένα σύνολο αντικειμένων τα οποία έχουν μεταβιβαστεί στον παίκτη ενός παιχνιδιού. Ο κάθε παίκτης έχει εικονική κτήση του συνόλου των αντικειμένων του, τα οποία παρουσιάζονται μέσω ενός τερματικού κάποιου υπολογιστή.

Εκφοβισμός (bullying): παρενόχληση μέσω επαναλαμβανόμενων απειλών, σεξουαλικών νύξων, σωματικών επιθέσεων, κλπ. που διαπράττονται από ένα ή περισσότερα άτομα.

Επεξεργαστής: η Μονάδα Κεντρικής Επεξεργασίας (CPU) είναι το τμήμα του υπολογιστή που επεξεργάζεται δεδομένα, παράγει σήματα ελέγχου, και καταχωρεί αποτελέσματα. Μαζί με τη μνήμη του υπολογιστή αποτελεί την κεντρική μονάδα του υπολογιστή.

Επιβλαβές λογισμικό: Λογισμικό με στόχο τη διεύθυνση σε σύστημα υπολογιστή χωρίς τη συγκατάθεση του ιδιοκτήτη και με κακόβουλες προθέσεις. Τα παρακάτω αποτελούν παραδείγματα επιβλαβούς λογισμικού: ιοί υπολογιστών, σκουλήκια, δούρειοι ίπποι, λογισμικά κατασκοπείας, κτλ.

Επιβλαβές περιεχόμενο: φωτογραφίες, κείμενα, έγγραφα, κλπ., το περιεχόμενο των οποίων είναι δυνατόν να προκαλέσει βλάβη στους ανήλικους χρήστες. Για παράδειγμα, οι εικόνες βίας είναι ακατάλληλες και επιζήμιες για τον ψυχισμό παιδιών και ανηλικών.

Ηλεκτρονική διεύθυνση: μια εικονική διεύθυνση στην οποία μπορούν να παραδοθούν μηνύματα ηλεκτρονικού ταχυδρομείου. Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου αποτελούνται από δύο μέρη που χωρίζονται με το σύμβολο @ (παπάκι).

Ηλεκτρονικό μήνυμα: ένα μέσο ηλεκτρονικής γραπτής επικοινωνίας, που σας επιτρέπει να στείλετε μηνύματα και να προσθέσετε, εάν θέλετε, διαφόρων ειδών συνημμένα ηλεκτρονικά αρχεία, όπως κείμενα, εικόνες, ήχο, κτλ.

Ηλεκτρονική παρενόχληση και εκφοβισμός (cyberbullying): αναφέρεται σε παρενόχληση μέσω ηλεκτρονικών μέσων, συνήθως άμεσων μηνυμάτων και ηλεκτρονικού ταχυδρομείου. Η παρενόχληση μπορεί να περιλαμβάνει επαναλαμβανόμενες απειλές, σεξουαλικά σχόλια, και υποτιμητικές ομιλίες. Οι θύτες ενίοτε δημοσιεύουν τα προσωπικά στοιχεία των θυμάτων τους ή διαπράττουν πράξεις και δημοσιεύουν υλικό στο όνομά τους με σκοπό τη δυσφήμιση ή τη γλειοποίηση τους.

Ηλεκτρονική φόρμα: ένα διαμορφωμένο έγγραφο που περιέχει κενά πεδία τα οποία μπορείτε να συμπληρώσετε με διάφορα στοιχεία. Η ηλεκτρονική φόρμα - έντυπο μπορεί να συμπληρωθεί με ελεύθερο κείμενο ή επιλέγοντας στοιχεία που προσφέρονται σε μορφή μενού (drop-downs). Μετά την υποβολή τους, τα δεδομένα αποστέλλονται σε μια εφαρμογή που τα επεξεργάζεται και τα αποθηκεύει σε βάση δεδομένων.

Θύρα: μια διασύνδεση του υπολογιστή η οποία χρησιμοποιείται για σύνδεση με μια άλλη συσκευή. Οι θύρες μπορεί να είναι εσωτερικές ή εξωτερικές. Οι εσωτερικές θύρες συνδέονται σε ένα δίσκο ή ένα δίκτυο, ενώ οι εξωτερικές συνδέονται με μια περιφερειακή συσκευή, όπως έναν εκτυπωτή ή ένα πληκτρολόγιο.

Ιός: ένα είδος κακόβουλου λογισμικού που διαδίδεται με τη μεσολάβηση των χρηστών. Συχνά

μεταδίδεται μέσω συνημμένων αρχείων ηλεκτρονικού ταχυδρομείου, αλλά και μολυσμένων συσκευών αποθήκευσης USB και CD-ROM.

Δωμάτια ανοιχτής επικοινωνίας (chat room): δημόσιος εικονικός χώρος για επικοινωνία σε πραγματικό χρόνο μέσω υπολογιστή συνδεδεμένου στο Διαδίκτυο. Αν τα παιδιά σας χρησιμοποιούν chat rooms, φροντίστε να είναι σχεδιασμένα ειδικά για την ηλικία τους και να διαθέτουν επίπτες και συντονιστές.

