ΟΔΗΓΟΣ Ασφαλούς Χρήσης του Διαδικτύου

για Γονείς και Παιδιά

Microsoft

ΜΙΚΡΟΙ ΕΘΕΛΟΝΤΕΣ
παιδιά έξω καρδιά 10 χρόνια προσφοράς

Περιεχόμενα

ΜΙΚΡΟΙ ΕΘΕΛΟΝΤΕΣ

Προσφώνηση Υπουργού Συγκοινωνιών και Έργων για τον «Οδηγό Ασφαλούς Χρήσης του Διαδικτύου»

Από το 1989 που δημιουργήθηκε ο πρόδρομος του Διαδικτύου, ως σήμερα, η εξέλιξη του είναι εντυπωσιακή. Το Διαδίκτυο αποτελεί ένα απαραίτητο πλέον εργαλείο με χρήστες από μικρά παιδιά ως ανθρώπους της τρίτης ηλικίας και περιλαμβάνεται σε κάθε πτυχή της ανθρώπινης δραστηριότητας. Το Διαδίκτυο έχει εξαπλωθεί σε κάθε γωνιά της γης, και έχει «εισβάλει» δυναμικά στην κοινωνική, επαγγελματική και οικονομική ζωή του καθενός ξεχωριστά.

Έχει χαρακτηριστεί, και όχι τυχαία, ως η επανάσταση του αιώνα, καθότι είναι ένα δυναμικό εργαλείο που εκμηδενίζει τις αποστάσεις, παρέχει μια ανεξάντλητη πηγή γνώσεων και πληροφοριών και αποτελεί το βασικό οδηγό της Κοινωνίας της Πληροφορίας και της Γνώσης.

Παρά την αδιαμφισβήτητη χρησιμότητά του, το Διαδίκτυο, εμπεριέχει κινδύνους και αρνητικά στοιχεία που προκαλούν προβληματισμό και απαιτούν προσοχή και ιδιαίτερη αντιμετώπιση, ιδιαίτερα στα παιδιά, που βρίσκονται σε μια ευαίσθητη σε κάθε ερέθισμα ηλικία και είναι περισσότερο εκτεθειμένα στους κινδύνους του Διαδικτύου.

Οι κίνδυνοι ποικίλλουν, ανάλογα με την ηλικία του παιδιού και το πόσο εξοικειωμένο είναι το παιδί με τον υπολογιστή. Το σημαντικότερο είναι να προστατεύει κανείς τα προσωπικά του δεδομένα που είναι αποθηκευμένα στον υπολογιστή του, αλλά και να πληροφορηθούν τόσο τα παιδιά όσο και οι γονείς τους, για τους κινδύνους που ενέχει το Διαδίκτυο, έτσι ώστε να συμπεριφέρονται με ασφαλή τρόπο, αλλά και να είναι έτοιμοι να αντιμετωπίσουν πιθανούς κινδύνους που θα προκύψουν κατά τη χρήση του Διαδικτύου.

ΜΙΚΡΟΙ ΕΘΕΛΟΝΤΕΣ

Είναι πολύ σημαντικό λοιπόν, να προστατεύσετε τον υπολογιστή σας, να προστατεύσετε τον εαυτό σας στο Διαδίκτυο και να ακολουθήσετε τους βασικούς κανόνες ασφάλειας που περιλαμβάνονται στον «Οδηγό Ασφαλούς Χρήσης του Διαδικτύου», ο οποίος έχει ως στόχο να σας εφοδιάσει με χρήσιμες πληροφορίες και συμβουλές σε θέματα που αφορούν την ασφαλή πλοήγηση και την αντιμετώπιση δύσκολων καταστάσεων που μπορεί να προκύψουν.

Συγχαίρω την Microsoft, η οποία στα πλαίσια της εταιρικής κοινωνικής της ευθύνης, ετοίμασε τον Οδηγό αυτό για την ασφαλή χρήση του διαδικτύου.

Δρ. Ερατώ Κοζάκου Μαρκουλλή
Υπουργός Συγκοινωνιών και Έργων

Εισαγωγή

Ο Οδηγός Ασφαλούς Χρήσης του Διαδικτύου για Γονείς και Παιδιά, αποτελεί κοινωνική προσφορά της Microsoft και των Μικρών Εθελοντών Κύπρου, σε μια προσπάθεια να αναβαθμίσουν την ετοιμότητα των γονέων και των παιδιών στην αντιμετώπιση των κινδύνων του Διαδικτύου.

Στο βιβλιάριο θα βρείτε τις απαραίτητες γνώσεις και συμβουλές που πρέπει να γνωρίζουν τόσο οι γονείς όσο και τα παιδιά για την ασφαλή πρόσβαση και χρήση του διαδικτύου. Το έντυπο είναι οργανωμένο σε αυτόνομα κεφάλαια και μπορεί να χρησιμοποιηθεί είτε σαν ένας ολοκληρωμένος οδηγός είτε για την κάλυψη συγκεκριμένων θεμάτων.

Πηγή: Ορισμένες από τις πληροφορίες αυτού του Οδηγού προσαρμόστηκαν, κατόπιν αδείας, από τον οργανισμό SafeInternet.

Ο Διαδικτυακός κόσμος

Το διαδίκτυο είναι ένα συναρπαστικό περιβάλλον στο οποίο μπορούμε να επικοινωνούμε, να ενημερωθούμε, να ψυχαγωγηθούμε, να εκπαιδευτούμε και να διεκπεραιώνουμε συναλλαγές από οπουδήποτε και οποτεδήποτε.

Το διαδίκτυο έχει καταργήσει κάθε εμπόδιο και κάθε όριο αποστολής και λήψης πληροφοριών, προσφέροντας πρόσβαση σε ένα τεράστιο χώρο περιεχομένου σε κάθε μορφή. Είναι ένας νέος συναρπαστικός κόσμος ο οποίος ασκεί ιδιαίτερη έλξη στα παιδιά. Σε αυτόν βρίσκουν παιχνίδια, εφαρμογές που τους επιτρέπουν την επικοινωνία με άλλους χρήστες του διαδικτύου και κάθε πληροφορία που μπορεί να χρειάζονται. Η ενασχόληση των παιδιών με τους ηλεκτρονικούς υπολογιστές, τις νέες τεχνολογίες και το διαδίκτυο μπορεί να προσφέρει πολλές δυνατότητες μάθησης, εκπαίδευσης και ψυχαγωγίας.

Προτερήματα Διαδικτύου

Τα βασικά πλεονεκτήματα της χρήσης του διαδικτύου περιλαμβάνουν την παγκόσμια πρόσβαση σε πληροφορίες, την προσφορά απεριόριστων πληροφοριών με μηδαμινό κόστος, τη δυνατότητα άμεσης ανταπόκρισης και τη συνεισφορά του στην εκπαιδευτική διαδικασία. Το διαδίκτυο επίσης προσφέρει ψυχαγωγία, επικοινωνία και συναλλαγές σε επίπεδο και εύρος που κανένας γονιός δεν θα μπορούσε ποτέ να φανταστεί.

Προκλήσεις του Διαδικτύου

Παρά την αδιαμφισβήτητη χρησιμότητά του, το διαδίκτυο υποκρύπτει κάποιους κινδύνους, ιδιαίτερα για τα παιδιά. Αυτοί οι κίνδυνοι αφορούν την έκθεση των παιδιών σε παράνομο ή πορνογραφικό περιεχόμενο, την εξαπάτησή τους από αγνώστους ενήλικες οι οποίοι υποκρίνονται ότι είναι ανήλικοι και την άσκηση πίεσης για αποκάλυψη προσωπικών στοιχείων. Χρησιμοποιείται επίσης για τη διανομή περιεχομένου το οποίο είναι παράνομο ή επιβλαβές.

Εφόσον ο κυβερνοχώρος δεν έχει εθνικά όρια, παράνομες δραστηριότητες μπορούν εύκολα να βρουν «εικονικό καταφύγιο» σε αυτό το μέσο.

Ασφάλεια και Διαδίκτυο

Ο κάθε χρήστης του διαδικτύου θα πρέπει να είναι επιφυλακτικός κατά την πλοήγηση του στο διαδίκτυο, ακόμη και όταν έχει ενημερωμένο τόσο το λειτουργικό σύστημα όσο και κάποιο πρόγραμμα κατά των ιών (anti-virus). Η ανεξέλεγκτη χρήση του διαδικτύου, σε οποιαδήποτε δραστηριότητα και τομέα μπορεί να σκιάσει τα σημαντικά οφέλη και να προκαλέσει προβλήματα. Αυτά περιλαμβάνουν την έκθεση των παιδιών σε ακατάλληλο περιεχόμενο και εμπλοκή τους σε δυσάρεστες καταστάσεις όπως πορνογραφία, παιδεραστία, εμπόριο παιδιών, περιεχόμενο με υπερβολική βία, παρενόχληση στον κυβερνοχώρο (cyber bullying), παραβατικότητα, κατάθλιψη ακόμη και αυτοκτονία.

ΜΙΚΡΟΙ ΕΘΕΛΟΝΤΕΣ

Ψηφιακό χάσμα

Υπάρχει ένα ψηφιακό χάσμα μεταξύ του γονιού και του παιδιού όσον αφορά τη χρήση και αξιοποίηση του διαδικτύου. Ο κύριος λόγος βασίζεται στο γεγονός ότι τα παιδιά έχουν γεννηθεί μετά την εξάπλωση του διαδικτύου θεωρώντας τη χρήση του ηλεκτρονική υπολογιστή και του διαδικτύου δεδομένη.

Για να μπορέσει ένας γονιός να αντιληφθεί τη δύναμη και την ανάγκη χρήσης και αξιοποίησης του διαδικτύου θα πρέπει και ο ίδιος να εξερευνήσει τον κόσμο αυτό. Κάθε γονιός θα πρέπει να γνωρίζει τις βασικές χρήσεις του υπολογιστή και να μπορεί να χρησιμοποιήσει το διαδίκτυο για ανεύρεση πληροφοριών αλλά και για να κατεβάσει ένα έγγραφο από το διαδίκτυο.

