3ο ΓΕΛ ΚΟΜΟΤΗΝΗΣ

Ασφάλεια στο Διαδίκτυο

ΟΜΑΔΑ 1 Dream-Team

Δημήτρης Τοροσιάν, Ανδρέας Μιχαηλίδης, Δημήτρης Πασχαλίδης

ΟΜΑΔΑ 2 Minion**s**

Μαριέττα Θωμά, Έλλη Στρατιάδου, Όλγα Σερμπέζη, Φίλιππος Σιμόπουλος

ΟΜΑΔΑ 3 Πασχαλίτσες

Τόλης Ντριβιντίδης, Νίκος Λεπίδας, Πολύδωρος Μανίτσας, Γιάννης Σαλακίδης

ΟΜΑΔΑ 4

Χουσεϊν Χαρούν, Σακαλλή Ογκιούν, Χούσκουγλου Κιουμπρά

ΟΜΑΔΑ 5 Λευκή Ομάδα

Ραφαέλλα-Ζωή Ηλιάδου, Αινούρ Ρεσήτ, Ζεληχά Αμέτις

Εκπαιδευτικός : Βερρή Ανδρονίκη, ΠΕ19

Σχολικό έτος 2013-2014

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ 2
ΠΡΟΛΟΓΟΣ 4
ΕΙΣΑΓΩΓΗ 5
ΠΛΑΙΣΙΟ - ΣΤΟΧΟΙ - ΣΠΟΥΔΑΙΟΤΗΤΑ - ΑΝΑΓΚΑΙΟΤΗΤΑ 5
ΕΡΕΥΝΗΤΙΚΑ ΕΡΩΤΗΜΑΤΑ 6
ΕΡΕΥΝΗΤΙΚΟ ΜΕΡΟΣ 6
ΧΡΟΝΟΣ ΚΑΙ ΤΡΟΠΟΣ ΔΙΕΞΑΓΩΓΗΣ ΤΗΣ ΕΡΕΥΝΑΣ 6
ΜΕΘΟΔΟΛΟΓΙΑ ΤΗΣ ΕΡΕΥΝΑΣ 6
ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΡΕΥΝΑ 7
Κίνδυνοι από τη χρήση του Διαδικτύου για τους Υπολογιστές 7
Λογισμικά Κακόβουλης Λειτουργίας 7
Hacker vs Crackers 16
Πειρατικό vs Νόμιμο Λογισμικού 17
Πώς να προστατέψω τον Η/Υ μου 23
Βασικά Μέτρα Προστασίας 23
Antivirus 24
Firewall 26
Αντίγραφα Ασφαλείας 27
Επαναφορά Αρχείων 28
Αντιμετώπιση ιων 29
Γονικός Έλεγχος 37
Παράνομες Δραστηριότητες στο Διαδίκτυο 39
Προσωπικά Δεδομένα 39
Ηλεκτρονικός Εκφοβισμός 43
Grooming: Σεξουαλική Αποπλάνηση 45
Παιδική Πορνογραφία στο Διαδίκτυο 46
Sexting 49

Κίνδυνοι από τη χρήση του Διαδικτύου για έναν παιδί-έφηβο 49
Phishing 50
Spam email 52
Hoaxes 53
Εθισμό στο Διαδίκτυο 53
Ψεύτικα profil 55
Διαδικτυακά Παιχνίδια 57
Social Media 59
Ασφαλείς Οικονομικές Συναλλαγές 62
Πώς να προστατέψω τον εαυτό μου 64
Βασικοί κανόνες χρήσης Διαδικτύου 64
Facebook 66
Κωδικοί Πρόσβασης 70
ηλεκτρονική εξαπάτηση 72
σωστή στάση του σώματος 74
Εθισμός στο Διαδίκτυο 75
Γονείς – Παιδία- Διαδίκτυο 75
ΔΗΜΟΣΚΟΠΙΚΗ ΕΡΕΥΝΑ - ΠΑΡΟΥΣΙΑΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΤΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ 80
Ερωτηματολόγιο Για Μαθητές 80
ΣΧΟΛΙΑΣΜΟΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ 81
ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΓΙΑ ΓΟΝΕΙΣ ΜΑΘΗΤΏΝ & ΚΑΘΗΓΗΤΕΣ 86
ΣΧΟΛΙΑΣΜΟΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ 87
Υποχρεώσεις και Δικαιώματα στο Διαδίκτυο 91
ΕΠΙΛΟΓΟΣ 93
ΒΙΒΛΙΟΓΡΑΦΙΑ 94
ΠΑΡΑΡΤΗΜΑ 97
Σύννεφα Λέξεων 97

ΠΡΟΛΟΓΟΣ

Αυτή η εργασία πραγματοποιήθηκε στα πλαίσια του μαθήματος Ερευνητική Εργασία της Β' Τάξης Γενικού Λυκείου Κομοτηνής. Ο χρόνος διεξαγωγής είναι το Σχ. Έτος 2013-2014 Α' Τετράμηνο. Το θέμα της εργασίας Ασφάλεια στο Διαδίκτυο, Κίνδυνοι και Προστασία.

Οι μαθητές χωρίστηκαν σε 5 ομάδες και δούλεψαν ξεχωριστές ενότητες.

1η Ομάδα

Είμαστε η ομάδα Dream-Team. Είμαστε οι Δημήτρης Τοροσιάν, Ανδρέας Μιχαηλίδης και Δημήτρης Πασχαλίδης. Είχαμε το θέμα για την προστασία του υπολογιστή από ιούς. Συνεργαστήκαμε μεταξύ μας ώστε να πετύχουμε τον στόχο που θέλαμε. Και τελικά μετά από πολλές ώρες δουλειάς τελειώσαμε με επιτυχία αυτό που θέλαμε. Και το πιο σημαντικό είναι πως μάθαμε πώς να προστατεύουμε τον υπολογιστή μας.

2η Ομάδα

Την ομάδας μας την ονομάσαμε minios. Είμαστε οι Μαριέττα Θωμά, Έλλη Στρατιάδου, Όλγα Σερμπέζη και Φίλιππος Σιμόπουλος. Ερευνήσαμε για τους κινδύνους του διαδικτύου για τους ανθρώπους και συνεργαστήκαμε αρμονικά μεταξύ μας. Μας άρεσε η δημιουργία του ερωτηματολογίου, αλλά μας δυσκόλεψε η δημιουργία των σχεδιαγραμμάτων. Τέλος μάθαμε αρκετά χρήσιμα πράγματα για την ασφάλεια στο διαδίκτυο.

3η Ομάδα

Είμαστε η ομάδα 3 ή αλλιώς οι πασχαλίτσες. Τα μέλη μας είναι

Τόλης Ντριβιντίδης

Νίκος Λεπίδας

Πολύδωρος Μανίτσας

Γιάννης Σαλακίδης

Ήμασταν υπεύθυνοι για το θέμα «Κίνδυνοι για τον υπολογιστή» Συναντήσαμε δυσκολίες στα ερωτηματολόγια. Λόγω swag δεθήκαμε και τελειώσαμε εύκολα.

Υπογραφές ομάδας:

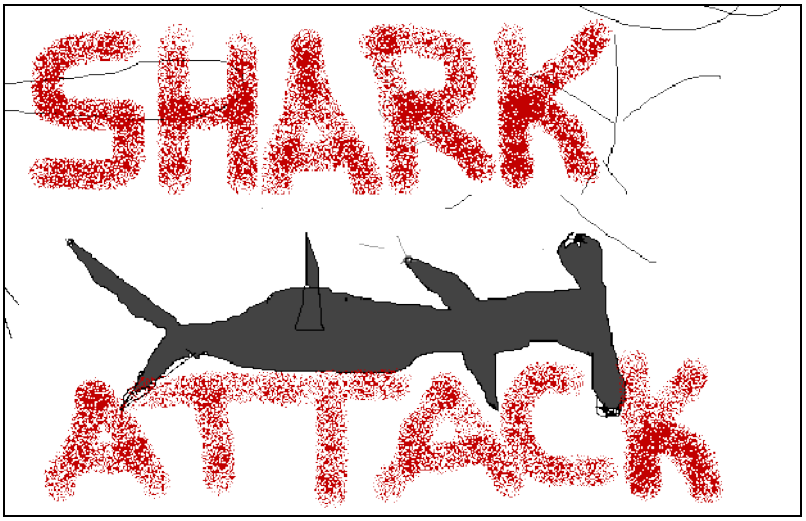
#yolo

#project

#School

#berh

#matrix



4η Ομάδα

Ονομαζόμαστε Χουσεϊν Χαρούν, Σακαλλή Ογκιούν και Χούσκουγλου Κιουμπρά. Είμαστε η ομάδα που ασχολήθηκε με το θέμα της προστασίας του εφήβου από διάφορους κινδύνους στο διαδίκτυο. Σκοπός μας ήταν να αναζητήσουμε τρόπους με τους οποίους οι έφηβοι μπορούν να προστατεύονται και αυτό που μας άρεσε ήταν ότι ενώ κάναμε την εργασία μαθαίναμε οι ίδιοι τους κανόνες συμπεριφοράς του ίντερνετ. Το γεγονός ότι στο διαδίκτυο έχει περισσότερο υλικό για τους κινδύνους παρά για την αντιμετώπισή τους, μας δυσκόλεψε πάρα πολύ.

5η Ομάδα

Είμαστε η λευκή ομάδα που αποτελείται από την:

Ραφαέλλα-Ζωή Ηλιάδου

Αινούρ Ρεσήτ

Ζεληχά Αμέτις

Επιλέξαμε αυτό το project γιατί θέλαμε να μάθουμε για την ασφάλεια στο διαδίκτυο. Ασχοληθήκαμε με το cyberbulling, sexting, phising,grooming, προσωπικά δεδομένα και απάτες με πιστωτικές κάρτες.

ΕΙΣΑΓΩΓΗ

Σήμερα το διαδίκτυο αποτελεί μια καθημερινή συνήθεια για παιδιά και εφήβους οι οποίοι χρησιμοποιούν το διαδίκτυο όλο και περισσότερο στις μέρες μας και περνούν αρκετή ώρα σερφάροντας, επικοινωνώντας και διασκεδάζοντας σε αυτό. Ωστόσο η χρήση του διαδικτύου κρύβει κινδύνους άλλοτε εύκολα αντιληπτούς και άλλοτε όχι, γι' αυτό είναι σημαντικό να ενημερωνόμαστε για αυτούς και να αποφεύγουμε την υπερβολική του χρήση. Υπάρχουν τρόποι να προστατευτούμε ή η μήπως η λύση είναι να μη χρησιμοποιούμε το διαδίκτυο; Με την κατάλληλη χρήση του διαδικτύου θα προστατευτούμε από τους κινδύνους που κρύβει. Η λύση δεν είναι να μη το χρησιμοποιούμε αφού μας προσφέρει χρήσιμες πληροφορίες αλλά και μας ψυχαγωγεί.

ΠΛΑΙΣΙΟ - ΣΤΟΧΟΙ - ΣΠΟΥΔΑΙΟΤΗΤΑ - ΑΝΑΓΚΑΙΟΤΗΤΑ

Ο λόγος για τον οποίο επιλέξαμε αυτό το θέμα είναι γιατί πιστεύουμε πως το διαδίκτυο είναι ένα επίκαιρο θέμα που μας αφορά εμάς τους εφήβους και ένα ενδιαφέρον θέμα για να ερευνήσουμε. Σκοπός μας ήταν να ασχοληθούμε με το διαδίκτυο όχι ως χρήστες, κάτι που ξέρουμε να το κάνουμε και μας αρέσει πολύ, αλλά ερευνώντας τους κινδύνους που υπάρχουν κατά την πλοήγηση μας και ανακαλύπτοντας τρόπους προστασίας για μας και για τον υπολογιστή μας.

