

Κίνδυνοι και κανόνες ασφαλείας στο διαδίκτυο

.....

Συχνά μας ρωτάτε πώς μπορείτε να προστάτεψε το παιδί σας κι εσάς τους ίδιους, από τους κινδύνους του διαδικτύου. Τι θα μπορούσατε να εγκαταστήσετε στον υπολογιστή ή το κινητό ώστε να αποφύγετε τους κινδύνους στο διαδίκτυο ή πώς θα παρακολουθείτε τις κινήσεις που κάνει το παιδί σας σε αυτό.

Συνήθως η απάντηση μας είναι ότι εκτός από ένα πρόγραμμα για την αντιμετώπιση της απειλής από τους ιούς δεν υπάρχει κάτι άλλο παρά μόνο να εισαχθούν κάποιοι κανόνες ασφαλείας. Κρίνεται αναγκαίο να γίνει συζήτηση μεταξύ εσάς και του παιδιού όσον αφορά τους προαναφερθέντες κινδύνους αλλά και να ενημερωθείτε για κάθε νέο τρόπο παραπλάνησης με τον οποίο προσπαθούν οι επιτήδριοι να κερδίσουν κάτι από εσάς ή το παιδί σας.

Το πρώτο πράγμα που θα πρέπει να συνειδητοποιήσει κάθε χρήστης του διαδικτύου είναι ότι ο παγκόσμιος ιστός (INTERNET) δεν διαφέρει σε τίποτα από μια πραγματική κοινωνία. Κρύβει λοιπόν, αντίστοιχους κινδύνους και απαιτεί αντίστοιχα μέτρα προστασίας από αυτούς. Η σωστή τακτική ενημέρωση σχετικά με την φύση των κινδύνων αλλά και τον τρόπο αντιμετώπισης τους γίνεται απαραίτητη προκειμένου να ελαχιστοποιηθεί ο κίνδυνος έκθεσης του χρήστη στους βασικότερους τουλάχιστον κινδύνους.....

.....

Βασικοί Κίνδυνοι :

- Αποπλάνηση Ανηλίκων (Grooming)
- Ηλεκτρονική Παρενόχληση (Cyberbullying)
- Διαδικτυακά Παιχνίδια
- Υπερβολική Χρήση και Εθισμός
- Ανεπιθύμητη Αλληλογραφία (Spam)
- Παραπλανητικά Μηνύματα (Scam)
- Ιοί (Viruses, Trojan)
- Ηλεκτρονικό «Ψάρεμα» (Phishing, Pharming)
- Λογισμικά υποκλοπής (Spyware, Adware, Malwares)
- Παράνομη Πρόσβαση στον Η/Υ

- Απάτες στο ηλεκτρονικό εμπόριο
 - Ανεπιθύμητο Περιεχόμενο
 - Διαδίκτυο και Κινητή Τηλεφωνία
-

Αποπλάνηση Ανηλίκων (Grooming)

- Παιδόφιλοι προσποιούμενοι ότι είναι έφηβοι, ή κάποιος γνωστός του γνωστού, χρησιμοποιώντας δωμάτια συνομιλίας, ιστοσελίδες κοινωνικής δικτύωσης, online παιχνίδια ή κι άλλους χώρους διαδικτυακής επικοινωνίας, προσπαθούν να προσεγγίσουν παιδιά με απώτερο στόχο τη σεξουαλική τους κακοποίηση.
- Πρώτος στόχος του παιδόφιλου είναι να κερδίσει την εμπιστοσύνη του παιδιού μέσω της προσοχής, της στοργής, της δωροδοκίας, επενδύοντας ουσιαστικά χρόνο και χρήμα
- Προσπαθεί να πείσει το παιδί να του στείλει προσωπικές φωτογραφίες ή video, ή κι ακόμα να του πει πού πηγαίνει σχολείο ή σε ποια περιοχή μένει, ώστε να καταφέρει μέσω όλων αυτών να συναντηθεί μαζί του.