Βασικά εργαλεία που πρέπει να γνωρίζει ο κάθε γονιός είναι η χρήση του ηλεκτρονικού ταχυδρομείου και των προγραμμάτων άμεσης επικοινωνίας. Ιδιαίτερα χρήσιμο είναι να έχει εμπειρίες με τη χρήση κοινωνικών δικτύων, όπως το Facebook. Οι γνώσεις αυτές θα τον βοηθήσουν να καταλάβει πώς ένα παιδί χρησιμοποιεί το διαδίκτυο δίνοντας του την απαιτούμενη επιτήρηση και καθοδήγηση στη χρήση του.

Όταν το παιδί αντιληφθεί ότι ο γονιός κατέχει συγκεκριμένες γνώσεις τότε χρησιμοποιεί το διαδίκτυο πιο επιφυλακτικά.

Γενικές συμβουλές

Οι γονείς έχουν δικαίωμα και θα πρέπει να επιβλέπουν και να φιλτράρουν το περιεχόμενο του Διαδικτύου ώστε να ελέγχουν ότι τα παιδιά τους δεν έχουν πρόσβαση σε περιεχόμενο που μπορεί να είναι επιβλαβές για την ανάπτυξη της προσωπικότητάς τους. Συγκεκριμένα θα πρέπει:

- Να θέτουν όρους και χρονικά πλαίσια όσον αφορά τη χρήση του διαδικτύου στο σπίτι.
- Να συνοδεύουν τα μικρότερα παιδιά όταν συνδέονται στο διαδίκτυο, ειδικά τις πρώτες φορές.
- Να τοποθετούν τον υπολογιστή με σύνδεση στο διαδίκτυο, σε ένα χώρο του σπιτιού με άμεση πρόσβαση από όλα τα μέλη της οικογένειας.
- Να προτείνουν στο παιδί τους τη χρήση ιστοσελίδων με επιμορφωτικό και ψυχαγωγικό περιεχόμενο κατάλληλο για την ηλικία του.

Οι γονείς θα πρέπει να προτρέπουν τα παιδιά τους ώστε να αποφεύγουν τη δημοσίευση προσωπικών τους στοιχείων (ονοματεπώνυμο, στοιχεία επικοινωνίας, διευθύνσεις, προτιμήσεις, ενδιαφέροντα κ.α.) κατά τη διάρκεια χρήσης του διαδικτύου, ιδιαίτερα όταν αυτά είναι σε συνδυασμό με φωτογραφίες.

Πλοήγηση (WEB BROWSING)

Ασφαλής πλοήγηση

Η πλοήγηση στις σελίδες του παγκοσμίου ιστού πραγματοποιείται μέσω ενός φυλλομετρητή (Internet Explorer Web browser) και απαιτεί ιδιαίτερη προσοχή από το χρήστη τόσο για την ασφάλεια των προσωπικών του δεδομένων όσο και για την ασφάλεια του υπολογιστή που χρησιμοποιεί.

Τα μέτρα τα οποία μπορεί να ληφθούν για να εξασφαλίσουν την όσο το δυνατόν ασφαλέστερη πλοήγηση στις σελίδες του παγκοσμίου ιστού εξαρτώνται είτε από τις υπηρεσίες που μπορεί να προσφέρει ο παροχέας σύνδεσης (Internet provider) ή / και τις ενέργειες που κάνει ο ίδιος ο χρήστης.

Οι ενέργειες του χρήστη περιλαμβάνουν την εγκατάσταση προγραμμάτων ασφαλείας στον υπολογιστή, την τακτική ενημέρωση του λειτουργικού συστήματος και των λογισμικών και την παραμετροποίηση του φυλλομετρητή. Θα πρέπει επίσης να δίνουν ιδιαίτερη προσοχή στις ιστοσελίδες που επισκέπτονται, στα αρχεία που κατεβάζουν (download) στον υπολογιστή τους και στις απαντήσεις που δίνονται σε αναδυόμενα παράθυρα (pop-up windows).

Τι είναι το κατέβασμα αρχείων (download);

Το Download είναι η διαδικασία απόκτησης (μέσω μεταφοράς) αρχείων στον προσωπικό μας υπολογιστή από κάποιον άλλον υπολογιστή ή ιστοσελίδα μέσω του διαδικτύου. Το Download είναι συνώνυμο με τη λέξη “λήψη”, ενώ το Upload είναι συνώνυμο με τη λέξη “μετάδοση”. Στη διαδικασία λήψης αρχείων περιλαμβάνονται η εγκατάσταση

προγραμμάτων, το άνοιγμα και η λήψη εικόνων, εγγράφων Word, λογιστικών φύλλων Excel ή μεταφορά μουσικών ή άλλων αρχείων.

Η διαδικασία της τοπικής αποθήκευσης προγραμμάτων στον προσωπικό σας υπολογιστή από το διαδίκτυο πρέπει να γίνεται με πολλή προσοχή διότι ενδέχεται τα προγράμματα αυτά να είναι μολυσμένα με ιούς, ή να αποτελούν τα ίδια ιούς που μπορούν να καταστρέψουν τα αρχεία του υπολογιστή σας. Για την αποφυγή τέτοιων προβλημάτων θα πρέπει προτού κατεβάσουμε οποιοδήποτε αρχείο από μια ιστοσελίδα ή από ένα ηλεκτρονικό μήνυμα, να βεβαιωνόμαστε για την εγκυρότητα της ιστοσελίδας και την αξιοπιστία του αποστολέα. Ειδικά όσον αφορά τα ηλεκτρονικά μηνύματα δεν θα πρέπει να ανοίγουμε ή να κατεβάζουμε αρχεία από αγνώστους ή αρχεία αγνώστου περιεχομένου.

Αναζήτηση πληροφοριών

Η τεράστια «δεξαμενή» πληροφοριών και εργαλείων του διαδικτύου είναι διάσπαρτη σε δισεκατομμύρια ιστοσελίδες που πρακτικά είναι αδύνατον να ερευνηθούν από το χρήστη χωρίς τη βοήθεια εξειδικευμένων προγραμμάτων, όπως οι μηχανές αναζήτησης. Οι μηχανές αναζήτησης χρησιμοποιούν ειδικά προγράμματα, τις λεγόμενες «αράχνες» (spiders), τα οποία «χτενίζουν» τις ιστοσελίδες αναζητώντας κείμενα και διευθύνσεις πληροφοριών με τα οποία δημιουργούν και διαχειρίζονται πολύπλοκα ευρετήρια πληροφοριών. Τα αποτελέσματα μιας αναζήτησης ανακτώνται με τη χρήση των ευρετηρίων αυτών.

Blogs

Τα blogs ή ιστολόγια, όπως λέγονται στα Ελληνικά, είναι εικονικά σημειωματάρια που μπορούν να δημιουργηθούν και να δημοσιευθούν στο διαδίκτυο πολύ εύκολα από οποιονδήποτε, καθώς η δημιουργία τους δεν απαιτεί εξειδικευμένες τεχνικές γνώσεις. Τα παιδιά θα πρέπει να διατηρούν τις επιφυλάξεις τους σχετικά με την αξιοπιστία των πληροφοριών που δημοσιεύονται στα blogs γιατί πολύ συχνά σε αυτά εκφράζονται γνώμες και προσωπικές απόψεις του εκάστοτε συγγραφέα.

Εάν ένα παιδί αποφασίσει να δημιουργήσει το δικό του blog θα πρέπει να προσέχει τι δημοσιεύει. Η δημοσίευση προσωπικών στοιχείων, φωτογραφιών και άλλων πληροφοριών, αφήνει ανεξέλεγκτη την πρόσβαση σε προσωπικά δεδομένα από οποιονδήποτε χρήστη του διαδικτύου. Αυτό σημαίνει ότι μεταξύ άλλων και επιτήδειοι μπορούν απλά και χωρίς κόπο να μάθουν λεπτομέρειες για το παιδί και τους φίλους του, τις συνήθειές του, τα χόμπι του, τις αγαπημένες ασχολίες του κ.λπ.

Η προστασία κατά την πλοήγηση και το νομικό πλαίσιο

Η ελευθερία της έκφρασης, της πληροφόρησης, της επικοινωνίας αλλά και γενικότερα της ανάπτυξης της προσωπικότητας καθώς επίσης και η προστασία της ιδιωτικής ζωής, είναι από τα σημαντικότερα δικαιώματα των πολιτών και τα οποία κατοχυρώνονται από Ευρωπαϊκές και Διεθνείς νομοθεσίες. Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιοδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων δια συστήματος ηλεκτρονικού υπολογιστή ή με τη χρήση διαδικτύου, τιμωρείται με αυστηρές ποινές.

Επίσης, είναι γνωστό ότι οι νέοι πολύ συχνά χρησιμοποιούν το διαδίκτυο για να κατεβάσουν στον υπολογιστή τους και να ανταλλάξουν μουσική, ταινίες ακόμη και προγράμματα. Θα πρέπει όμως να γνωρίζουν ότι οι δημιουργοί ενός έργου (φωτογραφία, βίντεο, μουσική, λογισμικό) έχουν τα πνευματικά δικαιώματα (copyrights) της προσωρινής ή μόνιμης χρήσης, αντιγραφής ή αναπαραγωγής με οποιοδήποτε τρόπο και σε οποιοδήποτε μέσο.

Θα πρέπει επίσης τα παιδιά να καταλάβουν ότι δεν μπορούν να «ανεβάζουν» στο διαδίκτυο φωτογραφίες, βίντεο, μουσική και άλλα αρχεία χωρίς την άδεια του δημιουργού τους. Ακόμα και αν το ίδιο το παιδί έχει δημιουργήσει ένα βίντεο ή μια φωτογραφία θα πρέπει, προτού τα δημοσιεύσει στο διαδίκτυο, να έχει την άδεια των συμμετεχόντων στο συγκεκριμένο ψηφιακό μέσο.

Διαδικτυακοί διαφθορείς

Το διαδίκτυο αποτελεί τον πλέον κατάλληλο χώρο δράσης για επιτήδειους διαφθορείς, οι οποίοι μέσω των ομάδων συζήτησης επιδιώκουν τη συνομιλία με ανήλικους χρήστες. Η ανωνυμία του διαδικτύου ευνοεί τη γρήγορη ανάπτυξη πίστης και οικειότητας. Το γεγονός ότι πρόκειται για δημόσιους χώρους διαδικτυακής επικοινωνίας, που επιτρέπουν την ανωνυμία, δημιουργεί την ψευδαίσθηση της ασφάλειας και παρασύρει τα παιδιά.