Ιστοσελίδα: ένας ηλεκτρονικός τόπος του Παγκόσμιου Ιστού, του World Wide Web. Κάθε ιστοσελίδα περιέχει μια αρχική σελίδα, η οποία είναι το πρώτο έγγραφο που βλέπετε όταν εισέρχεστε σε αυτήν. Οι ιστοσελίδες συνήθως περιέχουν συνδέσμους προς άλλες σελίδες και αρχεία. Οι ιστοσελίδες ανήκουν και ενημερώνονται από ιδιώτες, εταιρείες ή οργανισμούς.

Ιστοσελίδες κοινωνικής δικτύωσης: εικονικές πλατφόρμες ανοιχτές σε κοινότητες μελών με κοινά ενδιαφέροντα. Τα μέλη πρέπει να δημιουργήσουν προφίλ χρήστη. Με τη χρήση των διαφόρων εργαλείων που προσφέρονται στις ηλεκτρονικές αυτές πλατφόρμες, οι χρήστες μπορούν να αναρτούν κείμενα, εικόνες ή άλλα αρχεία, να γράφουν μηνύματα σε πίνακες μηνυμάτων και να λαμβάνουν μέρος σε φόρουμ. Πολλές ιστοσελίδες κοινωνικής δικτύωσης παρέχουν ειδικές ρυθμίσεις ασφάλειας. Επίσης πολλές από αυτές απαγορεύουν ρητά την πρόσβαση σε παιδιά κάτω των 13 ετών.

Ιδιωτικότητα: η ικανότητα ενός ατόμου ή μιας ομάδας να ελέγχουν την ροή των προσωπικών τους πληροφοριών και ως εκ τούτου να αποκαλύπτουν προσωπικά στοιχεία μόνο όταν θέλουν. Η προστασία της ιδιωτικής ζωής συνδέεται μερικές φορές με την ανωνυμία, την επιθυμία να μείνει κανείς απαρατήρητος σε δημόσιο χώρο.

Κάδος ανακύκλωσης: ένας κατάλογος του υπολογιστή όπου τα διαγραμμένα αρχεία αποθηκεύονται προσωρινά πριν διαγραφούν οριστικά από τους χρήστες. Πρέπει να αδειάζετε τακτικά τον κάδο ανακύκλωσης για να ελευθερώσετε χώρο στον σκληρό δίσκο, την εσωτερική μνήμη του υπολογιστή σας.

Κάμερα υπολογιστή: μια κάμερα που χρησιμοποιείται για να μεταδίδει εικόνες μέσω Διαδικτύου, για παράδειγμα μέσω υπηρεσιών άμεσης επικοινωνίας, τηλεσυνεδριάσεων, τσατ, κλπ. Οι κάμερες με διαδικτυακή πρόσβαση περιλαμβάνουν μια ψηφιακή φωτογραφική μηχανή η οποία φορτώνει φωτογραφίες σε ένα διακομιστή Διαδικτύου, συνεχώς, ή σε τακτά χρονικά διαστήματα.

Κατάλογος: μια οργανωτική μονάδα, την οποία χρησιμοποιεί ο υπολογιστής σας για να οργανώσει τους φακέλους και τα αρχεία σας ιεραρχικά, π.χ. Τα έγγραφά μου, Οι εικόνες μου, κλπ.

Κατάλογος επαφών: η συλλογή των επαφών σε προγράμματα ηλεκτρονικού ταχυδρομείου, εφαρμογές instant messaging, διαδικτυακά παιχνίδια, κινητά τηλέφωνα, κλπ. Οι επαφές μπορούν να προστεθούν, να απορριφθούν και να διαγραφούν.

Κατέβασμα: αναφέρεται στη διαδικασία της αντιγραφής ενός αρχείου από μια διαδικτυακή υπηρεσία σε έναν υπολογιστή.

Κινητό: μια ηλεκτρονική συσκευή τηλεπικοινωνιών, γνωστή και ως κινητό τηλέφωνο, κινητό, GSM, smart-phone, handphone. Έχει την ίδια βασική ικανότητα όπως και μια συμβατική σταθερή τηλεφωνική γραμμή. Σήμερα τα περισσότερα κινητά έχουν ενσωματωμένη φωτογραφική μηχανή και πολλά προσφέρουν δυνατότητα πρόσβασης στο Διαδίκτυο (παροχή υπηρεσιών επί πληρωμή).

Κλοπή ταυτότητας: κλοπή προσωπικών στοιχείων (π.χ. ονόματος, ημερομηνίας γέννησης, αριθμού πιστωτικής κάρτας) και παράνομη χρήση τους.

Κοινωνική δικτύωση: διαδικτυακές κοινότητες με μέλη, τα οποία μπορούν μέσω της χρήσης κατάλληλου λογισμικού να μοιράζονται κοινά ενδιαφέροντα, να επικοινωνούν και να κοινωνικοποιούνται σε απευθείας σύνδεση (βλ. ιστοσελίδες κοινωνικής δικτύωσης).

Κωδικός πρόσβασης: μια μυστική σειρά χαρακτήρων που επιτρέπει στον δικαιούχο να αποκτήσει πρόσβαση σε ένα αρχείο, υπολογιστή, λογαριασμό ή πρόγραμμα. Ο κωδικός πρόσβασης αποτελεί μέτρο ασφάλειας και προστασίας από χρήστες χωρίς άδεια πρόσβασης και με ενδεχόμενες κακές προθέσεις (βλέπε κεφάλαιο «Επικοινωνία»).

