ΚΙΝΔΥΝΟΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΔΙΑΔΙΚΤΥΑΚΟΙ ΚΙΝΔΥΝΟΙ

Η πρόσβαση στο Διαδίκτυο σήμερα δεν είναι ακίνδυνη, ανεξάρτητα από τον τρόπο χρήσης των υπηρεσιών του. Υπάρχουν κακόβουλοι χρήστες και αρκετές δυνατότητες πρόκλησης ζημιών, τόσο στο επίπεδο του χρησιμοποιούμενου λογισμικού και υλικού, όσο και σε προσωπικό επίπεδο.

ΠΡΟΚΛΗΣΗ ΖΗΜΙΩΝ ΣΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΣΥΣΤΗΜΑ

Ο κύριος κίνδυνος πρόκλησης ζημιών στο υπολογιστικό σύστημα ενός ανυποψίαστου χρήστη είναι η μόλυνση του συστήματος με κάποιον ιό. Η μόλυνση γίνεται όταν ο χρήστης καλείται να λάβει κάποιο -φαινομενικά αθώο- αρχείο όπως ένα κείμενο ή μια φωτογραφία και όταν δοκιμάσει να το χρησιμοποιήσει, ο ιός αναλαμβάνει δράση επιμολύνοντας το σύστημα. Μπορεί να καταστρέψει αρχεία ή και ολόκληρο το σκληρό δίσκο του συστήματος. Άλλες φορές είναι δυνατή η αποστολή ιού απευθείας από τον ιστότοπο που επισκέπτεται ο χρήστης, χωρίς να εμφανισθεί κάποια ένδειξη λήψης αρχείου. Η περίπτωση αυτή εκμεταλλεύεται κενά ασφαλείας στο λογισμικό του χρήστη. Παρόμοιας δράσης είναι και ένα πρόγραμμα που αποκαλείται worm (=σκουλήκι). Είναι παρόμοιο σε αποτέλεσμα με τον ιό, αλλά, αντίθετα από αυτόν, δεν απαιτεί την "προσκόλλησή" του σε ένα αρχείο, έχοντας έτσι περισσότερη αυτονομία. Η βλάβη που προκαλεί το worm δεν είναι τόσο ευρεία στο σύστημα, όσο στο δίκτυο σύνδεσης, επειδή καταναλώνει σημαντικό εύρος ζώνης bandwidth).Άλλος κίνδυνος είναι ο Δούρειος Ίππος, ένα πρόγραμμα που ξεγελά το χρήστη του, ο οποίος χρησιμοποιώντας το νομίζει ότι εκτελεί κάποια εργασία, ενώ στην πραγματικότητα εκτελεί κάποια άλλη, συνήθως εγκατάσταση άλλων κακόβουλων προγραμμάτων. Αντίθετα από τους ιούς, οι δούρειοι ίπποι δεν επιμολύνουν αρχεία.

ΠΑΡΑΠΛΑΝΗΣΗ

Αρκετές φορές οι χρήστες του Διαδικτύου χρησιμοποιούν τις υπηρεσίες του για να βρουν κάποιες πληροφορίες που χρειάζονται. Μερικοί ιστότοποι εμφανίζουν πληροφορίες, οι οποίες φαινομενικά είναι ακριβείς ή αναφέρουν απόλυτα αξιόπιστους δημιουργούς ή πηγές.

PHARMING

Η τεχνική του “pharming” αποτελεί μέθοδο εξαπάτησης μέσω του διαδικτύου παρόμοια με το “phishing” αλλά σαφώς πιο επικίνδυνη από αυτό. Ένα ειδικό πρόγραμμα εκμεταλλεύεται κενά ασφαλείας του συστήματος, διεισδύει στον υπολογιστή του θύματος και το επηρεάζει κατά τέτοιο τρόπο, ώστε, ακόμα κι αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου που θέλει να επισκεφτεί, θεωρώντας πως βρίσκεται σε ασφαλή χώρο, ο συγκεκριμένος υπολογιστής τον “οδηγεί” μόνο σε πλαστές ιστοσελίδες. Ειδικότερα, αν πρόκειται για ιστοσελίδα τράπεζας, η προσπάθεια του θύματος να πραγματοποιήσει τις συναλλαγές του μέσω on-line banking καταλήγει στη μεταφορά των χρημάτων του στους δράστες (Pharmers).Είναι σαφές ότι η αύξηση των ωρών χρήσης του διαδικτύου πολλαπλασιάζει τον κίνδυνο εγκατάστασης προγραμμάτων που καθιστούν δυνατό το “pharming”, το οποίο βαθμιαία εξελίσσεται σε μία από τις σοβαρότερες μορφές εγκληματικότητας στο διαδίκτυο.

ΙΟΙ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΑΡΧΕΙΑ SPAM

Τι είναι ιός;

Ένας ιός υπολογιστών είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό. Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, παραδείγματος χάριν από ένα χρήστη που στέλνει τον ιό μέσω δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB. Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα "σκουλήκια" υπολογιστών (worms) και τους δούρειους ίππους (trojan horses). Ένα "σκουλήκι" μπορεί να διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host), ενώ ένας δούρειος ίππος είναι ένα αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του. Πολλοί προσωπικοί υπολογιστές συνδέονται πλέον με το Διαδίκτυο και σε τοπικά δίκτυα και διευκολύνουν έτσι τη διάδοση του κακόβουλου κώδικα. Σήμερα οι ιοί μπορούν επίσης να εκμεταλλευθούν τις υπηρεσίες του Διαδικτύου, όπως το World Wide Web, το ηλεκτρονικό ταχυδρομείο και την υπηρεσία συνομιλιών (Internet Relay Chat, IRC).

Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων ή με τη μορφοποίηση (format) του σκληρού δίσκου. Μερικές, μάλιστα, φορές, δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου του. Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημία, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές αρκετά χιουμοριστικών. Όμως, ακόμη και αυτοί οι "καλοκάγαθοι" ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών: Καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και, κατά συνέπεια, προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του (system crash). Επιπλέον, πολλοί ιοί είναι, εγγενώς, γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων. Τέλος, ένα μεγάλο ποσοστό των ιών δεν έχει σκοπό την καταστροφή των δεδομένων του χρήστη ή την παρενόχλησή του, αλλά την κλοπή προσωπικών του δεδομένων ή την εισαγωγή του υπολογιστή-στόχου σε κάποιο παράνομο δίκτυο (botnet) χωρίς τη συγκατάθεση του χρήστη.

Τύποι ιών

Οι ιοί μπορούν να ταξινομηθούν σε δύο μεγάλες κατηγορίες:

- **Ανάλογα με το σημείο του υλικού ή του λογισμικού που μολύνουν:**
  - Τομείς σκληρού δίσκου συστήματος (system sectors)
  - Αρχεία
  - Ιοί μακροεντολών (Macros)
  - Ιοί πηγαίου κώδικα (Source Code Viruses)
  - Ιοί συμπλεγμάτων (σκληρού) δίσκου ((Hard) Disk Clusters)
- Ανάλογα με τον τρόπο με τον οποίο πραγματοποιούν τη μόλυνση:
  - Πολυμορφικοί ιοί
  - Αόρατοι ιοί (Stealth Viruses)
  - Θωρακισμένοι ιοί (Armored Viruses)
  - Πολυτμηματικοί ιοί (Multipartite Viruses)
  - Ιοί πλήρωσης κενών (Spacefiller Viruses)

- Ιοί παραλλαγής (Camouflage Viruses).

Τρόπος δράσης

Ανεξάρτητα από το τι και πώς μολύνει σε ένα σύστημα, ο ιός πρέπει να εξασφαλίσει ορισμένες βασικές συνθήκες, προκειμένου να δράσει. Συγκεκριμένα, πρέπει να μπορεί να εκτελέσει τον κώδικά του και να εξασφαλίσει πρόσβαση σε μέσα αποθήκευσης (κύρια στο σκληρό δίσκο, αλλά όχι μόνο). Γι' αυτό το λόγο, πολλοί ιοί προσκολλώνται σε εκτελέσιμα (executable) αρχεία είτε του λειτουργικού συστήματος είτε του κανονικού λογισμικού ενός συστήματος. Εξασφαλίζουν έτσι δύο πράγματα: Πρώτον, ότι θα μπορούν να αναπαραχθούν και δεύτερον ότι θα μπορέσουν να εκτελέσουν τον κώδικά τους.

Τρόποι διάδοσης

Οι ιοί διαδίδονται από τον ένα υπολογιστή στον άλλο με δύο τρόπους: Είτε μέσω φορητού μέσου αποθήκευσης είτε μέσω δικτύου. Ο δεύτερος τρόπος είναι σήμερα ο πλέον διαδεδομένος, λόγω της ευρείας διάδοσης του Διαδικτύου διεθνώς. Η βασική υπηρεσία διάδοσης ιών είναι αυτή του ηλεκτρονικού ταχυδρομείου (e-mail), μέσω του οποίου αποστέλλονται είτε ως συνημμένα είτε ως τμήμα αυτού καθαυτού του μηνύματος. Για το λόγο αυτό, πολλές υπηρεσίες e-mail προσφέρουν πρώτα σάρωση των μηνυμάτων και των συνημμένων τους με κάποιο αντιβιοτικό, πριν επιτρέψουν στο χρήστη να τα λάβει.

Τρόποι αντιμετώπισης

Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη - ορισμένοι, μάλιστα, ιοί, είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία. Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό (antivirus). Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο. Τα προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση, ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία τους νεοδημιουργούμενους ιούς. Σήμερα, αρκετοί οίκοι δημιουργίας λογισμικού ασχολούνται με τη δημιουργία τέτοιων προγραμμάτων. Τα αντιϊκά είναι σε θέση τόσο να εντοπίσουν μόλυνση τη στιγμή που αποπειράται, όσο και να "καθαρίσουν" τυχόν μολυσμένα αρχεία που εντοπίζουν.

Κάθε αντιϊκό έχει το δικό του τρόπο δράσης απέναντι στους ιούς. Ωστόσο, τα περισσότερα είναι σε θέση να εργάζονται σε πραγματικό χρόνο, εντοπίζοντας τους ιούς τη στιγμή ακριβώς που αποπειρώνται να μολύνουν το σύστημα. Ορισμένα τέτοια προγράμματα προσφέρονται δωρεάν για προσωπική χρήση (δεν καλύπτουν, ωστόσο, ούτε μικρό τοπικό δίκτυο υπολογιστών) και άλλα έναντι σχετικά χαμηλής τιμής (κανένα αντιϊκό για υπολογιστές δικτύου δεν προσφέρεται δωρεάν μέχρι σήμερα). Θα πρέπει να σημειωθεί ότι οι δημιουργοί ιών λαμβάνουν σοβαρά υπόψη τους τις μεθόδους εντοπισμού του "προϊόντος" τους και δημιουργούν ιούς, οι οποίοι προσπαθούν να αποφύγουν τον εντοπισμό, ακόμη και με απενεργοποίηση του αντιϊκού. Αυτό σημαίνει ότι ο χρήστης θα πρέπει να ενημερώνει τακτικότατα το λογισμικό του αλλά και να δημιουργεί τις ειδικές δισκέτες, που τα περισσότερα αντιβιοτικά προγράμματα προτείνουν τη δημιουργία τους, ώστε να είναι δυνατή η εκκαθάριση και η επαναφορά του συστήματος μετά από τυχόν μόλυνσή τους.

Τι είναι το spam;

Το spam είναι ο συνήθης όρος για την *αζήτητη ηλεκτρονική επικοινωνία*, δηλαδή τα ενοχλητικά μηνύματα που, χωρίς ποτέ να έχετε ζητήσει, κατακλύζουν το λογαριασμό ηλεκτρονικού ταχυδρομείου σας ή το κινητό σας τηλέφωνο διαφημίζοντας διαφόρων

ειδών προϊόντα ή υπηρεσίες. Οι αποστολείς μηνυμάτων spam είναι γνωστοί και ως *spammers*.

Γιατί το spam είναι τόσο σύνηθες στο Διαδίκτυο;

Το κόστος αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι πολύ χαμηλό για τους spammers και, επομένως, το ποσοστό ανταπόκρισης των χρηστών δεν χρειάζεται να είναι ιδιαίτερα υψηλό, δεδομένου ότι τελικά κάποιοι χρήστες θα αγοράσουν τα προϊόντα ή τις υπηρεσίες που αυτοί διαφημίζουν. Ενδεικτικά αναφέρεται ότι από σχετική μελέτη που έγινε στην Μεγάλη Βρετανία, 22% των χρηστών είχε αγοράσει τουλάχιστον μία φορά προϊόντα λογισμικού που διαφημίζονταν μέσω spam μηνυμάτων

Το spam περιλαμβάνει μόνο μηνύματα ηλεκτρονικού ταχυδρομείου;

Όχι, αν και αυτή είναι η πιο συνήθης περίπτωση. Το spam περιλαμβάνει επίσης μηνύματα που αποστέλλονται μέσω κινητού τηλεφώνου (SMS, MMS), υπηρεσίες instant messaging, blogs, κ.α.

Χρησιμοποιείστε λογισμικό φιλτραρίσματος

Το λογισμικό φιλτραρίσματος μπορεί να εντοπίσει μεταξύ των εισερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου αυτά που είναι spam και, ανάλογα με τις ρυθμίσεις που έχουν γίνει από τον χρήστη, είτε να "μπλοκάρει"τα μηνύματα spam, είτε να τα τοποθετήσει σε ειδικό φάκελο.

Το φιλτράρισμα είναι χρήσιμο, αλλά δεν είναι πάντα αποτελεσματικό. Μερικές φορές τα φίλτρα αποτυγχάνουν στον εντοπισμό των μηνυμάτων spam, ενώ άλλες χαρακτηρίζουν ως spam μηνύματα που δεν είναι spam.

Σήμερα υπάρχει μεγάλη ποικιλία λογισμικών φιλτραρίσματος, πολλά από τα οποία διατίθενται και στο Διαδίκτυο. Ο Πάροχος Υπηρεσιών Διαδικτύου σας μπορεί ενδεχομένως να σας συμβουλεύσει περαιτέρω ή και να σας παρέχει ανάλογα προϊόντα.

Μην γίνετε... spammer κατά λάθος

Αν δεν εφαρμόζετε κατάλληλα μέτρα ασφαλείας, οι spammers μπορούν να καταλάβουν τον υπολογιστή σας και να τον χρησιμοποιήσουν για να στέλνουν μηνύματα spam χωρίς εσείς να το γνωρίζετε. Φροντίστε για την ασφάλεια του υπολογιστή σας και των δεδομένων σας:

- Χρησιμοποιείστε λογισμικό καταπολέμησης των ιών (anti-virus) και φροντίστε για τη συχνή ανανέωση του.
- Εγκαταστήστε τα τελευταία security patches στον υπολογιστή σας.
- Χρησιμοποιείστε μεγάλους και τυχαίους κωδικούς πρόσβασης (passwords).
- Προσέξτε όταν "ανοίγετε" αρχεία συνημμένα σε μηνύματα ηλεκτρονικού ταχυδρομείου, καθώς πολλά από αυτά μπορεί να περιέχουν επικίνδυνο λογισμικό. Ανοίξτε τέτοια αρχεία μόνο όταν γνωρίζετε το πρόσωπο από το οποίο προέρχονται.