ΕΡΕΥΝΗΤΙΚΑ ΕΡΩΤΗΜΑΤΑ

Κατά την έρευνα μας χρησιμοποιήσαμε ιστοσελίδες όπως

- το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου: http://www.saferinternet.gr/,
- τον ενημερωτικός κόμβο Πανελλήνιου Σχολικού Δικτύου: http://internet-safety.sch.gr/,
- την Ελληνική ανοιχτή γραμμή για παράνομο περιεχόμενο στο διαδίκτυο (Safeline): http://www.safeline.gr/,
- επίσης το site του http://www.saferinternet.gr,
- την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα http://www.dpa.gr,
- καθώς και την http://www.youth-health.gr/gr/

και θελήσαμε να απαντήσουμε στα παρακάτω ερευνητικά ερωτήματα

1. Ποιοι είναι βασικοί κανόνες χρήσης Διαδικτύου από τους εφήβους;
2. Ποια είναι η σωστή συμπεριφοράς μας στα site κοινωνικής δικτύωσης;
3. Πώς επηρεάζουν την συμπεριφορά παιδιών και εφήβων όταν γίνεται κατάχρηση των διαδικτυακών παιχνιδιών;
4. Ποιοι είναι οι παράγοντες που οδηγούν τους νέους σε εθισμό στο διαδίκτυο και ποιες οι συνέπειες του εθισμού; Πώς αντιμετωπίζεται το πρόβλημα αυτό;
5. Ποια είναι τα βασικά τα είδη κακόβουλων προγραμμάτων;
6. Τι πρέπει να κάνουμε όταν ο υπολογιστή μας μολυνθεί από κάποιον ιό;
7. Ποια είναι τα κατάλληλα μέτρα ώστε να προστατεύσουμε τον υπολογιστή μας από κακόβουλο λογισμικό;
8. Τι σημαίνει πειρατεία λογισμικού; Πότε ένα λογισμικό είναι παράνομο; Ποια τα πλεονεκτήματα από τη χρήση νόμιμου λογισμικού;
9. Ποιες παράνομες δραστηριότητες μπορεί να συναρτήσουμε στο Διαδίκτυο και πώς προστατευόμαστε από το Νόμο;
10. Ποια είναι η σωστή στάση των γονέων απέναντι στα παιδιά τους ώστε να είναι ασφαλή όταν προηγούνται διαδίκτυο;

ΕΡΕΥΝΗΤΙΚΟ ΜΕΡΟΣ

ΧΡΟΝΟΣ ΚΑΙ ΤΡΟΠΟΣ ΔΙΕΞΑΓΩΓΗΣ ΤΗΣ ΕΡΕΥΝΑΣ

Τον περισσότερο χρόνο ασχοληθήκαμε με βιβλιογραφική έρευνα μέσω διαδικτύου για ενημέρωση για το θέμα συλλογή υλικού με βάση τα ερευνητικά ερωτήματα. Στη συνέχεια συντάχθηκαν ερωτηματολόγια για να γίνει έρευνα δημοσκόπησης. Κατόπιν έγινε στατιστική ανάλυση των αποτελεσμάτων και εξαγωγή συμπερασμάτων. Τέλος, έγινε η σύνταξη, η εκτύπωση και η παρουσίαση της εργασίας.

ΜΕΘΟΔΟΛΟΓΙΑ ΤΗΣ ΕΡΕΥΝΑΣ

Για την δημοσκοπική μας έρευνά μας, χρησιμοποιήθηκαν 2 διαφορετικά ερωτηματολόγια τα οποία περιείχαν ερωτήματα κλειστού τύπου (δηλαδή με απαντήσεις ναι ή όχι, πολύ – αρκετά – λίγο – καθόλου) και όχι ερωτήματα ανοιχτού τύπου, που θα έπρεπε να γράφει ο ερωτώμενος κείμενο που να εκφράζει την άποψή του. Αφού έγινε η σύνθεση και η σύνταξη των ερωτηματολογίων από τις ερωτήσεις που συζητήσαμε μέσα στην τάξη, τα ερωτηματολόγια εκτυπώθηκαν και μοιράστηκαν.

Το δείγμα μας για το 1^{ο} ερωτηματολόγιο ήταν μαθητές των τάξεων Α και Β και Γ. Σκεφτήκαμε να αποτελέσουν δείγμα μας οι μαθητές από το σχολείο μας διότι τους γνωρίζουμε και είναι συμμαθητές μας. Για να είμαστε σίγουροι πως τα παιδιά θα κατανοήσουν απόλυτα τις ερωτήσεις, η συμπλήρωση έγινε μέσα στην τάξη, προκειμένου να γίνουν οι απαραίτητες διευκρινίσεις εάν χρειαζόταν.

Το δείγμα μας για το 2^{ο} ερωτηματολόγιο ήταν γονείς μαθητών και καθηγητές για να διερευνήσουμε για το πόσο είναι ενημερωμένοι για τους κινδύνους του διαδικτύου.

Μετά τη συμπλήρωση και τη συλλογή των ερωτηματολογίων αναλύσαμε τα αποτελέσματα με τη δημιουργία γραφημάτων. Τέλος βγάλαμε συμπεράσματα. Η ανάλυση των δεδομένων έγινε με το πρόγραμμα λογιστικών φύλλων excel.

ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΡΕΥΝΑ

ΚΙΝΔΥΝΟΙ ΑΠΟ ΤΗ ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΓΙΑ ΤΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ

ΛΟΓΙΣΜΙΚΑ ΚΑΚΟΒΟΥΛΗΣ ΛΕΙΤΟΥΡΓΙΑΣ

Τι είναι το λογισμικό κακόβουλης λειτουργίας;

Το λογισμικό κακόβουλης λειτουργίας είναι ένας όρος που χρησιμοποιείται για κακόβουλο λογισμικό το οποίο έχει σχεδιαστεί για να προκαλεί βλάβες ή να εκτελεί ανεπιθύμητες ενέργειες στο σύστημα ενός υπολογιστή. Ακολουθούν μερικά ενδεικτικά παραδείγματα λογισμικού κακόβουλης λειτουργίας:

- Ιοί
- Ιοί τύπου worm
- Δούρειοι ίπποι
- Λογισμικό κατασκοπίας
- Παραπλανητικό λογισμικό ασφαλείας

Ιός

Ο ιός του υπολογιστή είναι ένα κομμάτι προγράμματος, το οποίο αντιγράφει τον εαυτό του και επισυνάπτεται σε ένα νομότυπο πρόγραμμα με σκοπό να «μολύνει» άλλα προγράμματα. Όταν το μολυσμένο πρόγραμμα εκτελεστεί (το λεγόμενο «άνοιγμα μολυσμένου αρχείου»), κάτω από ορισμένες συνθήκες, προσπαθεί να μολύνει και άλλα προγράμματα, να διαγράψει, να αλλάξει ή να κρυπτογραφήσει αρχεία. Η ύπαρξη ιών είναι ένα από τα σημαντικότερα προβλήματα του Διαδικτύου. Υπάρχουν σήμερα χιλιάδες διαφορετικοί ιοί, οι οποίοι προσβάλλουν εκατομμύρια υπολογιστών σε όλον τον κόσμο. Πολλοί έχουν τη δυνατότητα να μεταλλάσσονται και να διαφέρουν σε μεγάλο βαθμό από τον αρχικό ιό. Σε ΠΕΡΙΠΤΩΣΗ που μιλάμε για υπολογιστές δικτύων, η καταστροφή έχει ακόμα μεγαλύτερες διαστάσεις, καθώς μολύνονται και καταρρέουν αρχεία εταιρειών, πανεπιστημίων, υπουργείων, ακόμα και κυβερνήσεων.

Δούρειος Ίππος (Trojan horse)

Πρόκειται για ένα είδος προγράμματος, το οποίο δεν αναπαράγεται και δρα «υπογείως», χωρίς ο χρήστης του υπολογιστή να αντιλαμβάνεται αρχικά την ύπαρξή του. Το πρόγραμμα αυτό ενεργεί ως μέσο μεταφοράς άλλων μορφών επιβλαβούς λογισμικού (malware), ενεργοποιείται σε συγκεκριμένο χρόνο και δημιουργεί ένα αντίγραφο του αυθεντικού προγράμματος που χρησιμοποιείται από το χρήστη, το οποίο θα δουλεύει κανονικά, σα να ήταν το αυθεντικό. Όταν ο χρήστης εκτελέσει το συγκεκριμένο πρόγραμμα χρησιμοποιεί την έκδοση του Δούρειου Ίππου, ο οποίος δρα καταστροφικά.

Σκουλήκια (worms)

Πρόκειται για προγράμματα υπολογιστών τα οποία αντιγράφουν τον εαυτό τους σε δίκτυα Η/Υ. Χρησιμοποιούν το Internet ως μέσο διάδοσής τους (emails, irc chat κ.ά.). Αναπαράγονται από υπολογιστή σε υπολογιστή, εκμεταλλευόμενα τα σφάλματα των λειτουργικών προγραμμάτων των υπολογιστών. Οι μολυσμένοι υπολογιστές μετά από κάποιο διάστημα κατακλύζονται από αντίγραφα του «σκουληκιού» και δε μπορούν να λειτουργήσουν.

Μακρο-ιοί

Ως μακροεντολή ορίζουμε μια οδηγία που εκτελεί αυτόματα εντολές του προγράμματος. Οι μακρο-ιοί αποτελούν τέτοιες οδηγίες που αυτοαντιγράφονται. Το κύριο πρόβλημα με τους μακρο-ιούς είναι η συχνά αυτόματη κατά το άνοιγμα ενός εγγράφου ή ενός μηνύματος ηλεκτρονικής αλληλογραφίας.

Οι μακροιοί όχι μόνο μολύνουν αρχεία στον υπολογιστή του χρήστη, αλλά συχνά διαδίδονται και μέσω του τοπικού δικτύου ή και του Διαδικτύου.

Συχνά έχουν τη δυνατότητα να διαδίδονται αυτόματα μέσω e-mail χωρίς την παρέμβαση του χρήστη. Μάλιστα η συχνή ανταλλαγή ηλεκτρονικής αλληλογραφίας ή και εγγράφων έχει συμβάλλει στην μεγάλη διάδοσή τους.

Παρασιτικοί ιοί

Οι παρασιτικοί ιοί προσκολλώνται σε άλλα εκτελέσιμα προγράμματα. Όταν αυτά εκτελούνται φορτώνεται ο ιός στη μνήμη, ο οποίος στη συνέχεια καλεί το αρχικό πρόγραμμα ώστε να κρύψει την παρουσία του. Ο ιός γενικά γίνεται αντιληπτός μόνο από τις παρενέργειές του, αν ένας ιός δεν έχει κάποιες παρενέργειες μπορεί να αντιγράφει τον εαυτό του επί σημαντικό χρονικό διάστημα χωρίς να γίνει αντιληπτός από το χρήστη.