Λειτουργικό σύστημα: ένα πρόγραμμα που εκτελεί τις βασικές λειτουργίες ενός υπολογιστή και που στηρίζει τη λειτουργία των διαφόρων λογισμικών. Γνωστά παραδείγματα είναι τα Windows, Linux και Mac OS.

Λογαριασμός: για να χρησιμοποιήσετε μια ηλεκτρονική υπηρεσία, θα πρέπει να ανοίξετε ένα λογαριασμό χρήστη με όνομα και κωδικό πρόσβασης. Το λειτουργικό σύστημα του υπολογιστή σας, σας επιτρέπει να δημιουργήσετε ξεχωριστούς λογαριασμούς για κάθε μέλος της οικογένειας που θα χρησιμοποιεί τον υπολογιστή.

Λογισμικό: βλέπε ορισμό για πρόγραμμα υπολογιστή.

Λογισμικό ασφάλειας (firewall): συσκευή (ενσωματωμένη στο δρομολογητή σας), ή λογισμικό (εγκατεστημένο στον υπολογιστή σας) που διαθέτει ρυθμίσεις για την προστασία ενός υπολογιστή ή ενός δικτύου υπολογιστών συνδεδεμένου στο Διαδίκτυο από χρήστες με κακόβουλες προθέσεις (όπως για παράδειγμα χάκκερ και cracker, βλ. ορισμούς).

Λογισμικό: βλέπε ορισμό για πρόγραμμα υπολογιστή.

Λογισμικό κατασκοπείας (spyware): κακόβουλο λογισμικό το οποίο μπορεί να κρύβεται σε αρχεία τα οποία κατεβάζετε από το Διαδίκτυο και να εγκατασταθεί στον υπολογιστή σας για να παρακολουθεί τη δραστηριότητά του. Το κατασκοπικό λογισμικό στέλνει τις πληροφορίες σε τρίτους, συχνά εταιρείες οι οποίες ενδιαφέρονται για τη δημιουργία προσωπικών προφίλ χρήστη για την αποστολή διαφημιστικού υλικού ή άλλων πληροφοριών, ή άτομα με στόχο την παράνομη εισβολή σε συστήματα υπολογιστών και υποκλοπή προσωπικών δεδομένων.

Μαζικά διαδικτυακά παιχνίδια ρόλων (massively multiplayer online role-playing games): παιχνίδια που προσφέρουν ένα πλούσιο τρισδιάστατο κόσμο και φιλοξενούν χιλιάδες παίκτες, οι οποίοι παίζουν μεταξύ τους αναλαμβάνοντας ρόλους εικονικών χαρακτήρων. Παράδειγμα αποτελούν τα παιχνίδια ρόλων, όπου οι συμμετέχοντες δημιουργούν ιστορίες και πλοκές από κοινού.

Μελωδία (ήχος) κλήσης: ο ήχος που παράγει το κινητό τηλέφωνο στις εισερχόμενες κλήσεις. Υπάρχει μια μεγάλη ποικιλία προσαρμοσμένων ήχων και μουσικής, τα οποία οι ιδιοκτήτες κινητών τηλεφώνων μπορούν να κατεβάσουν από το Διαδίκτυο, συνήθως με χρέωση.

Μεταφορά αρχείων: η αποστολή αρχείων μέσω δικτύου υπολογιστών. Η μεταφορά αρχείων αναφέρεται συνήθως ως ανέβασμα και κατέβασμα (αρχείων).

Μηχανή αναζήτησης: εργαλείο για την αναζήτηση πληροφοριών που περιέχονται στις ιστοσελίδες. Οι πιο γνωστές μηχανές αναζήτησης είναι οι Google, Yahoo και MSN Search. Οι μηχανές αναζήτησης έχουν προηγμένες ρυθμίσεις οι οποίες μπορεί να περιλαμβάνουν ενδιαφέρουσες ρυθμίσεις ασφάλειας.

Μπάρα Εργαλείων: ένα σύνολο εικόνων ή κουμπιών, τα οποία είναι μέρος της διεπαφής χρήστη ενός προγράμματος, για παράδειγμα του πλοηγού (browser). Η Μπάρα Εργαλείων επιτρέπει στους χρήστες ενός προγράμματος να έχουν εύκολη πρόσβαση σε βασικές λειτουργίες.

Οικογενειακές ρυθμίσεις: γνωστές και ως γονικός έλεγχος. Ρυθμίσεις που χρησιμοποιούνται για να προσαρμόσετε έναν πλοηγό (browser) ή άλλο πρόγραμμα, προκειμένου να καταστεί πιο ασφαλές για παιδιά. Οι ρυθμίσεις περιλαμβάνουν λειτουργίες όπως φίλτράρισμα περιεχομένου, περιορισμό χρόνου χρήσης, έλεγχο παιχνιδιών, κλπ.

Όνομα χρήστη: όνομα που χρησιμοποιείται για να εκπροσωπεί ένα χρήστη μιας διαδικτυακής υπηρεσίας και ορίζεται από τον ίδιο. Αντιπροσωπεύει τους χρήστες σε λίστες επαφών, ιστοχώρους, κλπ. Ένα καλό όνομα χρήστη θα πρέπει να προστατεύει την ανωνυμία σας στο Διαδίκτυο.