Προστατεύστε τον αριθμό του κινητού σας τηλεφώνου

Το spam στα μηνύματα που αποστέλλονται μέσω κινητού τηλεφώνου έχει τελευταία αρχίσει να εξαπλώνεται και μπορεί να είναι ιδιαίτερα ενοχλητικό. Μην αποκαλύπτετε τον αριθμό κινητού τηλεφώνου σας σε άτομα ή οργανισμούς που δεν γνωρίζετε και χωρίς κάποιον συγκεκριμένο λόγο.

Μην απαντάτε στον αποστολέα

Όταν απαντάτε σε μηνύματα spam ουσιαστικά επαληθεύετε την εγκυρότητα της διεύθυνσης ηλεκτρονικού ταχυδρομείου σας και ενθαρρύνετε τους spammers να στέλνουν περισσότερα μηνύματα. Για το λόγο αυτό μην απαντάτε ηλεκτρονικά στον αποστολέα και μην ακολουθείτε συνδέσμους (links) που ενδεχομένως αναφέρονται στο μήνυμα, ακόμα και αν πρόκειται για συνδέσμους διαγραφής της διεύθυνσης σας από την λίστα του αποστολέα (unsubscribe links).

Σύμφωνα με την Ελληνική νομοθεσία, σε κάποιες περιπτώσεις επιτρέπεται η αποστολή μηνυμάτων μέχρι την εναντίωση του παραλήπτη ("opt-out"). Ακόμα και σε αυτές τις περιπτώσεις, είναι προτιμότερο η δήλωση εναντίωσης να μη γίνεται ηλεκτρονικά, αλλά π.χ. με τηλεφωνική επικοινωνία ή με γραπτή επιστολή.

Επικοινωνήστε με τον Πάροχο Υπηρεσιών Διαδικτύου

Μπορείτε να αναφέρετε προβλήματα spam στον Πάροχο Υπηρεσιών Διαδικτύου σας, ζητώντας ενδεχομένως τη φραγή συγκεκριμένων διευθύνσεων από τις οποίες σας αποστέλλονται μηνύματα spam. Επιπλέον, ο Πάροχος σας μπορεί να σας βοηθήσει σχετικά με τη χρήση ειδικού λογισμικού φιλτραρίσματος ή άλλων μέτρων ασφαλείας για την αποφυγή λήψης μηνυμάτων spam.

ΠΕΙΡΑΤΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Τι είναι η πειρατεία στο διαδίκτυο;

Πειρατεία ονομάζεται κάθε πράξη βίας ή αιχμαλώτισης ή απόσπασης η οποία διαπράττεται και στέφεται εναντίον προσώπων ή ιδιοκτησίας

• Η πειρατεία είναι από τα σοβαρότερα εγκλήματα του Διεθνούς Δικαίου. Ειδικότερα η πειρατεία στο διαδίκτυο γίνεται με το παράνομο κατέβασμα υλικού όπως μουσικής ταινιών ,τηλεοπτικών σειρών βιβλίων μέσο κάποιων ιστότοπων που καταπατούν τον νόμο περί πνευματικών δικαιωμάτων και παρέχουν δωρεάν σε όλους αυτό που αναζητούν

Ποιες είναι οι συνέπειες της εξάπλωσης της πειρατείας ;

• μείωση την εσόδων στην χώρα
• μείωση των τηλεοπτικών σειρών και ταινιών
• μείωση των μουσικών βιομηχανιών
• μείωση των καταστημάτων που προωθούν τα παραπάνω
• κλοπή πνευματικών δικαιωμάτων
• διαστρέβλωση των πληροφοριών
• απειλή των βιβλίων και τον βιβλιοπωλείων
• μείωση της πώλησης παιχνιδιών για υπολογιστές

Ποια είναι τα κατά της πειρατείας ;

• Είναι η απομόνωση μέσα στα σπίτια μπροστά από έναν υπολογιστή.
• αν και η πειρατεία εμάς μας συμφέρει έχει μεγάλες επιπτώσεις σε κάποιους ανθρώπους που έχουν κάποιο χρηματικό κέρδος.

Ποια προγράμματα είναι δύσκολα στον εντοπισμό της πειρατείας ;

• Υπάρχουν πολλά προγράμματα κατεβάσματος αλλά δεν είναι τόσο αξιόπιστα όπως είναι το Gnutella και το Freenet τα οποία είναι δύσκολο να εντοπιστούν και να αναγνωριστούν καθώς λειτουργούν χωρίς κεντρικό server .

Ποια ποινή θα έχουμε αν μας εντοπίσουν ;

• Καθώς στην Κύπρο 8 στους 10 πολίτες κατεβάζουν παράνομα αν εντοπιστούν θα υποστούν μηνύσεις. Για τους ιδρυτές κάποιων παράνομων σελίδων ή για προγράμματα κατεβάσματος προβλέπετε:
•Ποινική δίωξη για παράβαση του νόμου σε βαθμό κακουργήματος. Αλλά και για κάθε παράνομο αντίτυπο προβλέπετε πρόστιμο 1.000 ευρώ από το κράτος .
•Στις Η.Π.Α αντιμετωπίζουν το πρόστιμο που ξεκινάει από 750 έως και 150.000 δολάρια .
•Το 2012 στην Ελλάδα το Μονομελούς Πρωτοδικείου Αθηνών μετά από αίτημα οργανισμών συλλογικής διαχείρισης δικαιωμάτων επί μουσικών και οπτικοακουστικών έργων, υποχρεώνει τις ελληνικές εταιρείες παροχής υπηρεσιών σύνδεσης στο Διαδίκτυο να λάβουν τεχνολογικά μέτρα για να καταστεί αδύνατη η πρόσβαση των πελατών τους σε διαδικτυακές τοποθεσίες μέσω των οποίων πραγματοποιείται παράνομη παρουσίαση και ανταλλαγή έργων

Υπάρχει λύση για την πειρατεία ;

Δημιουργία:
•Πανευρωπαϊκών ιστοσελίδων με σκοπό το κατέβασμα να μην είναι παράνομο.
•Υπηρεσίας πληρωμών των πνευματικών δικαιωμάτων για τους καλλιτέχνες

ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ

Πνευματικά δικαιώματα ονομάζονται τα αποκλειστικά δικαιώματα των πνευματικών δημιουργών στο έργο τους . Παραχωρούνται από τον νόμο για ορισμένο χρόνο για να απαγορεύσουν σε τρίτους τη χρήση των έργων χωρίς την άδεια του δημιουργού . Το πνευματικό δικαίωμα υφίσταται σε έργα λογοτεχνίας και τέχνης, όπως βιβλία, θέατρο, ζωγραφική, γλυπτική, φωτογραφία, αρχιτεκτονική αλλά και άλλες δημιουργίες όπως λογισμικό ή βάσεις δεδομένων.

Πώς καταπατούνται τα Πνευματικά δικαιώματα ;

• Εάν παραλείπετε το όνομα του δημιουργού, αν παραμορφωθεί ή τροποποιηθεί το αρχικό έργο.
•Εάν "ανεβάσουμε" ή "κατεβάσουμε" παράνομα κάποια ξένη πνευματική ιδιοκτησία.

Δεν καταπατούνται:

• Όταν ανεβάσουν ένα μικρό δείγμα του έργου για να ασκηθεί κριτική.
• Όταν ο δημιουργός πεθάνει επιτρέπεται να ανεβαστεί το έργο του σε μορφή ανθολογίου.

Σε ερωτήσεις που έγιναν σε μαθητές λυκείου διαπιστώθηκε ότι :

Το 81% των μαθητών κατεβάζει παράνομα ταινίες και μουσική, ενώ μόνο το 59% αυτών γνωρίζει ότι όταν κατεβάζετε παράνομα καταπατάτε τον νόμο περί πνευματικών δικαιωμάτων

ΠΑΡΑΝΟΜΗ ΛΗΨΗ ΑΡΧΕΙΩΝ ΜΟΥΣΙΚΗΣ ΑΠΟ ΤΟ ΔΙΑΔΙΚΤΥΟ (INTERNET DOWNLOADING)

Η δύναμη της σύγχρονης τεχνολογίας των υπολογιστών σε συνδυασμό με την δυνατότητα διασύνδεσης στο Διαδίκτυο, έχει καταστήσει δυνατή την λήψη, την αποθήκευση και το παίξιμο μουσικής και βίντεο από υπολογιστές. Έτσι κατανοώντας τις δυνατότητες του Διαδικτύου δημιουργήθηκε το Napster, μια υπηρεσία η οποία επιτρέπει στους χρήστες των υπολογιστών να ανταλλάζουν και να μοιράζονται αρχεία μέσω ενός κεντρικού συστήματος. Παρόλο που αυτό το σύστημα θα μπορούσε να έχει πολλές χρήσεις, σύντομα έγινε ξεκάθαρο ότι οι περισσότεροι χρήστες του είχαν έναν συγκεκριμένο σκοπό: να λαμβάνουν δωρεάν μουσική! Καθώς πολλοί κορυφαίοι καλλιτέχνες αντέδρασαν έντονα σε αυτή την κατάσταση ο Napster ηττήθηκε από τους δικηγόρους της μουσικής βιομηχανίας και αναγκάστηκε να σταματήσει την λειτουργία του. Όμως καθώς είχαν ήδη δημιουργηθεί εκατοντάδες αντίγραφα για να αναπληρώσουν την απώλεια σήμερα πραγματοποιούνται καθημερινά δεκάδες εκατομμύρια παράνομες λήψεις αρχείων μουσικής από το Διαδίκτυο. Όμως το Napster έχει αντικατασταθεί σήμερα από παρά πολλά άλλα προγράμματα . Τα πιο διαδεδομένα είναι το torrent και το rapidshere. Ειδικότερα το Torrent είναι ένα σύνολο αρχείων που περιέχουν πληροφορίες για τα αρχεία στα οποία αναφέρεται το torrent και μέρος των οποίων θέλουμε να καταβιβάσουμε, κοινώς download.
Οι πληροφορίες ενός αρχείου είναι:
α) όνομα του αρχείου
β) το μέγεθος του
γ) πεδίο επαλήθευσης όλων των τμημάτων του αρχείου.
Το rapidshere είναι μία υπηρεσία όπου μπορείς να ανεβάσεις τα αρχεία σου και να τα μοιραστείς με τους φίλους σου σε όποιο σημείο του κόσμου και αν βρίσκονται. Επομένως είναι αποδεκτό να λαμβάνει κανείς παρανόμως αρχεία μουσικής από το διαδίκτυο; Με μια πρώτη ματιά, η ιδέα της απόκτησης δωρεάν μουσικής χωρίς να κλέβεις από κάποιον, ή να τον βλάπτεις δεν φαίνεται κακή. Αλλά πριν βρεθείτε μπροστά στον υπολογιστή σας και αρχίσετε να αντιγράφετε αρχεία πρέπει να ξέρετε ότι η μουσική βιομηχανία κάποιων χωρών έχει αρχίσει να λαμβάνει μέτρα εναντίων των ιδιωτών απαιτώντας αποζημίωση εκατοντάδων ευρώ για την παραβίαση των νόμων της πνευματικής ιδιοκτησίας. Δεδομένου όμως ότι είναι πάρα πολλοί αυτοί που το κάνουν , οι πιθανότητες να σας πιάσουν είναι λίγες, αλλά όμως υπάρχουν.

HACKERS-CRACKERS

HACKERS:

Γενικά:
Hacker ονομάζεται το άτομο το οποίο εισβάλει σε υπολογιστικά συστήματα και πειραματίζεται με κάθε πτυχή τους. Ένας hacker έχει τις κατάλληλες γνώσεις και ικανότητες να διαχειρίζεται σε μεγάλο βαθμό υπολογιστικά συστήματα. Συνήθως οι hackers είναι προγραμματιστές, σχεδιαστές συστημάτων αλλά και άτομα τα οποία ενώ δεν ασχολούνται επαγγελματικά με τομείς της πληροφορικής έχουν αναπτύξει τέτοιες δεξιότητες και δουλεύουν είτε σε ομάδες (hacking-groups), είτε μόνοι τους.

Γνωστοί Hackers:

- **Adrian Lamo:** Ο Lamo έχει μείνει στην ιστορία ως ένας από τους μεγαλύτερους hackers γιατί εισέβαλε σε συστήματα εταιριών όπως η Microsoft και η New York Times. Ο Lamo χρησιμοποιούσε ως επί το πλείστον δημόσιες συνδέσεις internet σε καφετέριες για να είναι πιο δύσκολο να εντοπιστεί, κάτι που του έδωσε το παρατσούκλι «άστεγος hacker». Η λίστα των εταιριών που απέκτησε πρόσβαση ο Lamo περιέχει επίσης τις, Yahoo!, Citigroup, Bank of America και Cingular, βέβαια στα πλαίσια της ομάδας White Hat Hackers οι οποίοι προσλαμβάνονται από τις ίδιες τις εταιρίες για να βρουν λάθη στο σύστημα προστασίας τους ο Lamo δεν διέπραξε κανένα έγκλημα αλλά παρέβη το νόμο όταν μπήκε στο ιδιωτικό σύστημα επικοινωνίας των New York Times. Αυτή την στιγμή ο Lamo έχει εκτίσει την διετή ποινή περιορισμού που του είχε επιβληθεί και είναι βραβευμένος δημοσιογράφος.
- **Jonathan James:** Στα 16 του χρόνια ο James, έγινε ο πρώτος ανήλικος που καταδικάζεται για ηλεκτρονικά εγκλήματα με ποινή φυλάκισης. Αργότερα παραδέχτηκε ο ίδιος ότι το έκανε για πλάκα και απολάμβανε τις προκλήσεις. Ο James εισέβαλε σε δημόσιους οργανισμούς όπως ένα παράρτημα του Υπουργείου Δικαιοσύνης και έπαιρνε κωδικούς για να έχει πρόσβαση σε απόρρητους λογαριασμούς e-mail. Εκτός από αυτά, ο James απέκτησε πρόσβαση στους υπολογιστές της NASA και έκλεψε πολύτιμα software συνολικής αξίας 1,7 εκατ. δολαρίων.
- **Kevin Poulsen:** Πιο γνωστός με το παρατσούκλι του, Dark Dante, ο Kevin Poulsen έγινε γνωστός εισβάλοντας στο τηλεφωνικό κέντρο του ραδιοφωνικού σταθμού KISS-FM του Los Angeles παρεμβαίνοντας στις κληρώσεις και κερδίζοντας μεγάλα δώρα μεταξύ των οποίων και μια Porsche. Το FBI άρχισε να ασχολείται με τον Poulsen αφού απέκτησε πρόσβαση στα αρχεία της και αποσπούσε σημαντικές και απόρρητες πληροφορίες. Η ειδικότητά του ήταν οι τηλεφωνικές γραμμές και αποκτούσε πρόσβαση σε μεγάλα δίκτυα, όπως το Los Angeles Radio και τον KIIS-FM προκαλώντας το χάος. Αφού συνελήφθη σε ένα σουπερμάρκετ καταδικάστηκε σε πέντε χρόνια φυλάκισης, και ενώ ήταν στην φυλακή δούλευε ως δημοσιογράφος και αργότερα εκδότης των Wired News.

Τα τελευταία χρόνια, οι hackers είναι ευρέως γνωστοί ως οι κακοί του κυβερνοχώρου και έχουν χαρακτηριστεί από την κοινωνία μας, ως εγκληματίες. Είναι γνωστοί επίσης ως crackers ή black hats. Ο όρος κράκερ χρησιμοποιήθηκε για να διακρίνει όσους αποκτούν πρόσβαση σε υπολογιστικά συστήματα, προκαλώντας όμως σ' αυτά και σοβαρές ζημιές.

