Οι Εφηβοι απεναντι στο διαδικτυο: Κίνδυνοι και Αντιμετώπιση

Μετά την έρευνα με ερωτηματολόγια, οι μαθητές που συμμετείχαν στο πρόγραμμα χωρίστηκαν ξανά σε ομάδες και αυτή τη φορά έψαξαν σε περιοδικά, εφημερίδες, βιβλία και ιστοσελίδες για πληροφορίες σχετικά με τους κινδύνους που εγκυμονεί το διαδίκτυο για τους σημερινούς εφήβους.

Τι είναι το Διαδίκτυο

Η λέξη Διαδίκτυο προέρχεται από τις λέξεις Διασύνδεση Δικτύων και αναφέρεται σε ένα σύνολο υπολογιστών και δικτύων που συνδέονται μεταξύ τους σε ένα παγκόσμιο δίκτυο έτσι ώστε να μπορούν να επικοινωνούν και να μοιράζονται πληροφορίες. Στα Αγγλικά η λέξη Internet προέρχεται από τις λέξεις International Network που σημαίνει Διεθνές Δίκτυο Υπολογιστών.

Το διαδίκτυο παρομοιάζεται με «υπερλεωφόρο πληροφοριών». Καθημερινά διακινούνται πλήθος δεδομένων με οποιαδήποτε μορφή – κείμενα , εικόνες , ήχοι, μουσική, βίντεο – φέρνοντας στην οθόνη του υπολογιστή μας ένα τεράστιο αριθμό ψηφιακών πηγών πληροφόρησης. Σε αυτή όμως την παγκόσμια Κοινωνία της Πληροφορίας είναι πολύ δύσκολο έως ακατόρθωτο να υπάρχει ένα είδος ελέγχου της ποιότητας, της εγκυρότητας και της καταλληλότητας των πληροφοριών που φτάνουν στον υπολογιστή μας. Είναι λοιπόν υποχρέωσή μας πλέον να ενημερωθούμε για τους κινδύνους του διαδικτύου και τους φορείς που μπορούν να μας βοηθήσουν να προστατέψουμε τους εαυτούς μας και να «σερφάρουμε» με ασφάλεια στο διαδίκτυο.

Κίνδυνοι του Διαδικτύου

Ηλεκτρονικός Εκφοβισμός (Cyber Bulling).

Μια ανερχόμενη απειλή του διαδικτύου είναι ο ηλεκτρονικός εκφοβισμός (cyber bulling). Με τον όρο αυτό εννοούμε ένα σύνολο ενεργειών που διαπράττονται από παιδιά με σκοπό να εκφοβίσουν συνομηλίκους επίσης χρησιμοποιώντας το διαδίκτυο, τα κινητά τηλέφωνα και επίσης ηλεκτρονικές τεχνολογίες. Πρόκειται δε και για μια νέα «μόδα» των εφήβων. Οι συμπεριφορές που μπορούν να προκύψουν περιλαμβάνουν:

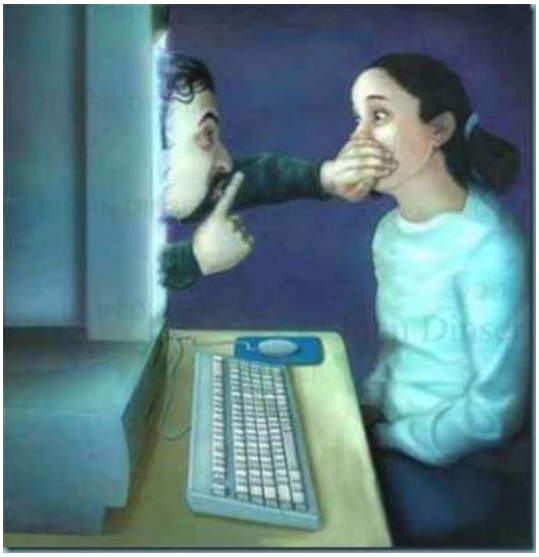
- Αποστολή κειμένων, e-mail, ή άμεσων μηνυμάτων με κακό περιεχόμενο.
- Η δημοσίευση δυσάρεστων φωτογραφιών ή μηνυμάτων για επίσης σε ιστολόγια (blogs) ή επίσης ιστοσελίδες.
- Χρήση του ονόματος ξένου χρήστη με σκοπό τη διάδοση φημών και ψεμάτων για κάποιον τρίτο (κλοπή ταυτότητας).
- Νεκρές κλήσεις.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

Αρκετές φορές προσβλητικά γραπτά μηνύματα επίσης κινητά τηλέφωνα στέλνονται μέσω ιστοσελίδων χρησιμοποιώντας ονόματα και τηλέφωνα ανθρώπων που δεν έχουν καμία σχέση με το μήνυμα αυτό, αλλά καταλήγουν να κατηγορούνται ότι το έστειλαν οι ίδιοι. Μια άλλη τεχνική που χρησιμοποιείται από όσους παρενοχλούν ηλεκτρονικά είναι η δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας επίσης να δημοσιεύουν μηνύματα μίσους.