Παιδική πορνογραφία: η παιδική πορνογραφία έχει διαφορετικούς νομικούς ορισμούς σε διαφορετικές χώρες. Η ελάχιστη ορίζει την παιδική πορνογραφία ως μια εικόνα που δείχνει ένα παιδί, το οποίο εμπλέκεται ή απεικονίζεται σε σαφή σεξουαλική δραστηριότητα.

Παράνομο περιεχόμενο: περιεχόμενο στο Διαδίκτυο το οποίο είναι παράνομο βάσει της εθνικής νομοθεσίας. Οι πιο κοινοί τύποι τέτοιου περιεχομένου είναι εικόνες σεξουαλικής κακοποίησης παιδιών, παράνομη δραστηριότητα σε χώρους συνομιλίας (π.χ. grooming δηλαδή, προσέγγιση ανήλικων από ενήλικες με στόχο την μετέπειτα σεξουαλική κακοποίηση των παιδιών) και ιστοσελίδες με περιεχόμενο για το μίσος και ξενοφοβία.

Παραποίηση: η διαδικασία αλλοίωσης μιας εικόνας, αρχείου, φωτογραφίας κλπ. με περισσότερο ή λιγότερο εμφανή τρόπο. Σήμερα, υπάρχουν πολλά εργαλεία που μπορούν να χρησιμοποιηθούν για τη στρέβλωση δεδομένων.

Πλοήγηση: η πράξη κατά την οποία, χρησιμοποιώντας έναν πλοηγό, επισκέπτεστε ιστοσελίδες και σερφάρετε στο Διαδίκτυο.

Πλοηγός (browser): ένα πρόγραμμα που χρησιμοποιείται για την προβολή ιστοσελίδων. Οι πιο συνηθισμένοι πλοηγοί για τα Windows είναι οι Firefox και Internet Explorer, ενώ για τους Mac είναι ο Safari. Οι πιο πρόσφατες εκδόσεις αυτών των πλοηγών περιλαμβάνουν καινοτόμα χαρακτηριστικά γονικού ελέγχου.

Πνευματικά δικαιώματα/Copyright: μια σειρά αποκλειστικών δικαιωμάτων που ρυθμίζουν τη χρήση μιας ιδέας, εργασίας ή πληροφορίας. Το Copyright αντιπροσωπεύεται διεθνώς από το σύμβολο "©".

Πρόγραμμα «antivirus»: λογισμικό το οποίο επιχειρεί να εντοπίσει, να απομονώσει και να εξαλείψει ιούς και άλλα επιβλαβή λογισμικά. Το antivirus σαρώνει αρχικά τα αρχεία ψάχνοντας για γνωστούς ιούς και στη συνέχεια εντοπίζει ύποπτες συμπεριφορές προγραμμάτων του υπολογιστή τα οποία υποδηλώνουν μόλυνση.

Πρόγραμμα «antispyware»: πρόγραμμα το οποίο καταπολεμά λογισμικά κατασκοπείας (spyware). Το πρόγραμμα σαρώνει όλα τα ύποπτα εισερχόμενα στοιχεία και στη συνέχεια αναστέλλει τις πιθανές απειλές, ή παρουσιάζει τα επιβλαβή στοιχεία προς διαγραφή σε λίστα.

Πρόγραμμα υπολογιστή: επίσης γνωστό και ως λογισμικό. Τα λογισμικά αποτελούνται από μια δομημένη ακολουθία οδηγιών, η οποία δημιουργήθηκε από προγραμματιστές Η/Υ και επιτρέπει στους υπολογιστές να επιτελούν διάφορες λειτουργίες. Όταν αγοράζετε ένα λογισμικό, συνήθως παραλαμβάνετε ένα CD-ROM (βλ. ορισμό), στο οποίο είναι αποθηκευμένο το λογισμικό αυτό.

Προσέλευση (grooming): η χρήση των δωματίων ανοιχτής επικοινωνίας από παιδεραστές για προσέλευση ανήλικων, προσποιούμενοι ότι είναι συνομήλικοί τους. Οι παιδεραστές ξεκινούν συζητήσεις με πιθανά θύματα για να αποσπάσουν πληροφορίες σχετικά με την τοποθεσία, τα ενδιαφέροντα, τα χόμπι και τη σεξουαλική τους εμπειρία. Επίσης, χρησιμοποιούν διάφορα μέσα για την προσέλευση των παιδιών σε συνομιλίες σεξουαλικής φύσης.

Προσωπικά δεδομένα: κάθε πληροφορία που μπορεί να συνδεθεί με ένα πρόσωπο. Όταν συλλέγονται προσωπικά δεδομένα για επεξεργασία και αποθήκευση, οι λόγοι πρέπει να αναφέρονται ρητά.

Προσωπικό: στοιχείο σχετικά με ένα άτομο ή μια ομάδα που δεν πρέπει να αποκαλυφθεί δημοσίως.

Ένα προσωπικό στοιχείο σημαίνει πληροφορία ιδιαίτερης φύσης ή προσωπικά ευαίσθητης.