Οι διαφθορείς εκμεταλλεύονται την ανωνυμία τους για να δημιουργήσουν διαδικτυακές σχέσεις με τα άπειρα νεαρά άτομα. Έρχονται σε επαφή με τα παιδιά μέσω συζητήσεων σε δωμάτια συνομιλίας, μέσω άμεσων μηνυμάτων ή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Προσπαθούν να παρασύρουν σταδιακά το θύμα τους μέσω της προσοχής, της στοργής, της ευγένειας, ακόμη και μέσω δώρων αφού συχνά επενδύουν σημαντικό χρόνο, χρήμα και ενέργεια σε

αυτήν τους την προσπάθεια. Για να κάμψουν τις αναστολές των νεαρών ατόμων, σταδιακά εισάγουν σεξουαλικό περιεχόμενο στις συζητήσεις τους ή προβάλλουν σεξουαλικά ακατάλληλο υλικό.

Πως μπορούμε να μειώσουμε τον κίνδυνο των διαδικτυακών διαφθορέων

- Μιλήστε στο παιδί σας σχετικά με τους σεξουαλικούς διαφθορείς και τους πιθανούς κινδύνους που κρύβει το διαδίκτυο.

- Εάν τα παιδιά σας συμμετέχουν σε δωμάτια συνομιλιών, φροντίστε να γνωρίζετε ποια επισκέπτονται και με ποιον συζητούν. Παρακολουθήστε κι εσείς οι ίδιοι τις περιοχές αυτές για να δείτε το είδος των συζητήσεων που διεξάγονται.

- Πείτε στα παιδιά σας να μην απαντούν ποτέ σε άμεσα μηνύματα ή σε μηνύματα ηλεκτρονικού ταχυδρομείου από αγνώστους. Εάν τα παιδιά σας χρησιμοποιούν υπολογιστές σε χώρους εκτός της επίβλεψής σας όπως δημόσιες βιβλιοθήκες, σχολείο ή στα σπίτια φίλων, μάθετε ποια προστατευτικά μέτρα χρησιμοποιούνται στους υπολογιστές.

- Εάν όλες οι προφυλάξεις αποτύχουν και τα παιδιά σας συναντήσουν κάποιον διαδικτυακό διαφθορέα, μην τα κατηγορήσετε. Η ευθύνη είναι αποκλειστικά του διαφθορέα. Δράστε αποφασιστικά, ώστε να σταματήσετε την περαιτέρω επαφή του παιδιού σας με το άτομο αυτό.

Έλεγχος των διαδικτυακών τοποθεσιών που επισκέπτεται ένα παιδί

Υπάρχουν τρόποι για να ελέγξετε τις διαδικτυακές τοποθεσίες που έχει επισκεφτεί το παιδί σας, αλλά έχετε υπόψη ότι τα παιδιά που γνωρίζουν καλά τους υπολογιστές, γνωρίζουν και τον τρόπο να καλύπτουν τα ίχνη τους στο διαδίκτυο.

Τα προγράμματα πλοήγησης, όπως ο Internet Explorer της Microsoft τηρούν συνήθως, ένα ιστορικό των τελευταίων διαδικτυακών τοποθεσιών (ιστοσελίδων) που επισκεφθήκατε. Για να ελέγξετε τις ιστοσελίδες που επισκέπτονται τα παιδιά σας, χρησιμοποιείτε το κουμπί Ιστορικού (History Button) που διαθέτουν οι περισσότερες εκδόσεις του Internet Explorer στην επάνω γραμμή εργαλείων (toolbar). Κάντε διπλό κλικ σε οποιοδήποτε στοιχείο του καταλόγου ιστορικού και θα προβληθεί η διαδικτυακή τοποθεσία.

Τα προγράμματα πλοήγησης δημιουργούν επίσης προσωρινά αντίγραφα των ιστοσελίδων, γνωστά ως αρχεία προσωρινής αποθήκευσης και τα αποθηκεύουν στον υπολογιστή σας. Για να προβάλετε τα προσωρινά αρχεία του Internet Explorer:

1. Στον Internet Explorer, κάντε κλικ στο μενού Tools (Εργαλεία) και επιλέξτε Internet Options (Επιλογές Internet).

2. Στην καρτέλα General (Γενικά), στην περιοχή Temporary Internet Files (Προσωρινά Αρχεία Internet), κάντε κλικ στο κουμπί Settings (Ρυθμίσεις).

3. Στην περιοχή Temporary Internet files folder (Φάκελος προσωρινών αρχείων Internet), κάντε κλικ στο κουμπί View Files (Προβολή αρχείων).

Θα πρέπει να δείτε έναν κατάλογο με τις ιστοσελίδες που εσείς ή το παιδί σας επισκεφτήκατε πρόσφατα, καθώς επίσης και εικόνες που είδατε ή αρχεία cookies που αποθηκεύτηκαν στον υπολογιστή σας.

Το cookie είναι ένα μικρό αρχείο το οποίο τοποθετείται στο σκληρό δίσκο του υπολογιστή του χρήστη από κάποιες ιστοσελίδες, μόλις ο χρήστης επισκεφτεί την συγκεκριμένη ιστοσελίδα. Το cookie καταγράφει προσωπικά στοιχεία του χρήστη, που χρησιμοποιούνται από τις ιστοσελίδες για να τον διευκολύνουν στην πλοήγησή του.

Υπάρχουν, επίσης, πολλά είδη προγραμμάτων λογισμικού που σας επιτρέπουν να παρακολουθήσετε τις διάφορες δραστηριότητες στο διαδίκτυο π.χ. το MSN Premium παρέχει μια συλλογή λειτουργιών γονικού ελέγχου, οι οποίες σας επιτρέπουν να φιλτράρετε το περιεχόμενο του διαδικτύου και σας στέλνει μια εβδομαδιαία αναφορά με λεπτομέρειες για τις τοποθεσίες που επισκέφτηκαν τα παιδιά σας στο διαδίκτυο, τους ανθρώπους με τους οποίους συνομίλησαν και πολλά άλλα.

Τι είναι ιός;

Ιός είναι ένα μικρό πρόγραμμα το οποίο έχει δημιουργηθεί για να αλλάξει τον τρόπο κατά τον οποίο λειτουργεί ένας ηλεκτρονικός υπολογιστής, χωρίς την άδεια ή τη γνώση του χρήστη. Είναι ένα τμήμα ηλεκτρονικού κώδικα ο οποίος προσκολλάται σε ένα λογισμικό ή ένα αρχείο, ώστε να μπορεί να μεταδοθεί από υπολογιστή σε υπολογιστή. Προσβάλει, καθώς μετακινείται, και μπορεί να καταστρέψει το λογισμικό σας, το υλισμικό σας και τα αρχεία σας.

Η απελευθέρωση ενός ιού μπορεί να προκαλέσει την καταστροφή δεδομένων του υπολογιστή σας ή να επιτρέψει την πρόσβαση τρίτων σε αυτόν, στο δίκτυο και σε όλους τους υπολογιστές που είναι συνδεδεμένος.

Με ποιόν τρόπο μεταδίδονται οι ιοί;

Ουσιαστικά όλοι οι ιοί δεν μπορούν να εξαπλωθούν εάν δεν ανοίξετε ή δεν εκτελέσετε κάποιο μολυσμένο πρόγραμμα. Ο κύριος τρόπος διάδοσης των πιο επικίνδυνων ιών είναι μέσω των συνημμένων του ηλεκτρονικού ταχυδρομείου, δηλαδή μέσω των αρχείων τα οποία

αποστέλλονται μαζί με κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου. Ο ιός εκτελείται όταν ανοίξετε ένα προσβλημένο συνημμένο αρχείο.

Άλλοι ιοί διαδίδονται μέσω προγραμμάτων ή αρχείων τα οποία κατεβάζετε από το διαδίκτυο ή από προσβλημένα CD's ή USB's. Ο πιο διαδεδομένος τρόπος να προσβληθεί ο υπολογιστής σας από ιό μέσω διαδικτύου είναι όταν κατεβάζουμε μουσική, παιχνίδια ή γενικά αρχεία από άγνωστες πηγές.

Λογισμικό υποκλοπής spyware

Το λογισμικό υποκλοπής spyware, είναι ένας γενικός όρος για λογισμικό το οποίο εκτελεί συγκεκριμένες ενέργειες, όπως προώθηση διαφημίσεων, συλλογή προσωπικών δεδομένων ή αλλαγή των ρυθμίσεων του υπολογιστή σας χωρίς την εκ των προτέρων συγκατάθεσή σας.

Οι πιο γνωστές μορφές προγραμμάτων υποκλοπής μπορούν να αλλάξουν τη συμπεριφορά του υπολογιστή σας, να τον καθυστερούν υπερβολικά, ακόμη και να του προκαλέσουν βλάβη. Περισσότερο επικίνδυνο είναι το γεγονός ότι τα προγράμματα υποκλοπής μπορούν να παρακολουθήσουν τις συνήθειες περιήγησης των παιδιών, να αποσπάσουν κωδικούς πρόσβασης καθώς επίσης και να επιτρέψουν σε κάποιον εισβολέα να πάρει τον έλεγχο του υπολογιστή σας. Κακόβουλα λογισμικά μπορεί να εγκατασταθούν στον υπολογιστή χωρίς το παιδί να το γνωρίζει ή χωρίς να συναινείτε.

Ένα κακόβουλο πρόγραμμα μπορεί να είναι ενσωματωμένο σε κάποιο πρόγραμμα που σκοπεύετε να κατεβάσετε από το Διαδίκτυο. Για παράδειγμα, ενώ το παιδί κάνει λήψη ενός παιχνιδιού, το "παιχνίδι" μπορεί να βρει στον υπολογιστή προσωπικά στοιχεία του και να τα στείλει σε επιτήδειο χρήστη. Κάποια είδη κακόβουλου λογισμικού

εξαπλώνονται αποστέλλοντας αυτόματα ηλεκτρονικά μηνύματα από τον "μολυσμένο" υπολογιστή όπου έχουν εγκατασταθεί σε κάθε ηλεκτρονική διεύθυνση που βρίσκουν αποθηκευμένη σε αυτόν.

Ο βασικότερος κανόνας για την αποφυγή λήψης και αποθήκευσης λογισμικού υποκλοπής είναι η προσεκτική ανάγνωση όλων των μηνυμάτων που εμφανίζονται στην οθόνη του υπολογιστή. Ο χρήστης δε θα πρέπει σε καμία περίπτωση να κάνει κλικ στο «Ναι» ή το «Όχι» των παραθύρων χωρίς να διαβάζει το περιεχόμενό τους, ενώ θα πρέπει να κλείνει το παράθυρο χωρίς να κάνει κλικ, όταν δεν το καταλαβαίνει.