ΑΝΤΙΜΕΤΩΠΙΣΗ:

Μην επιτρέπετε στους συνομήλικούς σας να σας φέρονται με αυτόν τον τρόπο. Μην ανέχεστε τέτοιες συμπεριφορές και μην απαντάτε με το ίδιο νόμισμα γιατί το πρόβλημα μπορεί να πάρει ανεξέλεγκτες διαστάσεις. Συμβουλευτείτε έναν μεγαλύτερο που εμπιστεύεστε πχ τους γονείς σας και καταγγείλετε αυτές τις συμπεριφορές. Στην Ελλάδα η ανοιχτή γραμμή επικοινωνίας για καταγγελίες τέτοιων προβλημάτων είναι η Safeline. Η SafeLine δέχεται καταγγελίες για ιστοχώρους (websites) ή υπηρεσίες νέων (newsgroups) που περιέχουν εικόνες κακομεταχείρισης των παιδιών, οπουδήποτε στον κόσμο, ρατσιστικό και ξενοφοβικό περιεχόμενο που παραβαίνει την Ελληνική νομοθεσία ή άλλο περιεχόμενο, παράνομο, κατά την άποψή σας.
Επίσης, υπάρχει και το Διεθνές Δίκτυο κατά του Διαδικτυακού Μίσους (INCHACH) που επίσης δέχεται καταγγελίες μέσω e-mail στο complaints@inach.net ή μέσω του website http://www.inach.net.

Ηλεκτρονική Αποπλάνηση (Grooming)



Ένας άλλος νέος κίνδυνος που έχουν να αντιμετωπίσουν οι νέοι σε ηλικία χρήστες του διαδικτύου είναι αυτός της «Ηλεκτρονικής Αποπλάνησης» ή grooming. Με τον όρο αυτό εννοούμε όλες αυτές τις διαδικασίες κατά τις οποίες ένας ενήλικας προσποιείται κάποιον άλλο μικρότερης ηλικίας για να προσελκύσει παιδιά και να έρθει σε επαφή μαζί τους στο φυσικό κόσμο με σκοπό τη σεξουαλική εκμετάλλευση ή / και κακοποίηση. Οι άνθρωποι αυτοί χρησιμοποιούν συνήθως τα chat rooms για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν.

Τα chat rooms φιλοξενούνται στο Διαδίκτυο και σε αυτά μπορεί να έχει πρόσβαση οποιοσδήποτε από οποιοδήποτε σημείο στον κόσμο. Συχνά θεωρούνται από τα παιδιά ασφαλείς τόποι συνομιλίας στο Διαδίκτυο, τόσο εξαιτίας της δημόσιας φύσης της συζήτησης αλλά και της λανθασμένης εκτίμησης των παιδιών ότι διατηρείται η ανωνυμία τους. Οι παιδόφιλοι ξεκινούν συζητήσεις με τα πιθανά θύματα με σκοπό να αναπτύξουν φιλική σχέση με αυτά και να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, τα ενδιαφέροντα, τα χόμπι και τις σεξουαλικές τους εμπειρίες. Μέσα από την σχέση αυτή προκαλούν σιγά σιγά συζητήσεις σεξουαλικής φύσεως και πολλές φορές οι παιδόφιλοι στέλνουν στα υποψήφια θύματα φωτογραφίες παιδικής πορνογραφίας αλλά και πορνογραφίας ενηλίκων για να δώσουν την αίσθηση ότι αυτό είναι κάτι το αποδεκτό και φυσιολογικό. Η τακτική αυτή χρησιμοποιείται για να υπονομεύσει την απροθυμία των παιδιών στο να λάβουν μέρος σε σεξουαλική επαφή. Χρησιμοποιείται επίσης για να αποτρέψει το θύμα από το να ζητήσει προστασία από τους γονείς και τους δασκάλους του, αφού καταλήγει να νιώθει ένοχο που έχει ανταλλάξει τέτοιου είδους φωτογραφίες.