Προφίλ (χρήστη): προσωπικές πληροφορίες που αντιστοιχούν σε χρήστες διαφόρων διαδικτυακών υπηρεσιών, όπως οι ιστοσελίδες κοινωνικής δικτύωσης, τα φόρουμ, τα δωμάτια ανοιχτής επικοινωνίας, τα διαδικτυακά παιχνίδια, κλπ. Το προφίλ μπορεί να είναι δημόσιο ή ιδιωτικό, και προσαρμοσμένο στις προτιμήσεις των χρηστών.

Ρύθμιση απορρήτου: ένα σύνολο στοιχείων που συνδέονται με ένα λογαριασμό χρήστη, τα οποία μπορούν να υποβληθούν σε ρυθμίσεις, ώστε να αποφεύγετε τη διάδοση πληροφοριών προσωπικού χαρακτήρα, να απενεργοποιήσετε τα cookies (βλ. ορισμό), κλπ.

Ρυθμίσεις ασφαλείας (προφίλ): ένα σύνολο προσαρμοσίμων επιλογών ασφαλείας οι οποίες συνδέονται με προφίλ χρήστη (βλέπε ορισμό). Συνήθως, αυτές οι επιλογές σχετίζονται με το άνοιγμα εικόνων και αρχείων, τον εντοπισμό αξιόπιστων φορέων παροχής πληροφοριών και το δικαίωμα πρόσβασης σε περιεχόμενο για ενήλικες.

Σύνδεση διαδικτύου: αναφέρεται στα μέσα σύνδεσης στο Διαδίκτυο. Οι πιο κοινές μέθοδοι πρόσβασης είναι οι παρακάτω: dial-up, dsl, Wi-Fi, δορυφορικά και κινητά τηλέφωνα.

Σύνδεσμος (link): παραπομπή σε έγγραφο διαθέσιμο στο Διαδίκτυο (ιστοσελίδα, κείμενο, εικόνα, κ.λπ.). Όταν κάνετε κλικ σε ένα σύνδεσμο, κατευθύνεστε σε μια νέα σελίδα του ίδιου ή άλλου ιστοχώρου. Οι σύνδεσμοι είναι συνήθως χρώματος μπλε και υπογραμμισμένοι, χωρίς αυτό όμως να είναι απαραίτητο. Μια εικόνα, για παράδειγμα, μπορεί επίσης να χρησιμεύσει ως σύνδεσμος.

Συνημμένο αρχείο: ένα ηλεκτρονικό αρχείο που αποστέλλεται μαζί με μήνυμα ηλεκτρονικού ταχυδρομείου. Τα συνημμένα αρχεία μπορούν να μεταφέρουν βλαβερά προγράμματα, όπως ιούς και σκουλήκια. Να θεωρείτε ύποπτα τα ηλεκτρονικά μηνύματα από άγνωστους αποστολείς, ιδιαίτερα όταν περιέχουν συνημμένα αρχεία.

Σάρωση (scan): η ενέργεια ή η διαδικασία μετατροπής έντυπου υλικού σε ψηφιακά αρχεία με τη χρήση ενός σαρωτή. Αυτή η μετατροπή σας επιτρέπει να τα δείτε ως ηλεκτρονικά αρχεία στον υπολογιστή σας και να τα διανέμετε στο Διαδίκτυο. Ο όρος αυτός χρησιμοποιείται, επίσης, για τον έλεγχο του υπολογιστή σας ή ενός συγκεκριμένου αρχείου για κακόβουλο λογισμικό.

Σκουλήκι: ένας ιδιαίτερος τύπος ιού, που αυτο-αναπαράγεται και μπορεί να εξαπλωθεί ακόμη και σε ολόκληρο δίκτυο ηλεκτρονικών υπολογιστών χωρίς ανθρώπινη παρέμβαση. Τα σκουλήκια μπορεί να καταναλώσουν τεράστια χωρητικότητα, να κλείσουν υπολογιστές, κλπ.

Συσκευή αποθήκευσης USB (Universal Serial Bus): συσκευή αποθήκευσης δεδομένων με υποδοχή USB (ενιαίο σειριακό δίαυλο). Οι συσκευές USB είναι συνήθως μικρές, ελαφρές και επανεγγραψίμες.

Τσατ (chat): σύγχρονη επικοινωνία μέσω του Διαδικτύου, μέσω γραπτών μηνυμάτων, μέσω δωματίων ανοιχτής επικοινωνίας και εφαρμογών τύπου instant messenger (π.χ. MSN).

Υλικό συστήματος (Hardware): το φυσικό μέρος ενός υπολογιστή που ξεχωρίζει από το λογισμικό, το οποίο είναι άυλο. Το hardware μπορεί να είναι εσωτερικό: μητρικές κάρτες, σκληροί δίσκοι, και RAM - που συχνά αναφέρονται και ως κατασκευαστικά στοιχεία - και εξωτερικό: οθόνες, πληκτρολόγια, εκτυπωτές, κλπ. - που ονομάζονται επίσης περιφερειακά υπολογιστών.

Φάκελος: μια οντότητα σε ένα σύστημα αρχείων το οποίο περιέχει μια ομάδα αρχείων ή / και άλλους καταλόγους. Οι φάκελοι μπορεί να περιέχουν πολλαπλά έγγραφα και χρησιμοποιούνται για την οργάνωση των πληροφοριών.

Φάκελος ανεπιθύμητων μηνυμάτων / junk: ένας φάκελος του προγράμματος ηλεκτρονικού

ταχυδρομείου, όπου αποθηκεύονται τα μηνύματα που θεωρούνται spam ή junk.