Ηλεκτρονική Παρενόχληση (Cyberbullying)

- Η συνεχής επιθετική συμπεριφορά εναντίον κάποιου μέσω διαδικτύου έτσι ώστε να αποκτηθεί δύναμη και εξουσία πάνω του (ψηφιακός εκφοβισμός)

Ανεπιθύμητη Αλληλογραφία (Spam)

- Είναι η παραλαβή μηνυμάτων χωρίς την έγκριση του παραλήπτη. Πρόκειται για μαζική αποστολή μηνυμάτων σε ηλεκτρονικές διευθύνσεις τις οποίες οι αποστολείς, είτε έχουν συλλέξει από διάφορες ιστοσελίδες, περιοδικά, λίστες συζητήσεων, βάσεις δεδομένων είτε ακόμα και να τις έχουν μαντέψει. Επίσης τα περισσότερα από αυτά έχουν κι ένα αρχείο μέσα στο μήνυμα που συνήθως είτε περιέχει ένα λογισμικό το οποίο εσείς σαν χρήστες δεν το βλέπετε και με το που ανοιχτεί μπορεί να σας κλέψει προσωπικά στοιχεία από τον Η/Υ, είτε αυτό το αρχείο να είναι ένας ιός που σκοπός του είναι να βλάψει τον Η/Υ. Σε αυτό το σημείο θα θέλαμε να σας ενημερώσουμε ότι τον τελευταίο καιρό τα μηνύματα που σας έρχονται χρησιμοποιούν λογότυπα, ή σαν θέμα μηνύματος ονόματα μεγάλων εταιριών, ώστε να κάνουν τον χρήστη να εμπιστευθεί

περισσότερο τον αποστολέα του μηνύματος και να τον ωθήσει να ανοίξει το μήνυμα (π.χ. τον τελευταίο καιρό έρχονται συχνά πυκνά μηνύματα σε διαφόρους χρήστες, υποτίθεται από την εταιρεία APPLE, που ούτε έχουν κάποια σχέση με την εταιρεία, ούτε έχουν κάποιο προϊόν της).

Παραπλανητικά Μηνύματα (Scam)

- Πρόκειται για παραπλανητικά μηνύματα το οποία σκοπό έχουν να δελεάσουν τους παραλήπτες με την προσφορά μεγάλων χρηματικών ποσών, δώρων (ταξίδι, αυτοκίνητο, μηχανή κ.α.), ή ευκαιριών καριέρας.
- Για την απόκτησή τους θα πρέπει να πληρώσετε προκαταβολικά κάποια έξοδα.

Ιοί (Virues, Trojan)

- Μικρά λογισμικά που μεταφέρονται και τρέχουν στον υπολογιστή με στόχο να αλλάξουν ή να καταστρέψουν, χωρίς ο χρήστης να το γνωρίζει. Τα συνήθη προβλήματα που προκαλούν είναι η διαγραφή αρχείων, αποστολή ηλεκτρονικών μηνυμάτων, δημιουργία εικονικής κίνησης προς το διαδίκτυο, απασχόληση πόρων του υπολογιστή. Η διάδοση τους γίνεται κυρίως από το ηλεκτρονικό ταχυδρομείο (email) διαφόρων δωρεάν προγραμμάτων κι από κάποιες ιστοσελίδες.

Ηλεκτρονικό Ψάρεμα (Phishing, Pharming)

- Phishing είναι η προσπάθεια υποκλοπής ευαίσθητων προσωπικών δεδομένων, όπως κωδικών, αριθμών πιστωτικών καρτών, αριθμών λογαριασμών κι άλλων προσωπικών στοιχείων με ψεύτικα προσχήματα.
- Οι προσεγγίσεις με σκοπό το 'Ηλεκτρονικό Ψάρεμα' γίνονται συνήθως μέσω ηλεκτρονικού ταχυδρομείου οι οποίες παραπέμπουν σε ιστοσελίδες παγίδες (Pharming).