Συνδυαστικοί ιοί

Οι συνδυαστικοί ιοί χρησιμοποιούν μια πληθώρα τεχνικών με σκοπό την διάδοσή τους. Μεταξύ άλλων στέλνουν αυτόματα τον εαυτό τους μέσω ηλεκτρονικού ταχυδρομείου, εκμεταλλεύονται προβλήματα ασφαλείας του λειτουργικού συστήματος για να μολύνουν αυτόματα μεγάλα σύνολα υπολογιστικών συστημάτων, δημιουργούν μια πληθώρα μηχανισμών αυτόματης εκτέλεσης κατά την εκκίνηση του λειτουργικού συστήματος και φυσικά έχουν διάφορες ανεπιθύμητες παρενέργειες. Ουσιαστικά αυτοί οι ιοί συνδυάζουν τις τεχνικές των μακρο-ιών και των παρασιτικών ιών και χρησιμοποιούν την υποδομή του Διαδικτύου ώστε να μολύνουν σε διάστημα λίγων ημερών από την εμφάνισή τους εκατομμύρια υπολογιστικών συστημάτων ανά τον κόσμο.

Spyware

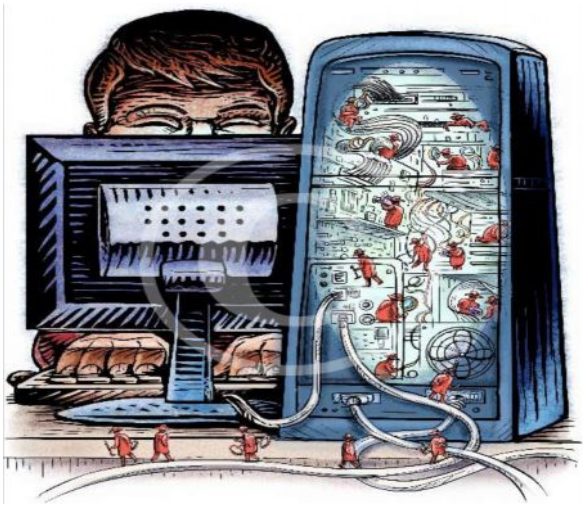
Με τον όρο **Spyware (Λογισμικό Κατασκοπίας)** αναφερόμαστε σε ένα είδος κακόβουλου λογισμικό το οποίο φορτώνεται κρυφά (με ύπουλο τρόπο) σε έναν υπολογιστή χωρίς να το ξέρει ο χρήστης και εκτελείται στο παρασκήνιο κάνοντας διάφορα πράγματα πίσω από την πλάτη του χρήστη. Το Spyware κρύβεται ώστε να μην μπορεί το θύμα να τον εντοπίσει εύκολα, συγκεντρώνει στοιχεία σχετικά με το χρήστη (ιστοσελίδες που επισκέπτεται, κωδικούς πρόσβασης, ακόμη και αριθμούς πρόσβασης πιστωτικών καρτών). Επίσης αλλάζει ρυθμίσεις και εκτελεί άλλες κακόβουλες και ενοχλητικές δραστηριότητες.

Κατηγορίες Spyware

Μάρκετινγκ, στο οποίο συλλέγει πληροφορίες και τις στέλνει στον κύριό του, συνήθως με σκοπό την καλύτερη στόχευση της διαφήμισης σε συγκεκριμένες μηχανές.

Παρακολούθησης, όπου η εταιρείες τοποθετούν εσκεμμένα λογισμικό κατασκοπίας στις μηχανές των υπαλλήλων ώστε να παρακολουθούν τι κάνουν και ποιες τοποθεσίες Ιστού επισκέπτονται.

Η τρίτη κατηγορία πλησιάζει το κλασικό κακόβουλο λογισμικό, όπου η μολυσμένη μηχανή γίνεται τμήμα μίας στρατιάς ζόμπι.



Τρόποι εξάπλωσης spyware

- Με την εγκατάσταση προγραμμάτων: Συνήθως με προγράμματα ανταλλαγής αρχείων (peer-to-peer π.χ. το Kazaa)
- Με την εγκατάσταση πρόσθετων (Add-ons): Τα Add-ons είναι προγράμματα που ενισχύουν τον browser. Μπορεί να είναι γραμμές εργαλείων, κουμπιά αναζήτησης, κινούμενες εικόνες κλπ.
- Με την επίσκεψη σε δικτυακούς τόπους: Μερικοί δικτυακοί τόποι προσπαθούν να κατεβάσουν και να εγκαταστήσουν αυτόματα στον υπολογιστή σας spyware.

Τι κάνει το Spyware

1. Αλλαγή της αρχικής σελίδας του browser
2. Τροποποίηση της λίστας αγαπημένων (σελιδοδεικτών) του browser
3. Προσθήκη νέων γραμμών εργαλείων στο browser
4. Εμφανίζουν συνεχώς παράθυρα με ανεπιθύμητες διαφημίσεις
5. Ξεκινάνε μαζί με τον υπολογιστή κατά την εκκίνηση του και πιάνουν μνήμη και υπολογιστική ισχύ.
6. Το spyware κάποιες φορές απενεργοποιεί το firewall, αφαιρεί ανταγωνιστικό λογισμικό κατασκοπίας και εκτελεί άλλες κακόβουλες ενέργειες.

Τα πρώτα τρία στοιχεία αλλάζουν τη συμπεριφορά του browser, με τέτοιο τρόπο ώστε ακόμη κ η επανεκκίνηση του συστήματος δεν επαναφέρει τις προηγούμενες τιμές. Η επίθεση αυτή είναι γνωστή ως **πειρατεία φυλλομετρητή (browser hijacking)**.

Dialers

Οι dialers είναι μια υποκατηγορία των κακόβουλων προγραμμάτων spyware που είναι σχεδιασμένα με σκοπό να υποκλέπτουν σημαντικές πληροφορίες (κωδικοί πρόσβασης, αριθμοί πιστωτικών καρτών, στοιχεία λογαριασμών κλπ) για τον χρήστη, χωρίς τη γνώση και έγκρισή του. Σκοπός των δημιουργών προγραμμάτων spyware είναι η προσκόμιση πολλών χρημάτων εύκολα και γρήγορα. Οι dialers αλλάζουν τις ρυθμίσεις του δικτύου μέσω τηλεφώνου (dial up networking) ώστε να υποχρεώσουν το χρήστη να καλεί έναν συγκεκριμένο άγνωστο σε αυτόν αριθμό που είθισται να είναι διεθνής κλήση με υψηλό κόστος. Στη συνέχεια προχωρούν στη διαγραφή του αριθμού του παρόχου υπηρεσιών διαδικτύου (ISP) που χρησιμοποιεί ο χρήστης και τον αντικαθιστούν με τον δικό τους πάροχο. Με αυτόν τον τρόπο κάθε φορά που ο χρήστης συνδέεται στο διαδίκτυο χρησιμοποιεί τον αριθμό του dialer και όχι τον αριθμό του δικού του παρόχου υπηρεσιών διαδικτύου.

Λογική βόμβα

Οι λογικές βόμβες είναι μικρά προγράμματα που προστίθενται σε κάποιο υπάρχον πρόγραμμα ή τροποποιούν κάποιον υπάρχοντα κώδικα. Ονομάζονται έτσι λόγω του

γεγονότος ότι είναι προγραμματισμένες να «εκραγούν» ηλεκτρονικά κάτω από ορισμένες προϋποθέσεις. Η λογική βόμβα προστίθεται στο πρόγραμμα από χρήστη ο οποίος έχει πρόσβαση στο σύστημα και φυσικά την απαιτούμενη γνώση για την εγκατάσταση της. Είναι περισσότερο επικίνδυνες από τα σκουλήκια και τους δούρειους ίππους γιατί κατασκευάζονται ευκολότερα και έχουν δυνατότητα να προκαλέσουν σοβαρές ζημιές ακόμα και καταστροφές σε σωσμένα αρχεία αλλά και σε ολόκληρο το λογισμικό ενός ηλεκτρονικού υπολογιστή.

Rootkits

Τα rootkits είναι ένα σύνολο εργαλείων και υπηρεσιών που ο χάκερ μπορεί να χρησιμοποιήσει για να διατηρήσει την πρόσβαση του στο σύστημα που έχει χακάρει από τη στιγμή που θα εισβάλει σε αυτό. Τα εργαλεία του rootkit θα του επιτρέψουν να αναζητήσει ονόματα χρηστών και κωδικούς πρόσβασης, να εξαπολύσει επιθέσεις κατά συστημάτων από απόσταση και να αποκρύψει τις δράσεις του με την απόκρυψη αρχείων και την διαγραφή κάθε δραστηριότητας από τα αρχεία καταγραφής του συστήματος.Μια και με το rootkit αποκτά πρόσβαση, μπορεί να κάνει σχεδόν ότι θέλει, έχοντας δικαιώματα διαχειριστή, παραδείγματος χάριν, να ελέγξει την κίνηση, την πληκτρολόγηση, να επιτίθεται σε άλλους υπολογιστές στο δίκτυο, ή να δημιουργήσει κερκόπορτες συστήματος για την εξυπηρέτηση των εισβολέων.

Ransomware

Είναι μια κατηγορία κακόβουλου λογισμικού, το οποίο από απόσταση κρυπτογραφεί δεδομένα του χρηστή και για να τα αποκρυπτογραφήσει απαιτεί «λύτρα».

Bots – zombies

Μία «bot» είναι ένα είδος κακόβουλου λογισμικού που επιτρέπει σε έναν εισβολέα να αποκτήσει τον πλήρη έλεγχο πάνω στον «πληγέντα» υπολογιστή. Οι υπολογιστές που έχουν μολυνθεί με bot γενικά αναφέροντα ως ζόμπι. Υπάρχουν κυριολεκτικά χιλιάδες υπολογιστές στο Ιντερνετ που έχουν μολυνθεί με κάποιο είδος bot και δεν το συνειδητοποιούν ακόμα. Συχνά ο ιδιοκτήτης δεν γνωρίζει ότι έχει εξαπολύσει έναν ιό ή εγκαταστήσει έναν δούρειο ίππο ο οποίος ενεργοποιεί τον υπολογιστή να λειτουργήσει σαν ένα Zombie. Ο εισβολέας μπορεί να χρησιμοποιήσει το μολυσμένο υπολογιστή για να επιτεθεί ή να στείλει spam σε άλλους υπολογιστές χωρίς να το ξέρουν οι ιδιοκτήτες τους.

Scareware

Το scareware είναι προγράμματα εξαπάτησης. Γνωστά και ως fraudware, τα οποία τις περισσότερες φορές εμφανίζονται με τη μορφή pop-up παραθύρων, με σκοπό να εκφοβίσουν τους χρήστες του διαδικτύου (π.χ. προειδοποιώντας τους ότι ο υπολογιστής τους έχει μολυνθεί με κακόβουλο λογισμικό) και να τους πείσουν να προβούν στην αγορά ή/και εγκατάσταση συγκεκριμένου λογισμικού που υποτίθεται πως θα τους προστατέψει από επιθέσεις και απειλές.

Βακτήρια (bacteria)

Τα βακτήρια (bacteria) είναι προγράμματα που δεν καταστρέφουν εμφανώς αρχεία. Ο μοναδικός τους σκοπός είναι να πολλαπλασιάζονται. Ένα τυπικό βακτήριο μπορεί να μην κάνει τίποτε περισσότερο από το να τρέχει ταυτόχρονα δύο αντίγραφά του σε ένα πολυπρογραμματιζόμενο σύστημα ή πιθανόν να δημιουργεί δύο νέα αρχεία, καθένα απ' τα οποία είναι αντίγραφο του αρχικού αρχείου που περιέχει το βακτήριο. Και τα δύο αυτά προγράμματα μπορούν στη συνέχεια να αντιγράψουν τον εαυτό τους δύο φορές κ.ο.κ. Τα βακτήρια αναπαράγονται εκθετικά και τελικά καταλαμβάνουν όλη τη χωρητικότητα του επεξεργαστή, της μνήμης ή του δίσκου, στερώντας τους πόρους αυτούς από τους χρήστες.