Φίλτρο: εφαρμογή η οποία ρυθμίζει την πρόσβαση σε πληροφορίες ή σε συγκεκριμένες διαδικτυακές υπηρεσίες, προειδοποιεί για προβληματικές ιστοσελίδες, κρατάει ιστορικό πλοήγησης, μπλοκάρει ρισκοκίνδυνες ιστοσελίδες. Σε κάποιες περιπτώσεις, το φίλτρο μπορεί ακόμη και να προβεί στην πλήρη απενεργοποίηση του υπολογιστή. Φίλτρα μπορούν να εγκατασταθούν σε μεμονωμένους υπολογιστές, διακομιστές, τηλέφωνα με πρόσβαση στο Διαδίκτυο, κλπ.

Φίλτρο ανεπιθύμητης αλληλογραφίας: μια εφαρμογή που μπλοκάρει ανεπιθύμητα ηλεκτρονικά μηνύματα από το να αποθηκευτούν στα εισερχόμενα του ηλεκτρονικού σας ταχυδρομείου.

Φόντο επιφάνειας εργασίας: μια εικόνα που χρησιμοποιείται ως φόντο στην επιφάνεια εργασίας του υπολογιστή σας.

Φόρουμ: ηλεκτρονική ομάδα συζήτησης, όπου συμμετέχοντες με κοινά ενδιαφέροντα μπορούν δημόσια να ανταλλάσσουν απόψεις για διάφορα θέματα.

Χάκερ (hacker): ο όρος που χρησιμοποιείται για να αναφερθεί σε ένα πρόσωπο το οποίο ασχολείται με την παράνομη εισβολή σε συστήματα υπολογιστών (βλ. και «cracker»). Μπορεί, επίσης, να χρησιμοποιηθεί για να περιγράψει ένα πρόσωπο που έχει πάθος με τους υπολογιστές.

Ψηφιακό παιχνίδι: ένα παιχνίδι που δημιουργήθηκε από προγραμματιστές παιχνιδιών και το οποίο μπορεί να παιχτεί σε υπολογιστή. Ως διαδικτυακό παιχνίδι ορίζεται το ψηφιακό παιχνίδι που χρειάζεται μια ενεργή σύνδεση δικτύου για να παιχτεί. Τα διαδικτυακά παιχνίδια δίνουν συχνά τη δυνατότητα αλληλεπίδρασης μεταξύ πολλαπλών παικτών.

Αγγλικοί όροι

Avatar: ένα προφίλ χρήστη μπορεί να εκπροσωπείται από ένα όνομα χρήστη (βλ. ορισμό) σε συνδυασμό με μια εικόνα, εικονίδιο, ή ακόμη και τρισδιάστατο χαρακτήρα στην περίπτωση των ψηφιακών παιχνιδιών και εικονικών κόσμων.

Blog: σύντομη έκδοση της λέξης weblog. Αναφέρεται σε ψηφιακό ημερολόγιο (το λεγόμενο ιστολόγιο), στο οποίο ένα άτομο ή μια ομάδα δημιουργεί περιεχόμενο, συνήθως σε καθημερινή βάση, και το οποίο μπορεί να αποτελείται από κείμενα, εικόνες, οπτικοακουστικά αρχεία και συνδέσμους.

Blogging: η δραστηριότητα συγγραφής ή ανανέωσης ενός blog.

CD-ROM: ακρωνύμιο των λέξεων Compact Disc Read Only Memory – Συμπαγής δίσκος μνήμης μόνο για ανάγνωση. Είναι μη εγγράψιμος δίσκος που μπορεί να διαβαστεί από υπολογιστές. Τα CD-ROM χρησιμοποιούνται και για τη διανομή λογισμικών.

Cookies: αρχείο που τοποθετείται στον πλοηγό σας από μια ιστοσελίδα. Κάθε φορά που χρησιμοποιείτε την εν λόγω ιστοσελίδα, το cookie στέλνεται πίσω στο διακομιστή που φιλοξενεί την ιστοσελίδα. Τα cookies συλλέγουν έτσι πληροφορίες για τις προτιμήσεις σας και χρησιμοποιούνται για τη διευκόλυνση αγορών μέσω Διαδικτύου. Εάν απενεργοποιήσετε τα cookies, κάποιες σελίδες δεν θα είναι χρησιμοποιήσιμες.

Crack (ρήμα): παράνομη αντιγραφή εμπορικού λογισμικού, η οποία γίνεται παραβιάζοντας τα πνευματικά δικαιώματα.

Cracker: ένα πρόσωπο το οποίο εισβάλλει παράνομα σε σύστημα υπολογιστών με στόχο το παράνομο κέρδος.

Emoticon: εικονίδιο που χρησιμοποιείται για να μεταφέρει συναισθήματα, π.χ. smiley (χαμογελαστό

προσωπάκι). Τα emoticons μπορεί κανείς να τα αναπαράσχησει με συγκεκριμένους χαρακτήρες και σημεία στίξης χρησιμοποιώντας το πληκτρολόγιο ή επιλέγοντας τα σχετικά εικονίδια και τους προκατασκευασμένους χαρακτήρες που προσφέρουν οι διάφορες υπηρεσίες Διαδικτύου και κινητής τηλεφωνίας.