ΑΝΤΙΜΕΤΩΠΙΣΗ:

Είναι εύκολο να συνομιλήσετε με ασφάλεια, ακολουθώντας μερικούς απλούς κανόνες. Οι εικονικοί φίλοι μπορεί να είναι διαφορετικοί από αυτό που δείχνουν. Μη δίνετε ποτέ προσωπικές πληροφορίες, όπως τη διεύθυνση ηλεκτρονικού ταχυδρομείου, τη διεύθυνση του σπιτιού σας, ή τον αριθμό του κινητού σας τηλεφώνου. Ποτέ μη δίνετε πληροφορίες για την οικογένειά σας, τους φίλους σας και τρίτους. Αν νιώθετε ότι κάποιος σας παρενοχλεί, θυμηθείτε: μπορείτε να βγείτε από το chat room με ένα απλό «κλικ». Πρέπει πάντα να θυμάστε ότι έχετε τον έλεγχο. Εάν κάνετε chat, και αισθανθείτε ότι κάποιος σας

ενοχλεί, μπορείτε απλά να σταματήσετε την συνομιλία με ένα κλικ.

Εάν κάποιος συνεχίσει να σας παρενοχλεί χρησιμοποιώντας το ηλεκτρονικό σας ταχυδρομείο, τότε το καλύτερο που μπορείτε να κάνετε είναι να μπλοκάρετε τα μηνύματα αυτά, έτσι ώστε να μην φτάνουν στον υπολογιστή σας. Τέλος, μπορείτε να αλλάξετε την ηλεκτρονική σας διεύθυνση. Μην ξεχνάτε ποτέ, ότι οι άνθρωποι που γνωρίσατε μέσα από το Διαδίκτυο δεν είναι πάντοτε αυτοί που σας λένε. Πολλές φορές λένε ψέματα για την ηλικία τους, και ενώ συστήνονται ως συνομήλικοί σας, μπορεί να είναι στην πραγματικότητα πολύ μεγαλύτεροί σας. Μην ξεχνάτε ποτέ, ότι τέτοιοι άνθρωποι είναι πολύ υπομονετικοί, και δεν έχουν κανένα πρόβλημα να περιμένουν πολλούς μήνες μέχρι να σας πείσουν να τους εμπιστευτείτε και τελικά να τους συναντήσετε σε κάποιο μέρος που θα σας προτείνουν αυτοί, με πρόθεση να σας βλάψουν.
Η αποθήκευση των συζητήσεων είναι ένας πολύ σημαντικός τρόπος για να συλλέξετε στοιχεία για οποιαδήποτε άσχημη συμπεριφορά. Υπάρχουν τρεις τρόποι με τους οποίους μπορείτε να αποθηκεύσετε μία συζήτηση. Η μέθοδος που θα χρησιμοποιήσετε θα εξαρτηθεί από το πρόγραμμα που χρησιμοποιείτε:

Μέθοδος 1 - Αποθηκεύστε τη συζήτηση.

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

Μέθοδος 2 – Αντιγράψτε τη συζήτηση

- Επιλέξτε με το ποντίκι σας το κείμενο της συζήτησης και πατήστε συγχρόνως τα πλήκτρα CTRL + C. Πηγαίνετε σε ένα πρόγραμμα επεξεργασίας κειμένου (π.χ. Word), και δημιουργήστε ένα νέο αρχείο. Πατήστε συγχρόνως τα πλήκτρα CTRL + V για να αντιγράψετε τη συζήτηση.
- Σώστε το αρχείο που δημιουργήσατε ή εκτυπώστε το για να το χρησιμοποιήσετε σε περίπτωση καταγγελίας ή για να το δείξετε στους γονείς σας αν είστε ανήλικοι.

Μέθοδος 3 – Εκτυπώστε την οθόνη

- Πατήστε το πλήκτρο «PrtScn» στο πληκτρολόγιο σας (δηλαδή «Print Screen»). Το πλήκτρο αυτό βρίσκεται συνήθως δεξιά επάνω στο πληκτρολόγιό σας, δεξιά από το πλήκτρο «Print», και αριστερά από το πλήκτρο «Pause».