Τρόποι δράσης:

- **Sniffer:** Μία μέθοδος επίθεσης των hackers έχει να κάνει με τη χρήση των λεγομένων sniffers ("λαγωνικά"). Το sniffer είναι ένα μικρό πρόγραμμα το οποίο χωρίς να γίνεται αντιληπτό εισχωρεί σ' ένα σύστημα όπου ψάχνει και αναλύει τα

αρχεία του με σκοπό τη συλλογή συγκεκριμένων πληροφοριών τις οποίες διαβιβάζει στη συνέχεια στον χρήστη του.

- **Ιοί και σκουλήκια:** Τα σκουλήκια και οι ιοί είναι αυτοαναπαραγόμενα προγράμματα, τα οποία μπορούν να εξαπλώνονται σε ευρεία κλίμακα σε όλο το διαδίκτυο. Συνήθως οδηγούν στην καταστροφή και δυσλειτουργία συστημάτων και αρχείων. Τα σκουλήκια αντιγράφονται από υπολογιστή σε υπολογιστή χωρίς να απαιτούν τη συμβολή κανενός άλλου προγράμματος ή αρχείου. Το διασημότερο σκουλήκι **ILOVEYOU** υπολογίζεται ότι επηρέασε περίπου 45 εκατ. υπολογιστές.

Επιπτώσεις Δράσης

Οι ενέργειες των hackers επιφέρουν κοινωνικές, οικονομικές, πολιτικές, καθώς και επιχειρησιακές συνέπειες. Οι χρήστες μπορούν να πέσουν θύματα κλοπής των χρημάτων τους από τραπεζικούς λογαριασμούς ή πιστωτικές κάρτες.

Τα ανυποψίαστα θύματα μπορούν να γίνουν δέκτες εκβιασμών, εν αγνοία τους να γίνουν κόμβος ενός botnet, να γίνουν ενδιάμεσοι κόμβοι παροχής κακόβουλου λογισμικού, αποστολείς μηνυμάτων spam, να φιλοξενούν παράνομους servers κ.α.

Σε οργανισμούς και ιδιώτες δημιουργείται οικονομικό αντίκτυπο καθώς μπορεί να σπιλωθεί η φήμη μιας επιχείρησης με αποτέλεσμα η επιχείρηση να χάσει τους πελάτες της, ειδικότερα όταν πρόκειται για την προστασία των προσωπικών δεδομένων των πελατών.

Με τις ιδιωτικές προσωπικές πληροφορίες προσβάσιμες σε όλους υπάρχει κίνδυνος της υποκλοπής της ταυτότητάς τους και άλλων εμπιστευτικών τους πληροφοριών από άτομα με κακή πρόθεση. Οι χάκερ χρησιμοποιούν εργαλεία που είναι διαθέσιμα στα υπόγεια, ευρετική και μεθόδους "κοινωνικής μηχανικής" για να υπαινιχθεί το δρόμο τους σε υπολογιστές και δίκτυα υπολογιστών. Κοινωνική μηχανική είναι η ικανότητα του να πάρει τους κωδικούς πρόσβασης ή άλλες πληροφορίες σχετικά με τα συστήματα από τους ανθρώπους που πρέπει να γνωρίζουν καλύτερα.

CRACKERS:

Γενικά:

Cracking είναι η πράξη του να εισβάλλει ένας cracker σε ένα σύστημα υπολογιστή, συχνά σε ένα δίκτυο. Ένας Cracker μπορεί να κάνει αυτό για το κέρδος, κακόβουλα, ή επειδή η πρόκληση είναι εκεί. Cracker ονομάζεται ένα άτομο που χωρίς εξουσιοδότηση αποκτα παράνομη πρόσβαση σε ένα σύστημα υπολογιστών και στα δεδομένα του, με σκοπό την πρόκληση οικονομικής ή άλλου είδους ζημιάς και την κλοπή πληροφοριών.

Ένα πράγμα που μπορεί να κανει ενας cracker είναι να υποκλέψει ευαίσθητα δεδομένα - πολύ σαν "υποκλοπές". Υπάρχουν πολλές θέσεις και τους τρόπους για την αξιοποίηση των δεδομένων σας. Μερικοί την αποκαλούν «fiber-tapping» επειδή τα δεδομένα ταξιδεύουν στο διαδίκτυο με ίνες γυαλιού τις περισσοτερες φορες. Ωστόσο, «secure sites» έχουν σχεδόν εξαλειψει τον κίνδυνο αυτό.

Οι crackers προσπαθούν παράνομα να μπουν σε συστήματα υπολογιστών με σκοπό να υποκλέψουν δεδομένα και να προκαλέσουν ζημιά στις πληροφορίες που βρίσκονται στους φακέλους του συστήματος. Για παράδειγμα, μόλις αποκτήσουν έναν αριθμό πιστωτικής κάρτας, τον χρησιμοποιούν προς όφελός τους. Η πιο εμφανής και αμφιλεγόμενη δράση του Cracking λογισμικού είναι η απελευθέρωση της πλήρως λειτουργικής ιδιόκτητου λογισμικού χωρίς καμία προστασία κατά της αντιγραφής. Οι crackers

θεωρούνται ως οι κακόβουλοι hackers και έχουν ως στόχο την πρόκληση ζημιάς σε δίκτυα υπολογιστών, την εισβολή σε υπολογιστές χρηστών χωρίς εξουσιοδότηση, την δημιουργία ιών, την παραβίαση κωδικών ασφαλείας, την καταστροφή ή και την αλλοίωση δικτυακών τόπων (Web sites) όπου αφήνουν περήφανα την δικτυακή τους σφραγίδα με το ψευδώνυμό τους, την δημιουργία πειρατικών αντιγράφων προγραμμάτων ή τραγουδιών ή και βίντεο κ.ά.

Με απλά λόγια, πρόκειται για hackers οι οποίοι προβαίνουν σε πράξεις που παραβιάζουν διατάξεις του κοινού ποινικού κώδικα. Συνήθως πρόκειται για άτομα με έντονη ανάγκη για επίδειξη, οι οποίοι διεισδύουν σε συστήματα και προκαλούν ζημιές. Οι κυριότερες διαφορές τους από τους hackers είναι ότι δεν έχουν ιδιαίτερες γνώσεις για την πληροφορική και τον προγραμματισμό καθώς και το ότι δεν διέπονται από κανενός είδους ηθική αρχή. Για τους λόγους αυτούς μπορούν πολύ εύκολα να καταστρέψουν ολόκληρα συστήματα υπολογιστών απλά και μόνο για να κάνουν το κέφι τους, όταν βρουν βέβαια την κατάλληλη ευκαιρία.

Τρόποι δράσης:

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

ΑΠΑΤΕΣ ΚΑΙ ΛΗΣΤΕΙΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ!

Οι συνηθέστερες μορφές διαδικτυακής απάτης είναι οι ακόλουθες:

α) Χρεώσεις της πιστωτικής κάρτας πολιτών μέσω του διαδικτύου για αγορές, οι οποίες δεν πραγματοποιήθηκαν από τους ίδιους.

- Στις περιπτώσεις αυτές, κάποιος κακόβουλος χρήστης του διαδικτύου δημιουργεί μια πλασματική ιστοσελίδα και με αυτόν τον τρόπο καταφέρνει να συγκεντρώνει στοιχεία κι αριθμούς πιστωτικών καρτών χρηστών του διαδικτύου, οι οποίοι έχοντας εξαπατηθεί, νομίζουν ότι πρόκειται για κάποιο διαδικτυακό κατάστημα και κάνουν τις αγορές τους.
- Επιπλέον, αρκετές είναι οι περιπτώσεις όπου επιτήδειοι καταφέρνουν να αποκτούν φυσική πρόσβαση στα στοιχεία πιστωτικών καρτών πολιτών τα οποία εν συνεχεία χρησιμοποιούν σε διαδικτυακές αγορές, καθώς για τις αγορές αυτές δεν

είναι απαραίτητη η φυσική κατοχή της πιστωτικής κάρτας, παρά μόνο τα στοιχεία αυτής.

- Επιπροσθέτως, σε αρκετές περιπτώσεις οι χρήστες του διαδικτύου δίνουν οι ίδιοι άθελά τους τα στοιχεία σε κακόβουλους χρήστες του διαδικτύου (phishing). Ειδικότερα, ο ανυποψίαστος πολίτης λαμβάνει μήνυμα ηλεκτρονικού ταχυδρομείου από Πιστωτικό Ίδρυμα, στο οποίο τηρεί λογαριασμό, με το οποίο του ζητείται να συμπληρώσει τα στοιχεία του (ονοματεπώνυμο, αριθμό λογαριασμού και πιστωτικής κάρτας κλπ.), για λόγους πχ. ενημέρωσης των αρχείων της τράπεζας. Το μήνυμα, μέσω υπερσυνδέσμου, τους οδηγεί σε μια πλασματική ιστοσελίδα της τράπεζας, με αποτέλεσμα ο πολίτης να πείθεται και να χορηγεί τα επίμαχα στοιχεία.

β) Διακίνηση μηνυμάτων με απατηλό περιεχόμενο, που επιδιώκουν την εξαπάτηση ανυποψίαστων πολιτών.

- Ειδικότερα, ο τρόπος δράσης των κακόβουλων δραστών στην εν λόγω μορφή απάτης, που περιγράφεται υπό τον όρο «Ισπανικό Λόττο», είναι η μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους ενημερώνουν ότι έχουν κερδίσει ένα μεγάλο χρηματικό ποσό της τάξεως των εκατομμυρίων δολαρίων σε ηλεκτρονική κλήρωση του διαδικτύου.
- Οι δημιουργοί των μηνυμάτων αυτών, για να γίνουν πιστευτοί, χρησιμοποιούν παραπλήσια ονόματα μεγάλων εταιρειών (πχ. Microsoft , Yahoo κλπ) και συνοδεύουν τα μηνύματα που αποστέλλουν με πλαστά πιστοποιητικά όσον αφορά στην υποτιθέμενη ηλεκτρονική κλήρωση.
- Η απάτη έγκειται στο γεγονός ότι ζητούν από τους υποτιθέμενους νικητές την προπληρωμή κάποιων φόρων ή/και εξόδων εκταμίευσης των χρημάτων, ποσό που συνήθως είναι της τάξης των μερικών χιλιάδων δολαρίων.

γ) «Απάτες 419» ή «Νιγηριανές Απάτες»

- Στις περιπτώσεις αυτές αποστέλλονται, μηνύματα σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους πληροφορούν ότι κάποιος κάτοχος ιδιαίτερα μεγάλης περιουσίας έχει αποβιώσει και είτε δεν υφίσταται κανείς κληρονόμος και ο παραλήπτης του μηνύματος έχει επιλεγεί ούτως ώστε να κληρονομήσει αυτός την περιουσία, είτε για να καταστεί δυνατό να αποδεσμευτεί η περιουσία, χρειάζεται αυτή να μεταφερθεί σε τραπεζικό λογαριασμό του εξωτερικού και ο παραλήπτης του μηνύματος ενημερώνεται ότι εάν διαθέσει το λογαριασμό του, θα αποκτήσει κάποιο ποσοστό επί της περιουσίας αυτής.
- Σε άλλες περιπτώσεις, άτομα από τη Νιγηρία αναζητούν τη βοήθεια επιχειρηματιών ή ελεύθερων επαγγελματιών με σκοπό να μεταφέρουν τα κεφάλαιά τους, τα οποία προέρχονται από εγκληματικές πράξεις (λαθρεμπόριο, απάτες, δωροδοκία κλπ.), υποσχόμενοι για τη συνεργασία αυτή υψηλό ποσοστό αμοιβής. Για το σκοπό αυτό, κάνουν χρήση τίτλων επίσημων φορέων της χώρας τους (Υπουργεία, Κεντρική Τράπεζα, Εθνική Εταιρεία Πετρελαίων Νιγηρίας κλπ.), χρησιμοποιούν τίτλους κυβερνητικών ή στρατιωτικών παραγόντων με υπαρκτά και ψεύτικα ονόματα ή προφασίζονται σχέση τους με «διάσημα» ή «σημαντικά» πρόσωπα.
- Η απάτη έγκειται στο γεγονός ότι οι αποστολείς των μηνυμάτων ζητούν από τους παραλήπτες να τους αποστείλουν τα προσωπικά τους στοιχεία, τα στοιχεία των τραπεζικού λογαριασμού και πιστωτικής κάρτας κλπ. προκειμένου επιτευχθεί η συνεργασία τους και η αποκόμιση των χρηματικών ποσών.

Απάτες στο Internet

Είναι κοινή πια παραδοχή πως όσο περνάει ο καιρός και αυξάνονται οι χρήστες του δικτύου, τόσο περισσότερο πλησιάζει το Internet την διάρθρωση και λειτουργία μιας

πραγματικής κοινωνίας με δική της γλώσσα, συνήθειες, κώδικα συμπεριφοράς και ηθικής.
Όπως όμως συμβαίνει σε κάθε κοινωνία, μερικά μέλη της, δεν ενστερνίζονται τις ηθικές αρχές του συνόλου, αλλά προτιμούν να λειτουργούν σε βάρος των πολλών αποκομίζοντας οικονομικά κυρίως οφέλη.
Βέβαια, ακόμη και οι απατεώνες του δικτύου δεν μπορούν να ξεφύγουν από τους περιορισμούς που αυτό επιβάλλει. Δεν έχουμε δει ακόμη ένοπλη ληστεία ή φόνο στο Internet (αν και είμαι βέβαιος πως κάποια στιγμή θα γίνει και αυτό). Οι τρόποι που χρησιμοποιούνται μέσα στο δίκτυο είναι πιο εγκεφαλικοί. Δεν είναι όμως λιγότερο επικίνδυνοι.
Σύμφωνα με την Internet Fraud Watch, η πιο δημοφιλής απάτη στο Internet είναι τα συστήματα τύπου "Αεροπλανάκι" (όπως το γνωστό MAKE MONEY FAST) όπου οι πρώτοι συμμετέχοντες πληρώνουν χρήματα που προσδοκούν πως θα πάρουν πολλαπλάσια από τους επόμενους, χωρίς σχεδόν ποτέ να το καταφέρνουν. Τα χρήματα που διακινούνται σε τέτοιες περιπτώσεις, δεν είναι καθόλου ευκαταφρόνητα αν σκεφτεί κανείς ότι σε μία μόνο περίπτωση, (που δημιούργησε μια εταιρεία με το όνομα Fortuna Alliance) ο συνολικός τζίρος έφτασε τα 6 εκατομμύρια δολλάρια ΗΠΑ!
Δεύτερη σε δημοτικότητα κατηγορία είναι αυτή των Αεριτζήδων Παροχέων Υπηρεσιών Internet. Στις περισσότερες περιπτώσεις πρόκειται για άτομα ή επιχειρήσεις που εισπράττουν προκαταβολές για δημιουργία παρουσιάσεων στο Web ή παροχή πρόσβασης στο Internet και στην συνέχεια εξαφανίζονται.
Το τρίτο σε δημοτικότητα κόλπο είναι η πώληση "άριστης ποιότητας" υλικού (hardware) σχετικού με το Internet σε αφάνταστα χαμηλές τιμές που όμως στην πράξη άλλες φορές αποδεικνύεται χαμηλής ποιότητας και άλλες απλώς δεν παραδίδεται ποτέ.
Η τέταρτη πιο συνηθισμένη πρακτική είναι η εξαπάτηση επενδυτών που θέλουν να μπουν στο Internet με πλαστά στοιχεία (π.χ. εμείς κατασκευάσαμε αυτό το site και έχει 5.000.000 hits τη μέρα, ο ιδιοκτήτης του μας πλήρωσε 100.000$ και τώρα κερδίζει 200.000$ την εβδομάδα κτλ.). Η αλήθεια δεν γίνεται γνωστή παρά μόνο όταν γίνει η επένδυση οπότε είναι πλέον αργά.
Τέλος, η πέμπτη πιο συνηθισμένη μέθοδος, στρέφεται κατά ελευθέρων επαγγελματιών και ανθρώπων που παρέχουν υπηρεσίες εργαζόμενοι από το σπίτι τους. Διάφοροι υποτιθέμενοι επενδυτές τους υπόσχονται πλουσιοπάροχες αμοιβές για απλές εργασίες όπως η επεξεργασία κειμένου ή η μετατροπή (conversion) αρχείων γραφικών από το ένα format στο άλλο. Για να συνεργαστεί όμως με τους "επενδυτές" το θύμα, θα πρέπει να αγοράσει από αυτούς ή από συνενόχους τους πανάκριβο λογισμικό. Όταν δε το κάνει, και αρχίσει η συνεργασία, λαμβάνει ένα ευγενικό γράμμα που το πληροφορεί πως η ποιότητα της εργασίας που παρέδωσε δεν καλύπτει τα ποιοτικά πρότυπα της εταιρείας και για τον λόγο αυτό η συνεργασία μαζί του διακόπτεται.
Δεν υπάρχει κανείς ασφαλής τρόπος για να προστατευτούν από τις απάτες οι χρήστες του Internet και οι λόγοι γι' αυτό είναι πολλοί:

1. Το Internet είναι ένα νέο μέσο με τρόπο λειτουργίας που αφήνει την φαντασία ελεύθερη να ακολουθήσει νέους δρόμους. Διαρρήκτες και καταχραστές υπάρχουν στον πραγματικό κόσμο εδώ και αιώνες και λίγο πολύ έχουμε μάθει να αναγνωρίζουμε τις πιο κραυγαλέες περιπτώσεις και να φυλαγόμαστε από αυτές. Στο Internet όμως όλα είναι καινούρια. Δεν υπάρχει η συλλογική πείρα για να μας προστατεύσει ούτε οι μηχανισμοί για να το επιτύχουμε μόνοι μας.
2. Όλο και περισσότερος κόσμος συνδέεται για πρώτη φορά στο Internet. Έτσι το ίδιο επιτυχημένο κόλπο που οι "παλιοί" το έχουν πλέον μάθει μπορεί να χρησιμοποιηθεί και πάλι στους καινούριους και ακόμα ασυνήθιστους με τον τρόπο λειτουργίας του δικτύου χρήστες.

3. Οι ταχύτατοι ρυθμοί με τους οποίους αναπτύσσεται το Internet, δημιουργούν ή κλείνουν καθημερινά πάμπολλες επιχειρήσεις. Λίγοι άνθρωποι έχουν παρελθόν στο δίκτυο. Οι περισσότεροι μπήκαν μόλις πρόσφατα στην αγορά και δεν υπάρχει λόγος να το κρύψουν. Το πεδίο είναι λοιπόν ελεύθερο σε οποιονδήποτε να δηλώνει τα πιο απίθανα πράγματα χωρίς κανείς να μπορέσει εύκολα να τον διαψεύσει.
4. Το ίδιο το Internet αλλάζει με εφιαλτικά γρήγορο ρυθμό. Νέες πολλά υποσχόμενες τεχνολογίες εμφανίζονται καθημερινά και λίγοι έχουν την γνώση και την κρίση να ξεχωρίσουν το πραγματικά αξιόλογο από τις ευφάνταστες ανοησίες.
5. Το Internet, με τον τρόπο που λειτουργεί, ενθαρρύνει την ανωνυμία. Θετικό σε πάρα πολλές περιπτώσεις αυτό, αλλά και επικίνδυνο για προφανείς λόγους.
6. Η αγορά του δικτύου είναι πια παγκόσμια. Όμως οι δικαστικές και αστυνομικές αρχές παραμένουν εθνικές. Έτσι, τα αδικήματα που γίνονται μέσω δικτύου δημιουργούν συχνά αξεπέραστα νομικά προβλήματα τόσο στην αναζήτηση των ενόχων όσο και στην προσαγωγή τους στην δικαιοσύνη.

Τρόποι Προστασίας

1. Ποτέ μην κάνετε δουλειές με ανθρώπους που δεν τους γνωρίζετε ή δεν έχετε πάρει πληροφορίες για αυτούς από μια αξιόπιστη πηγή.
2. Ότι φαίνεται πολύ καλό συνήθως δεν είναι και αληθινό. Αν ήταν, αυτός που προσπαθεί να σας το πουλήσει θα το κράταγε για τον εαυτό του.
3. Αν συναντήσετε παράνομες δραστηριότητες μέσα στο δίκτυο καταγγείλετέ τες σε κάποιον αρμόδιο φορέα, π.χ. The Internet Fraud Watch (http://www.fraud.org e-mail nfic@internetmci.com). Μην ξεχνάτε πως σύμφωνα με τον Σωκράτη: "αν ανέχομαι την αδικία που κάνει κάποιος άλλος είναι σαν να αδικώ εγώ".

Όμως Προσοχή! Μην προβαίνετε εσείς οι ίδιοι σε καταγγελίες σε δημόσιους χώρους (usenet, mailing lists κτλ.) όσο σίγουροι και αν είστε για αυτές. Κανείς μας δεν είναι αλάνθαστος και αν κάνετε λάθος κινδυνεύετε να καταστρέψετε την υπόληψη ή την εργασία κάποιου που δεν φταίει σε τίποτε. Καλύτερα λοιπόν να αφήνετε το έργο αυτό σε άλλους πιο αρμόδιους.

Ασφάλεια Προσωπικών Δεδομένων – Phising

Προσωπικά δεδομένα είναι κάθε πληροφορία που σε χαρακτηρίζει, όπως για παράδειγμα το όνομά σου, η διεύθυνσή σου, το τηλέφωνό σου, τα ενδιαφέροντά σου, οι επιδόσεις σου στο σχολείο, οι φωτογραφίες σου, οι απόψεις σου, κ.α. Μερικές φορές τα προσωπικά σου δεδομένα αφορούν ιδιαίτερα ευαίσθητα στοιχεία της ιδιωτικής σου ζωής, όπως στο θρήσκευμά σου, στις πολιτικές σου πεποιθήσεις, στην κατάσταση της υγείας σου ή στην ερωτική σου ζωή.

Πολλές από τις καθημερινές σου δραστηριότητες βασίζονται στην επεξεργασία των προσωπικών σου δεδομένων:

· Η φόρμα που συμπληρώνεις για συμμετοχή στο διαγωνισμό της εταιρείας ηλεκτρονικών παιχνιδιών περιέχει προσωπικά σου στοιχεία, όπως όνομα, τηλέφωνο, διεύθυνση και ηλικία.

· Το ίδιο συμβαίνει και κατά την εγγραφή σου σε ένα διαδικτυακό (on-line) κατάστημα βιβλίων.

· Το σχολείο σου τηρεί δεδομένα για τους βαθμούς και τις επιδόσεις σου.

· Ο γιατρός που επισκέφτηκες τηρεί τις ιατρικές σου εξετάσεις και άλλα σχετικά στοιχεία για την υγεία σου.

· Ο αθλητικός σύλλογος στον οποίο είσαι μέλος τηρεί τα στοιχεία που έδωσες κατά την εγγραφή σου, καθώς και ιατρικά πιστοποιητικά.
· Το προφίλ σου στο Facebook περιέχει πληροφορίες για τους φίλους σου, τα ενδιαφέροντά σου, αλλά και άλμπουμ με φωτογραφίες σου.
· Το ηλεκτρονικό φόρουμ για μουσική που παρακολουθείς περιέχει στοιχεία για τις μουσικές προτιμήσεις σου και τους καλλιτέχνες που σε ενδιαφέρουν.
Αν δεν προσέξεις πώς και πού τα δημοσιοποιείς ή αν πέσουν σε λάθος χέρια, τα προσωπικά σου δεδομένα μπορούν να χρησιμοποιηθούν από κάποιους για να σε δυσφημίσουν ή να σε φέρουν σε δύσκολη θέση, αποκαλύπτοντας ιδιωτικές σου στιγμές... Οι πληροφορίες αυτές είναι δυνατόν να δυσκολέψουν τη ζωή σου στο μέλλον, π.χ. όταν θα ψάχνεις για δουλειά ή θα θες να σπουδάσεις στο πανεπιστήμιο ή να πάρεις δάνειο από μία τράπεζα. Σε ακραίες περιπτώσεις μπορεί να πέσεις ακόμα και θύμα υποκλοπής ταυτότητας (δηλαδή κάποιος που έχει τα δεδομένα σου μπορεί να προσποιείται ότι είσαι εσύ) ή θύμα παρενόχλησης και εξαπάτησης.

Μερικοί τρόποι για να σου κλέψουν τα προσωπικά σου δεδομένα

Διαβάζεις το e-mail σου – ο πάροχος ηλεκτρονικών επικοινωνιών καταγράφει την ώρα που μπήκες στο λογαριασμό σου, τον αποστολέα του μηνύματός σου, καθώς και την ώρα που σου έστειλε το μήνυμα.
7:30 «Κατεβάζεις» ένα τραγούδι στο iPod – η εταιρεία που σου πουλάει το τραγούδι καταγράφει το e-mail σου και τις μουσικές σου προτιμήσεις.
7:50 Η μητέρα σου σε πάει με το αυτοκίνητο στο σχολείο – το αυτοκίνητο διαθέτει συσκευή GPS που καταγράφει τη διαδρομή σας από το σπίτι στο σχολείο. Σε κάποια σημεία της διαδρομής υπάρχουν κάμερες ρύθμισης της κυκλοφορίας και ελέγχου παραβιάσεων του Κώδικα Οδικής Κυκλοφορίας.
10:10 Μπαίνεις στην τάξη – στο απουσιολόγιο του τμήματός σου καταγράφονται οι απόντες για κάθε διδακτική ώρα. Ο σχολικός σου φάκελος περιλαμβάνει τους βαθμούς και τις αξιολογήσεις που σε αφορούν.
12:00 Ο κολλητός σου σε τραβάει μια φωτογραφία με το κινητό – η φωτογραφία είναι αστεία και λέει πως μπορεί αργότερα να την ανεβάσει στο facebook.
15:00 Σερφάρεις στο διαδίκτυο από το σπίτι – ο browser που χρησιμοποιείς καταγράφει τις σελίδες που επισκέπτεσαι. Κάποιες σελίδες εγκαθιστούν στον υπολογιστή σου μικρά αρχεία (cookies) ώστε να μπορούν να σε αναγνωρίζουν όταν θα τις ξαναεπισκεπτείς.Μάθε περισσότερα.
15:15 Κλικάρεις μια διαφήμιση που έχει ενδιαφέρον – η διαφημιστική εταιρεία καταγράφει τις προτιμήσεις σου ώστε να μπορεί να σου στέλνει προσφορές για προϊόντα που σε ενδιαφέρουν.
15:30 Στέλνεις μια ηλεκτρονική κάρτα σε έναν φίλο που έχει γενέθλια – για την αποστολή της κάρτας πρέπει να συμπληρώσεις μια φόρμα με διάφορα προσωπικά σου στοιχεία και το email σου.
16:00 Ψάχνεις στοιχεία για την έκθεση που πρέπει να παραδώσεις αύριο – στο google καταγράφονται όλες οι αναζητήσεις που πραγματοποιείς, μαζί με την χρονική στιγμή της αναζήτησης και τη διεύθυνση δικτύου (IP) με την οποία ο υπολογιστής σου συνδέεται, μέσω του Παρόχου, στο διαδίκτυο.
18:00 Πηγαίνεις στο γυμναστήριο – στην είσοδο υπάρχει κάμερα που καταγράφει όσους μπαίνουν και βγαίνουν. Στην υποδοχή «περνάς» την κάρτα μέλους σου από το ειδικό μηχάνημα που την σκανάρει και εμφανίζει τα στοιχεία σου στην οθόνη.
19:00 Ακούς τα φωνητικά σου μηνύματα στο κινητό – το τηλέφωνο σου καταγράφει όλους όσους σε κάλεσαν, τους αριθμούς τηλεφώνου τους και τις ώρες κλήσης.

22:00 Μπαίνεις στο Facebook – διαβάζεις τι έκαναν σήμερα οι φίλοι σου και γράφεις τα δικά σου νέα. Βλέπεις ότι έχεις γίνει tagged στην σημερινή φωτογραφία που ήδη ανέβασε ο κολλητός σου και κάποιοι έχουν ήδη βάλει σχόλια. Αποδέχεσαι τα friend requests για δύο νέους φίλους, παρόλο που τον έναν δεν το ξέρεις πολύ καλά.

Συμβουλές

Προσπάθησε να διατηρείς τον έλεγχο των προσωπικών σου δεδομένων:

· Ρώτα γιατί είναι απαραίτητα τα δεδομένα σου – Σκέψου ποιος είναι αυτός που τα ζητάει. Είναι κάποιος που εμπιστεύεσαι; Πώς πρόκειται να τα χρησιμοποιήσει; Θα τα αποστείλει σε άλλους και, αν ναι, σε ποιους; Αν δεν είσαι σίγουρος για κάτι από όλα αυτά, ρώτα και μάθε πριν διαθέσεις πληροφορίες που σε αφορούν.

· Σκέψου πριν αποκαλύψεις δεδομένα – Αν λαμβάνεις γράμματα, e-mails, μηνύματα στο κινητό ή στο Facebook που σου ζητούν πληροφορίες, μην απαντήσεις αν δεν είσαι σίγουρος από ποιον προέρχονται.

· Διάβαζε προσεκτικά τα «ψιλά γράμματα» - Κάποιες εταιρείες μπορεί να γράφουν εκεί όρους για την χρησιμοποίηση των δεδομένων σου, π.χ. για διαφημιστικούς σκοπούς. Θυμήσου ότι πρέπει πάντα να δίνεις τη συγκατάθεσή σου γι' αυτό.

· Διάβαζε την πολιτική ιδιωτικότητας στις ιστοσελίδες που επισκέπτεσαι – μάθε πώς χρησιμοποιούν τα δεδομένα σου, π.χ. αν εγκαθιστούν αρχεία cookies και αν προωθούν τις πληροφορίες που σε αφορούν σε διαφημιστικές εταιρείες.

· Εμπιστεύσου το ένστικτό σου – Αν δεν είσαι σίγουρος για την ασφάλεια μιας ιστοσελίδας ή δεν νιώθεις άνετα με τον τρόπο που πρόκειται να χρησιμοποιηθούν τα προσωπικά σου δεδομένα, προτίμησε κάποια άλλη.

· Δυσκόλεψε τους… «κακούς» – Χρησιμοποίησε διαφορετικά συνθηματικά στους λογαριασμούς σου (π.χ. e-mail, Facebook, Twitter). Διάλεξε συνθηματικά που είναι εύκολο για σένα να θυμάσαι, αλλά δύσκολο για τους άλλους να μαντέψουν.