Λογισμικά υποκλοπής (Spywarew, Adwarew, Malwares)

- Προγράμματα εγκατεστημένα στον υπολογιστή χωρίς την έγκριση του ιδιοκτήτη τα οποία έρχονται ως κρυφά μέρη άλλων, συνήθως δωρεάν, προγραμμάτων.
- Ένα λογισμικό υποκλοπής μπορεί να παρακολουθεί τη συμπεριφορά του χρήστη στο διαδίκτυο, να καταγράφει όλες τις ενέργειες του υπολογιστή, να αλλάξει την παραμετροποίηση του υπολογιστή, να παρεμβαίνει στη λειτουργία άλλων

προγραμμάτων (malware), να παρουσιάζει διαφημίσεις μέσα από αναδυόμενα παράθυρα (Adware), να κάνει τον υπολογιστή πιο αργό ή να θέσει τον υπολογιστή υπό τον έλεγχο άλλου.

Κανόνες Ασφαλείας μας στο διαδίκτυο

.....

- Ποτέ δεν επικοινωνούμε με άγνωστα άτομα στο διαδίκτυο
- Ποτέ δεν δίνουμε προσωπικά στοιχεία σε άγνωστα άτομα
- Ποτέ μα ποτέ δεν συναντούμε κάποιον που γνωρίσαμε στο διαδίκτυο
- Ποτέ δεν απαντούμε σε ανώνυμα ή προσβλητικά μηνύματα
- Προσπαθούμε να μην παραμένουμε πολλή ώρα συνδεδεμένοι στον υπολογιστή μας
- Κλείνουμε τη σύνδεση αν δούμε ή διαβάσουμε κάτι που μας ενόχλησε
- Προσπαθούμε να μην κατεβάζουμε οποιαδήποτε αρχεία στον υπολογιστή μας
- Να θυμόμαστε πάντα πως ότι αναρτάται στο διαδίκτυο παύει να είναι πλέον προσωπικό στοιχείο
- Να ενημερώνω αμέσως τους γονείς μου ή τους δασκάλους μου σε περίπτωση που κάποιος με ενοχλεί στο διαδίκτυο
- Εξερευνούμε μόνοι μας το διαδίκτυο ή παρέα με το παιδί μας
- Φροντίζουμε να υπάρχουν κανόνες χρήσης του διαδικτύου (πόση ώρα και ποιες ώρες μπορεί το παιδί να συνδεθεί στο διαδίκτυο)
- Ο υπολογιστής να είναι σε χώρο που ελέγχεται εύκολα από τους γονείς
- Δεν απαγορεύουμε στα παιδιά μας την πρόσβαση στο διαδίκτυο
- Μαθαίνουμε στο παιδί μας από μικρή ηλικία να επισκέπτεται σελίδες ειδικά σχεδιασμένες για παιδιά (π.χ. μηχανή αναζήτησης το kiddie)
- Χρησιμοποιούμε λογισμικό φιλτραρίσματος περιεχομένου
- Μαθαίνουμε στα παιδιά μας να μας εμπιστεύονται και να μας μιλάνε για τις διαδικτυακούς τους φίλους και δραστηριότητες
- Μαθαίνουμε στα παιδιά μας να προστατεύουν την ιδιωτική τους ζωή στο διαδίκτυο όπως και στον πραγματικό τους κόσμο.

Επίσης μην ξεχνάμε ότι πλέον έχουμε την ελληνική ανοικτή γραμμή για καταγγελία παράνομου περιεχομένου στο διαδίκτυο και μην διστάσετε ποτέ να την χρησιμοποιήσετε: <http://www.safeline.gr/>

Πηγή κειμένου Protection Plus Security Άμεση Προστασία και Ασφάλεια :

<https://protectionplus.gr/%CE%BA%CE%AF%CE%BD%CE%B4%CF%85%CE%BD%CE%BF%CE%B9-%CE%BA%CE%B1%CE%B9-%CE%BA%CE%B1%CE%BD%CF%8C%CE%BD%CE%B5%CF%82-%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%AF%CE%B1%CF%82-%CF%83%CF%84%CE%BF-%CE%B4%CE%B9/>