Τέλος, εάν πιστεύετε ότι βρήκατε μια ιστοσελίδα στην οποία υπάρχει παράνομο υλικό, τότε σας προτρέπουμε να έρθετε σε επαφή με την Ελληνική Ανοιχτή Γραμμή SafeLine.
Η SafeLine συνεργάζεται με τους Φορείς Παροχής Υπηρεσιών Διαδικτύου (ISP), το Ακαδημαϊκό Δίκτυο ΕΔΕΤ και το Σχολικό Δίκτυο, Ερευνητικά και Πολιτιστικά Ιδρύματα, Ενώσεις Καταναλωτών και την Ελληνική Αστυνομία για τον περιορισμό της ροής του παράνομου περιεχομένου στο διαδίκτυο.
Η SafeLine υποστηρίζεται από το πρόγραμμα της Ευρωπαϊκής Ένωσης "Σχέδιο Δράσης για την Ασφαλέστερη Χρήση του Διαδικτύου" και λειτουργεί από την

SAFENET, το συλλογικό όργανο των ISPs της Ελλάδας. Η SafeLine είναι σε στενή επαφή με όλες τις Ευρωπαϊκές ανοιχτές γραμμές επικοινωνίας, ως μέλος τηςΕυρωπαϊκής Ένωσης των hotlines INHOPE.

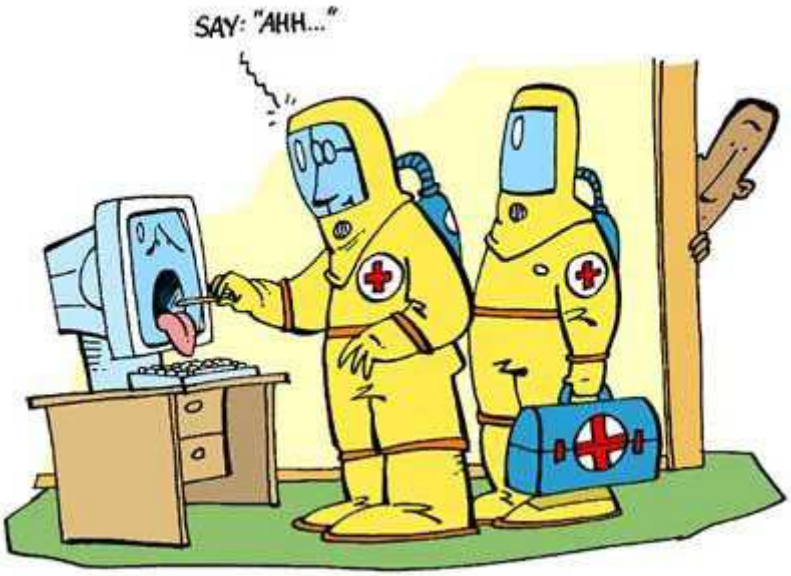
Κακόβουλο Λογισμικό (Ιοί - Virus και Spyware)

Ιοί - Viruses

Οι ιοί είναι ίσως ο πιο παλιός τρόπος μόλυνσης ενός υπολογιστή. Αρχικά μεταδίδονταν μέσα από δισκέτες και εκτελέσιμα αρχεία, τα οποία μπορούσαν να διεισδύσουν σε ζωτικά σημεία του λειτουργικού και του σκληρού δίσκου και να τα καταστρέψουν. Με την ανάπτυξη και τη διάδοση του Ίντερνετ, οι ιοί σήμερα ταξιδεύουν με την ηλεκτρονική αλληλογραφία αλλά και με προγράμματα δωρεάν διάδοσης - freeware.

ΑΝΤΙΜΕΤΩΠΙΣΗ:

Ο βασικότερος τρόπος αντιμετώπισης ενός ιού, αλλά και κάθε κινδύνου, είναι φυσικά η πρόληψη ώστε να μη διεισδύσει στο σύστημα του υπολογιστή. Η εγκατάσταση ενός προγράμματος anti-virus θεωρείται δεδομένη για κάθε οικιακό υπολογιστή, ωστόσο, δεν αρκεί αυτό. Θα πρέπει να φροντίζετε για την ενημέρωση του προγράμματος με τις τελευταίες εκδόσεις αντιμετώπισης ιών, αλλά και να «τρέχετε» το αντιϊικό πρόγραμμα σε τακτά χρονικά διαστήματα ώστε να ελέγχονται όλες οι μονάδες αποθήκευσης δεδομένων.



Κακόβουλο Λογισμικό - Spyware

Το spyware σήμερα θεωρείται η μεγαλύτερη απειλή στην οποία εκτίθεται ο χρήστης. Πρόκειται για κώδικα λογισμικού που μπορεί να βρίσκεται κρυμμένος σε αρχεία ή
ακόμη και ιστοσελίδες που επισκέπτεται ο χρήστης.
Όταν το spyware εγκατασταθεί στον υπολογιστή, το πρώτο πράγμα που κάνει είναι να ενημερώσει τον αποστολέα του ότι έχει πλέον τον έλεγχο του υπολογιστή. Έτσι, ο απομακρυσμένος hacker μπορεί να χειριστεί τον υπολογιστή του χρήστη, ο οποίος δεν γνωρίζει καν τι συμβαίνει. Με τον τρόπο αυτό, δημιουργούνται ολόκληρα δίκτυα από «υπολογιστές-ζόμπι» που χρησιμοποιούνται για επιθέσεις DOS (Denial of Service) σε servers μεγάλων συνήθως εταιρειών.