Απάτη με τη Νιγηριανή Επιστολή

Η Νιγηριανή απάτη είναι μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) που περιέχουν πλασματικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεάζοντας τους με τεράστια κέρδη. Ο αποστολέας-απατεώνας συστήνεται ως ένα σημαντικό πρόσωπο του καθεστώτος της

Νιγηρίας (συνήθως ως κάποιος υψηλόβαθμος αξιωματούχος ή στέλεχος κρατικής εταιρίας). Επικαλούμενος κυρίως λόγους πολιτικής φύσεως, ο δράστης ζητάει τη βοήθεια του θύματος-παραλήπτη της επιστολής, προκειμένου να διοχετεύσει εκτός χώρας (Νιγηρίας) κάποιο τεράστιο χρηματικό ποσό. Με άλλα λόγια το ανυποψίαστο θύμα καλείται να διευκολύνει το δράστη λειτουργώντας ως αποδέκτης του ποσού έτσι ώστε να γίνει δεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός Νιγηρίας. Για τη βοήθεια που θα προσφέρει θα ανταμειφτεί με προμήθεια ένα σημαντικό χρηματικό ποσό. Όταν το σύνολο του ποσού θα έχει μεταφερθεί στον τραπεζικό λογαριασμό του υποψήφιου θύματος τότε υποτίθεται ότι έναντι μιας υψηλής προμήθειας θα πρέπει να το παραδώσει στον αποστολέα του e-mail. Αρχικά αυτό που ζητείται είναι η συγκατάθεση του παραλήπτη του e-mail και η παροχή πληροφοριών σχετικών με τους τραπεζικούς λογαριασμούς του και άλλων στοιχείων που θα

βοηθούσαν στην πραγματοποίηση της συναλλαγής. Η επόμενη φάση της απάτης ξεκινάει από τη στιγμή που κάποιος αποφασίζει να απαντήσει στην αρχική προσφορά και έτσι να την αποδεχτεί. Ξεκινάει λοιπόν, μια διαδικασία ανταλλαγής επιστολών και υπογραφή κάποιου συμφωνητικού μέσω fax ή ταχυδρομείου. Το θύμα έχει αρχίσει να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του χρηματικού ποσού. Στην πορεία και μετά την αποστολή των χρημάτων από την πλευρά του θύματος, θα διακοπεί η επικοινωνία με το δράστη. Υπάρχει επίσης και η ΠΕΡΙΠΤΩΣΗ που ο δράστης γνωρίζοντας τα στοιχεία της ταυτότητας του θύματος να χρεώνει τον τραπεζικό του λογαριασμό με υπέρογκα ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης

«419», από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν.

Επιθέσεις Άρνησης Εξυπηρέτησης(DoS, Denial of Service)

Οι επιθέσεις άρνησης εξυπηρέτησης (DoS), είναι ηλεκτρονικές επιθέσεις ενός εισβολέα ο οποίος προσπαθεί να υπερφορτώσει ή να σταματήσει τη λειτουργία μιας υπηρεσίας δικτύου, για παράδειγμα ενός διακομιστή ιστοσελίδας(web server) ή ενος διακομιστή ρχείων(file server). Ο υπολογιστής- θύμα για ένα χρονικό διάστημα, δεν είναι σε θέση να εξυπηρετήσει αιτήσεις από άλλους χρήστες, λόγω του τεράστιου πλήθους των «ψεύτικων» αιτήσεων που δέχεται από τον επιτιθέμενο. Οι επιθέσεις άρνησης εξυπηρέτησης επηρεάζουν άμεσα τις επιδόσεις του δικτύου (κάνοντας τες σαφώς χαμηλότερες έως και μηδενικές) καθώς επίσης την ακεραιότητατων δεδομένων και τη γενικότερη λειτουργία του συστήματος. Οι βασικότεροι στόχοι που επιτυγχάνονται με τις επιθέσεις άρνησης εξυπηρέτησης είναι:

• Η παρεμπόδιση της μετάδοσης δεδομένων στο δίκτυο.

• Η αδυναμία σύνδεσης μεταξύ δύο σημείων, με άμεση συνέπεια τη μη πρόσβαση σε συγκεκριμένες υπηρεσίες.

• Υποβάθμιση της ποιότητας των προσφερόμενων υπηρεσιών στους χρήστες.

Ποιοι είναι οι τρόποι μετάδοσης;

1. Από μολυσμένο αποθηκευτικό μέσο (δισκέτα, cd, flash disk κ.λπ.)
2. Από εκτέλεση ή άνοιγμα μολυσμένων αρχείων του υπολογιστή
3. Από εκτέλεση ή άνοιγμα μολυσμένων αρχείων που επισυνάπτονται σε μηνύματα ηλεκτρονικής αλληλογραφίας
4. Από άνοιγμα ή ανάγνωση αγνώστων μηνυμάτων ηλεκτρονικής αλληλογραφίας που περιέχουν καταστροφικό κώδικα (malicious code)
5. Από άνοιγμα ή ανάγνωση μολυσμένων ιστοσελίδων .htm και .html

Τρόπος κατάργησης λογισμικού κακόβουλης λειτουργίας όπως ιούς, λογισμικό κατασκοπίας ή παραπλανητικό λογισμικό ασφαλείας

Η κατάργηση ενός ιού υπολογιστή ή ενός λογισμικού κατασκοπίας μπορεί να είναι δύσκολη χωρίς τη βοήθεια εργαλείων αφαίρεσης κακόβουλου λογισμικού. Ορισμένοι ιοί υπολογιστών και άλλα ανεπιθύμητα λογισμικά επανεγκαθίστανται από μόνα τους, μετά από τον εντοπισμό και την κατάργηση των ιών και του λογισμικού κατασκοπίας. Ευτυχώς, ενημερώνοντας τον υπολογιστή και χρησιμοποιώντας εργαλεία αφαίρεσης κακόβουλου λογισμικού, μπορείτε να καταργήσετε μόνιμα το ανεπιθύμητο λογισμικό.

Πώς μπορώ να διαπιστώσω εάν ο υπολογιστής μου έχει ιό;

Είναι η λειτουργία του υπολογιστή σας πολύ αργή; Ένα κοινό σύμπτωμα μόλυνσης από ιό είναι η σημαντικά πιο αργή από το κανονικό λειτουργία του υπολογιστή. Ωστόσο, για τη χαμηλή ταχύτητα ενδέχεται να υπάρχουν άλλα αίτια, συμπεριλαμβανομένης της ανάγκης ανασυγκρότησης του σκληρού δίσκου, της απαίτησης του υπολογιστή για περισσότερη μνήμη (RAM) ή της ύπαρξης λογισμικού υποκλοπής spyware ή λογισμικού ανεπιθύμητων διαφημίσεων (adware). Για περισσότερες πληροφορίες σχετικά με το λογισμικό υποκλοπής spyware, ανατρέξτε στο θέμα.

Λαμβάνετε μη αναμενόμενα μηνύματα ή κάποια προγράμματα εκκινούνται αυτόματα; Ορισμένοι ιοί μπορούν να προκαλέσουν βλάβες στα Windows ή σε κάποια προγράμματά σας. Στα αποτελέσματα των βλαβών αυτών ενδέχεται να συμπεριλαμβάνεται η απροσδόκητη εμφάνιση μηνυμάτων, η αυτόματη εκκίνηση ή κλείσιμο προγραμμάτων ή ο ξαφνικός τερματισμός λειτουργίας των Windows.

Λειτουργεί για υπερβολικά μεγάλα χρονικά διαστήματα το μόντεμ ή ο σκληρός σας δίσκος; Ένας ιός ηλεκτρονικού ταχυδρομείου λειτουργεί αποστέλλοντας πολλά αντίγραφα του εαυτού του μέσω ηλεκτρονικού ταχυδρομείου. Μια ένδειξη ότι συμβαίνει αυτό είναι η συνεχώς αναμμένη φωτεινή ένδειξη δραστηριότητας στο μόντεμ ευρείας ζώνης ή στο εξωτερικό μόντεμ, ενώ μια άλλη ένδειξη είναι η συνεχής λειτουργία του σκληρού δίσκου του υπολογιστή σας. Αυτά δεν είναι πάντοτε συμπτώματα ιού υπολογιστή, αλλά όταν συνδυάζονται με άλλα προβλήματα μπορεί να υποδεικνύουν μόλυνση από ιό.

Για να πραγματοποιήσετε έλεγχο για ιούς, πραγματοποιήστε σάρωση του υπολογιστή με ένα πρόγραμμα προστασίας από ιούς. Νέοι ιοί εμφανίζονται καθημερινά, συνεπώς είναι σημαντικό να διατηρείτε ενημερωμένο το πρόγραμμα προστασίας από ιούς.

Ο πρώτος ιός υπολογιστή

Ο πρώτος ιός υπολογιστών εμφανίσθηκε στα μέσα της δεκαετίας του 1980 και ήταν δημιούργημα δύο Πακιστανών ονόματι Basit και Amjad Alvi, οι οποίοι όταν ανακάλυψαν ότι το πρόγραμμα για υπολογιστή (λογισμικό) που είχαν δημιουργήσει αντιγραφόταν παράνομα από κάποιους άλλους, αποφάσισαν να δημιουργήσουν ένα μικρό προγραμματάκι το οποίο αντέγραφε τον εαυτό του και εμφάνιζε ένα προειδοποιητικό μήνυμα copyright σε κάθε παράνομο αντίγραφο που έκαναν οι πελάτες τους. Για την ιστορία, ο ιός έμεινε γνωστός με το όνομα Brain.

Γνωστοί ιοί

Γνωστοί ιοί υπολογιστών που άφησαν εποχή ήταν ο Melissa, ο Michelangelo (διέγραφε τον σκληρό δίσκο όταν η ημερομηνία του υπολογιστή έδειχνε 6 Μαρτίου), ο I Love You,

oSlammer, ο Chernobyl (διέγραφε το BIOS όταν η ημερομηνία του υπολογιστή έδειχνε 26 Απριλίου), ο Blaster, ο MyDoom, ο Jerk, ο Yankee, ο LoveLet-A, ο NightShade (κλείδωνε με κωδικό τα αρχεία που δουλεύουμε όταν η ημερομηνία του υπολογιστή έδειχνε Παρασκευή και 13) κ.ά.

Το 1988 ο φοιτητής Robert Morris δημιούργησε το πρώτο worm, που έφερε το όνομά του, και κατάφερε να μολύνει σχεδόν το 10% των συνδεδεμένων στο Internet υπολογιστών. Ο ιός Michelangelo έκανε την εμφάνισή του το 1992, ήταν ο πρώτος ιός που απέκτησε μεγάλη δημοσιότητα και ανάγκασε τις εταιρείες να δημιουργήσουν προγράμματα antivirus.