Flaming: εχθρική και προσβλητική επικοινωνία μεταξύ χρηστών του Διαδικτύου, που συνήθως εμφανίζεται σε ομάδες συζητήσεων, Internet Relay Chat (IRC), ή ακόμα και μέσω ηλεκτρονικού ταχυδρομείου.

Freeware και shareware: σε γενικές γραμμές, τα λογισμικά προστατεύονται από πνευματικά δικαιώματα και επομένως δεν είναι διαθέσιμα για δωρεάν αντιγραφή / κατέβασμα από το Διαδίκτυο. Τα Freeware, ωστόσο, είναι λογισμικά των οποίων οι δημιουργοί και κάτοχοι των αντίστοιχων πνευματικών δικαιωμάτων επιτρέπουν τη χρήση χωρίς χρέωση. Τα shareware από την άλλη επιτρέπουν την ελεύθερη χρήση μόνο για μια δοκιμαστική περίοδο. Μετά την πάροδο της δοκιμαστικής περιόδου, ο χρήστης πρέπει να αγοράσει το πρόγραμμα, εάν θέλει να συνεχίσει να το χρησιμοποιεί.

MP3: μορφή κωδικοποίησης δεδομένων ειδική για τον ήχο. Ένα αρχείο MP3 έχει περίπου το ένα δέκατο του μεγέθους του αρχικού αρχείου ήχου, αλλά η ποιότητα του ήχου είναι σχεδόν ίδια με αυτή των CD. Λόγω του μικρού μεγέθους και της πιστότητάς τους, τα αρχεία MP3 έχουν γίνει ένας δημοφιλής τρόπος για την αποθήκευση αρχείων μουσικής σε υπολογιστές, όπως και σε φορητές συσκευές.

Net: συντομογραφία για το Internet - Διαδίκτυο.

Netiquette: δεοντολογία και κώδικας συμπεριφοράς / επικέτα που εφαρμόζεται στις επικοινωνίες μέσω Διαδικτύου.

Newsgroup: βλέπε ορισμό για το φόρουμ (forum).

Second Life: μια γνωστή τρισδιάστατη δικτυακή κοινότητα που παρέχεται από την Αμερικάνικη εταιρεία Linden Labs. Στο Second Life, οι χρήστες μπορούν να επικοινωνούν μέσω ενός ειδώλου / avatar (βλέπε ορισμό), να δημιουργούν σπίτια και διάφορα περιβάλλοντα, να συναλλάσσονται και να κερδίζουν εικονικά νομίσματα, κλπ. Βλέπε www.secondlife.com

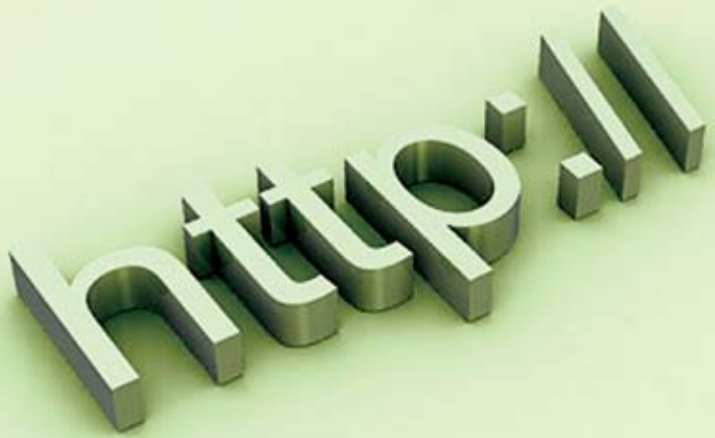
SIP Bench: μια μελέτη που υποστηρίζεται από την Ευρωπαϊκή Επιτροπή, η οποία εξέτασε τα πιο γνωστά εργαλεία γονικού ελέγχου και φίλτρων, με στόχο να εκτιμήσει την αποτελεσματικότητά τους αναφορικά με την προστασία των παιδιών από επιβλαβές περιεχόμενο στο Διαδίκτυο.

Spam: ανεπιθύμητο μήνυμα ηλεκτρονικού ταχυδρομείου, συνήθως εμπορικού χαρακτήρα, που αποστέλλεται μαζικά. Η αποστολή spam αποτελεί μια από τις πιο γνωστές παραβιάσεις που λαμβάνουν χώρα στο Διαδίκτυο.

URL (Uniform Resource Locator): η διεύθυνση μιας συγκεκριμένης ιστοσελίδας ή αρχείου στο Διαδίκτυο. Δεν περιέχει ειδικούς χαρακτήρες ή κενά διαστήματα και χρησιμοποιεί καθέτους που παραπέμπουν σε διαφορετικές ενότητες. Το πρώτο μέρος της διεύθυνσης καθορίζει το πρωτόκολλο χρήσης, το δεύτερο καθορίζει τη διεύθυνση IP ή το όνομα του χώρου όπου βρίσκεται η πηγή.

Voice over Internet Protocol (VoIP): μια τεχνολογία που επιτρέπει την ομιλία μέσω του Διαδικτύου, μετά από την εγκατάσταση σχετικού λογισμικού. Οι υπηρεσίες VoIP παρέχουν συχνά δωρεάν κλήσεις για τους χρήστες της ίδιας υπηρεσίας (π.χ. Skype, Voicebuster). Επίσης, οι υπηρεσίες VoIP συνήθως προσφέρουν εφαρμογές τσατ και ανταλλαγής αρχείων.