ΑΝΤΙΜΕΤΩΠΙΣΗ:

Όπως για την αντιμετώπιση των ιών, έτσι και για τα spyware κυκλοφορούν στο εμπόριο αλλά και σε μορφή freeware πολλά προγράμματα προστασίας. Εκτός από αυτά όμως τα anti-spyware προγράμματα να χρησιμοποιούνται σε συνδυασμό με κάποιο πρόγραμμα επίβλεψης και καθαρισμού του registry, του πιο ζωτικού σημείου του υπολογιστή για τη λειτουργία του λογισμικού, αφού εκεί εγκαθίστανται τα spyware στην πλειοψηφία των περιπτώσεων. Σε συνδυασμό με τα μέτρα πρόληψης απέναντι σε ιούς και spyware, πρέπει να τονιστεί η σημασία τόσο του Firewall, όσο και των σωστών ρυθμίσεων προστασίας του modem ή router που χρησιμοποιούμε για πρόσβαση στο Διαδίκτυο. Το Firewall αποτελεί το απαραίτητο τείχος προστασίας του υπολογιστή από επιτήδειους που προσπαθούν να επικοινωνήσουν με τον υπολογιστή. Η εύρεση ενός καλού και αξιόπιστου firewall δεν είναι δύσκολη υπόθεση αφού κυκλοφορούν πολλές διαφορετικές εκδόσεις που μπορούν να εξυπηρετήσουν από τον «ανυποψίαστο» μέχρι τον επαγγελματία χρήστη.
Ταυτόχρονα, ένα από τα πρώτα πράγματα που πολλοί χρήστες συχνά αγνοούν όταν αποκτήσουν πρόσβαση στο Διαδίκτυο, είναι η ρύθμιση του router που χρησιμοποιούν ώστε να προστατεύσουν το οικιακό τους δίκτυο. Ειδικά όταν χρησιμοποιείται ασύρματο router, είναι επιτακτική η ενεργοποίηση κωδικού πρόσβασης στο ασύρματο δίκτυο που δημιουργείται στην εμβέλεια του router. Με τον τρόπο αυτό περιορίζεται η πρόσβαση μόνο στους υπολογιστές που κάνουν χρήση του κωδικού, ή που συνδέονται με καλώδιο εντός του σπιτιού.
Η μη χρήση κωδικού ασφαλείας του ασύρματου δικτύου εκτός του ότι επιτρέπει την πρόσβαση σε ανεπιθύμητους υπολογιστές, κυριότερα δίνει τη δυνατότητα σε κάποιον

ακόμη και με στοιχειώδεις γνώσεις, να διεισδύσει στο δίκτυο μας, να αλλάξει τις ρυθμίσεις και να δημιουργήσει γενικότερα προβλήματα στην πρόσβασή μας στο Ίντερνετ.

Ενοχλητική Αλληλογραφία (Spam Email και Phishing)

Spam Email

Τα μηνύματα spam περιέχουν συνήθως πληροφορίες και διαφημίσεις που στην πλειοψηφία των περιπτώσεων δεν ενδιαφέρουν τον χρήστη. Αν και στις περισσότερες φορές το να ξεφορτωθεί κάποιος ένα τέτοιο email είναι εύκολη υπόθεση, το γεγονός ότι αυτά συνεχίζουν να έρχονται ανά διαστήματα ωρών πολλές φορές μπορεί να προκαλέσει πρόβλημα στον χρήστη.

ΑΝΤΙΜΕΤΩΠΙΣΗ:

Το κυριότερο που πρέπει να γνωρίζει ο χρήστης είναι να μην απαντήσει σε αυτά τα μηνύματα και ακόμη σημαντικότερα, να μην επισκεφθεί τις ιστοσελίδες που περιλαμβάνονται στο μήνυμα και να μην ανοίξει οποιοδήποτε συνημμένο αρχείο. Ο περιορισμός λήψης τέτοιων μηνυμάτων είναι η ρύθμιση των σχετικών φίλτρων που έχουν τα διάφορα προγράμματα αλληλογραφίας, ώστε να σβήνονται απευθείας από τη θυρίδα του χρήστη.