· Σκέψου ποιος μπορεί να βλέπει τα δεδομένα σου – Μην επισκέπτεσαι ιστοσελίδες που δεν θα ήθελες οι άλλοι να γνωρίζουν όταν μοιράζεσαι τον υπολογιστή σου με άλλους.

· Σκέψου πριν αγοράσεις στο διαδίκτυο – Χρησιμοποίησε ασφαλείς ιστοσελίδες, στις οποίες φαίνονται καθαρά τα στοιχεία επικοινωνίας της εταιρείας και οι οποίες διαθέτουν πολιτική ιδιωτικότητας. Έλεγχε αν είναι ασφαλές το κανάλι επικοινωνίας (π.χ. θα πρέπει η διεύθυνση της σελίδας να ξεκινάει με https και στο πρόγραμμα πλοήγησης στο διαδίκτυο να εμφανίζεται ένα λουκέτο ως εικονίδιο).

· Θυμήσου να αποσυνδέεσαι από τις ιστοσελίδες, στις οποίες έχεις εισέλθει/συνδεθεί με χρήση συνθηματικών (π.χ. όταν κάνεις αγορές από το διαδίκτυο ή την ιστοσελίδα κοινωνικής δικτύωσης).

· Κράτα τον υπολογιστή σου ασφαλή – Χρησιμοποίησε προγράμματα τείχους ασφαλείας (firewall) και προστασίας από ιούς (antivirus). Φρόντισε τα προγράμματα αυτά να είναι ενημερωμένα.

Phising

Ένα μήνυμα phishing είναι ένα μήνυμα ηλεκτρονικού ταχυδρομείου που προσπαθεί να σας ξεγελάσει ώστε να αποκαλύψετε προσωπικές πληροφορίες, καθώς φαίνεται ότι προέρχεται από νόμιμη πηγή, όπως μια τράπεζα (ή την Ομάδα Google!).

Τα μηνύματα ή οι ιστότοποι που «ψαρεύουν» πληροφορίες μπορεί να σας ζητήσουν να εισαγάγετε αυτά τα στοιχεία:

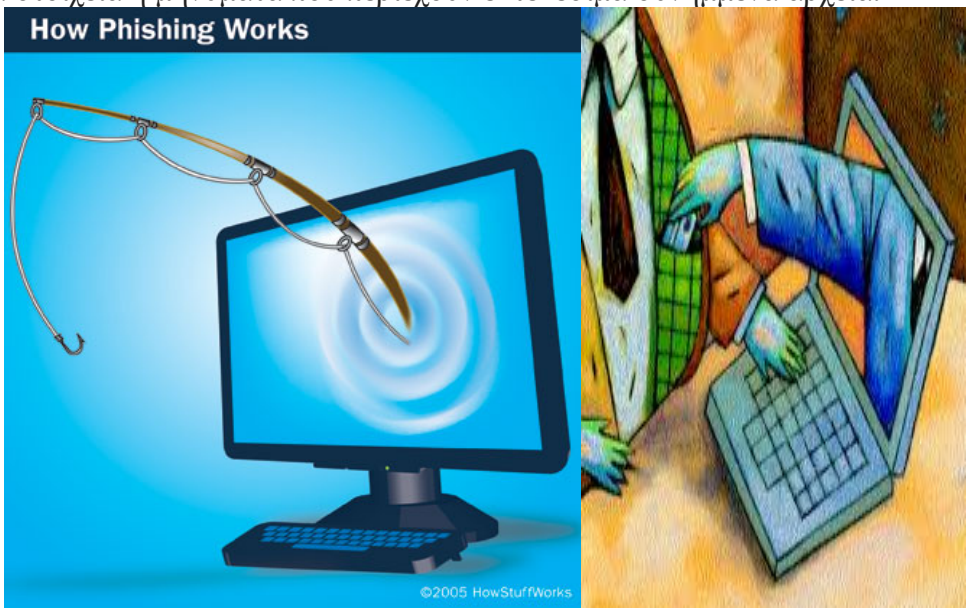
- Ονόματα χρήστη και κωδικούς πρόσβασης
- Αριθμούς κοινωνικής ασφάλισης
- Αριθμούς τραπεζικού λογαριασμού
- PIN (Προσωπικούς αναγνωριστικούς αριθμούς)

- Αριθμούς πιστωτικής κάρτας
- Το πατρικό όνομα της μητέρας σας
- Τα γενέθλιά σας

Οι phishers συχνά ζητούν προσωπικά στοιχεία επιχειρώντας να υποκλέψουν τον λογαριασμό σας Google, τα χρήματα, την πιστωτική κάρτα ή τα στοιχεία της ταυτότητάς σας.

Θα πρέπει πάντοτε να είστε επιφυλακτικοί σε οποιοδήποτε μήνυμα ζητά τα προσωπικά σας στοιχεία ή μηνύματα τα οποία σας παραπέμπουν σε μια ιστοσελίδα που ζητά προσωπικά στοιχεία.

Εάν λάβετε αυτόν τον τύπο μηνύματος, ιδιαίτερα από μια πηγή που υποστηρίζει ότι είναι το Google ή το Gmail, μη δώσετε τα στοιχεία που ζητούνται. Η Google δεν θα στείλει ποτέ ανεπιθύμητα μαζικά μηνύματα ζητώντας τον κωδικό πρόσβασής σας ή προσωπικά στοιχεία ή μηνύματα που περιέχουν εκτελέσιμα συνημμένα αρχεία.



Εθισμός στο διαδίκτυο

Ο εθισμός στο Διαδίκτυο (internet addiction) μια σχετικά νέα μορφή εξάρτησης, προτάθηκε ως όρος πρώτη φορά από τον Goldberg (1995) και έγινε δημοφιλής με την καινοτόμο έρευνα της Young (1996), αναφέρεται στην «καταναγκαστική, υπερβολική χρήση του διαδικτύου και τον εκνευρισμό ή δυσθυμική συμπεριφορά που παρουσιάζεται κατά τη στέρησή της» (Mitchell, 2000). Ο εθισμός στο Διαδίκτυο αν και δεν έχει επισήμως αναγνωρισθεί ως κλινική οντότητα παρά μόνο σε Κίνα, Ν.Κορέα και Ταιβάν, αποτελεί μια κατάσταση, που προκαλεί σημαντική έκπτωση στην κοινωνική και επαγγελματική ή ακαδημαϊκή λειτουργικότητα του ατόμου. Οι ειδικοί της ψυχικής υγείας όλο και συχνότερα καλούνται, να προσεγγίσουν θεραπευτικά άτομα με προβληματική χρήση του Διαδικτύου. Ήδη στην επόμενη έκδοση του διαγνωστικού εγχειριδίου της Αμερικανικής Ψυχιατρικής Εταιρείας, DSM-V, θα συμπεριληφθεί ως χρήζουσα περισσότερη έρευνα η οντότητα "Internet Use Gaming Disorder", ένας όρος που δεν έχει χρησιμοποιηθεί σε έρευνες ως σήμερα. Συνηθέστερη ορολογία πέρα από τον εθισμό στο Διαδίκτυο (Internet Addiction Disorder - IAD) είναι επίσης οι "Pathological Internet Use" (Παθολογική χρήση του διαδικτύου)», "Problematic Internet Use" (Προβληματική χρήση του διαδικτύου), "Excessive Internet Use" (Υπερβολική χρήση του διαδικτύου) και "Compulsive Internet Use" (Καταναγκαστική χρήση του διαδικτύου) (Widyanto & Griffiths, 2006).

Αίτια

Το Διαδίκτυο έχει την ικανότητα να καλύψει συγκεκριμένες ψυχολογικές ανάγκες ενός ατόμου. Ένα από τα χαρακτηριστικά του μέσου που προκύπτει από τη φύση του είναι ότι μπορεί να δημιουργήσει μια «ιδανική κατάσταση εαυτού», όπου το άτομο μπορεί να εξερευνήσει διάφορες πτυχές της προσωπικότητας του χωρίς να έχει περιορισμούς και συνέπειες. Στο Διαδίκτυο δεν υπάρχουν άμεσες συνέπειες των πράξεων, ο χρήστης μπορεί να μπει και να βγει όποτε θέλει, ενώ μπορεί να καλύψει την όποια εξωτερική εμφάνιση, αφού δεν υπάρχει οπτική επαφή. Ταυτόχρονα, ο έφηβος μπορεί να ενσαρκώσει διαφορετικούς ρόλους, ή να υιοθετήσει διαφορετικές ταυτότητες ανάλογα με την εκάστοτε διαδικτυακή εμπειρία, εξαιτίας της ανωνυμίας, που συνιστά κατεξοχήν χαρακτηριστικό του Διαδικτύου. Συνήθως, τα παιδιά που αντιμετωπίζουν το πρόβλημα του εθισμού στο διαδίκτυο είναι αγόρια και μεγαλώνουν σε δύσκολες καταστάσεις (δυσλειτουργικές οικογένειες). Πρόσφατες έρευνες στην Ελλάδα κατέδειξαν τη σημασία της γονικής μέριμνας και φροντίδας στην ανάπτυξη του εθισμού στο Διαδίκτυο (Siomos, 2012). Η βέλτιστη παροχή γονικής μέριμνας χαρακτηρίζεται από φροντίδα και υγιή προστατευτικότητα, ούτως ώστε το παιδί να κατευθύνεται και να καθοδηγείται με επάρκεια σε ένα ασφαλές περιβάλλον, χωρίς να παρεμποδίζονται οι προσπάθειες του για την ανάδειξη προσωπικής ταυτότητας και αυτονόμησης. Αντίθετα, υπερπροστατευτικότα των γονέων και χαμηλά επίπεδα φροντίδας συνιστούν το πρότυπο μέριμνας 'affectionless control' (έλεγχος χωρίς στοργή) το οποίο συνδέθηκε με υψηλότερες βαθμολογίες εθισμού στο Διαδίκτυο.

Όλοι στο σπίτι μας έχουμε έναν υπολογιστή. Όλοι μας, χρησιμοποιούμε τα μέσα κοινωνικής δικτύωσης (facebook, twitter, skype κ.α) για να επικοινωνήσουμε πλέον με τους «διαδικτυακούς» μας φίλους. Το διαδίκτυο έχει μπει για τα καλά στη ζωή μας, έχει γίνει καθημερινή συνήθεια και το κουβαλάμε σχεδόν πάντα μαζί μας, είτε με ένα i-pad ή με το smart-phone – ακόμη και στο σχολείο ή στο φροντιστήριο…
Νιώθεις ότι δεν είσαι εξαρτημένος από το διαδίκτυο , πόσο σίγουρος είσαι;
Διάβασε μερικά από τα συμπτώματα που μπορούν να εμφανιστούν από τη διαρκή ενασχόληση μας με το διαδίκτυο.

Συμπτώματα

1. Ασχολούμαστε πολύ ώρα με τον υπολογιστή μας
2. Αρχίζουμε να παραμελούμε τα μαθήματά μας και τις εξωσχολικές μας δραστηριότητες.
3. Προτιμάμε να μείνουμε στο σπίτι μας και να ασχοληθούμε με το διαδίκτυο από το να πάμε μια βόλτα με τους φίλους μας
4. Αδιαφορούμε για πράγματα που πριν μας έδιναν ευχαρίστηση, όπως για παράδειγμα, να πάμε σινεμά με την παρέα μας, να ασχοληθούμε με κάποιο άθλημα που μας αρέσει κλπ
5. Η συμπεριφορά μας αρχίζει και αλλάζει. Γινόμαστε νευρικοί και απότομοι, νευριάζουμε με όλους και με όλα και κυρίως τσακωνόμαστε με την οικογένεια μας και με τα άτομα που βρίσκονται στο άμεσο κονωνικό και φιλικό μας περιβάλλον
6. Οι πονοκέφαλοι είναι έντονοι, ενώ τα μάτια μας ξηραίνονται και κοκκινίζουν από την πολύωρη ενασχόληση μας με τον υπολογιστή
7. Ξεχνάμε να φάμε.
8. Παραμελούμε την προσωπική μας υγιεινή, πχ. Δεν μας νοιάζει αν θα κάνουμε μπάνιο κλπ
9. Παθαίνουμε μυοσκελετικές παθήσεις καθώς βρισκόμαστε διαρκώς σε μια καρέκλα

ακινητοποιημένοι και οι πόνοι στη μέση και στη πλάτη μας κάνουν την εμφάνιση τους 10. Υπάρχουν διαταραχές στον ύπνο μας, ο οποίος πλέον είναι ελάχιστος ή όποτε υπάρξει είναι ανήσυχος.

Πότε το διαδίκτυο γίνεται επικίνδυνο;

Όταν, η επικοινωνία με τους φίλους μας γίνεται μόνο μέσω διαδικτύου και όχι μέσω μια βόλτας πραγματικής και όχι διαδικτυακής, όταν η μόνη μας σκέψη είναι μετά το σχολείο να τρέξουμε στο σπίτι, για να τσεκάρουμε τα email μας ή να συνεχίσουμε το παιχνίδι που παίζαμε χθες το βράδυ και όταν ανακαλύπτουμε πως δεν έχουμε πρόσβαση στο διαδίκτυο τότε μας πιάνει πανικός, μήπως πρέπει να αρχίσουμε να σκεφτόμαστε ότι έχουμε αρχίσει και εθιζόμαστε σε αυτό…

Πότε το διαδίκτυο είναι ακίνδυνο;

Όταν χρησιμοποιείται ως συμπληρωματικό μέσο ενημέρωσης, εκπαίδευσης, έρευνας, διασκέδασης και ψυχαγωγίας καθώς με «κλικ» βρισκόμαστε σε μέρη που δεν γνωρίζουμε και μπορεί να μην επισκεφθούμε ποτέ!

Το διαδίκτυο δεν είναι κάτι «κακό», το οποίο δεν πρέπει να βρίσκεται στη ζωή μας, αλλά θα πρέπει να μάθουμε να το χρησιμοποιούμε σωστά και προς όφελος μας και να μην κοινοποιούμε ευαίσθητα προσωπικά μας δεδομένα.

Ποιες ηλικιακές ομάδες εμφανίζουν συχνότερα εξάρτηση

Το φαινόμενο συνήθως εμφανίζεται αρχικά σε εφήβους κατά την πρώιμη εφηβεία (10-14 ετών) ή και σε μικρότερη ακόμη ηλικία. Είναι πιο έντονο κατά την μέση εφηβεία (15-17 ετών), κατά την οποία οι έφηβοι πειραματίζονται και σταδιακά αυτονομούνται, καθώς και κατά την όψιμη εφηβεία (> 17 ετών). Οι περισσότεροι εξαρτημένοι έφηβοι ασχολούνται με ηλεκτρονικά διαδικτυακά παιχνίδια στο σπίτι ή τα internet cafe. Ένας ακόμα πληθυσμός υψηλού κινδύνου είναι αυτός των φοιτητών, οι οποίοι καλούνται πολλές φορές για πρώτη φορά να οριοθετήσουν οι ίδιοι τη χρήση Διαδικτύου στην οποία προβαίνουν, μακριά από οικογενειακό έλεγχο αλλά και χωρίς το ξεκάθαρα δομημένο πλαίσιο υποχρεώσεων του σχολείου μέσης εκπαίδευσης. Σποραδικά εμφανίζεται το πρόβλημα και σε μεγαλύτερες ηλικίες όπου κυρίως αφορά περιπτώσεις υπέρμετρης ενασχόλησης με κοινωνική δικτύωση αλλά και διαδικτυακό τζόγο, όπως και διαδικτυακή πορνογραφία.