Web: σύντομη εκδοχή του World Wide Web, του Παγκόσμιου Ιστού. Πρόκειται για συλλογή από ηλεκτρονικά έγγραφα σε γλώσσα HTML (Hypertext Markup Language), τα οποία περιέχουν συνδέσμους προς άλλα έγγραφα, καθώς και γραφικά, ήχο, βίντεο και αρχεία. Το Web αποτελεί μέρος του Διαδικτύου.



Ε. Χρήσιμες διαδικτυακές διευθύνσεις

SAFERINTERNET.GR

Πλοηγηθείτε στο Διαδίκτυο με ασφάλεια! Εκμεταλλευτείτε τα οφέλη του, γνωρίζοντας τους κανόνες ορθής χρήσης. Ενημερωθείτε για τους πιθανούς online κινδύνους και μάθετε πώς μπορείτε να τους αποφεύγετε και να προφυλάσσετε εσάς και τα παιδιά σας. Επισκεφθείτε την ιστοσελίδα:

<http://www.saferinternet.gr>

ΑΝΟΙΧΤΗ ΓΡΑΜΜΗ ΚΑΤΑΓΓΕΛΙΩΝ

Αναφέρατε παράνομο περιεχόμενο ή παράνομη συμπεριφορά στο Διαδίκτυο. Επικοινωνήστε μαζί μας μέσω της ηλεκτρονικής μας φόρμας <http://www.safeline.gr/report>. Για περισσότερες πληροφορίες ανατρέξτε στην ιστοσελίδα μας:

<http://www.safeline.gr>

ΓΡΑΜΜΗ ΒΟΗΘΕΙΑΣ «ΥΠΟΣΤΗΡΙΖΩ 800 11 800 15»

Εάν το Διαδίκτυο δυσκολεύει τη ζωή του παιδιού σας, ζητήστε βοήθεια. Επικοινωνήστε μαζί μας στο τηλέφωνο 800 11 800 15 καθημερινά, 9:00 15:00 (χωρίς χρέωση για αστικά και υπεραστικά), ή στείλτε μας μήνυμα στη διεύθυνση:

help@saferinternet.gr

ΠΑΝΕΥΡΩΠΑΪΚΟ ΣΥΣΤΗΜΑ ΠΛΗΡΟΦΟΡΗΣΗΣ ΓΙΑ ΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΠΑΙΧΝΙΔΙΑ – PEGI

Το PEGI (Pan European Game Information) είναι ένα πανευρωπαϊκό σύστημα αποτίμησης των ορίων ηλικίας και του περιεχομένου για τα ηλεκτρονικά παιχνίδια και τα βιντεοπαιχνίδια. Κατηγοριοποιεί τα παιχνίδια ως προς την ηλικιακή καταλληλότητα (3+, 7+, 12+, 16+, 18+) και ως προς το περιεχόμενο (βία, χυδαία γλώσσα, φόβος, σεξ, ναρκωτικά, ρατσισμός, τζόγος). Αναλυτικές πληροφορίες βρίσκετε στη διεύθυνση:

<http://www.pegi.info/gr/>

ΠΑΝΕΥΡΩΠΑΪΚΟ ΔΙΚΤΥΟ ΕΘΝΙΚΩΝ ΚΕΝΤΡΩΝ ΕΝΗΜΕΡΩΣΗΣ ΚΑΙ ΕΠΑΓΡΥΠΝΗΣΗΣ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ – INSAFE

Το Πανευρωπαϊκό Δίκτυο Εθνικών Κέντρων Ενημέρωσης και Επαγρύπνησης για την ασφάλεια στο Διαδίκτυο τελεί υπό την αιγίδα της Ευρωπαϊκής Επιτροπής. Εκπρόσωπός του στην Ελλάδα είναι το [Saferinternet.gr](http://www.saferinternet.gr). Στην ιστοσελίδα του Insafe ο επισκέπτης μπορεί να βρει πληροφορίες και υλικό από τα εθνικά κέντρα που συνθέτουν το δίκτυο. Στα αγγλικά, στη διεύθυνση:

<http://www.saferinternet.org>



ins@fe

@ferinternet.gr

Με τη στήριξη της:



Τίτλος: Οικογενειακός οδηγός ασφάλειας στο Διαδίκτυο • Δημιουργήθηκε από το Insafe, με την υποστήριξη της Liberty Global/UPC το έτος 2008
Prefix: 9789078209 • Id 51950 • ISBN-NUMBER: 9789078209577 • EAN: 9789078209577

Πνευματικά δικαιώματα: Το παρόν έργο υπόκειται στην άδεια Creative Commons Αναφορά προέλευσης-Μη Εμπορική Χρήση-Όχι Παράγωγα Έργα 3.0 Μη εισαγόμενο. Για περισσότερες πληροφορίες, επισκεφθείτε το σχετικό ιστοχώρο:
<http://creativecommons.org/licenses/by-nc-nd/3.0/deed.el>

Μετάφραση - πνευματικά δικαιώματα κειμένων για την Ελληνική γλώσσα: Δρ. Βερόνικα Σαμορά