Phishing

Πρόκειται για παρεμφερή πρακτική με τα spam emails. Ένα μήνυμα phishing επιχειρεί να ξεγελάσει τον χρήστη ώστε να απαντήσει στον αποστολέα και να του δώσει κάποια προσωπικά στοιχεία, αριθμούς λογαριασμού, πιστωτικής κάρτας, ή να τον πείσει να μεταβιβάσει ένα χρηματικό ποσό από τον λογαριασμό του σε κάποιον άλλο.
Όσο και αν θεωρηθεί παράξενο, υπάρχουν πολλοί χρήστες που, μη γνωρίζοντας, δίνουν τα προσωπικά τους στοιχεία χωρίς δεύτερη σκέψη, με αποτέλεσμα να δώσουν πρόσβαση όχι μόνο στον υπολογιστή τους αλλά και στους τραπεζικούς τους λογαριασμούς.

ΑΝΤΙΜΕΤΩΠΙΣΗ:

Ο μόνος τρόπος για να αντιμετωπίσει το phishing ο χρήστης είναι να είναι υποψιασμένος και κυρίως να γνωρίζει ότι, όπως και στην πραγματική ζωή, έτσι και στο Ίντερνετ, κανείς δε θα θελήσει να του χαρίσει κάποιο υπέρογκο ποσό ζητώντας του τον αριθμό τραπεζικού λογαριασμού για να κάνει την κατάθεση.

Κοινωνική Δικτύωση – Προσωπικά Δεδομένα

Οι υπηρεσίες κοινωνικής δικτύωσης (social networks) που στοχεύουν στη δημιουργία on-line κοινοτήτων από ανθρώπους με κοινά ενδιαφέροντα και δραστηριότητες έχουν γίνει ιδιαιτέρως δημοφιλείς στις μέρες μας. Οι υπηρεσίες αυτές λειτουργούν κυρίως στο Διαδίκτυο και προσφέρουν πολλαπλούς τρόπους επικοινωνίας και διάδρασης στους εγγεγραμμένους χρήστες τους που συνήθως προϋποθέτουν τη δημιουργία προσωπικών προφίλ των χρηστών.

Οι χρήστες των υπηρεσιών αυτών μπορούν να δημοσιοποιούν και να μοιράζονται προσωπικές πληροφορίες με άλλες ομάδες χρηστών, όπως π.χ. θέματα σχετικά με τα χόμπι τους, την εργασία τους, τις προτιμήσεις τους, τα αγαπημένα τους πρόσωπα, κ.α. μέσα από το προσωπικό τους προφίλ, αλλά και υπό μορφή μηνυμάτων, φωτογραφιών, βίντεο, κ.ο.κ.

Αναμφίβολα οι υπηρεσίες κοινωνικής δικτύωσης αποτελούν μία νέα μορφή εκκοινώνισης και επικοινωνίας, ιδιαιτέρως ανάμεσα στους νέους αλλά όχι μόνο. Ταυτόχρονα όμως, οι υπηρεσίες αυτές προσδίδουν και μια καινούργια διάσταση στην έννοια του “προσωπικού χώρου”, δημιουργώντας σοβαρές ανησυχίες για παραβίαση της ιδιωτικότητας των χρηστών τους, των οποίων τα προσωπικά δεδομένα δημοσιοποιούνται στο Διαδίκτυο με πρωτοφανή τρόπο και ποσότητα.

Το θέμα αυτό απασχολεί τις Αρχές Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης. Το Μάρτιο του 2008 η Διεθνής Ομάδα για την Προστασία των Προσωπικών Δεδομένων στις Τηλεπικοινωνίες (IWGDPT) εξέδωσε ένα έγγραφο συστάσεων για τις υπηρεσίες κοινωνικής δικτύωσης. Το έγγραφο, στη διαμόρφωση της οποίας συμμετείχε ενεργώς και η ελληνική Αρχή, απευθύνεται στους παρόχους και στους χρήστες των υπηρεσιών αυτών.

ΑΝΤΙΜΕΤΩΠΙΣΗ:

Αν χρησιμοποιείτε υπηρεσίες κοινωνικής δικτύωσης ενδεικτικά συνίσταται να:

- Είστε προσεκτικοί όταν δημοσιεύετε προσωπικά δεδομένα, καθώς όλα όσα δημοσιεύονται γίνονται αυτόματα διαθέσιμα σε άγνωστο αριθμό ατόμων στο Διαδίκτυο.

- Σέβεστε την ιδιωτικότητα των άλλων και να μην δημοσιεύετε προσωπικά δεδομένα τρίτων χωρίς την συγκατάθεση τους.