Αντιμετώπιση

Για την αντιμετώπιση του φαινομένου έχει προταθεί η κινητοποιητική συνέντευξη, το γνωστικό- συμπεριφορικό μοντέλο θεραπείας, η συμβουλευτική παρέμβαση στην οικογένεια, οι ομάδες απεξάρτησης, ενώ υπάρχουν κάποια δεδομένα και για το ρόλο της φαρμακοθεραπείας στη θεραπεία. Ιδιαίτερα σημαντική για την αντιμετώπιση του εθισμού στα παιδιά και στους εφήβους είναι η ύπαρξη κοινής στάσης των γονέων, η παροχή υποστήριξης αλλά όχι κάλυψης και η τοποθέτηση του υπολογιστή σε ένα ορατό σημείο στο σπίτι και όχι στο δωμάτιο του παιδιού. Σημαντικό ρόλο στην αντιμετώπιση του εθισμού στο Διαδίκτυο έχει και η συμβουλευτική στην οικογένεια, έτσι ώστε να δημιουργηθεί ένα υποστηρικτικό πλαίσιο, που θα δράσει ευοδωτικά στη θεραπεία. Η κινητοποιητική συνέντευξη μπορεί να είναι ιδιαίτερα αποτελεσματική στον χειρισμό της άρνησης του προβλήματος, ένα συχνό εμπόδιο που παρατηρείται σε όλες τις ηλικίες. Στα πλαίσια της γνωστικό- συμπεριφορικής θεραπείας, εντοπίζονται οι γνωστικές διαστρεβλώσεις που εκλύουν και διατηρούν την προβληματική χρήση του Διαδικτύου, προωθείται η γνωσιακή αναδόμηση και ένας πιο ισορροπημένος και προσαρμοστικός τρόπος σκέψης. Παράλληλα χρησιμοποιούνται μια σειρά από συμπεριφορικές στρατηγικές, όπως η ανα-

γνώριση του πρότυπου χρήσης του Διαδικτύου και η εφαρμογή ενός διαμετρικά αντίθετου προγράμματος χρήσης, η οριοθέτηση των περιόδων χρήσης με διάφορα εξωτερικά μέσα, παρακίνηση για ενασχόληση με ευχάριστες εναλλακτικές δραστηριότητες, η χρήση καρτών υπενθύμισης, η πλήρης αποχή από ιδιαίτερα προβληματικές διαδικτυακές εφαρμογές, η ενσωμάτωση καθορισμένων διαστημάτων χρήσης στο εβδομαδιαίο πρόγραμμα του χρήστη. Οι ομάδες απεξάρτησης χρησιμοποιούν τις πρακτικές των ομάδων απεξάρτησης από άλλους εθισμούς, όπως το πρόγραμμα των 12 βημάτων ή βασίζονται στις αρχές της ομαδικής ψυχοθεραπείας. Σε ό,τι αφορά τη φαρμακοθεραπεία, η χρήση της εσιταλοπράμης φάνηκε αποτελεσματική σε μικρή ανοικτή μελέτη, έχει προταθεί η ναλτρεξόνη λόγω του μηχανισμού δράσης της στα κέντρα ανταμοιβής του εγκεφάλου, ενώ η μεθυλφενιδάτη αποδείχθηκε αποτελεσματική σε μια ανοικτή μελέτη σε παιδιά με Διαταραχή Ελλειμματικής Προσοχής-Υπερκινητικότητα (ΔΕΠΥ) και εθισμό σε διαδικτυακά παιχνίδια. Σε κάθε περίπτωση, ο εθισμός στο Διαδίκτυο, ως ψυχική διαταραχή, χρήζει αντιμετώπισης από επαγγελματίες ψυχικής υγείας εξειδικευμένους στο συγκεκριμένο αντικείμενο.

Παιδοφιλία – Πορνογραφία - Βία στο διαδίκτυο

Υπάρχουν άνθρωποι που μπροστά στο κέρδος δεν υπολογίζουν τίποτα. Υπάρχουν άνθρωποι διεστραμμένοι και ψυχικά διαταραγμένοι που για να ικανοποιήσουν τη δική τους διαστροφή, είναι ικανοί να πληγώσουν ανεπανόρθωτα ό,τι πολυτιμότερο υπάρχει σ' αυτόν τον κόσμο, τις ψυχές απλών, καθημερινών ανθρώπων.

Η παιδική πορνογραφία αποτελεί την πιο κερδοφόρα βιομηχανία του Διαδικτύου. Είναι γεγονός ότι ιστοσελίδες με αρκετές χιλιάδες συνδρομητές και εκατοντάδες χιλιάδες επισκέπτες χρεώνουν τις εικόνες ανηλίκων σε σεξουαλικές πράξεις ακόμα και με 100 ευρώ το λεπτό(!) Το έτος 2005, για πρώτη φορά στην Ελλάδα αστυνομικοί εξάρθρωσαν κύκλωμα παιδόφιλων, που όχι μόνο διακινούσε, αλλά αναπαρήγαγε το φωτογραφικό υλικό στην Ελλάδα. Αποτελούνταν από σχεδόν 30 άτομα, τα περισσότερα υπεράνω υποψίας, όπως καθηγητές, δικηγόροι και γνωστοί επιχειρηματίες.

Το σοκαριστικό παράδειγμα της Amanda Todd

Η Amanda Todd, γεννημένη το Νοέμβριο του 1996, ήταν ένα από τα –δυστυχώς- αναρίθμητα θύματα της παιδοφιλίας και πορνογραφίας μέσω του διαδικτύου. Συγκεκριμένα, στις 7 Σεπτεμβρίου του 2012 ανέβασε σε γνωστό διαδικτυακό τόπο βίντεο με τις εμπειρίες της τα τελευταία χρόνια σε καρτέλες γραμμένες απ' την ίδια. Μόλις ένα μήνα αργότερα βρέθηκε κρεμασμένη στο σπίτι της, ενώ χαρακτηριστικά ανέφερε επανειλλημένα στο βίντεο ότι θέλει να δώσει τέλος στην εφιαλτική της ζωή. Ήταν κι αυτή ένα θύμα εκβιασμού, βίας, ένα κορίτσι που το λάθος της την ακολούθησε μέχρι και την τελευταία της πνοή.

Ακόμα και σήμερα, πολλοί χρήστες του διαδικτύου που έμαθαν για το θάνατο της 16 χρονης μαθήτριας εξακολουθούν να την κατηγορούν για τις πράξεις της, ενώ λίγοι ήταν αυτοί που στάθηκαν δίπλα της...

Το πιο θλιβερό είναι πως η Amanda ήταν μόνο ένα παράδειγμα. Σε 850 ανέρχονται οι συλληφθέντες για παιδική πορνογραφία από το 2004 έως το 2012, ενώ 350 αστυνομικές έρευνες έχουν πραγματοποιηθεί για τον εντοπισμό και τη σύλληψη παιδόφιλων στο Διαδίκτυο... Όσον αφορά τη βία σε κάθε της κλίμακα, τα νούμερα δεν μπορούν να περιγράψουν την κατάσταση.

Σύμφωνα με τα στατιστικά στοιχεία του Τμήματος Δίωξης Ηλεκτρονικού Εγκλήματος, οι ηλικίες που έχουν απασχολήσει τις διωκτικές αρχές για θέματα παιδικής πορνογραφίας και παιδοφιλίας μέσω Διαδικτύου είναι άνδρες από 15 έως 72 ετών, ενώ η ηλικία των θυμάτων ξεκινά από μωρά δύο μηνών!

Το διαδίκτυο βοηθά αυτούς τους ανθρώπους να προσεγγίσουν ανηλίκους, εντελώς ανώνυμα και άμεσα, να μιλούν μαζί τους μέσω μιας «πλαστής» ταυτότητας και να τα κατευθύνουν στις ανήθικες πράξεις τους. Πολλοί από αυτούς είναι έμπειροι χρήστες του διαδικτύου, όχι μόνο του γνωστού σε εμάς "world wide web" αλλά και του βαθέος διαδικτύου, ενός κόσμου άγνωστου στον απλό χρήστη και πολύ δύσκολα προσβάσιμου. Εκεί διακινείται ένα μεγάλο μέρος της διαδικτυακής πορνογραφίας, μαζί με άλλες παράνομες εμπορίες.

Παρόλ' αυτά γίνονται μεγάλες προσπάθειες για τον περιορισμό και τη σύλληψη των επιτήδειων. Ας γίνουμε κι εμείς βοηθοί στον αγώνα ξεκινώντας πρώτα από τον εαυτό μας και τη συμπεριφορά μας....

Παραπληροφόρηση και προπαγάνδα

Παραπληροφόρηση είναι η μεταφορά διαφόρων ψευδών ή αναληθών ή τροποποιημένων πληροφοριών. Πιθανός σκοπός είναι η παραπλάνηση του δέκτη προς εκπλήρωση προσωπικών σκοπιμοτήτων του παραπληροφορούντος, οπότε η παραπληροφόρηση είναι κακή πράξη. Άλλος πιθανός σκοπός είναι η προστασία ατόμων με την απόκρυψη πληροφοριών που θα ήταν επιβαρυντικές γι' αυτά, οπότε η παραπληροφόρηση είναι καλή πράξη ή επιβάλλεται από τον νόμο.

Αυτός που παραπληροφορεί, αν είναι η πηγή της πληροφορίας, έχει όλη την ευθύνη. Αν δεν είναι η πρωτογενής πηγή της πληροφορίας, αλλά απλώς μεταφέρει όσα γνωρίζει, έχει περιορισμένη ευθύνη στο ότι δεν έχει διασταυρώσει τις πηγές του.
Κατά την παραπληροφόρηση γίνεται προβολή των επιλεγμένων πτυχών ενός γεγονότος, κατασκευάζονται ψευδείς αλήθειες, γίνεται παραποίηση της αλήθειας και διαβάλλονται τα εμπλεκόμενα πρόσωπα.

Σχετικά με τις ειδήσεις που μεταφέρονται από κάποιο Μέσο Μαζικής Ενημέρωσης (ΜΜΕ), μπορεί να ισχύει περίπτωση παραπληροφόρησης. Αν το μέσο είναι η πηγή της πληροφορίας, η παραπληροφόρηση θα οφείλεται :

1. Στο ότι το ΜΜΕ λειτουργεί με βάση κομματικά ή άλλα οργανωμένα συμφέροντα, άρα είναι γενικά αναξιόπιστο.
2. Στο ότι το ΜΜΕ προστατεύει εθνικά ή άλλα συμφέροντα με την απόκρυψη των στοιχείων, άρα αυτολογοκρίνεται.
Οι αναγνώστες (ακροατές, θεατές) οφείλουν να διασταυρώνουν τις πηγές των πληροφοριών τους για να αποφεύγουν την παραπληροφόρηση.
Η παραπληροφόρηση σαν ευρύτερη έννοια θα μπορούσε να εννοηθεί και η σκόπιμη διάδοση ιδεών και απόψεων για ένα θέμα για το οποίο υπάρχει συγκεκριμένη επιστημονική ή φιλοσοφική αντίληψη. Για παράδειγμα, η αστρολογία είναι η παραπληροφόρηση της αστρονομίας αφού καμία πραγματική έννοια σχετική με το σύμπαν δεν αποδεικνύεται χρησιμοποιώντας τις αστρολογικές μεθόδους.

Προπαγάνδα είναι η παρουσίαση ενός μηνύματος με έναν συγκεκριμένο τρόπο ώστε να εξυπηρετήσει συγκεκριμένους σκοπούς. Ετυμολογικά, προπαγάνδα σημαίνει «διάδοση μίας φιλοσοφίας ή άποψης». Ιστορικά, ο όρος χρησιμοποιείται ως επί το πλείστον εντός πολιτικού συγκειμένου και ιδιαίτερα αναφορικά με συγκεκριμένες κινήσεις που προωθούνται από κυβερνήσεις ή πολιτικές ομάδες. Το προπαγανδιστικό μήνυμα διαφέρει από την γενικότερη διαφήμιση στο ότι περιέχει τρανταχτές και επιτηδευμένες ψευδολογίες ή/και παραλείπει τέτοιον όγκο αληθειών/γεγονότων σχετικών με το θέμα που καθίσταται έντονα παροδηγητικό.

<u>Σκοπός της προπαγάνδας</u>

Σκοπός της προπαγάνδας είναι να αλλάξει δραστικά τις απόψεις των άλλων αντί απλώς να μεταδώσει γεγονότα. Για παράδειγμα, η προπαγάνδα μπορεί να επιστρατευτεί προκειμένου να προϊδεάσει θετικά ή αρνητικά σε σχέση με κάποια ιδεολογική θέση, αντί να παρουσιάσει την ίδια την θέση. Η προπαγάνδα διαφοροποιείται από την «κανονική» επικοινωνία, επειδή επιδιώκει να διαμορφώσει απόψεις με έμμεσες και συχνά δόλιες μεθόδους. Για παράδειγμα, η προπαγάνδα συχνά μεταδίδεται με τέτοιον τρόπο ώστε να προκαλεί ισχυρά συναισθήματα και αυτό το κάνει κυρίως με το να υπονοεί παράλογες (μη ενορατικές) σχέσεις μεταξύ ιδεών.
Η επίκληση στο συναίσθημα είναι ίσως η πιο απροκάλυπτη μέθοδος προπαγάνδας, αφού υπάρχουν πολλές άλλες μέθοδοι, λιγότερο φανερές και μάλιστα δόλιες. Για παράδειγμα, η προπαγάνδα μπορεί να διαδίδεται έμμεσα. Μπορεί να μεταδίδεται ως εύλογη προκατάληψη εντός μιάς φαινομενικά ισορροπημένης και δίκαιης δημόσιας συζήτησης ή επιχειρηματολογίας. Αυτό μπορεί να επιτευχθεί ακόμη καλύτερα σε συνδυασμό με την μέθοδο μετάδοσης ειδήσεων των μέσων μαζικής επικοινωνίας.
Ιδού ένα υποθετικό παράδειγμα όπου υποτίθεται ότι αντιπαρατίθενται αντίθετες απόψεις: το γεράκι λέει: «Πρέπει να παραμείνουμε στην πορεία μας»· και το περιστέρι απαντά: «Ο πόλεμος απέβη καταστροφικός και απέτυχε». Τότε το γεράκι αποκρίνεται: «Στον πόλεμο τα πράγματα σπάνια πηγαίνουν ομαλά, και δεν πρέπει να επιτρέπουμε σε ένα κώλυμα να μειώνει την αποφασιστικότητά μας». Τότε το περιστέρι ανταπαντά: «Τα κωλύματα είναι κωλύματα και οι αποτυχίες είναι αποτυχίες». Όπως φαίνεται από το παράδειγμα, πουθενά δεν εξετάζεται το αν ο πόλεμος είναι τελικά νόμιμος και θεμιτός. Λακωνικά, συνοπτικά και απλουστευτικά σχόλια ονομάζονται *sound bites*. Όταν σε έναν δημόσιο διάλογο (που να αφορά ένα ζήτημα υπό επιχειρηματολογία που πράγματι να χρήζει διαλόγου) οι συνδιαλεγόμενοι εκφέρουν επιχειρήματά που πηγάζουν από τις ίδιες βασικές προϋποθέσεις, αλλά δίνουν την εντύπωση ότι πρεσβεύουν αντίθετες απόψεις, τότε ο διάλογος εμμέσως κατηχεί αυτές τις προκαταλήψεις ως απρόσβλητες αλήθειες, καθιστώντας τις κοινώς αποδεκτά δεδομένα για το εν λόγω ζήτημα.
Η μέθοδος της προπαγάνδας είναι επίσης βασική όσον αφορά και το τι θα σημαίνει «προπαγάνδα» σε κάθε περίπτωση. Ένα μήνυμα δεν πρέπει να είναι απαραιτήτως ψευδές για να αποτελεί προπαγάνδα. Στην πραγματικότητα, τα μηνύματα της σύγχρονης

προπαγάνδας δεν είναι κραυγαλέα ψευδή. Ωστόσο, ακόμη και αν το μήνυμα μεταδίδει μόνον «αληθείς» πληροφορίες, αυτές συνήθως περιέχουν φατριακούς προϊδεασμούς και δεν εκθέτουν το μήνυμα με πλήρη και ισορροπημένο τρόπο. Ένα επιπρόσθετο χαρακτηριστικό της προπαγάνδας είναι ό μεγάλος όγκος της. Δηλαδή, ένας προπαγανδιστής μπορεί να προσπαθήσει να επηρεάσει τις γνώμες με το να κάνει το μήνυμά του να ακουστέι σε όσο περισσότερα μέρη γίνεται και όσο πιο συχνά γίνεται. Σκοπός αυτής της προσέγγισης είναι (α) να ενισχύσει τις ιδέες του μέσω επανάληψης και (β) να καταπνίξει όλες τις εναλλακτικές ιδέες.
Στα ελληνικά, η λέξη «προπαγάνδα» φέρει έντονα αρνητική (καθώς και πολιτική) χροιά, μολονότι αυτό δεν ίσχυε πάντοτε.