Το 2002 αμερικανικό δικαστήριο καταδίκασε σε φυλάκιση 20 μηνών τον David Smith, τον δημιουργό του ιού Melissa. Ήταν από τους πρώτους ιούς που μεταδιδόταν μέσω μηνυμάτων e-mail με τη μορφή ενός συνημμένου αρχείου Word και προξένησε ζημιές εκατομμυρίων δολαρίων. Ο ιός δημιουργήθηκε το έτος 1999. Αν ο χρήστης έκανε το λάθος να ανοίξει το επισυναπτόμενο αρχείο, ο ιός ενεργοποιείτο, αναπαρήγαγε τον εαυτό του και έστελνε ένα ανάλογο μήνυμα στους πρώτους 50 παραλήπτες που έβρισκε στο βιβλίο διευθύνσεων (address book) του θύματος. Η ποινή θεωρήθηκε ελαστική καθώς συνεκτιμήθηκε η προσφορά του δράστη στην ανίχνευση και τον εντοπισμό άλλων ιών.

Ο ιός I Love You εξαπλώθηκε ταχύτατα το έτος 2000 σ' όλον τον κόσμο και προκάλεσε μεγάλη αναστάτωση και κινητοποίηση. Ως δράστης συνελήφθη ένας 23χρονος από τις Φιλιππίνες, ο οποίος ισχυρίσθηκε ότι δεν δημιούργησε τον ιό αλλά ότι απλά τον βελτίωσε. Ο ιός αυτός έδειξε μια ιδιαίτερη προτίμηση σε αρχεία πολυμέσων τύπου .jpg, .mpeg και .mp3 και εκτιμάται ότι προκάλεσε ζημιές ύψους 8-10 δισ. δολαρίων σ' ολόκληρο τον κόσμο.

Ιος σε site κοινωνικής δικτύωσης - Koobface

Koobface είναι ένα πολυ-πλατφόρμα ιό τύπου worm που είχαν αρχικά προβλεφθεί χρήστες των ιστοσελίδων δικτύωσης όπως το Facebook , το Skype , Yahoo Messenger και το e-mail ιστοσελίδες όπως το Google Mail , το Yahoo Mail και AOL Mail , MySpace, hi5 , Bebo , Friendster και το Twitter. Στις νεότερες εκδόσεις έχει σταματήσει τη χρήση αυτών δικτυακό τόπο, διότι η βελτίωση της προστασίας τους. Koobface έχει σχεδιαστεί για να μολύνει τα Microsoft Windows και Mac OS X , αλλά επίσης μπορεί να μολύνει το Linux.

Μόλυνση

Koobface επιχειρεί τελικά, μετά την επιτυχή μόλυνση, για να συγκεντρώσει τα στοιχεία σύνδεσης για FTP sites, το Facebook, το Skype και άλλες κοινωνικές πλατφόρμες μέσων μαζικής ενημέρωσης, αλλά όχι οποιαδήποτε ευαίσθητα οικονομικά στοιχεία.Στη συνέχεια, χρησιμοποιεί υπολογιστές που έχουν δεχτεί να οικοδομήσουμε ένα peer-to-peer botnet . Α κίνδυνο επαφές υπολογιστή άλλους σε κίνδυνο υπολογιστές να λαμβάνουν εντολές σε μια μόδα peer-to-peer. Το botnet χρησιμοποιείται για την εγκατάσταση πρόσθετων pay-per-install malware σε κίνδυνο υπολογιστή, καθώς και αεροπειρατείας ερωτήματα αναζήτησης για την εμφάνιση διαφημίσεων. Peer-to-peer τοπολογία του είναι, επίσης, χρησιμοποιείται για την επίδειξη πλαστά μηνύματα σε άλλους χρήστες με σκοπό την επέκταση του botnet. Εντοπίστηκε για πρώτη φορά τον Δεκέμβριο του 2008 και μια πιο ισχυρή έκδοση εμφανίστηκε το Μάρτιο του 2009. Μια μελέτη από το Information Warfare Monitor , μια κοινή συνεργασία από την Ομάδα SecDev και το Εργαστήριο Πολίτη στη Σχολή Munk των Διεθνών Υποθέσεων στο Πανεπιστήμιο Τορόντο, αποκάλυψε ότι οι φορείς εκμετάλλευσης του εν λόγω καθεστώτος έχουν δημιουργήσει πάνω από 2.000.000 δολάρια σε έσοδα από Ιούνιος 2009 - Ιούνιος 2010.

Koobface αρχικά εξαπλώθηκε με την παράδοση Facebook μηνύματα στους ανθρώπους που είναι «φίλοι» ενός χρήστη του Facebook οποίου ο υπολογιστής έχει ήδη μολυνθεί. Κατά την παραλαβή, το μήνυμα κατευθύνει τους παραλήπτες σε μία ιστοσελίδα τρίτων (ή άλλο Koobface μολυσμένα PC), όταν σας ζητηθεί να κατεβάσετε ό, τι ισχυρίζεται για να είναι μια ενημερωμένη έκδοση του Adobe Flash player. Αν κατεβάσετε και να εκτελέσετε το αρχείο, Koobface είναι σε θέση να μολύνει το σύστημά τους. Μπορεί να επιτάξει στη συνέχεια, αναζητήστε τη χρήση του υπολογιστή του κινητήρα και να την κατευθύνουν σε μολυσμένες ιστοσελίδες. Μπορεί επίσης να υπάρχουν συνδέσεις με την ιστοσελίδα τρίτων στον τοίχο του Facebook του φίλου το μήνυμα προήλθε από, μερικές φορές έχοντας σχόλια όπως LOL ή το YouTube. Αν ο σύνδεσμος

ανοίγει ο ιός trojan θα μολύνει τον υπολογιστή και ο υπολογιστής θα γίνει ένα ζόμπι ή κεντρικό υπολογιστή.

Μεταξύ των συνιστωσών κατεβάσει από Koobface είναι ένας DNS φίλτρο πρόγραμμα που εμποδίζει την πρόσβαση σε γνωστές ιστοσελίδες ασφαλείας και ένα proxy εργαλείο που επιτρέπει στους επιτιθέμενους να κάνουν κατάχρηση του μολυσμένου υπολογιστή. Σε ένα χρόνο η συμμορία Koobface που χρησιμοποιείται, επίσης, Limbo , ένα κωδικό πρόσβασης κλέβει πρόγραμμα.

Αρκετές παραλλαγές του worm έχουν εντοπιστεί:

Worm:! Win32/Koobface.gen F

Net-Worm.Win32.Koobface.a, η οποία επιτίθεται MySpace

Net-Worm.Win32.Koobface.b, η οποία επιτίθεται Facebook

WORM_KOOBFACE.DC, η οποία επιτίθεται Twitter

W32/Koobfa-Gen, η οποία επιτίθεται στο Facebook , MySpace , hi5 , Bebo , Friendster , MyYearbook, Tagged, Netlog, Badoo και fubar

W32.Koobface.D

OSX / Koobface.A, ένα Mac έκδοση που εξαπλώνεται μέσω των κοινωνικών δικτύων όπως το Facebook, το MySpace και το Twitter.

Τον Ιανουάριο του 2012, οι *New York Times* ανέφεραν ότι το Facebook είχε την πρόθεση να ανταλλάσσουν πληροφορίες σχετικά με τη συμμορία Koobface, και ονομάστε αυτά που πίστευε ήταν υπεύθυνοι. Έρευνες από το Γερμανό ερευνητή Jan Droemer - και το Πανεπιστήμιο της Αλαμπάμα στο κέντρο του Μπέρμιγχαμ για τη διασφάλιση πληροφοριών και κοινή έρευνα ιατροδικαστικών ειπώθηκαν για να έχουν βοηθήσει αποκαλύψει τις ταυτότητες των υπευθύνων.

Facebook αποκάλυψε τελικά τα ονόματα των υπόπτων πίσω από το σκουλήκι στις 17 Ιανουαρίου 2012. Περιλαμβάνουν Stanislav Avdeyko (leDed) , **Alexander Koltyshev (Floppy)**, **Anton Korotchenko (KrotReal)** , **Roman Π. Koturbach (PoMuc)** , **Svyatoslav E. Polichuck (PsViat και PsycoMan)** . Τα πρότυπα αυτά βασίζονται στην Αγία Petersburg ,Ρωσία . Η ομάδα είναι μερικές φορές αναφέρεται ως Ali Baba & 4 με Stanislav Avdeyko ως ηγέτης. Η έρευνα συνδέεται επίσης με Avdeyko CoolWebSearch spyware.

Ο γνωστός Ιός της Αστυνομίας

Ήδη από το πρώτο τρίμηνο του 2012 καταγράφεται σημαντική αύξηση του επιθέσεων σε υπολογιστές για λύτρα, του επονομαζόμενου ransomware, μας ενημερώνουν τα Panda Labs.

Ο ιός, γνωστός ως Police Virus ή «Ιός της Αστυνομίας» εμφανίζει μηνύματα με τα σήματα των υπηρεσιών επιβολής του νόμου (αστυνομία, οργανώσεις κλπ). Έτσι, επιχειρείται να ξεγελαστεί ο χρήστης και να πιστέψει ότι ο υπολογιστής του έχουν «κλειδωθεί» από την

αστυνομία -πράγματι, μπλοκάρεται. Το μήνυμα γράφει ότι ο υπολογιστής κλειδώθηκε επειδή χρησιμοποιήθηκε για επισκέψεις σε «ακατάλληλες» ιστοσελίδες ή το κατέβασμα «πειρατικού» υλικού, δύο μάλλον κοινά «αμαρτήματα» που μπορεί να καταστήσουν το μήνυμα δικαιολογημένο.

Πως μπορώ να δημιουργήσω έναν ιό

Πηγαίνετε στο site :

http://www.insomnia.gr/topic/313118-%CF%86%CF%84%CE%B9%CE%AC%CE%BE%CF%84%CE%B5-%CF%84%CF%81%CE%BF%CE%BC%CE%B1%CE%BA%CF%84%CE%B9%CE%BA%CE%BF%CF%8D%CF%82-%CE%B9%CE%BF%CF%8D%CF%82-d/

BLASTER VIRUS

1. Δεξί click στο Desktop > New > Shortcut
2. Γράψε μέσα το ακόλουθο:

shutdown -s -t 600 -c "This is a Virus. THis Virus can erase all data on your Hard Disk."

Next

4. Βάλτε το όνομα p.x Music
5. Δεξί click στο εικονίδιο που φτιάξατε > Properties (ιδιότητες στα ελληνικά windows)
5. Change Icon > και βάλτε μια εικόνα που ταιριάζει με το όνομα που του δώσατε προηγούμενος p.x. σε σχέση με μουσική

Για να σταμάτησε πηγαίνετε στο start > run > και γράψτε το ακόλουθο:

shutdown -a

HACKER VS CRACKERS

Τρόπος που λειτουργούν οι hacker

Όπως είχαμε δει σε παλαιότερο άρθρο, υπάρχουν 2 είδη hackers οι άσπροι (whitehats) και οι μαύροι (blackhat). Ανεξάρτητα με το σκοπό τους, λειτουργούν με παρόμοιους τρόπους. Βέβαια, δεν υπάρχει σχολή hackers. Ο καθένας μαθαίνει μόνος του και οι γνώσεις τους ποτέ δεν είναι ίδιες.

Με ποιους τρόπους κάνουν επίθεση

Πέρα από τις τεχνικές γνώσεις, οι άνθρωποι αυτοί έχουν και κοινωνικές δεξιότητες. Ένας καλός hacker πρέπει να μην μοιάζει με αυτό που είναι, να περνάει την εντύπωση ότι είναι έμπιστο άτομο και να συμπεριφέρεται έξυπνα. Ο πιο γνωστός hacker όλων των εποχών Kevin Mitnick, στο βιβλίο του Η τεχνική της Απάτης (The art of deception), αναφέρει ελάχιστα πράγματα για υπολογιστές. Αναφέρει όμως, πώς ένα άτομο μπορεί να αποσπάσει πληροφορίες με την παρατήρηση και με μεθόδους κοινωνικής μηχανικής.