Συμβουλές για να μην "κολλήσει" ο υπολογιστής σας ιό;

Υπάρχουν πολλοί τρόποι αποφυγής λήψης ιών στον υπολογιστή σας και αποφυγής της πρόσβασης σε ιστοσελίδες με κακόβουλα προγράμματα. Ο πιο βασικός έχει να κάνει με το πόσο ασφαλής είναι η Μηχανή Αναζήτησης που χρησιμοποιείτε.

Η μηχανή αναζήτησης Bing της Microsoft (www.bing.com) προσφέρει δύο βασικές λειτουργίες για την ασφαλή πρόσβαση στο διαδίκτυο. Η πρώτη λειτουργία ενεργοποιείται όταν ένας χρήστης επιλέξει ιστοσελίδα από τα αποτελέσματα της αναζήτησης για να κατεβάσει (download) αρχεία από το διαδίκτυο. Αν η ιστοσελίδα που έχει επιλέξει έχει μολυνθεί από κακόβουλα προγράμματα (malware) ή έχει καταλειφθεί από χάκερς τότε το Bing δεν οδηγεί το χρήστη στη μολυσμένη ιστοσελίδα αλλά τον ενημερώνει για το πρόβλημα.

Η δεύτερη βασική λειτουργία ασφαλείας που προσφέρει το Bing είναι η ικανότητα να μην παρουσιάζει στα αποτελέσματα της αναζήτησης ιστοσελίδες που περιέχουν κακόβουλα προγράμματα (malware) ηλεκτρονικής απάτης (social networking / engineering phishing).

Άλλες γενικές συμβουλές είναι οι εξής:

- Μην κατεβάζετε λογισμικό από πηγή την οποία δεν εμπιστεύεστε.
- Μην ανοίγετε οποιαδήποτε συνημμένα αρχεία ηλεκτρονικού ταχυδρομείου, από μια άγνωστη, ύποπτη ή μη έμπιστη πηγή ή εάν το ΘΕΜΑ (subject) είναι αμφισβητήσιμο ή απροσδόκητο.

- Διαγράφετε τα μηνύματα διαφημιστικού περιεχομένου (spam) και μην απαντάτε σε κανένα από αυτά.

- Προσοχή κατά το σώσιμο (saving) των αρχείων από το διαδίκτυο. Εξασφαλίστε ότι η πηγή είναι νόμιμη και αξιόπιστη. Σιγουρευτείτε ότι ένα πρόγραμμα anti-virus ελέγχει τα αρχεία που σώζονται στο χώρο σας. Εάν δεν είστε βέβαιοι, μην εκκινείτε μια τέτοια διαδικασία.

- Κρατήστε τα σημαντικά σας αρχεία σε κάποιο αποθηκευτικό μέσο (back up). Σε περίπτωση που κάποιος ιός καταστρέψει τα αρχεία σας, θα μπορείτε με αυτόν τον τρόπο να τα αντικαταστήσετε, αποκαθιστώντας τη ζημιά που πιθανόν να έχουν υποστεί.

Ενημερώσεις λειτουργικού συστήματος και προγραμμάτων

Δεν υπάρχει σίγουρος τρόπος να γνωρίζετε εάν το σύστημά σας έχει προσβληθεί από ιό, εκτός εάν κρατάτε ενημερωμένο το λογισμικό προστασίας από ιούς. Οι σημαντικές ενημερώσεις και οι ενημερώσεις υψηλής προτεραιότητας τόσο του λειτουργικού συστήματος όσο και του λογισμικού ασφάλειας του υπολογιστή είναι κρίσιμες για την ασφάλεια και την αξιοπιστία του υπολογιστή σας. Προσφέρουν την πιο πρόσφατη προστασία ενάντια σε κακόβουλες ηλεκτρονικές δραστηριότητες.

Πώς θα βοηθήσετε τα παιδιά να εντοπίζουν την παραπληροφόρηση;

Το διαδίκτυο παρέχει ανεξάντλητους πόρους και ευκαιρίες μάθησης. Περιέχει, όμως, και πάρα πολλές πληροφορίες που μπορεί να μην είναι ούτε ωφέλιμες ούτε αξιόπιστες. Οι χρήστες θα πρέπει να αναπτύξουν ικανότητες κριτικής σκέψης, ώστε να κρίνουν την ακρίβεια των πληροφοριών αυτών. Αυτό ισχύει ιδιαίτερα για τα παιδιά, που συνήθως πιστεύουν πως "Εάν είναι στο διαδίκτυο, πρέπει να είναι αλήθεια".

Μάθετε στα παιδιά σας ότι ο καθένας μπορεί να δημιουργήσει μια διαδικτυακή τοποθεσία και να καταχωρήσει περιεχόμενο, χωρίς να τον ελέγχει κανείς. Μάθετε τα παιδιά σας να χρησιμοποιούν μεγάλο εύρος πηγών πληροφοριών και να ελέγχουν, να αμφισβητούν και να διασταυρώνουν όσα βλέπουν στο διαδίκτυο. Διδάξτε στα παιδιά σας αποτελεσματικές τεχνικές για την εύρεση πληροφοριών στο διαδίκτυο έτσι ώστε να βελτιωθεί σημαντικά η ικανότητά τους να βρίσκουν ποιοτικές πληροφορίες.

Χρόνος χρήσης στο Διαδίκτυο

Η διατήρηση μια υγιούς ισορροπίας μεταξύ των μέσων ψυχαγωγίας και των υπόλοιπων δραστηριοτήτων στις ζωές των παιδιών υπήρξε ανέκαθεν πρόκληση για τους γονείς. Το διαδίκτυο έχει κάνει αυτήν την πρόκληση ακόμη δυσκολότερη. Για την εξισορρόπηση του χρόνου εντός και εκτός του διαδικτύου χρησιμοποιείτε τις ακόλουθες συμβουλές:

- Υπολογίστε πόση ώρα δαπανούν στο διαδίκτυο τα παιδιά σας.
- Αναρωτηθείτε εάν η χρήση του διαδικτύου από το παιδί σας επηρεάζει την απόδοσή του στο σχολείο, την υγεία του και τις σχέσεις του με τα άλλα μέλη της οικογένειας και τους φίλους.
- Εάν τα παιδιά σας ενδιαφέρονται αποκλειστικά για διαδικτυακά παιχνίδια, δοκιμάστε να τους προτείνετε κάτι σχετικό εκτός διαδικτύου.
- Καθιερώστε την ισορροπία. Ενθαρρύνετε και υποστηρίξτε τη συμμετοχή του παιδιού σας σε άλλες δραστηριότητες, ειδικά αθλοπαιδιές με άλλα παιδιά και προτείνετε τους να χρησιμοποιούν το διαδίκτυο για να υποστηρίξουν τις δραστηριότητες αυτές.
- Βοηθήστε το παιδί σας να αποκτήσει κοινωνικές σχέσεις εκτός του διαδικτύου. Ενθαρρύνετε τις δραστηριότητες που θα φέρουν το παιδί σας σε επαφή με άλλα παιδιά με παρόμοια ενδιαφέροντα.
- Παρακολουθήστε τα παιδιά σας. Αναζητήστε προγράμματα λογισμικού που παρακολουθούν και περιορίζουν τη χρήση του διαδικτύου, όπως τα εργαλεία γονικού ελέγχου.
- Ο τελικός σας στόχος θα πρέπει να είναι να βοηθήσετε το παιδί σας να αναπτύξει αυτοέλεγχο, πειθαρχία και υπευθυνότητα στη χρήση του διαδικτύου.

Συμπεριφορά στο Διαδίκτυο

Η περιήγηση στο διαδίκτυο, μπορεί να είναι διασκεδαστική, χρήσιμη και κοινωνικά ωφέλιμη, τόσο για ενήλικες όσο και για παιδιά. Αλλά είναι σημαντικό για όλους τους νέους "πολίτες" του διαδικτύου, οι οποίοι ονομάζονται και netizens, να θυμούνται ότι υπάρχουν και άλλοι περιηγητές στο διαδίκτυο. Όπως και σε όλες τις άλλες δημόσιες δραστηριότητες, υπάρχουν κανόνες συμπεριφοράς που πρέπει να ακολουθούνται.

Το διαδίκτυο έχει το δικό του savoir vivre που ονομάζεται «Network Etiquette» ή απλά «Netiquette». Με τον όρο «Netiquette» ονομάζουμε ένα σύνολο κανόνων για την ευγενική και φιλική «συμβίωση» στους εικονικούς κόσμους. Υπάρχουν τρόποι επικοινωνίας και ενέργειες που θεωρούνται «απρεπείς» και θα πρέπει να αποφεύγονται. Παραθέτουμε κάποιους από τους βασικούς κανόνες:

- Να ακολουθείτε το χρυσό κανόνα: Να φέρεστε στους άλλους όπως θέλετε να σας φέρονται και αυτοί.
- Ακολούθησε τους ίδιους κανόνες καλής συμπεριφοράς που έχετε μάθει και στην αληθινή ζωή. Στο διαδίκτυο ισχύει το ίδιο επίπεδο ηθικής και σωστής συμπεριφοράς.
- Να θυμάστε πάντα ότι στο άλλο άκρο της σύνδεσης βρίσκεται ένας άνθρωπος, και όχι μια μηχανή, άσχετα αν επικοινωνείς μέσω αυτής. Σκεφτείτε πριν γράψετε κάτι, αν θα το λέγατε με τις ίδιες λέξεις στον παραλήπτη, έχοντάς τον μπροστά σας. Είναι απίστευτα εύκολο να γίνει παρεξήγηση μέσω ενός ηλεκτρονικού μηνύματος, απλά επειδή ο παραλήπτης δεν μπόρεσε να καταλάβει το ύφος και το περιεχόμενο του μηνύματός σας
- Η συγγραφή ενός ηλεκτρονικού ταχυδρομείου με ΚΕΦΑΛΑΙΑ γράμματα ισοδυναμεί με φωνές. Μην το κάνετε, εκτός και εάν είναι πραγματικά απαραίτητο.