Είδη προπαγάνδας

Πινακίδες με προπαγανδιστικά μυνήματα κατά της ομοφυλοφιλίας.

Το modus operandi της προπαγάνδας είναι παρόμοιο με αυτό της διαφήμισης. Για την ακρίβεια, η διαφήμιση μπορεί και να οριστεί ως προπαγάνδα υπέρ κάποιου συγκεκριμένου προϊόντος. Η λεξη προπαγάνδα αφορά κυρίως πολιτικούς ή εθνικιστικούς σκοπούς και την προώθηση αντιστοίχων ιδεών. Η προπαγάνδα σχετίζεται επίσης με εκστρατείες πληροφόρησης από μέρους των κυβερνήσεων, οι οποίες στοχεύουν στην προώθηση ή στην αποθάρρυνση συγκεκριμένων πρακτικών (βλέπε χρήση ζωνών ασφαλείας, κάπνισμα, κλπ). Ακόμη και σε αυτές τις περιπτώσεις, ο χαρακτήρας της προπαγάνδας παραμένει πολιτικός. Η προπαγάνδα μπορεί να λαμβάνει χώρα με φυλλάδια, αφίσες, μέσω τηλεοπτικών και ραδιοφωνικών εκπομπών ή και άλλων μέσων.

ΠΑΡΕΝΟΧΛΗΣΗ - ΕΚΦΟΒΙΣΜΟΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

ΟΡΙΣΜΟΣ ΤΟΥ BULLYING:

Παρενόχληση (bullying) είναι η επιθετική συμπεριφορά από πρόθεση, που επαναλαμβάνεται με τον καιρό και περιλαμβάνει μια ανισορροπία δύναμης και εξουσίας. Τα παιδιά που γίνονται αντικείμενο παρενόχλησης αντιμετωπίζουν δυσκολίες στο να υπερασπιστούν τον εαυτό τους. Με απλά λόγια, παρενόχληση είναι όταν κάποιος κάνει ή να λέει πράγματα για να έχει δύναμη πάνω σε κάποιον άλλον. Μερικοί τρόποι να φοβερίσει κανείς τους άλλους είναι να τους βρίζει, να λέει ή να γράφει δυσάρεστα πράγματα γι αυτούς, να τους απομονώνει, να μην τους μιλάει, να τους απειλεί, να τους φοβερίζει, να παίρνει ή να καταστρέφει τα πράγματά τους, να τους χτυπά ή να τους ωθεί να κάνουν πράγματα παρά τη θέλησή τους. Τα περιστατικά παρενόχλησης μεταξύ παιδιών και εφήβων δεν εκδηλώνονται μόνο μέσω καβγάδων και επιθετικότητας, αλλά και μέσω διαφορετικών τύπων εκφοβισμού που αφήνουν το θύμα εκτεθειμένο (λεκτικοί και ψυχολογικοί εκφοβισμοί, σωματική επιθετικότητα, κοινωνική απομόνωση).

CYBER-BULLYING Ή ΚΥΒΕΡΝΟΕΚΦΟΒΙΣΜΟΣ

Μέσα σε λιγότερο από 20 χρόνια το διαδίκτυο από ένα μέσο μεταφοράς πληροφοριών μεταξύ επιστημόνων και μυστικών υπηρεσιών μεταμορφώθηκε σε ένα από τα πιο πολυχρησιμοποιημένα μέσα επικοινωνίας. Κατάφερε να αλλάξει τα δεδομένα στον τρόπο οργάνωσης της εργασίας μας, την επικοινωνία με γνωστούς και φίλους, την διασκέδαση και, φυσικά, την ενημέρωση. Όπως συμβαίνει και με κάθε άλλη αλλαγή στο ανθρώπινο περιβάλλον και ιδιαίτερα στον τρόπο επικοινωνίας , έτσι και εδώ η συμπεριφορά μας δεν έμεινε ανεπηρέαστη. Όπως ήταν φυσικό το διαδίκτυο έγινε μια νέα δίοδος διοχέτευσης των συναισθημάτων και των σκέψεών μας. Μία από τις πιο χαρακτηριστικές περιπτώσεις μεταφοράς μοτίβων ανθρώπινης συμπεριφοράς στο διαδίκτυο είναι και η βία. Στην

αγγλική βιβλιογραφία μάλιστα το φαινόμενο της διαδικτυακής βίας έχει και όνομα: cyber- bullying. Ένας γενικός όρος που θα μπορούσε να δοθεί στο φαινόμενο αυτό, ώστε να διαχωριστεί από τις περιπτώσεις ψυχολογικής, λεκτικής και σωματικής βίας εκτός διαδικτύου (bullying) είναι πως πρόκειται για μια επιθετική και συνειδητή ομαδική ή ατομική πράξη μέσω της χρήσης του διαδικτύου και άλλων ηλεκτρονικών μέσων, η οποία στρέφεται εναντίον ενός ατόμου το οποίο είναι δύσκολο να υπερασπιστεί τον εαυτό του. Μάλιστα θα μπορούσε κάποιος να ισχυριστεί πως η βία αυτή εμπεριέχεται στην ψυχική βία, η οποία καθίσταται πολλές φορές και σπουδαιότερη της σωματικής.

ΤΙ ΠΕΡΙΛΑΜΒΑΝΕΙ Ο ΕΚΦΟΒΙΣΜΟΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΠΟΙΑ ΕΙΝΑΙ ΤΑ ΜΕΣΑ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΓΙ' ΑΥΤΟΝ ΤΟ ΣΚΟΠΟ;

1. Πειράγματα με στόχο τη διασκέδαση.
2. Διάδοση άσχημων- προσβλητικών φημών on-line.
3. Αποστολή ανεπιθύμητων μηνυμάτων (υβριστικά, προσβλητικά, χλευαστικά, ακόμη και απειλητικά).
4. Δυσφήμηση σε τρίτους μέσω του ηλεκτρονικού ταχυδρομείου, ιστοσελίδων, blogs, chat- rooms κ.ά.
5. Παρενόχληση μέσω IM .
6. Δημοσίευση προσωπικών στοιχείων και φωτογραφιών χωρίς την συγκατάθεσή μας.

Ο εκφοβισμός μέσω του Διαδικτύου μπορεί να είναι άμεσος ή έμμεσος εμπλέκοντας και άλλα άτομα που ενδεχομένως να μη γνωρίζει καν το θύμα. Τα μέσα που χρησιμοποιούνται για τον εκφοβισμό μέσω του Διαδικτύου είναι το ηλεκτρονικό ταχυδρομείο (e-mail), τα γραπτά μηνύματα (text messaging), οι ιστότοποι κοινωνικής δικτύωσης (social networking sites), τα μέρη συζητήσεως στο Διαδίκτυο (chat-rooms), τα blogs, τα web-sites , ακόμα και τα διαδικτυακά παιχνίδια (Internet gaming).

ΠΟΙΟΥΣ ΑΦΟΡΑ; ΠΟΙΟΣ ΕΙΝΑΙ Ο ΘΥΤΗΣ ΚΑΙ ΠΟΙΟ ΤΟ ΘΥΜΑ;

Αν και οι περισσότερες περιπτώσεις βίαιης παρενόχλησης εκτός διαδικτύου αφορούν κυρίως παιδιά σχολικής και εφηβικής ηλικίας ,η διαδικτυακή παρενόχληση είναι ένα φαινόμενο που αγγίζει τόσο τους νεαρούς, όσο και τους ενήλικες, καθώς θύτες και θύματα μπορούν να βρεθούν και στις δύο ηλικιακές ομάδες (αν και η αλήθεια είναι πως το φαινόμενο αυτό παρουσιάζεται πιο έντονο στις νεαρότερες ηλικίες). Τα θύματα του εκφοβισμού είναι συνήθως ήσυχοι και ευαίσθητοι νέοι, αγχώδεις και ανασφαλείς. σπάνια αμύνονται ακόμη και όταν δέχονται προσβολές. Το κυριότερο χαρακτηριστικό των θυμάτων είναι ότι υστερούν σε δύναμη και εξουσία από τον θύτη. Είναι ντροπαλά και ήσυχα άτομα, έχουν λίγους φίλους εκτός σχολείου και ενδεχομένως κανένα στενό φίλο στο σχολείο, με αποτέλεσμα να είναι απομονωμένοι. Υπεισέρχονται και άλλοι παράγοντες που τους χαρακτηρίζουν όπως είναι η σωματική αναπηρία και ο ρατσισμός. Οι θύτες χρησιμοποιούν τις νέες τεχνολογίες για να απειλήσουν, να παρενοχλήσουν, να δυσφημίσουν, να υποδυθούν αυτούς που εκφοβίζουν, να υποκλέψουν την ταυτότητά τους, να χλευάσουν, να συκοφαντήσουν. Τέλος, οι εκφοβιστές έχουν ανάγκη να νοιώθουν δυνατοί και αντλούν ευχαρίστηση με το να κακομεταχειρίζονται τους άλλους. Παράλληλα είναι ανυπάκουοι, προκλητικοί και φέρονται να έχουν υπερβολική αυτοεκτίμηση. Τους διακρίνει επίσης το ότι έχουν μάθει, να αντεπιτίθενται με βιαιότητα για να διαχειριστούν όποια προβλήματα έχουν.

ΠΟΙΑ ΕΙΝΑΙ ΤΑ ΣΥΜΠΤΩΜΑΤΑ ΘΥΤΗ ΚΑΙ ΘΥΜΑΤΟΣ;

Από τη μια οι θύτες έχουν προβλήματα με την οργάνωση και διευθέτηση εργασιών, και παρουσιάζουν συμπτώματα γενικότερης αντικοινωνικής συμπεριφοράς και από την άλλη τα θύματα αναπτύσσουν συναισθηματικά προβλήματα, ανασφάλεια και έντονα σωματικά συμπτώματα (πονοκέφαλος, πόνος στο στομάχι, προβλήματα ύπνου). Επιπλέον, τα τελευταία νιώθουν μοναχικά, δυστυχή, φοβισμένα και αισθάνονται ανασφαλή. Χάνουν την εμπιστοσύνη στον εαυτό τους και μπορεί να μην θέλουν να ξαναπάνε στο σχολείο, στη δουλειά ή να θέλουν να απομονωθούν από τις παρέες τους.

ΠΟΙΑ ΠΡΕΠΕΙ ΝΑ ΕΙΝΑΙ Η ΣΤΑΣΗ ΤΩΝ ΓΟΝΕΩΝ ΑΠΕΝΑΝΤΙ ΣΤΟ ΘΕΜΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ;

Είναι σημαντικό οι γονείς να ακούσουν προσεχτικά τι λέει το παιδί για τις online εμπειρίες του και να εξοικειωθούν και οι ίδιοι με το Διαδίκτυο, καθώς αποτελεί αναπόσπαστο πλέον κομμάτι της ζωής μας, αλλά και να επισκεφτούν τα site που το παιδί τους επισκέπτεται. Η εμπιστοσύνη του παιδιού στην κατανόηση που θα λάβει από την οικογένειά του , χωρίς πανικούς και συναισθηματικές εξάρσεις, είναι η εγγύηση ότι θα τη πλησιάσει για οτιδήποτε το απασχολεί και το επιβαρύνει συναισθηματικά. Ωστόσο, ιδιαίτερα σημαντική είναι και η προληπτική δράση των γονέων. Πιο συγκεκριμένα, προτού τα παιδιά αρχίσουν να εξερευνούν το Διαδίκτυο, καλό θα είναι να βεβαιωθεί κανείς πως καταλαβαίνουν τι πρέπει και τι δεν πρέπει να κάνουν και είναι σημαντικό αυτό να γίνει όταν τα παιδιά είναι ακόμα σε μικρή ηλικία. Ένας τρόπος είναι, να καθίσουν οι γονείς με τα παιδιά και να προδιαγράψουν από κοινού έναν οικογενειακό κώδικα συμπεριφοράς στον οποίο θα πρέπει να συμφωνήσουν όλοι. Μπορεί να δημιουργηθεί ένα είδος συμβολαίου διαφορετικό για κάθε παιδί στην οικογένεια, με κανόνες χρήσης του Διαδικτύου κατάλληλους για την ηλικία του. Οι γονείς ,επίσης είναι σημαντικό να μιλήσουν στα παιδιά τους για τους ηθικούς κανόνες που πρέπει να διέπουν την διαδικτυακή τους επικοινωνία, οι οποίοι είναι αντίστοιχοι με αυτούς της πραγματικής επικοινωνίας όπως ο σεβασμός του άλλου, η ευγένεια, η κατανόηση και η αποδοχή. Τέλος, είναι σημαντικό να βοηθήσουν τα παιδιά τους να καταλάβουν πως μία ιστοσελίδα που μπορεί να δημιουργήσουν, είναι εμφανής και επισκέψιμη όχι μόνο σε φίλους και γνωστούς, αλλά και σε αγνώστους, επομένως θα πρέπει τα παιδιά να είναι πολύ προσεχτικά στο τι γράφουν και τι στοιχεία παρουσιάζουν για τον εαυτό τους ή και για άλλους.