Τι εργαλεία χρησιμοποιούν

Προστασία από τους hacker δεν μας προσφέρει ένα καλό firewall ούτε ένα antivirus. Ο πραγματικός hacker θα φτιάξει τα εργαλεία που θα σου κάνει επίθεση μόνος του. Αυτό θα τα κάνει μη-εντοπίσημα από προγράμματα ασφάλειας. Επίσης, πολύ πιθανό είναι να έρθει σε προσωπική επαφή μαζί σου για να σου αποσπάσει, φαινομενικά άχρηστες πληροφορίες. Αυτό μπορεί να το κάνει με την πραγματική του εμφάνιση ή με κάποιο ψεύτικο προφίλ σε σελίδες κοινωνικής δικτύωσης (facebook, email κτλ).

Πράγματα που ίσως θέλει να μάθει ένας hacker είναι λεπτομέρειες από την παιδική σου ηλικία, ο τρόπος με τον οποίο γράφεις στον υπολογιστή, το user name που έχεις σε λογαριασμούς σου, ακόμα και το πως συνηθίζεις να οργανώνεις τα αρχεία σου στον υπολογιστή. Αυτές οι πληροφορίες, μαζί ίσως με άλλες, μπορούν να δημιουργήσουν ένα προφίλ για σένα, το οποίο θα χρησιμοποιηθεί για να σπάσει η ασφάλειά σου.

Πως δραστηριοποιούνται οι crackers

Αντίθετα, οι *crackers (criminal hackers)* 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.

Το hacking είναι ποινικό αδίκημα σε πολλές χώρες καθώς η κοινωνία μας εξαρτάται όλο και περισσότερο από τους υπολογιστές και το Internet και πιο συγκεκριμένα τιμωρείται όποιος αποκτήσει χωρίς εξουσιοδότηση πρόσβαση σε συστήματα πληροφοριών, προκαλέσει ζημιά, αποκομίσει από τις ενέργειές του οικονομικό όφελος ή αποδειχθεί ότι είναι μέλος ενός δικτύου οργανωμένου εγκλήματος.

ΠΕΙΡΑΤΙΚΟ VS ΝΟΜΙΜΟ ΛΟΓΙΣΜΙΚΟΥ

Πειρατεία Λογισμικού

Ο όρος **πειρατεία λογισμικού** αναφέρεται στην αναπαραγωγή ή/και διάθεση

προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους36.

Μορφές πειρατείας λογισμικού

Οι κυριότερες μορφές πειρατείας λογισμικού είναι οι εξής:

1) Χρήση ενός προγράμματος σε περισσότερους υπολογιστές καθ' υπέρβαση της αδείας χρήσης: Είναι η πιο συνηθισμένη μορφή παράνομης χρήσης εφόσον απαιτείται ξεχωριστή άδεια για κάθε υπολογιστή στον οποίο χρησιμοποιείται το ίδιο πρόγραμμα.

εκδηλώνεται δε ως εξής:

α. Με αντιγραφή χωρίς άδεια χρήσης από ιδιώτες ή εταιρίες.

β. Με δήλωση μικρότερου από τον πραγματικό αριθμού εγκαταστάσεων σε μια εταιρεία που διαθέτει άδειες για έναν συγκεκριμένο αριθμό χρηστών υπολογιστών (η άδεια χρήσης παραδίδεται μαζί με το λογισμικό καθώς ορίζεται πως αφορούν σε ένα και μοναδικό εμπόρευμα).

γ. Με δανεισμό προϊόντων λογισμικού μεταξύ φίλων και συνεργατών .

δ. Με διανομή αντιγράφων λογισμικού από τους πωλητές στους πελάτες τους.

Συχνά οι πωλητές υπολογιστών προκειμένου να κάνουν την αγορά ενός υπολογιστή πιο ελκυστική προσφέρουν προγράμματα χωρίς τις άδειες. Έτσι χρειάζεται μεγάλη προσοχή και έλεγχος των αδειών κατά την αγορά υπολογιστή που διαθέτει προεγκατεστημένα προγράμματα. Το λογισμικό αυτό δεν συνοδεύεται από οδηγίες χρήσης ή βοηθητικές δισκέτες για προγράμματα.

2) Πλαστογράφηση ή αλλιώς πλήρης απομίμηση του προϊόντος: Η παράνομη αναπαραγωγή και πώληση λογισμικού με τέτοιο τρόπο ώστε να φαίνεται νόμιμο. Περιλαμβάνει πιστή απομίμηση της συσκευασίας, των λογοτύπων και συχνά των ολογραμμάτων. Το λογισμικό και η συσκευασία του αντιγράφονται με σύνθετες τεχνικές και έπειτα, επαναδιανέμονται ως απομίμηση νόμιμου προϊόντος. Η αυξανόμενη επιλογή του εμπορίου μέσω ιντερνέτ έχει αυξήσει και τις πιθανότητες να βρεθούν οι καταναλωτές αντιμέτωποι με το πρόβλημα της χρήσης

πλαστών προϊόντων. Η όλο και περισσότερο εξελιγμένη τεχνολογία που χρησιμοποιούν οι πλαστογράφοι, καθιστούν ακόμα και τους πιο απαιτητικούς καταναλωτές συχνά ανήμπορους να διακρίνουν το νόμιμο λογισμικό από το πλαστό. Το πλαστό λογισμικό συνήθως κατασκευάζεται και προωθείται με τρόπο ώστε να μοιάζει και να ανταγωνίζεται το αυθεντικό προϊόν.

Site που διακινείται παράνομα λογισμικό

Pirate Bay
Iso Hunt
Kick Ass Torrents
gamato.info
tainiomania.com
Torlock
Seedpeer.me
Vertor

Πλεονεκτήματα χρήσης νόμιμου λογισμικού

- Μπορούμε να τα χρησιμοποιήσουμε νόμιμα,για να παράγουμε και εμείς με τη σειρά μας τη δική μας πνευματική εργασία.
- Έχουμε τεχνική υποστήριξη από τους κατασκευαστές (π.χ. τη ζήτηση βοήθειας από τους κατασκευαστές μέσω e-mail κ.ά.)
- Μας παρέχονται τα απαραίτητα εγχειρίδια χρήσης,για να μάθουμε να χρησιμοποιούμε σωστά το νέο πρόγραμμα.

- Το προϊόν που παίρνουμε είναι ελεγμένο και δοκιμασμένο.
- Είμαστε βέβαιοι ότι το CD ή DVD που κρατάμε στα χέρια μας δεν περιέχει ιούς ή κακόβουλα προγράμματα**.**

Πλεονεκτήματα Peer-2-Peer

1) Είναι εύκολο στην εγκατάσταση και έτσι είναι η διαμόρφωση των υπολογιστών σε αυτό το δίκτυο,

2) Όλα τα μέσα και το περιεχόμενο μοιράζονται σε όλους τους μαθητές, σε αντίθεση με την αρχιτεκτονική server-client όπου τα μερίδια διακομιστή δεν μοιράζονται τα περιεχόμενα και τους πόρους.

3) Δεν υπάρχει ανάγκη για πλήρη απασχόληση διαχειριστή του συστήματος. Κάθε χρήστης είναι ο διαχειριστής της μηχανής του. Ο χρήστης μπορεί να ελέγξει τους κοινόχρηστους πόρους τους.

4) Πάνω από όλα-το κόστος κατασκευής και συντήρησης αυτού του τύπου δικτύου είναι συγκριτικά πολύ λιγότερο.

Αναφορές στον κίνδυνο αποθήκευσης/διαμοιρασμού παράνομου υλικού εν αγνοία του χρήστη

Είναι πλέον κοινή γνώση ότι οι χρήστες αυτών των προγραμμάτων διαμοιρασμού κατεβάζοντας αρχεία από το emule και κάθε αντίστοιχο πρόγραμμα κατεβάζουν και υλικό που δεν έχουν ζητήσει. Όλα τα φόρουμ ανταλλαγής απόψεων πάνω στο θέμα της ανταλλαγής αρχείων μέσω τεχνολογίας P2P αναφέρονται στο θέμα αυτό. Είναι πασίγνωστο και για τον λόγο αυτό επίσημες κρατικές πηγές στο ίντερνετ αναφέρουν συμβουλές προς τους χρήστες τέτοιων προγραμμάτων.

Πώς μένεις ανώνυμος στο ίντερνετ?

Το cryptoparty είναι μια σύναξη στην οποία πηγαίνει όποιος θέλει με το λάπτοπ του ή την ταμπλέτα του και εκπαιδεύεται από ειδικούς στην ασφαλή και ανώνυμη χρήση του Διαδικτύου. Το πρώτο έγινε στη Μελβούρνη και μέσα σε λίγους μήνες η ιδέα εξαπλώθηκε. Ειδικά στη Γερμανία, μετά και τις πρόσφατες αποκαλύψεις περί παρακολουθήσεων, το ενδιαφέρον έχει αυξηθεί - ένα cryptoparty διοργανώθηκε, μάλιστα, και στο Κοινοβούλιο. Σκοπός των ακτιβιστών είναι να μυηθούν όσο το δυνατόν περισσότεροι στην κρυπτογράφηση. Μέχρι πριν από λίγο καιρό οι «καλεσμένοι» ήταν άνθρωποι που έχουν σχέση με υπολογιστές ή νέοι με πολιτικές ανησυχίες. Σιγά-σιγά η σύνθεση αλλάζει, αφού αρκετοί δικηγόροι και δημοσιογράφοι ή επαγγελματίες που διαχειρίζονται ευαίσθητα δεδομένα δείχνουν ενδιαφέρον, ενώ υπάρχουν

και άνθρωποι με συγγενείς σε «δύσκολες» χώρες, όπου καταστρατηγείται το απόρρητο των επικοινωνιών.

Οι δύο ακτιβιστές προσπαθούν να εξηγήσουν ότι καμία online συζήτηση δεν είναι ιδιωτική. Η μυστικότητα δεν υφίσταται στον παγκόσμιο ιστό. «Και αν αυτό δεν σας τρομάζει, διότι γράφετε θεατρικές κριτικές και όχι αποκαλυπτικά ρεπορτάζ, δεν πρέπει να ξεχνάτε πως, όπου μπορούν να παρεισφρήσουν οι μυστικές υπηρεσίες μπορούν και οι απατεώνες», επισημαίνει ο Λάγκινγκ. «Ακόμη και αν κανείς νομίζει πως δεν έχει τίποτα να κρύψει, αυτό το οποίο διακυβεύεται είναι η δημοκρατία. Μπορεί τώρα να μη σας ενδιαφέρει, αλλά τα δεδομένα σας είναι άφθαρτα, αποθηκεύονται και μπορούν να χρησιμοποιηθούν εναντίον σας στο μέλλον», προσθέτει. «Μπορούμε να παρομοιάσουμε τις παρακολουθήσεις με το τσιγάρο ή τη ραδιενέργεια. Μέχρι να πεθάνουν μερικές εκατοντάδες χιλιάδες, δεν ξέραμε τίποτα. Επρεπε να βγουν μελέτες, να μιλήσουν οι επιστήμονες, για να καταλάβουμε τι συμβαίνει και να λάβουμε μέτρα προστασίας», παρεμβαίνει ο Ντικ.