- Η αποστολή ηλεκτρονικού ταχυδρομείου junk ή spam απαγορεύεται, και είναι πολύ ενοχλητική.
- Να συγχωρείτε τα λάθη των άλλων, ιδίως των νεοφερμένων.
- Να διατηρείτε πάντοτε την ψυχραιμία σας, ιδίως όταν κάποιος σας προσβάλει (ή νομίζετε ότι σας προσέβαλε).
- Μην χρησιμοποιείτε ακατάλληλη ή προσβλητική γλώσσα.
- Μην στέλνετε και μην προωθείτε άχρηστη αλληλογραφία (Spam)
- Να προσέχετε την ορθογραφία σας, να είστε σαφής και να γράφετε σύντομα μηνύματα.
- Όταν λαμβάνετε μέρος σε δωμάτια συνομιλίας, μην διακόπτετε τους άλλους και μην ξεφεύγετε από το θέμα.
- Χρησιμοποιήστε φατσούλες για να μεταδώσετε το χιούμορ και το σαρκασμό, και μάθετε τις συνηθισμένες διαδικτυακές συντομογραφίες.

Φατσούλες

Οι πρώτοι χρήστες του Διαδικτύου εφηύραν τις φατσούλες (εικονικές εκφράσεις του προσώπου που αποτελούνται από βασικούς χαρακτήρες του πληκτρολογίου) για την καλύτερη επικοινωνία και τη μεταφορά κάποιων συναισθημάτων μέσω ενός ηλεκτρονικού μηνύματος. Ορισμένα παραδείγματα από φατσούλες που χρησιμοποιούνται συχνά είναι:

:-) ή :) Χαρούμενο ή αστειευόμενο

;-) Κλείσιμο ματιού

:-(Λύπη

:-I Αμφιβολία

:-o Έκπληξη ή ανησυχία

:-x Δεν λέω τίποτα

:-p Βγάλσιμο της γλώσσας (συνήθως για αστείο)

Διαδικτυακές συντομογραφίες

Καθώς η ομιλία είναι ταχύτερη από τη γραφή, οι έμπειροι χρήστες συνηθίζουν να μειώνουν τις κοινές εκφράσεις σε μερικά μόνο γράμματα.

Ορισμένα παραδείγματα συχνά χρησιμοποιούμενων συντομογραφιών είναι:

ASAP (As soon as possible - το συντομότερο δυνατό)
BBL (Be back later - θα επιστρέψω αργότερα)
BRB (Be right back - επιστρέφω σε λίγο)
LOL (Laughing out loud - Έντονο γέλιο)
ROTFL (Rolling on the floor laughing - Ξεκαρδίστηκα)
BTW (By the way - Με την ευκαιρία)
OIC (Oh, I see - Κατάλαβα)
CUL (See you later - Τα λέμε)
OTOH (On the other hand - Από την άλλη)
GMTA (Great minds think alike - Τα μεγάλα πνεύματα συναντιόνται)
IMHO (In my humble opinion - Κατά την ταπεινή μου γνώμη)
RUOK (Are you OK? - Είσαι εντάξει;)
TIA (Thanks in advance - Ευχαριστώ εκ των προτέρων)
J/K (Just kidding - Αστειεύομαι)
TTFN (Ta-ta for now - Γεια χαρά)

Χρήση οικογενειακών κανόνων

Προτού τα παιδιά σας αρχίσουν να εξερευνούν το νέο ορίζοντα του Διαδικτύου, καλό θα είναι να βεβαιωθείτε πως καταλαβαίνουν τι πρέπει και τι δεν πρέπει να κάνουν στο χώρο αυτό. Μια ιδέα είναι να γράψετε έναν κώδικα συμπεριφοράς στο διαδίκτυο που θα συμφωνήσουν όλοι να τηρούν. Μπορείτε να δημιουργήσετε διαφορετικούς κανόνες χρήσης για κάθε παιδί στην οικογένεια, με κανόνες χρήσης του διαδικτύου κατάλληλους για την κάθε ηλικία.

ΜΙΚΡΟΙ ΕΘΕΛΟΝΤΕΣ

Παραθέτουμε πιο κάτω ένα υπόδειγμα κανόνων χρήσης για κάθε οικογένεια. Οι κανόνες είναι εισηγήσεις που μπορείτε να αντιγράψετε και να αλλάξετε, ανάλογα με τις ανάγκες της οικογένειας. Μόλις όλοι στην οικογένεια συμφωνήσουν να τηρούν τους κανόνες, κολλήστε τους πλάι σε κάθε υπολογιστή του σπιτιού, ώστε να παραμείνουν μια συνεχής υπενθύμιση για όλους.

- Συζητώ με τους γονείς μου για να μάθω τους κανόνες χρήσης του διαδικτύου, οι οποίοι περιλαμβάνουν τις τοποθεσίες που επιτρέπεται να επισκεφθώ, τι μπορώ να κάνω, πότε μπορώ να συνδέομαι στο διαδίκτυο και για πόση ώρα μπορώ να παραμείνω συνδεδεμένος (____ λεπτά ή ____ ώρες).
- Ποτέ δεν αποκαλύπτω προσωπικά δεδομένα, όπως η διεύθυνση του σπιτιού, ο αριθμός τηλεφώνου, η διεύθυνση εργασίας των γονέων μου ή ο αριθμός τηλεφώνου, αριθμούς πιστωτικών καρτών ή το όνομα του σχολείου μου, χωρίς την άδεια των γονιών μου.
- Ενημερώνω αμέσως τους γονείς μου, εάν δω ή λάβω κάτι από το διαδίκτυο που με ενοχλεί ή νιώθω ότι με απειλεί. Σε αυτά συγκαταλέγονται μηνύματα ηλεκτρονικού ταχυδρομείου, άμεσα μηνύματα, διαδικτυακές τοποθεσίες ή ακόμη και κάτι στην τακτική αλληλογραφία με διαδικτυακούς φίλους.
- Ποτέ δε θα συμφωνήσω να συναντήσω κάποιον που γνώρισα στο διαδίκτυο, χωρίς την άδεια των γονέων μου.
- Ποτέ δε θα στείλω φωτογραφίες δικές μου ή μελών της οικογένειάς μου σε άλλους, μέσω του διαδικτύου ή με την τακτική αλληλογραφία, χωρίς την άδεια των γονιών μου.
- Ποτέ δε θα αποκαλύψω τους κωδικούς πρόσβασης στο διαδίκτυο σε κανέναν (ούτε και στους καλύτερούς μου φίλους), παρά μόνο στους γονείς μου.
- Θα φέρομαι σωστά όταν βρίσκομαι στο διαδίκτυο και δε θα κάνω τίποτα που μπορεί να προσβάλει ή να εξοργίσει άλλους ή είναι παράνομο.
- Ποτέ δε θα κατεβάσω, δε θα εγκαταστήσω και δε θα αντιγράψω, ακατάλληλο, παράνομο ή προσωπικό περιεχόμενο.
- Ποτέ δε θα κάνω κάτι στο διαδίκτυο που κοστίζει χρήματα, χωρίς την άδεια των γονιών μου.

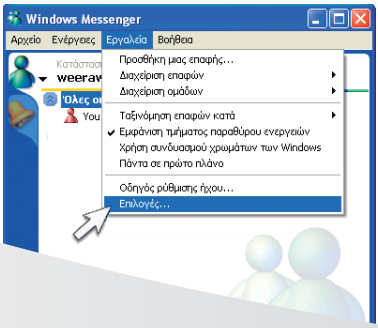
Άμεσα Μηνύματα (Instant Messages)

Ανταλλαγή άμεσων μηνυμάτων (MSN)

Η ανταλλαγή άμεσων μηνυμάτων (Instant Messages) και η συζήτηση στα διαδικτυακά δωμάτια συνομιλίας (chat rooms) είναι ένας τρόπος επικοινωνίας μέσω διαδικτύου με τον οποίο μπορείς να στέλνεις γραπτά μηνύματα σε άλλους χρήστες, τα οποία οι τελευταίοι θα βλέπουν άμεσα στην οθόνη τους. Η διαφορά μεταξύ της επικοινωνίας μέσω προγραμμάτων άμεσων μηνυμάτων, όπως το Windows Live Messenger και τα chat rooms, είναι ότι στα πρώτα επικοινωνείς με άτομα που έχεις επιλέξει να είναι στη λίστα των επαφών σου.

Ανεπιθύμητα άμεσα μηνύματα

Όπως μπορείτε να λάβετε ανεπιθύμητα μηνύματα στο ηλεκτρονικό σας ταχυδρομείο έτσι μπορείτε να λάβετε και ανεπιθύμητα άμεσα μηνύματα (Instant messaging, Messenger, IRC κ.α.) που συχνά αναφέρονται ως "spim". Αυτά τα άμεσα μηνύματα μπορεί να προέρχονται από κάποιον τελείως άγνωστο ή και από ανθρώπους που γνωρίζετε. Μπορεί επίσης να περιέχουν και επικίνδυνους ιούς.



ΜΙΚΡΟΙ ΕΘΕΛΟΝΤΕΣ

Κοινωνική δικτύωση

Ιστοσελίδες κοινωνικής δικτύωσης (Facebook)

Οι τοποθεσίες διαδικτύου κοινωνικής δικτύωσης είναι πολύ δημοφιλείς όχι μόνο μεταξύ παιδιών αλλά και μεταξύ μεγάλων. Τα παιδιά χρησιμοποιούν τις τοποθεσίες διαδικτύου κοινωνικής δικτύωσης για να συνδέονται με άλλα παιδιά που ίσως να ζουν στην άλλη άκρη του κόσμου και με παιδιά που συναντούν κάθε μέρα στους διαδρόμους του σχολείου. Τα παιδιά μπορούν να χρησιμοποιήσουν τοποθεσίες κοινωνικής δικτύωσης για να εκφράσουν τα συναισθήματά τους, να ανεβάσουν φωτογραφίες ή ακόμα και να ελέγξουν, ανεπίσημα, τα παιδιά που συναντούν σε κοινωνικές και άλλες εκδηλώσεις.

Χρήση ιστοσελίδων κοινωνικής δικτύωσης με μεγαλύτερη ασφάλεια

Τα παιδιά χρησιμοποιούν τοποθεσίες κοινωνικής δικτύωσης που είναι σχεδιασμένες για ενηλίκους, όπως Windows Live Spaces, YouTube, MySpace, Flickr, Twitter, Facebook και άλλα. Θα πρέπει να κατανοήσουν ότι πολλές από αυτές τις ιστοσελίδες είναι προσβάσιμες τόσο από φιλικά τους άτομα όσο και από άγνωστα.