ΤΙ ΠΡΕΠΕΙ ΝΑ ΚΑΝΟΥΝ ΟΙ ΓΟΝΕΙΣ ΕΑΝ ΠΑΡΕΝΟΧΛΕΙΤΑΙ ΤΟ ΠΑΙΔΙ ΤΟΥΣ;

Εάν συμβεί παρενόχληση, μπορούν να αποκλείσουν το πρόσωπο που στέλνει τα μηνύματα με τις επιλογές αποκλεισμού που διαθέτουν πολλά προγράμματα ηλεκτρονικού ταχυδρομείου και άμεσων μηνυμάτων. Έπειτα αποθηκεύουν τα μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν παρενοχλήσεις και τα προωθούν στον παροχέα υπηρεσιών ηλεκτρονικού ταχυδρομείου. Οι περισσότεροι παροχείς διαθέτουν κατάλληλες πολιτικές χρήσης που απαγορεύουν την παρενόχληση. Τα παιδιά παρενοχλούνται, επίσης, όταν παίζουν διαδικτυακά παιχνίδια. Εάν η παρενόχληση οφείλεται σε σχόλια που εμφανίζονται σε κάποια διαδικτυακή τοποθεσία, μπορούν να επικοινωνήσουν με τον παροχέα υπηρεσιών Διαδικτύου (ISP) και να ζητήσουν βοήθεια για να εντοπίσουν τον ISP που φιλοξενεί τη διαδικτυακή τοποθεσία. Στη συνέχεια, πρέπει να επικοινωνήσουν με τον παροχέα και να τον ενημερώσουν για τα σχόλια. Επίσης, οφείλουν να ειδοποιήσουν την αστυνομία. Η ειδική γραμμή τηλεφωνικών καταγγελιών της Δίωξης Ηλεκτρονικού Εγκλήματος είναι το 11012 και λειτουργεί όλο το 24ωρο. Η παρενόχληση είναι έγκλημα, τόσο στον πραγματικό κόσμο όσο και στον κόσμο του Διαδικτύου. Είναι παράνομο να

επικοινωνείτε επανειλημμένα με κάποιον, εάν η επικοινωνία αυτή του προκαλεί φόβο για την ασφάλειά του ή για την ασφάλεια άλλων.

ΕΚΠΑΙΔΕΥΤΙΚΟΙ ΚΑΙ ΠΡΟΛΗΨΗ ΤΟΥ ΕΚΦΟΒΙΣΜΟΥ ΜΕΣΩ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ:

Ο εκπαιδευτικός από την πλευρά του μπορεί να βοηθήσει στην πρόληψη φαινομένων εκφοβισμού, που σύμφωνα με τις έρευνες εμφανίζεται με μεγάλη συχνότητα στο χώρο του σχολείου. Ειδικότερα, οφείλουν : 1) Να αντιμετωπίζουν με ιδιαίτερη κατανόηση την παιδική επιθετικότητα, 2) Να γνωρίζουν ότι μερικές φορές η βία είναι κραυγή και έκκληση που κρύβει πολύ πόνο και απογοήτευση. Ο εκπαιδευτικός έχει καθήκον, να μην απαντά στη βία με βίαιη αντίδραση, γιατί γνωρίζει ότι η βία γεννά βία. Η πιο σημαντική συνέπεια μιας κατασταλτικής δράσης του εκπαιδευτικού είναι η δημιουργία φόβου στα παιδιά, εξαιτίας του οποίου δυσκολεύονται να εκφράσουν τι αισθάνονται, έτσι οδηγούνται σε δύο επιλογές: ή να γίνουν επιθετικά, ή να κλειστούν στον εαυτό τους. Είναι σημαντικό ο εκπαιδευτικός να αναγνωρίσει την έκταση του προβλήματος στο σχολείο του και να συλλέξει ανώνυμα στοιχεία από τους μαθητές του. Να μεταδώσει στους μαθητές ότι όλες οι μορφές εκφοβισμού είναι απαράδεκτες και υπόκεινται σε πειθαρχικά μέσα, να ξεκαθαρίσει τους κανόνες χρήσης του Η/Υ και του Διαδικτύου και να τοποθετήσει πόστερ σε στρατηγικά σημεία. Επίσης, ο εκπαιδευτικός μπορεί να δώσει την ευκαιρία σε μεγαλύτερους μαθητές να διδάξουν και να συμβουλεύσουν τους νεώτερους (peer education). Τέλος, μπορούν να έχουν μία σταθερή συνεργασία με ειδικούς επαγγελματίες για σωστή ενημέρωση και καθοδήγηση.

ΕΙΣΑΙ ΘΥΜΑ ΠΑΡΕΝΟΧΛΗΣΗΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ;

Σε περίπτωση που έχεις πέσει θύμα εκφοβισμού μέσω του διαδικτύου, τότε πρέπει άμεσα να απευθυνθείς στους γονείς σου και μαζί να προβείτε σε μία σειρά ενεργειών:

1) Εάν έχεις δεχτεί απειλητικά ή προσβλητικά μηνύματα τότε κρίνεται σκόπιμο να τα αποθηκεύσεις και όχι να τα διαγράψεις, να κρατήσεις δηλαδή όλα τα αποδεικτικά στοιχεία. Μπορείς επίσης να τα εκτυπώσεις για να τα δείξεις στους γονείς σου.
2) Σε περιπτώσεις όπου τα μηνύματα επιμένουν και προέρχονται από άγνωστο αποστολέα, οι γονείς μπορούν να πάρουν πληροφορίες για την Ασφαλή Πλοήγηση στο Διαδίκτυο.
3) Σε περιπτώσεις που ένας «διαδικτυακός φίλος» σου στέλνει μηνύματα προσβλητικά μπορείς εύκολα να τον «αποκλείσεις» από το email σου.
4) Εάν ο θύτης είναι γνωστό σου πρόσωπο, σε αυτή την περίπτωση είναι σημαντικό να ενημερωθούν οι γονείς του παιδιού για τη συμπεριφορά του με βασικό σκοπό να περιοριστεί ο θύτης.
5) Εάν αισθάνεσαι αγχωμένος ή φοβισμένος είναι σημαντικό εσύ και οι γονείς σου να ζητήσετε βοήθεια από ψυχολόγο ειδικό σε τέτοιου είδους θέματα.
6) Εφόσον έχεις αντιληφθεί κάποια ιστοσελίδα όπου χρησιμοποιούνται προσωπικά δεδομένα σου ή φιλοξενούνται ρατσιστικά σχόλια για εσένα μπορείτε να την αναφέρετε στην Ελληνική Ανοικτή Γραμμή για το παράνομο περιεχόμενο στο Διαδίκτυο (www.safeline.gr) οι οποίοι και θα προβούν στις απαραίτητες ενέργειες.

Παρακάτω αναφέρουμε ενδεικτικά κάποιες περαιτέρω δυνατότητες εφόσον ο εκφοβισμός διεξήχθη μέσω κάποιας ιστοσελίδας κοινωνικής δικτύωσης ή chat- room:

1) Facebook: Μπορείς να κάνεις αναφορά επιλέγοντας την επιλογή ‘Report’ (‘αναφορά) που υπάρχει στις σελίδες ή να στείλεις e-mail στο abuse@facebook.com. Ένας καλός οδηγός ασφάλειας για παιδιά και γονείς βρίσκεται στο

www.facebook.com/safety. Οι χρήστες κάτω των 13 απαγορεύονται κι οι γονείς μπορούν να αναφέρουν την ύπαρξη τους στο http://www.facebook.com/help/contact.php?show_form=underage.

2) Youtube: Υπάρχει επιλογή 'Flag content as inappropriate' κάτω από κάθε βίντεο. Επίλεξε ακόμα το 'Security Center' έχοντας διαλέξει την Ελληνική ως γλώσσα περιήγησης.
3) Instant messaging(MSN – YAHOO) : Επιλέγοντας το 'Help' tab θα ανοίξει πολλαπλές επιλογές μία εκ των οποίων είναι το 'Report Abuse'.
4) Chat-rooms : Στη συντριπτική πλειοψηφία τους υπάρχουν ρυθμιστές (moderators) που είναι συνήθως πολύ αυστηροί με περιπτώσεις κακόβουλης επίθεσης. Μία επικοινωνία στο e-mail τους με το συγκεκριμένο πρόβλημα είναι συνήθως αρκετή.

ΤΟ CYBER-BULLYING ΣΤΗΝ ΕΛΛΑΔΑ :

Το φαινόμενο του εκφοβισμού μέσω Διαδικτύου απασχολεί ολοένα και περισσότερο τους σύγχρονους ερευνητές, καθώς λαμβάνει χώρα αρκετά συχνά πλέον σε παγκόσμιο επίπεδο αλλά και στην ελληνική πραγματικότητα. Σύμφωνα με τα στοιχεία που προέκυψαν από απογραφική έρευνα στην νήσο Κω, προέκυψε ότι το 14,7% του δείγματος είχε δεχτεί παρενόχληση μέσω του Διαδικτύου. Από αυτό το ποσοστό το 15,2% ήταν αγόρια και το 19,5% κορίτσια (Πρακτικά 1ου Πανελληνίου Συνεδρίου Ε.Ε.Μ.Δ.Ε.Δ, 2009).Επιπλέον δεν βρέθηκε αξιόλογη διαφορά ως προς τον μ.ο ηλικίας μεταξύ όσων εφήβων βίωσαν cyber-bullying και όσους όχι. Αριθμητικά συχνότερη ήταν η αναφορά από 17χρονους, όμως εξίσου πιθανό ήταν να το αναφέρουν και 14χρονοι που πλοηγούνται στο Διαδίκτυο.

Η οργάνωση ΝΕΟΙ πραγματοποίησε έρευνα στο Ν. Θεσσαλονίκης από τον Απρίλιο έως Σεπτέμβριο 2009 με στόχο τη μελέτη και έκταση της αυξανόμενης χρήσης του διαδικτύου από παιδιά και νέους, τον τρόπο τέλεσης του και τις επιπτώσεις του στα θύματα. Η έρευνα διενεργήθηκε σε 422 εφήβους από 13-18 ετών (275 αγόρια & 147 κορίτσια) με ειδικά διαμορφωμένο έντυπο & ανώνυμο ερωτηματολόγιο. Τα αποτελέσματα που προκύπτουν από την έρευνα εμφανίζονται ως ποσοστό επί του συνολικού δείγματος ηλικίας 13 – 18 ετών :

1) 16% από τα αγόρια ηλικίας 13-18 ετών δηλώνουν ότι έχουν πέσει θύματα κυβερνοεκφοβισμού .
2) Από αυτό το ποσοστό, το 9% δηλώνει ότι η πράξη έγινε μέσα από ιστοχώρο κοινωνικής δικτύωσης (HI5, TWITTER) και το 6% δηλώνει ότι έγινε μέσω Instant Messaging Services.
3) 32% είχαν δεχθεί εκφοβισμό με δημοσίευση στο διαδίκτυο προσωπικών τους φωτογραφιών, 11% λεκτικό – αποκάλυψη γεγονότων προσωπικού ενδιαφέροντος και ένα 3,5% δήλωσε ότι έγινε με χυδαίο λεξιλόγιο – ύβρεις.
4) Ένα 10% των αγοριών απάντησε θετικά στην ερώτηση, εάν έχουν εκφοβίσει μέσω διαδικτύου και νέων τεχνολογιών κάποιον συμμαθητή, φίλο ή γνωστό τους.

Το πιο σημαντικό είναι ότι στο σύνολο του δείγματος ένα 42% απάντησε ότι ξέρουν ή έχουν ακούσει για κάποιον γνωστό που έχει πέσει θύμα εκφοβισμού, μέσω διαδικτύου και νέων τεχνολογιών.Αναφορικά με το δείγμα των κοριτσιών τα ποσοστά ήταν λίγο πιο ψηλά με ένα 22% να απαντά θετικά στο ότι έχει πέσει θύμα κυβερνοεκφοβιμού και ένα 9% να δηλώνει ότι γνώριζε τον εκφοβιστή του. Όταν ρωτήσαμε τα παιδιά αυτά να μας πούνε τους λόγους αυτού του φαινομένου το 13% μας απάντησε ότι έγινε για λόγους εκδίκησης, το 31% για να γελάσουνε και ένα 56% για δυσφήμιση».

ΠΑΡΑΔΕΙΓΜΑΤΑ ΑΥΤΟΚΤΟΝΙΩΝ ΑΠΟ ΑΡΝΗΤΙΚΗ ΕΠΙΡΡΟΗ ΧΡΗΣΤΩΝ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ:

Μία 16χρονη δήλωσε σε συνομιλία της στο Facebook ότι επιθυμεί να βάλει τέλος στη ζωή της και λίγη ώρα αργότερα κατάπιε χάπια για να αυτοκτονήσει. Αργότερα εξήγησε στους αστυνομικούς -που την έσωσαν την τελευταία στιγμή μεταφέροντάς την στο νοσοκομείο- ότι ο λόγος που την οδήγησε στην αυτοκτονία ήταν ότι χρήστες του διαδικτύου κατέκριναν τις απόψεις της.Κάτι ανάλογο συνέβη και με έναν 14χρονο, ο οποίος γνωστοποίησε σε chat room ότι θέλει να αυτοκτονήσει, επειδή ο διαχειριστής διαδικτυακού παιχνιδιού, όπως είπε, τον απέκλεισε από το πρόγραμμα, γιατί παραβίασε τους κανόνες. Δεκάδες νέοι ανακοινώνουν μέσω ίντερνετ ότι θα αυτοκτονήσουν!

ΠΗΓΕΣ

- http://el.wikipedia.org/wiki/Spam
- http://www.e-yliko.gr/htmls/pc_use/srules.aspx
- www.ethnos.gr
- http://eprl.korinthos.uop.gr
- http://news.jeebboo.com
- http://www.kessaris.edu.gr/goneis2013/ekfovismosdiadiktio.html
- http://www.tsantiri.gr/ellada/page/1415
- psychologein.dagorastos.net/.../cyberbullying/
- http://www.nd.gr/web//secretary-socialwelfare/press/-/journal_content/56_INSTANCE_1wmJ/48962/800456
- http//eimaimama.blogstop.com
- http://katerina-soumpassi.blogspot.gr/2012/06/e.html
- Viruslist.com
- TechTarget.com
- About.com για τους ιούς
- Περισσότερα για τον ιό Brain
- Computer Knowledge
- http://www.dpa.gr
- http://lyk-fdil.sam.sch.gr/autosch/joomla15/images/multimedia_ARXEIA/e-emporio.pdf
- http://el.wikipedia.org/wiki/%CE%A7%CE%91%CE%9A%CE%95%CE%A1_(HACKER)
- http://en.wikipedia.org/wiki/Software_cracking
- http://www.google.gr
- http://www.astynomia.gr/index.php?Itemid=128&id=3686&option=ozo_content&perform=view ,
- http://www.eeei.gr/interbiz/articles/apates.htm
- http://support.google.com/chrome/bin/answer.py?hl=el&answer=99020

- http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/YOUTH/YOUTH_INTRO/YOUTH_BOOKLET.PDF
- http://www.google.gr/search?q=phishing+foto&hl=el&tbm=isch&tbo=u&source=univ&sa=X&ei=iYFqUZn3L-nJ0QXt4ICgCQ&ved=0CCwQsAQ&biw=1024&bih=677#imgrc=95jEvmKkcWgh6M%3A%3B4l3LqHN63N2HUM%3Bhttp%253A%252F%252Fstatic.ddmcdn.com%252Fgif%252Fphishing-1.jpg%3Bhttp%253A%252F%252Fwww.howstuffworks.com%252Fphishing.htm%3B400%3B425
- http://www.otyposnews.gr/archives/4057#ixzz2P8Ox2RnK
- www.tovima.gr/society/article/?aid=493605
- http://en.wikipedia.org/wiki/Suicide_of_Amanda_Todd
- http://www.ego.gr/news/article.asp?catid=17826&subid=2&pubid=129139201
- http://hamomilaki.pblogs.gr/tags/paidofilia-gr.html