Το ίδιο βράδυ, ένα ακόμη cryptoparty με περίπου 60 καλεσμένους διοργανώνεται στην περιοχή Νόικελν, στο Βερολίνο. Η Λέντσι, ο Νικολάι και ο Ντικ εξηγούν ότι η ασφάλεια στο Διαδίκτυο δεν μπορεί να επιτευχθεί μόνο με μερικές εφαρμογές, αλλά είναι μια διαδικασία, ένας «αγώνας» ανάμεσα σε εκείνους που παρακολουθούν και σε εκείνους που δεν το δέχονται. Δεν δίνουν απαντήσεις, κυρίως θέτουν ερωτήσεις. «Γιατί είναι σημαντική η ιδιωτικότητα; Διότι τα αρχεία μου, οι επαφές μου, οι αναζητήσεις μου, όλα όσα κάνω ή γράφω στον υπολογιστή μου και στο Διαδίκτυο ανήκουν σ' εμένα και σε κανέναν άλλο;» Σκέφτομαι τις πρόσφατες αποκαλύψεις των Anonymous για τις αναζητήσεις στο Google προσώπου της ελληνικής επικαιρότητας: «Βότανο για αιμορροΐδες, κρίση στο γάμο, προβλέψεις ζωδίων, μασάζ αισθησιακό βίντεο...». Αμέσως μετά χωριζόμαστε σε ομάδες, ανάλογα με το τι μας ενδιαφέρει να μάθουμε: ανώνυμη περιήγηση στο Διαδίκτυο, κρυπτογράφηση e-mails και συνομιλιών σε chat. Γίνεται φανερή η ανάγκη χρήσης ελεύθερου λογισμικού όπως και ότι όλες οι κρυπτογραφικές λύσεις έχουν κενά. Τα δε προγράμματα κατά των ιών είναι αμφιβόλου αποτελεσματικότητος. «Ωστόσο, όσο περισσότερα εμπόδια βάζεις στους "κακούς", όποιοι και αν είναι αυτοί, τόσο πιο δύσκολο είναι να τα καταφέρουν».

Ποια είναι η πιο συνηθισμένη μέθοδος παρακολούθησης; «Τα πάντα βασίζονται σε αλγόριθμους: βρες μου όλους όσοι ζουν στο Βερολίνο, είναι Αμερικανοί και γράφουν στα mails τους τις τάδε λέξεις. Οσο πιο καλός ο αλγόριθμος, τόσο καλύτερα τα αποτελέσματα. Βέβαια, αν το τελευταίο διάστημα έχεις επικοινωνήσει μέσω e-mail με τον Στρέμπελε (σημ.: τον Γερμανό πολιτικό των Πρασίνων που συνάντησε τον Σνόουντεν), τότε τη συγκεκριμένη αλληλογραφία είναι βέβαιο ότι θα τη διαβάσει ανθρώπινο μάτι».

Και πώς τα ξέρουμε όλα αυτά; ξαναρωτάω. «Από τα ντοκουμέντα του Σνόουντεν. Δηλαδή τα ξέραμε και πριν, αλλά τώρα αποδείχτηκαν». Η βραδιά συνεχίζεται με επιτυχία και το ενδιαφέρον παραμένει αμείωτο. Οι εθελοντές ειδικοί τα εξηγούν όλα με απλά λόγια και έχουν μεγάλη υπομονή. Μας γίνεται σαφές ότι, όταν χρησιμοποιείς το Facebook ή παρόμοιες εφαρμογές, αλλά και τον τραπεζικό σου λογαριασμό, είναι αδύνατον να είσαι ανώνυμος. Ωστόσο, για όλα υπάρχουν λύσεις. Αποφασίζω να κατεβάσω ένα πρόγραμμα για να λαμβάνω τα e-mails που διατηρώ στο Google και το Yahoo, χωρίς να είμαι εκτεθειμένη στα κενά ασφαλείας των δύο αυτών παρόχων. Παραπονιέμαι στον εθελοντή ότι λατρεύω το Gmail, πως είναι ό,τι πιο φιλικό για τους χρήστες έχω δοκιμάσει, ότι θα μου λείψει και όλα αυτά που προσφέρει είναι εντελώς δωρεάν. «Φυσικά και είναι δωρεάν, αφού του χαρίζεις όλα σου τα δεδομένα... Να σου ζητήσει και χρήματα από πάνω;» με αποστομώνει.

Από Linux μέχρι «κλειδιά» για chat

Γενικός κανόνας: Αποκτάμε συνείδηση ότι ο ηλεκτρονικός κόσμος δεν είναι τόσο ασφαλής όσο παρουσιάζεται. Καλό είναι να ενημερωνόμαστε και να μην εμπιστευόμαστε άκριτα τις ευκολίες που μας παρέχονται: δεν νοείται να είμαστε απλώς πελάτες, οι οποίοι αγοράζουν και καταναλώνουν. Λύσεις υπάρχουν, ακόμη και για αρχάριους, και μάλιστα δωρεάν.

Στο τέλος του πάρτι έχω ανακαλύψει ότι ο υπολογιστής μου είναι γεμάτος ιούς που γνωρίζουν τα passwords μου. Η μόνη λύση είναι να βγάλω τα Windows και να εγκαταστήσω το Linux, το πλέον ασφαλές λογισμικό. «Το χρησιμοποιεί το γερμανικό υπουργείο Εξωτερικών σε

όλους τους υπολογιστές που διαχειρίζονται ευαίσθητα δεδομένα», μου εξηγούν. Ξαφνικά μου έχει κοπεί εντελώς η όρεξη να χρησιμοποιήσω το λάπτοπ. Νιώθω σαν να μπήκαν κλέφτες στο σπίτι μου. «Και γιατί δεν έχουν ήδη καταχραστεί τον τραπεζικό μου λογαριασμό;» θέλω να μάθω. «Ετυχε… Υπάρχουν πολλών ειδών απατεώνες», με διαφωτίζει ο Νικολάι, φοιτητής Ανθρωπολογίας. «Ισως να θέλουν απλώς τη μνήμη του υπολογιστή σου για να ανεβάζουν πορνό ή τη σύνδεσή σου στο Ιντερνετ, για να στέλνουν spam. Ποιος ξέρει τι γίνεται εκεί έξω, στον αχανή παγκόσμιο ιστό;»

1. Εγκαθιστούμε ελεύθερο λειτουργικό Linux. Το κατεβάζουμε από το Διαδίκτυο και, αν είμαστε στοιχειωδώς εξοικειωμένοι, μπορούμε εύκολα να κάνουμε την εγκατάσταση. Δεν έχει «τρύπες», από τις οποίες κάποιος θα εισέλθει στον υπολογιστή μας. Οι ιοί που το απειλούν είναι ελάχιστοι. Το περιβάλλον του, για έναν συνηθισμένο χρήστη, είναι οικείο. Κατόπιν, μπορούμε να κατεβάσουμε ελεύθερα προγράμματα, όπως επεξεργαστές κειμένου ή εικόνας. Συνήθως όλα διατίθενται και στα Ελληνικά. Δοκιμάζουμε το Linux Xubuntu, το οποίο είναι αρκετά εύκολο για αρχάριους.

2. Για να σερφάρουμε ανώνυμα, μπορούμε να κατεβάσουμε το TorProjekt, το οποίο διαθέτει τον Tor browser. Με τον συγκεκριμένο browser, κανείς δεν γνωρίζει το IP μας. Ενα τεστ: Ανοίγουμε τον κανονικό μας browser (π.χ. Explorer, Chrome, Firefox) και πληκτρολογούμε τη διεύθυνση www.wieistmeineip.de. Θα εμφανιστεί το IP και η χώρα μας. Αν ανοίξουμε τον Tor browser και κάνουμε την ίδια διαδικασία, θα δούμε ένα ωραιότατο anonymous. Είναι εξαιρετικά χρήσιμο αν δεν θέλουμε να αποθηκεύονται οι αναζητήσεις μας και όσα διαβάζουμε. Μια άλλη λύση, για να κάνουμε αναζητήσεις ως ανώνυμοι, είναι να χρησιμοποιούμε τις σελίδες https://startpage.com ή https://duckduckgo.com.

3. Τα passwords είναι σαν το κλειδί του σπιτιού μας. Δεν το ξεχνάμε, δεν δίνουμε αντίγραφα, δεν έχουμε το ίδιο για το εξοχικό, το σπίτι, το γραφείο, το αυτοκίνητο, τη θυρίδα. Είναι εξαιρετικά επικίνδυνο να χρησιμοποιούμε το ίδιο password ή δύο-τρία ίδια παντού. Πρόσφατα, χάκερ έκλεψαν από την Adobe περίπου 150 εκατομμύρια συνθηματικά. Οι χρήστες δεν αρκεί να αλλάξουν τον κωδικό τους μόνο στην Adobe. Αν χρησιμοποιούν τον ίδιο και σε άλλα sites και εφαρμογές, τότε οι υποκλοπείς μπορούν να μπουν και εκεί. Passwords όπως τα ονόματα των παιδιών μας ή η ημερομηνία γέννησής μας ή ένα απλό 12345 είναι εξαιρετικά επισφαλή. Κάλλιστα μπορούμε να προσθέσουμε μερικά σύμβολα, όπως &,*,), !.

4. Οι τραπεζικές συναλλαγές είναι πολύ ασφαλείς. Πρόβλημα δημιουργείται όταν έχουμε ιούς οι οποίοι «χρησιμοποιούν» ένα key logger και διαβάζουν τα passwords. Με το Linux, σύμφωνα με τους ακτιβιστές, η πιθανότητα αυτή σχεδόν μηδενίζεται. Μετά την εγκατάστασή του, λοιπόν, καλό θα ήταν να αλλάξουμε όλα τα passwords.

5. Για ακόμη πιο αναβαθμισμένη αυτοπροστασία, μπορείτε να κρυπτογραφείτε τα e-mails και τις συνομιλίες σας στα chat-rooms (προϋποθέτει να κάνει το ίδιο και ο συνομιλητής σας). Κατεβάζετε το Mozilla Thunderbird και το λογισμικό κρυπτογράφησης PGP (Pretty Good Privacy). Η πρόταση των ακτιβιστών είναι να κατεβάσει κανείς το GnuPG (www.gnupg.org) με το οποίο δημιουργείτε τα δικά σας «κλειδιά» και «κλειδώνετε» τα mails σας. Πληροφορίες στο www.cryptography.org/getpgp.htm και -για instant messaging- στο www.jabbim.com. Τέλος, η συμβουλή των ειδικών είναι να έχουμε τον δικό μας e-mail server, δηλαδή να διατηρούμε διευθύνσεις e-mail σε ένα δικό μας domain. Κοστίζει ελάχιστα, πολλές φορές λιγότερο και από 1 ευρώ το μήνα.

6. Βάζουμε όρια! Αντί να πετάξουμε το παλιό μας λάπτοπ, το διαμορφώνουμε μόνοι ή με τη βοήθεια ειδικού και κατόπιν το χρησιμοποιούμε μόνο για συναλλαγές και αγορές. Ετσι, δεν θα στερηθούμε από τον «κανονικό» υπολογιστή μας τα διαδεδομένα εμπορικά λογισμικά και θα έχουμε και έναν εφεδρικό για αγορές και τραπεζικές συναλλαγές.