Πέρα από τη δυνατότητα ανταλλαγής μηνυμάτων, υπάρχουν ομάδες συζητήσεων, παιχνίδια και ένα σωρό εφαρμογές καθώς και η δυνατότητα να μοιράζεται κανείς με την παρέα του ένα βίντεο που είδε στο διαδίκτυο ή ακόμη και ένα ενδιαφέρον άρθρο.

Μαζί με όλα αυτά όμως, οι χρήστες μοιράζονται προσωπικά τους δεδομένα. Υπάρχουν αρκετοί τρόποι με τους οποίους μπορείτε να βοηθήσετε τα παιδιά σας να χρησιμοποιούν τις τοποθεσίες κοινωνικής δικτύωσης με μεγαλύτερη ασφάλεια:

- Να μην ανεβάζουν στο προφίλ τους φωτογραφίες όπου φαίνεται καθαρά η τοποθεσία στην οποία βρίσκονται (σπίτι, σχολείο ή μέρη που συχνάζουν) ή φωτογραφίες που θα τους έφερναν σε δύσκολη θέση.
- Να γνωρίζουν ότι από τη στιγμή που προσθέτουν στη λίστα των φίλων τους κάποιο άτομο, αυτό αποκτά πρόσβαση στα προσωπικά δεδομένα που εμφανίζονται στο προφίλ τους, μεταξύ των οποίων η ηλικία, φωτογραφίες και τα στοιχεία επικοινωνίας τους.
- Από τη στιγμή που δημιουργούν το εικονικό τους προφίλ θα πρέπει να πάνε στο μενού των ρυθμίσεων για τη διαχείριση των προσωπικών τους δεδομένων (συνηθέστερα θα το βρείτε στα αγγλικά ως privacy settings) και να αλλάξουν τις προεπιλεγμένες ρυθμίσεις.
- Συζητήστε με τα παιδιά σας για τις εμπειρίες τους. Ενθαρρύνετε τα παιδιά σας να σας ενημερώσουν αν συναντήσουν σε μια από αυτές τις τοποθεσίες κάτι που θα τα κάνει να νιώσουν ανήσυχα, άσχημα ή ότι απειλούνται. Διατηρήστε την ψυχραιμία σας και υπενθυμίστε στα παιδιά σας ότι δεν θα τιμωρηθούν εάν σας ενημερώσουν για οτιδήποτε. Δουλέψετε μαζί τους για να τους βοηθήσετε να επιλύσουν την κατάσταση για ένα θετικό αποτέλεσμα.
- Να επιμένετε ώστε τα παιδιά σας να μην συναντήσουν προσωπικά κάποιο άτομο με το οποίο επικοινωνούν αποκλειστικά μέσω διαδικτύου και ενθαρρύνετέ τα να επικοινωνούν με πρόσωπα που γνωρίζουν εκτός του διαδικτύου.
- Πολλές τοποθεσίες κοινωνικής δικτύωσης επιτρέπουν στα παιδιά να συμμετέχουν σε δημόσιες ομάδες που περιλαμβάνουν όλους όσους πηγαίνουν σε κάποιο συγκεκριμένο σχολείο. Συμβουλεύστε τα παιδιά σας να μην δημοσιεύουν στοιχεία τα οποία μπορούν να αναγνωριστούν από αγνώστους.
- Τα παιδιά χρησιμοποιούν τις ιστοσελίδες κοινωνικής δικτύωσης για να γράφουν άρθρα και ποιήματα, στα οποία συχνά εκφράζουν έντονα τα συναισθήματά τους. Τα παιδιά θα πρέπει να είναι πολύ προσεκτικά για το τι εκμυστηρεύονται στις σελίδες αυτές καθώς υπάρχουν επιτήδειοι διαφθορείς που εκμεταλλεύονται τέτοιες προσωπικές στιγμές παρέχοντας στοργή και φιλία για να εξαπατήσουν ένα παιδί.

Ηλεκτρονικό Ταχυδρομείο (e-Mail)

Ηλεκτρονικό Ταχυδρομείο

Στην απλούστερη μορφή του, το ηλεκτρονικό ταχυδρομείο (e-mail) δεν είναι τίποτε άλλο από ένα ηλεκτρονικό μήνυμα από έναν υπολογιστή προς κάποιον άλλο. Μέσω του e-mail επιτυγχάνεται η γρήγορη μεταβίβαση αλληλογραφίας καθώς επίσης αρχείων εικόνας και κειμένου. Κάποιος μπορεί να λάβει προσωπικά ή επαγγελματικά μηνύματα, επισυνάπτοντας μάλιστα σε αυτά οποιουδήποτε τύπου αρχεία, είτε αυτό θα είναι εικόνα, ήχος, βίντεο είτε κάποιο αρχείο Word ή Excel.

Για τη χρήση του Ηλεκτρονικού Ταχυδρομείου, απαιτείται η κατοχή λογαριασμού με κάποια από τις υπηρεσίες πρόσβασης στο διαδίκτυο. Κάθε λογαριασμός Ηλεκτρονικού Ταχυδρομείου, είναι συνυφασμένος με μια διεύθυνση Ηλεκτρονικού Ταχυδρομείου. Ο λογαριασμός αυτός επιτρέπει την αποθήκευση και διαχείριση όλων των εισερχόμενων και εξερχόμενων μηνυμάτων.

Αν και οι περισσότερες υπηρεσίες πρόσβασης στο διαδίκτυο χρεώνουν τους λογαριασμούς αυτούς, εντούτοις, υπάρχουν υπηρεσίες, οι οποίες παρέχουν τέτοιου είδους λογαριασμούς δωρεάν, όπως το hotmail της Microsoft.

Απάτες Ηλεκτρονικού Ταχυδρομείου

Μια καλή κυρία από τη Νιγηρία θέλει να μοιραστεί μαζί σου την κληρονομιά που της άφησε μια θεία της, η οποία έφυγε πρόσφατα από το μάταιο τούτο κόσμο. Και σαν να μην έφτανε αυτό, κέρδισες και σε κλήρωση που έγινε στην Ισπανία, ένα τεράστιο ποσό! Το μόνο που πρέπει να κάνεις είναι να συμπληρώσεις μερικά στοιχεία στο διαδίκτυο και μετά μπορείς να πας να διαλέξεις το κότερο που θα αγοράσεις.

Τέτοια μηνύματα λαμβάνουν εκατομμύρια χρήστες την ημέρα ανά τον κόσμο. Πρόκειται για μηνύματα απάτης που σκοπό έχουν να αποσπάσουν χρήματα και στοιχεία τραπεζικών λογαριασμών από τα υποψήφια θύματα και είναι γνωστά ως phishing και scams.

Phishing

Το "Phishing" είναι ένας τύπος εξαπάτησης που έχει σχεδιαστεί για την κλοπή της ταυτότητάς σας. Οι επιτήδειοι της ηλεκτρονικής απάτης σας πλησιάζουν με ψεύτικα προσχήματα και προσπαθούν να σας πείσουν να κοινοποιήσετε σημαντικές προσωπικές πληροφορίες, όπως αριθμούς πιστωτικών καρτών, κωδικούς πρόσβασης ή δεδομένα του λογαριασμού σας. Οι απάτες ψαρέματος μπορεί να γίνουν αυτοπροσώπως ή μέσω τηλεφώνου, ενώ διακινούνται μέσω ανεπιθύμητων ηλεκτρονικών μηνυμάτων, pop-up windows ή άμεσων μηνυμάτων (Instant messaging).

Πώς να διακρίνετε μια απάτη ψαρέματος;

Μια κοινή τεχνική ψαρέματος είναι το άνοιγμα ενός ψεύτικου αναδυόμενου παραθύρου (pop-up window) όταν κάποιος κάνει κλικ σε ένα ηλεκτρονικό μήνυμα που παρουσιάζεται στη οθόνη του. Μπορεί να φαίνεται πολύ πειστικό ή μπορεί να εμφανίζεται πάνω από ένα παράθυρο που εμπιστεύεστε. Ακόμη και εάν το αναδυόμενο παράθυρο φαίνεται πολύ επίσημο ή διακηρύσσει πως είναι ασφαλές, θα πρέπει να αποφεύγετε να εισάγετε ευαίσθητα προσωπικά δεδομένα γιατί δεν υπάρχει τρόπος να ελέγξετε την πιστοποίηση ασφάλειας που παρέχει.

Ανεπιθύμητα μηνύματα (Spam)

Το e-mail spam είναι συνήθως ένα ανεπιθύμητο / διαφημιστικό ηλεκτρονικό μήνυμα. Εάν λάβετε ένα ηλεκτρονικό μήνυμα που πιθανόν να είναι ανεπιθύμητο, δεν θα πρέπει να απαντήσετε σε αυτό, να κάνετε

κλικ ή να το προωθήσετε. Εάν είναι δυνατόν θα πρέπει να το διαγράψετε χωρίς να το ανοίξετε ή να κάνετε κλικ σε κάποιο σύνδεσμο μέσα σε αυτό.

Το spam είναι ενοχλητικό, γιατί πιθανόν να εμπεριέχει απάτη να μολύνει τον υπολογιστή σας με ιό ή άλλο κακόβουλο λογισμικό. Μερικά βήματα που μπορείτε να ακολουθήσετε ώστε να προστατευτείτε από τα ανεπιθύμητα μηνύματα είναι:

- Μην δίνετε σε οποιονδήποτε την ηλεκτρονική σας διεύθυνση.
- Χρησιμοποιήστε ενημερωμένα φίλτρα κατά των ανεπιθύμητων μηνυμάτων (anti-spam).
- Ποτέ μην ανοίγετε τα συνημμένα των μηνυμάτων εκτός και αν γνωρίζετε περί τίνος πρόκειται.

Απάτη με pharming (παραπλάνηση)

"Pharming" σημαίνει παραπομπή από μία ιστοσελίδα σε μια άλλη πανομοιότυπη, έτσι ώστε να σας ξεγελάσουν και να καταχωρήσετε το όνομα χρήστη και τον κωδικό χρήστη στη βάση δεδομένων της πλαστής ιστοσελίδας. Ιστοσελίδες τραπεζών ή αντίστοιχων οικονομικών οργανισμών είναι συχνά στόχοι τέτοιων επιθέσεων, κατά τις οποίες εγκληματίες προσπαθούν να αποσπάσουν προσωπικά δεδομένα, με σκοπό να βρουν πρόσβαση στον τραπεζικό σας λογαριασμό, να κλέψουν την ταυτότητά σας ή να διαπράξουν άλλου είδους απάτη στο όνομά σας.