- Χρησιμοποιείτε ρυθμίσεις φιλικές προς την ιδιωτικότητα, π.χ. περιορισμό της διαθεσιμότητας των προσωπικών σας δεδομένων σε μηχανές αναζήτησης.

- Χρησιμοποιείτε διαφορετικά αναγνωριστικά και κωδικούς πρόσβασης από αυτά που χρησιμοποιείτε σε άλλους διαδικτυακούς τόπους που επισκέπτεστε (π.χ. υπηρεσίες web-banking ή ηλεκτρονικού ταχυδρομείου).

- Προσέχετε ώστε να μη δίνετε κατά λάθος τη συγκατάθεση σας για διάθεση των προσωπικών σας δεδομένων για διαφημιστικούς σκοπούς.

- Να προτιμάτε τη χρήση ανώνυμων προφίλ.

Εθισμός στο Διαδίκτυο

Καταστροφικές συνέπειες έχει για τους νέους μια νέα μορφή εθισμού, ο εθισμός στο διαδίκτυο, που τείνει να πάρει επικίνδυνες διαστάσεις στη χώρα μας. Στην Ελλάδα ο εθισμός των χρηστών φτάνει στο 8,2%, ποσοστό που της δίνει την πρώτη θέση παγκοσμίως. Το παράδοξο είναι ότι η χώρα μας παρουσιάζει ταυτόχρονα το μικρότερο ποσοστό διείσδυσης στο διαδίκτυο, όταν την ίδια στιγμή, σε χώρες όπου η διείσδυση είναι αυξημένη, τα ποσοστά εθισμού είναι πολύ μικρότερα.

Τα συμπτώματα του εθισμού

Τι σημαίνει, όμως, εθισμός στο Internet και πώς αυτός ορίζεται; Για να κριθεί ένα άτομο εθισμένο στο Διαδίκτυο, πάσχον δηλαδή από μια ψυχική διαταραχή, πρέπει να πληροί ορισμένα συγκεκριμένα επιστημονικά κριτήρια. Σε αυτά, όπως εξηγεί ο κ. Σιώμος, διδάκτωρ της Ιατρικής Σχολής του Πανεπιστημίου Θεσσαλίας και υπεύθυνος σχεδιασμού και οργάνωσης του πρώτου στην Ελλάδα Ειδικού Ψυχιατρικού Ιατρείου για τον εθισμό στο Διαδίκτυο στο Ιπποκράτειο Νοσοκομείο Θεσσαλονίκης, στο «Βήμα», περιλαμβάνονται εκτός από την πολύωρη ημερήσια ενασχόληση με το Διαδίκτυο τα ακόλουθα:

- Εξιδανίκευση του μέσου. Ο χρήστης θεωρεί τον ηλεκτρονικό υπολογιστή ή το Διαδίκτυο το σημαντικότερο «κεφάλαιο» της καθημερινότητάς του.

- Τροποποίηση της διάθεσης. Σε όσους εθίζονται στα ηλεκτρονικά παιχνίδια παρουσιάζεται αύξηση της παραγωγής του νευροδιαβιβαστή του εγκεφάλου ντοπαμίνη, η οποία συνδέεται με την ευχαρίστηση.

- Ανοχή. Το άτομο χρειάζεται σταδιακά όλο και περισσότερες ώρες χρήσης του υπολογιστή ώστε να νιώθει ευχαρίστηση.

- Σύγκρουση. Ενώ το παιδί αισθάνεται ότι έχει πρόβλημα, δεν μπορεί να κάνει κάτι για να περιορίσει τη χρήση του υπολογιστή.

- Ενασχόληση αρχικώς με ηπιότερες και όχι τόσο εθιστικές λειτουργίες του Διαδικτύου, όπως είναι η αποστολή ηλεκτρονικών μηνυμάτων, και σταδιακή μετάβαση σε πιο διαδραστικές διαδικτυακές λειτουργίες όπως τα δωμάτια

συνομιλιών (chat room), οι ομάδες ειδήσεων ή ακόμη και τα αποκαλούμενα κοινωνικά παιχνίδια όπως το «Second Life», στο οποίο κάθε χρήστης φτιάχνει μια νέα «εικονική» διαδικτυακή ζωή με όλες τις εκφάνσεις της (αξίζει να σημειωθεί ότι έχει ήδη προκληθεί θόρυβος σχετικά με τέτοιου είδους παιχνίδια, καθώς σε κάποιες περιπτώσεις η «εικονική» ζωή του χρήστη παρενέβαινε στη φυσιολογική ζωή του, ενώ παράλληλα η πλατφόρμα του παιχνιδιού γινόταν έρμαιο παιδεραστών και διακινητών πορνογραφικού υλικού).