Παιχνίδια (Games)

Παιχνίδια και το Διαδίκτυο

Ίσως το διαδίκτυο να μην ήταν και τόσο συναρπαστικό για τα παιδιά αν δεν υπήρχαν τόσα παιχνίδια. Υπάρχουν πολλών ειδών παιχνίδια στο διαδίκτυο που είτε παίζονται μέσω του διαδικτύου με πολλούς παίχτες είτε ένα παιδί μπορεί να το κατεβάσει στον υπολογιστή του και να παίζει από εκεί. Ένα παιδί μπορεί να επιλέξει μεταξύ διαφόρων ειδών παιχνίδια, όπως παιχνίδια δράσης, εξομοίωσης, σπαζοκεφαλιές, αθλητικά, στρατηγικής κ.λπ.

Τα παιδιά και το παιχνίδι

Μερικά παιχνίδια μπορεί να έχουν περιεχόμενο που να ενοχλεί και που ενδεχομένως να είναι ακατάλληλο για την ηλικία του παιδιού σας. Ζητάτε από τα παιδιά σας να σας συμβουλευτούν πριν χρησιμοποιήσουν ή αγοράσουν κάποιο παιχνίδι. Σαν γονείς βεβαιωθείτε ότι είναι κατάλληλο, διασκεδαστικό και εκπαιδευτικό για το παιδί σας.

Υπάρχουν παιχνίδια τα οποία ταξιδεύουν τα παιδιά σε ένα απέραντο εικονικό κόσμο. Ελέγξτε εάν ο εικονικός κόσμος που χρησιμοποιείται από τα παιδιά σας έχει γονικό έλεγχο ή οποιοδήποτε εργαλείο που φιλτράρει ανεπιθύμητες ιστοσελίδες.

Μπορείτε να κάνετε την εμπειρία των παιχνιδιών του παιδιού σας ασφαλή, κατάλληλη για την ηλικία του, φιλική, διασκεδαστική, ακόμη και εκπαιδευτική εάν ενημερωθείτε για την κοινότητα των παιχνιδιών, τις αξιολογήσεις των παιχνιδιών και τον τρόπο χρήσης των εργαλείων προστασίας προσωπικών δεδομένων και ασφαλείας, που είναι ενσωματωμένα στα παιχνίδια.

Ακολουθούν μερικές βασικές συμβουλές για να προστατεύσετε τα παιδιά σας, όταν παίζουν παιχνίδια και ανταγωνίζονται στο διαδίκτυο:

- Οι γονείς πρέπει να εξοικειώνονται με τα παιχνίδια και να γνωρίζουν πώς τα παιδιά ξοδεύουν το χρόνο τους στο διαδίκτυο. Προσπαθήστε να αναζητήσετε μια σύνοψη ή μια κριτική παρουσίαση του περιεχομένου του παιχνιδιού ή ακόμα καλύτερα, παίξτε το εσείς οι ίδιοι πρώτα.

- Παρακολουθείτε τα όταν παίζουν και συζητήστε μαζί τους γι' αυτά. Εξηγήστε τους γιατί ορισμένα παιχνίδια δεν είναι κατάλληλα.

- Τα online παιχνίδια συνήθως παίζονται σε διαδικτυακές κοινότητες όπου απαιτείται η αλληλεπίδραση των παικτών με άγνωστους συμπαίκτες. Παρακολουθήστε τις συνομιλίες και τα μηνύματα κατά τη διάρκεια του παιχνιδιού. Εάν κάποιος παίκτης χρησιμοποιεί ακατάλληλη γλώσσα, ενθαρρύνετε το παιδί σας να σας το αναφέρει αμέσως. Γνωρίζοντας το όνομα του χρήστη αυτού θα μπορέσετε να αποκλείσετε τα μηνύματά του ή / και να τον αναφέρετε στους διαχειριστές του παιχνιδιού.

- Αναζητάτε πάντοτε την ηλικιακή ταξινόμηση στη συσκευασία ενός παιχνιδιού ή μέσω της μηχανής αναζήτησης στον παρόντα διαδικτυακό τόπο. Θα πρέπει να έχετε υπόψη σας ότι τα online παιχνίδια μερικές φορές επιτρέπουν τη λήψη επιπλέον λογισμικού, το οποίο μπορεί να τροποποιήσει το περιεχόμενο του παιχνιδιού και επακόλουθα την ηλικιακή του ταξινόμηση.

- Προσπαθήστε να καθορίζετε από πριν ποια παιχνίδια, για πόση ώρα και πότε μπορούν να παίζουν τα παιδιά σας.

- Το παιδί θα πρέπει να είναι επιφυλακτικό στην επικοινωνία που πραγματοποιεί με τους συμπαίκτες του σε διαδικτυακά παιχνίδια.

- Ενθαρρύνετε τα παιδιά σας να επικοινωνούν και να μοιράζονται τις εμπειρίες τους από τα παιχνίδια και να κάνουν συγκρίσεις με τις καταστάσεις της πραγματικής ζωής.

- Χρησιμοποιήστε τη φωνητική συνομιλία με σύνεση. Ορισμένα συστήματα παιχνιδιού επιτρέπουν τη φωνητική συνομιλία με άλλους παίκτες, με τη χρήση σετ ακουστικών (η λειτουργία αυτή δεν συνίσταται για μικρά παιδιά).

- Πείτε στο παιδί σας να χρησιμοποιεί ονόματα χρήστη ή «χαρακτήρα» τα οποία να μην αποκαλύπτουν τα προσωπικά του στοιχεία ή να μην υποκινούν την παρενόχληση.

Διαδικτυακός τζόγος

Κατά τη διάρκεια διερεύνησης του διαδικτύου τα παιδιά ανακαλύπτουν τοποθεσίες τυχερών παιχνιδιών. Οι τοποθεσίες τυχερών παιχνιδιών συνήθως περιέχουν παιχνίδια με κάρτες, πίνακες, λέξεις, arcade ή παζλ, με αυτόματη παρακολούθηση και προβολή του σκορ και συνήθως αφορούν το κέρδος ή την απώλεια αληθινών χρημάτων.

Η χρήση των τυχερών παιχνιδιών από παιδιά είναι παράνομη. Θα πρέπει σαν γονείς να συμβουλεύετε τα παιδία σας για τους κινδύνους του τζόγου και να τα καθοδηγείτε ώστε να αποφεύγουν να παίζουν τέτοιου είδους παιχνίδια. Εξηγήστε τους ότι ο διαδικτυακός τζόγος είναι εθιστικός.

Η συμμετοχή σε τυχερά παιχνίδια στο διαδίκτυο απαιτεί συνήθως τη χρήση πιστωτικής κάρτας. Βεβαιωθείτε ότι τα παιδιά σας δεν έχουν πρόσβαση στην πιστωτική σας κάρτα χωρίς την άδεια σας.

Αγορές από το Διαδίκτυο (e-Commerce)

Ηλεκτρονικό κατάστημα

Ένα ηλεκτρονικό κατάστημα είναι ένας διαδικτυακός χώρος όπου μπορείτε να βρείτε πληροφορίες για προϊόντα μέσω διαθέσιμων καταλόγων, να επιλέξετε και να αγοράσετε προϊόντα και να πληρώσετε μέσω πιστωτικής κάρτας ή με άλλο ηλεκτρονικό μέσο. Η ασφαλής πρόσβαση και συναλλαγή με ένα ηλεκτρονικό κατάστημα εξαρτάται από το κύρος και την υποδομή που διαθέτει το συγκεκριμένο κατάστημα.

Χρήση του Διαδικτύου για αγορά προϊόντων

Τα παιδιά εξοικειώνονται πολύ γρήγορα στη χρήση του διαδικτύου για αγορά προϊόντων. Κάθε τέτοια αγορά θα πρέπει να γίνεται με τη συγκατάθεση των γονιών. Η συγκατάθεση θα πρέπει να δίνεται μετά από τους πιο κάτω ελέγχους:

- Ελέγξτε πρώτα το υπόβαθρο του καταστήματος που θα αγοράσετε. Αναζητήστε μια διεύθυνση, ζητήστε να σας στείλουν ταχυδρομικώς έναν κατάλογο ή τηλεφωνήστε και μιλήστε σε κάποιον εκπρόσωπο της εταιρείας.

- Ερευνήστε την τοποθεσία Web για σφραγίδες έγκρισης από τρίτους όπως BBBOnLine (Better Business Bureau Online) ή στην ενότητα TRUSTe. Οι εταιρείες μπορούν να βάλουν αυτές τις σφραγίδες στις τοποθεσίες τους εάν πληρούν τα αυστηρά πρότυπα του φορέα, π.χ. σχετικά με την αντιμετώπιση των παραπόνων και των διαφορών και τη χρήση των προσωπικών δεδομένων. Εάν δεν υπάρχουν οι σφραγίδες αυτές σε εμφανές σημείο της τοποθεσίας, ψάξτε στην πολιτική απορρήτου ή στους "Όρους χρήσης", η πρόσβαση στους οποίους θα πρέπει να είναι εύκολη από την τοποθεσία Web.

- Μάθετε τη γνώμη των υπόλοιπων αγοραστών σχετικά με κάποιο ηλεκτρονικό κατάστημα σε συγκριτικές τοποθεσίες, όπως η Epionions και η Bizrate.

- Ελέγξτε τις μεθόδους και τις πολιτικές αποστολής για να βρείτε τους μεταφορείς που χρησιμοποιούν, τα έξοδα αποστολής, καθώς και εάν παρέχουν παρακολούθηση και ασφάλιση της αποστολής.

- Μάθετε τον τρόπο προέλευσης της αποστολής. Τα αγαθά αποστέλλονται συχνά από διεθνής προορισμούς, που απαιτούν τελωνιακή έγκριση και επιπλέον χρόνο.

- Εμπιστευτείτε το ένστικτό σας, εάν κάποια τοποθεσία ικανοποιεί όλα τα παραπάνω κριτήρια τότε, κατά πάσα πιθανότητα, η τοποθεσία είναι νόμιμη και αξιόπιστη. Αλλά, όπως γίνεται και με τα περισσότερα πράγματα εντός και εκτός διαδικτύου, εάν κάτι δεν σας αρέσει σε αυτό το κατάστημα, αγνοήστε το και ψωνίστε από κάπου αλλού.

Χρήση πιστωτικής κάρτας στο Διαδίκτυο

Προτού υποβάλλετε τα στοιχεία της πιστωτικής σας κάρτας ή άλλα προσωπικά σας στοιχεία σε ένα ηλεκτρονικό κατάστημα βεβαιωθείτε για την ασφάλεια και την αξιοπιστία του.

Προτού πληκτρολογήσετε τον αριθμό της πιστωτικής σας κάρτας, βεβαιωθείτε ότι το κατάστημα που επιλέξατε τηρεί τους παρακάτω κανόνες:

- Η εταιρεία πρέπει να απαιτεί μόνο τα προσωπικά δεδομένα που είναι απαραίτητα για την ολοκλήρωση της αγοράς. Πιθανόν να πληκτρολογήσετε τον αριθμό της πιστωτικής σας κάρτας, τη διεύθυνση και τον αριθμό τηλεφώνου. Να είστε επιφυλακτικοί όταν σας ζητούν άλλες πληροφορίες, όπως τον αριθμό κοινωνικής ασφάλισης ή αριθμούς τραπεζικών λογαριασμών.

- Το ηλεκτρονικό κατάστημα που επισκέπτεστε θα πρέπει να χρησιμοποιεί ασφαλή τεχνολογία. Όταν μεταβείτε στην οθόνη εισαγωγής του αριθμού της πιστωτικής σας κάρτας ή άλλων προσωπικών στοιχείων, βεβαιωθείτε ότι η διεύθυνση Web αρχίζει με τα γράμματα https (π.χ. https://www.tailspintoys.com/) και ότι στο κάτω μέρος της οθόνης εμφανίζεται ένα κλειδωμένο λουκέτο.

- Εάν πιστεύετε πως πέσατε θύμα απάτης με την πιστωτική σας κάρτα, θα πρέπει το ταχύτερο δυνατό να επικοινωνήσετε με το κέντρο εξυπηρέτησης της JCC ή με το κέντρο εξυπηρέτησης της τράπεζάς σας.

- Κάθε φορά που λαμβάνετε τις αναλυτικές καταστάσεις της πιστωτικής σας κάρτας εξετάστε τις προσεκτικά. Ψάξτε για συναλλαγές που δεν κάνατε, λογαριασμούς που δεν ανοίξατε και ανεξήγητες χρεώσεις.

Ασφαλείς ιστοσελίδες

Η εμφάνιση του εικονιδίου με το κίτρινο λουκέτο σε μια διαδικτυακή τοποθεσία είναι σημάδι ασφαλούς ιστοσελίδας, επειδή το κλειστό λουκέτο υποδεικνύει πως η ιστοσελίδα χρησιμοποιεί κρυπτογράφηση για την προστασία των ευαίσθητων προσωπικών πληροφοριών που εισάγετε (αριθμός της πιστωτικής σας κάρτας ή άλλη πληροφορία ταυτοποίησης). Όμως, το εικονίδιο με το κίτρινο λουκέτο μπορεί να είναι ψεύτικο. Για να διασφαλίσετε τη γνησιότητά του κάντε διπλό κλικ για να διαπιστώσετε το πιστοποιητικό ασφαλείας της τοποθεσίας. Το όνομα που ακολουθεί το "Issued to" (Εκδόθηκε για), θα πρέπει να αντιστοιχεί με το όνομα της διαδικτυακής τοποθεσίας. Εάν το όνομα διαφέρει, πιθανόν να βρίσκεστε σε μια ψεύτικη τοποθεσία, γνωστή και ως "spoofed" (πλαστή) τοποθεσία. Εάν δεν είστε σίγουροι εάν το πιστοποιητικό είναι νόμιμο, μην εισάγετε προσωπικά δεδομένα.

Ασφάλεια του υπολογιστή σας

Βασικά βήματα για την ασφάλεια του υπολογιστή σας

- Εγκαταστήστε και χρησιμοποιείστε κάποιο πρόγραμμα προστασίας από ιούς. Να το ενημερώνετε συχνά (ακόμα και μια φορά τη μέρα), με όλες τις νέες εκδόσεις ιών που κυκλοφορούν.

- Να κρατάτε Backup των αρχείων του υπολογιστή σας, ώστε ακόμη και αν συμβεί κάτι στον υπολογιστή σας, να μπορείτε να ανακτήσετε ξανά τα δεδομένα σας.

- Να προστατεύεται τους κωδικούς ασφαλείας σας. Μην τους μοιράζεστε με κανέναν, ακόμη και με το φίλο σας ή το διαχειριστή του μηχανήματος σας.

- Να είστε πολύ προσεκτικοί με μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) ή ιστοσελίδες, που σας ζητούν να τους παραχωρήσετε προσωπικές πληροφορίες ή σας προτρέπουν να κατεβάσετε κάποιο αρχείο.

- Να κρατάτε το λειτουργικό σας σύστημα πάντοτε ενημερωμένο (updated).

Εγκατάσταση προγραμμάτων ασφαλείας

Για την προστασία του υπολογιστή σας συστήνεται η εγκατάσταση, χρήση και συνεχής αναβάθμιση των ακόλουθων προγραμμάτων:

- Εγκαταστήστε και χρησιμοποιείστε κάποιο τείχος προστασίας (firewall) στον υπολογιστή του σπιτιού σας. Οι νεότερες εκδόσεις των Windows προσφέρουν ενσωματωμένο πρόγραμμα firewall.

- Χρησιμοποιήστε ένα φίλτρο ανεπιθύμητων μηνυμάτων (spam). Το Microsoft Outlook διαθέτει ισχυρές άμυνες απέναντι στα ανεπιθύμητα μηνύματα (junk e-mail), αλλά μπορείτε επίσης να ενισχύσετε την άμυνα σας απέναντι στα ανεπιθύμητα μηνύματα. Ρυθμίστε το πρόγραμμα προστασίας από ιούς ώστε να ανιχνεύει όλα τα εισερχόμενα αρχεία και τα συνημμένα των ηλεκτρονικών μηνυμάτων πριν τα ανοίξετε.

- Εγκαταστήστε και εκτελέστε ένα πρόγραμμα για τον εντοπισμό και την αφαίρεση λογισμικού υποκλοπής (anti-spyware). Τα πακέτα υπηρεσίας που προσφέρουν ορισμένοι πάροχοι υπηρεσιών Διαδικτύου (ISP) περιλαμβάνουν λογισμικό προστασίας από υποκλοπή. Εάν ο πάροχος δεν σας το παρέχει, εξετάστε την περίπτωση του Microsoft Windows Anti-Spyware ή λογισμικού προστασίας από υποκλοπή άλλων εταιρειών.

- Εγκατάσταση και χρήση Φίλτρου ηλεκτρονικού "ψαρέματος". Το Φίλτρο ηλεκτρονικού "ψαρέματος" διατίθεται στον Windows Internet Explorer 8 για τα Windows XP Service Pack 2 (SP2), Windows Vista και Windows 7.

Υπηρεσία Ελεγχόμενης Πρόσβασης (Web-Filtering)

Τα εργαλεία ελεγχόμενης πρόσβασης χρησιμοποιούνται για να αποκόπτετε το παιδί σας από την πρόσβαση σε σελίδες με παράνομο ή ακατάλληλο περιεχόμενο. Ο έλεγχος περιλαμβάνει τις παρακάτω κατηγορίες περιεχομένου:

- Aggressive (σελίδες που προπαγανδίζουν την επιθετική συμπεριφορά και το ρατσισμό)
- Drugs (σελίδες που προωθούν τα ναρκωτικά)
- Gampling (σελίδες που προωθούν τα τυχερά παιχνίδια)
- Porn (σελίδες με πορνογραφικό περιεχόμενο)
- Violence (σελίδες που προπαγανδίζουν τη βία)

Ρύθμιση και αναβάθμιση του φυλλομετρητή (Internet Explorer)

Ο Internet Explorer 8 περιλαμβάνει βελτιωμένες δυνατότητες στον τομέα της ασφάλειας που σας διευκολύνουν να δείτε ποιες τοποθεσίες παρέχουν ασφαλέστερη ανταλλαγή δεδομένων, ώστε να μπορείτε να έχετε ασφαλή πλοήγηση στο διαδίκτυο και να κάνετε τις ηλεκτρονικές σας συναλλαγές με ασφάλεια. Οι φυλλομετρητές προσφέρουν τη δυνατότητα ρύθμισης των επιπέδων ασφαλείας κατά την πλοήγηση στο διαδίκτυο. Για να μάθετε περισσότερα επισκεφτείτε την ιστοσελίδα του Internet Explorer 8 για να κάνετε άμεσα λήψη και εγκατάσταση του προγράμματος περιήγησης (www.microsoft.com/hellas/windows/internet-explorer).

ΜΙΚΡΟΙ ΕΘΕΛΟΝΤΕΣ

Χρήσιμες ιστοσελίδες

http://ec.europa.eu/information_society/activities/sip
EU Safer Internet Programme

www.pegi.info/gr/
Pan European Game Information

www.helpline.cyberethics.info
Ιστοσελίδα Εθνικού Κέντρου Ασφαλούς Διαδικτύου Cyberethics

www.microsoft.com/hellas/protect
Microsoft

http://explore.live.com/windows-live-family-safety
Windows Live Family Safety 2011

www.microsoft.com/security_essentials
Microsoft Security Essentials

Microsoft Κύπρου
Τ.Θ. 22867
1524 Λευκωσία
ΚΥΠΡΟΣ

Τηλ.: +357 22 456077
www.microsoft.com/athome

Μικροί Εθελοντές
Τ.Θ. 25108
1307 Λευκωσία

Τηλ: 70001870
www.youngvolunteers.org
e-mail: president@youngvolunteers.com

Cyprus Safer Internet Center - Cyberethics
Προμηθέως 5,
1065 Λευκωσία

Τηλ.: +357 22873820
www.cyberethics.info
e-mail: contact@cyberethics.info

Ομάδα Σύνταξης:
Virtual IT Ltd

Τ.Θ. 12514
2250 Λευκωσία
ΚΥΠΡΟΣ

Τηλ.: +357 22 660690
www.virtual-it.com.cy
e-mail: info@virtual-it.com.cy