Όλα αυτά έχουν, όπως είναι επόμενο, σοβαρές επιπτώσεις σε διάφορους τομείς της λειτουργικότητας του ατόμου. Μειώνεται ο χρόνος που περνάει ο έφηβος με την οικογένειά του, περιορίζονται τα χόμπι και οι κοινωνικές συναναστροφές του, αυξάνεται ο κίνδυνος εμφάνισης παχυσαρκίας, μυοσκελετικών προβλημάτων και οφθαλμικών παθήσεων λόγω των πολλών ωρών- ακινησίας- μπροστά στην οθόνη. Παράλληλα, οι εθισμένοι στο Διαδίκτυο νεαροί παραμελούν τη σωματική τους υγιεινή, ενώ κάνουν πολλές απουσίες στο σχολείο με αποτέλεσμα ακόμη και να χάνουν τάξεις.

Δεν είναι ανάγκη, όμως, να φθάσουν τα πράγματα σε αυτά τα άκρα. Υπάρχουν προειδοποιητικά καμπανάκια και οι γονείς πρέπει να έχουν ανοικτά τα αφτιά τους ώστε να τα ακούσουν, λέει ο κ. Σιώμος. «Αν οι γονείς δουν ότι οι σχολικές επιδόσεις του παιδιού πέφτουν χωρίς να υπάρχει άλλος λόγος εκτός από τη συνεχή ενασχόληση με τον υπολογιστή, αν καταλάβουν ότι το παιδί χάνει την κοινωνικότητά του και απομονώνεται, πρέπει να αντιδράσουν, να βρουν τρόπο διαχείρισης της κατάστασης, θέτοντας ένα πλαίσιο ώστε να απομακρύνουν τον έφηβο από τη μόνιμη ασχολία του με το Διαδίκτυο».

ΑΝΤΙΜΕΤΩΠΙΣΗ:

"Η διατήρηση ενός καλού επιπέδου επικοινωνίας στην οικογένεια είναι θεμελιώδους σημασίας για την προστασία του εθισμένου παιδιού στη χρήση του διαδικτύου. Αυτό επιτυγχάνεται με τον καθορισμό των στόχων από την πλευρά των γονέων, την επιλογή της κατάλληλης στιγμής για συζήτηση, η οποία πρέπει να είναι πριν την πλοήγηση στο διαδίκτυο και όχι κατά τη διάρκεια ή στο τέλος της", σημειώνει ο κ. Σιώμος.

- Οι γονείς οφείλουν να χρησιμοποιούν επιχειρήματα, να είναι προετοιμασμένοι για την αρνητική στάση του παιδιού και εάν αποτύχουν να σκεφτούν νέους τρόπους επικοινωνίας με τα παιδιά τους, υπογραμμίζει ο ίδιος.
- "Αν γίνουν αυτά τα βήματα, στις περισσότερες περιπτώσεις δεν διαταράσσεται η επικοινωνία στην οικογένεια. Επίσης, είναι σημαντικό οι γονείς να έχουν κοινή στάση στην αντιμετώπιση του προβλήματος, να δείχνουν στο παιδί τους πόσο νοιάζονται, να βάζουν λογικούς κανόνες στη χρήση του διαδικτύου, η τοποθέτηση του υπολογιστή θα πρέπει να είναι σε κοινό χώρο στο σπίτι για να ελέγχεται το είδος της χρήσης και τέλος πρέπει να ενθαρρύνουν το παιδί να βρει εναλλακτικές δραστηριότητες".
- Στις περιπτώσεις, όμως, όπου η χρήση του διαδικτύου δεν ελέγχεται και οι ώρες αυξάνονται, παρ' όλο που οι γονείς ακολούθησαν τις παραπάνω οδηγίες, υπάρχουν συνέπειες στη σχολική επίδοση και την οργάνωση της καθημερινότητας και οι οικογενειακές σχέσεις επηρεάζονται αρνητικά, είναι απαραίτητο οι γονείς να απευθυνθούν σε ειδικούς ψυχικής υγείας εξειδικευμένους στον εθισμό στο Διαδίκτυο, συνιστά ο κ. Σιώμος.

- Για την αντιμετώπιση της κατάστασης έχουν δημιουργηθεί δύο μονάδες, μία στην Αθήνα και μία στη Θεσσαλονίκη, στην οποία απευθύνονται βεβαίως πρωτίστως οι γονείς. Η θεραπεία γίνεται με συμβουλευτική παρέμβαση και ειδικό εξατομικευμένο πρόγραμμα περιορισμού της υπερβολικής χρήσης.