Επικοινωνία ιών υπολογιστή μέσω ήχου;

Έντονες συζητήσεις στον χώρο της ασφάλειας υπολογιστών έχουν προκαλέσει οι ισχυρισμοί του Ντράγκος Ρούιου, ερευνητή από το Βανκούβερ, ο οποίος και δημοσίευσε στο Ίντερνετ λεπτομέρειες σχετικά με μία υπόθεση που τιτλοφορείται πλέον «badBIOS», καθώς ξεκίνησε ως μια «παράξενη» αναβάθμιση στο BIOS του MacBook Air του.

Κατά τον Ρούιου, μέσα σε διάστημα τριών ετών, οι υπολογιστές του παρουσιάζουν «παράξενη» συμπεριφορά, ακόμα και με το Wi-Fi και το Bluetooth κλειστά και τα καλώδια Ethernet αποσυνδεδεμένα. Ο ίδιος θεωρεί ότι στα συστήματά του υπάρχουν ιοί, οι οποίοι είναι σε θέση να επικοινωνούν μέσω σημάτων υπερήχων, από τον έναν υπολογιστή στον άλλον.

Ο Ρούιου διηγήθηκε την ιστορία του στο Ars Technica, το οποίο αφιέρωσε στην υπόθεση εκτενές δημοσίευμα, υπό τον τίτλο «Meet “badBIOS”, the mysterious Mac and PC malware that jumps airgaps». Σε αυτό περιγράφεται η συνολική του εμπειρία, που πολλές φορές παραπέμπει σε θρίλερ επιστημονικής φαντασίας, με συστήματα τα οποία προβαίνουν σε διαγραφές δεδομένων ή αλλαγές στα settings χωρίς εξήγηση.

Κατά τον ίδιο, τα φαινόμενα έχουν συνεχιστεί μέσα σε διάστημα τριών ετών, παρά όλα τα μέτρα και τις «θεραπείες» που έχει δοκιμάσει: μέσα σε ώρες ή εβδομάδες από τη συνολική διαγραφή/ εκκαθάριση ενός προβληματικού συστήματος, η παράξενη συμπεριφορά κάνει ξανά την εμφάνισή της.

Ο Ρούιου στράφηκε στα κοινωνικά δίκτυα, καθώς και σε άλλους επαγγελματίες του χώρου της ασφάλειας, για να μοιραστεί την εμπειρία του, καθώς και τη θεωρία του, που προσέλκυσε έντονο ενδιαφέρον, καθώς πολλοί την θεωρούν πολύ «τραβηγμένη»: κατά τον ίδιο, το malware μπορεί να μεταδίδεται μέσω USB drives και να μολύνει τα βασικότερα επίπεδα του hardware, επιβιώνοντας από τις προσπάθειες εκκαθάρισής του. Ωστόσο, ακόμα πιο «ακραία» είναι η υπόθεση ότι το συγκεκριμένο malware μπορεί να ενεργοποιείται μέσω του αέρα, ξεπερνώντας το αποκαλούμενο «air gap», μέσω σημάτων υψηλής συχνότητας που προωθούνται μέσω ηχείων και μικροφώνων. Ο ίδιος ανέφερε έναν διαπεραστικό ήχο στο ηχοσύστημά του, το οποίο φαίνεται να προκαλείται από παρεμβολές από υπερήχους που μεταδίδονται μεταξύ ηχείων και μικροφώνων- μεταδόσεις οι οποίες έπαψαν όταν ο ίδιος σταμάτησε τη λειτουργία των μικροφώνων.

«Καταγράψαμε σήματα ήχου υψηλής συχνότητας μεταξύ των υπολογιστών μας και είδαμε τους υπολογιστές μας να αλλάζουν μυστηριωδώς τις ρυθμίσεις τους, ακόμα και όταν δεν είχαν σύνδεση σε δίκτυα, κάρτες Wi-Fi ή Bluetooth. Και τους λειτουργούσαμε με μπαταρίες, έτσι ώστε να μην έχουν καν πρόσβαση στο δίκτυο ηλεκτροδότησης» δήλωσε ο ίδιος στο New Scientist.

Σύμφωνα με την «εξωτική» θεωρία του, το συγκεκριμένο κακόβουλο λογισμικό (το οποίο βαφτίστηκε badBIOS) εγκαταστάθηκε στο hardware, όπου και «κοιμάται» μέχρι να λάβει ηχητικό σήμα και να «ξυπνήσει». Στα «μολυσμένα» συστήματά του δεν έχει βρεθεί κανενός είδους κακόβουλος κώδικας υπολογιστή.

Αν και κάποιοι σπεύδουν να χαρακτηρίσουν τη θεωρία του ως «αστικό θρύλο», ο ίδιος αποτελεί επαγγελματία του χώρου της ασφάλειας υπολογιστών, ο οποίος έχει αρκετά υψηλό προφίλ, ως διοργανωτής των συνδιασκέψεων CanSecWest και PacSec και ιδρυτής του διαγωνισμού hacking Pwn2Own – γενικότερα, θεωρείται αξιόπιστος από πολλούς επαγγελματίες του τομέα. Με το θέμα ασχολούνται πολλοί ειδικοί ασφαλείας, οι απόψεις των οποίων ποικίλλουν, καθώς, εάν τελικά οι θεωρίες του είναι πραγματικότητα θα πρόκειται για ένα λογισμικό το οποίο είναι πιο εξελιγμένο ακόμη και από το «υπερόπλο» Stuxnet, το οποίο χρησιμοποιήθηκε κατά των πυρηνικών εγκαταστάσεων του Ιράν στο Νατάνζ και αποτελεί το μόνο άλλο παράδειγμα malware που μπόρεσε να ξεπεράσει «air gaps» (μέσω USB sticks τα οποία έφτασαν στα χέρια προσωπικού και της εκμετάλλευσης του autorun των Windows).

ΠΩΣ ΝΑ ΠΡΟΣΤΑΤΕΨΩ ΤΟΝ Η/Υ ΜΟΥ

ΒΑΣΙΚΑ ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

Ποια είναι τα κατάλληλα μέτρα προστασίας για τον υπολογιστή μας για να έχουμε ασφαλή πλοήγηση στο διαδίκτυο;

- Διατηρήστε το λειτουργικό σύστημα ενημερωμένο.
- Χρησιμοποιείτε πρόγραμμα προστασίας από τους ιούς.
- Χρησιμοποιείτε τείχος προστασίας.
- Δημιουργείτε αντίγραφα ασφαλείας των σημαντικών αρχείων.
- Προσέχετε όταν κάνετε λήψη περιεχομένου.

Πώς μπορώ να διατηρήσω το λογισμικό μου ενημερωμένο;

- Επιλογή ενός καλού antivirus προγράμματος
- Συνεχής ανανέωση (update) του antivirus και τακτική ανίχνευση όλου του δίσκου
- Έλεγχος κάθε flash memory με το antivirus πριν την ανοίξετε
- Τήρηση αντιγράφων ασφαλείας όλων των αρχείων σας σε flash memory ή σκληρό δίσκο
- Συχνές επισκέψεις στην τοποθεσία των κρίσιμων ενημερώσεων των Windows (το πιο ευάλωτο λειτουργικό) όπου προσφέρονται δωρεάν προγράμματα (patches) διόρθωσης/κάλυψης των πιθανών ελλείψεων του λειτουργικού σας.
- Αν χρησιμοποιείτε IRC chat, απενεργοποιείστε την επιλογή αυτόματης αποδοχής αρχείων και αυτόματης εκτέλεσης των αρχείων που σας στέλνουν.
- Επιλέξτε την πλήρη εμφάνιση των τύπων αρχείων στον Η/Υ σας. Ίσως κάποιος να σας στείλει μια «φωτογραφία» ως photo.jpg.vbs. Αν δεν έχετε την παραπάνω επιλογή ενεργοποιημένη, θα εκτελέσετε το αρχείο το οποίο θα περιέχει κάθε άλλο παρά φωτογραφία.

- Διατηρείτε και ανανεώνετε συχνά μια δισκέτα για αποκατάσταση ζημιών από ιούς, την οποία προσφέρουν συνήθως τα ίδια τα αντιβιοτικά προγράμματα.
- Διατήρηση της ανωνυμίας σας με την ενημέρωση του φυλλομετρητή που χρησιμοποιείτε. Προτιμήστε πάντα την πιο πρόσφατη έκδοση και φυσικά φροντίστε να την ενημερώνετε τακτικά. Στον Internet Explorer, για να απενεργοποιήσετε τα «third party cookies» (τα cookies που «φυτεύονται» στο σύστημα όχι από τα sites που επισκέπτεστε αλλά από τριτογενείς φορείς)
- Σωστή ρύθμιση των δικτυακών εφαρμογών. Οι περισσότεροι φυλλομετρητές διαθέτουν ρυθμίσεις ασφαλείας που καθορίζουν ποια πρόσθετα μπορούν να «εκτελεστούν», ενώ επιτρέπουν πλέον και μια πιο έξυπνη και ασφαλή διαχείριση των cookies.
- Αν χρησιμοποιείτε instant messengers, να αποφεύγετε να συνομιλείτε με ξένους

ANTIVIRUS

Ποιες κατηγορίες antivirus υπάρχουν

Η διασπορά ιών είναι μια από τις πιο διαδεδομένες μορφές επίθεσης στο διαδίκτυο. Η χρήση λογισμικού αντιβιοτικού είναι η πιο συνηθισμένη μέθοδος αντιμετώπισης τους. Ένα τέτοιο πρόγραμμα που πρέπει να είναι εγκατεστημένο σε κάθε ηλεκτρονικό υπολογιστή επιτελεί τρείς βασικές λειτουργίες. Αυτές είναι:

1. Ανίχνευση των ιών : Η λειτουργία αυτή πραγματοποιείται κατόπιν ενέργειας του χρήστη (έλεγχος του σκληρού δίσκου μέσω του antivirus λογισμικού) ή μπορεί να γίνει και αυτόματα (έλεγχος από το antivirus λογισμικό που είναι φορτωμένο στη μνήμη RAM του ηλεκτρονικού υπολογιστή).

2. Προσδιορισμός ταυτότητας ιών: Στην ΠΕΡΙΠΤΩΣΗ που το σύστημα έχει προσβληθεί από κάποιον ιό, το λογισμικό θα ενημερώσει το χρήστη για την ταυτότητα του.

3. Καθαρισμός των ιών : Αφού έχει προηγηθεί ο εντοπισμός του ιού, ακολουθεί η αφαίρεσή του. Το λογισμικό antivirus επιδιορθώνει το μολυσμένο από τον ιό αρχείο ή ακόμα μπορεί και να το διαγράψει

Δωρεάν

Malwarebytes Anti-Malware

Είναι μια antimalware εφαρμογή που μπορεί να αφαιρέσει με επιτυχία ακόμη και τις πιο προηγμένες απειλές απο malware. Περιλαμβάνει μια σειρά από σύγχρονα χαρακτηριστικά. Μπλοκάρει κακόβουλες διαδικασίες προτού να αρχίσουν. Παρακολουθεί το σύστημά σας συνεχώς για να παραμείνει ασφαλές και σίγουρο.

IObit Malware Fighter

Προστατεύει τον υπολογιστή σας από τα διάφορα spyware, adware, trojans, keyloggers, bots, worms και hijackers. Ανιχνεύει τα πιο σύνθετα και δυσκολα στην αντιμετώπιση spyware και malware. Πολύ χρήσιμο κατά την περιήγηση σας στο internet αφού μπορεί να σας προστεύσει ενεργά από κακόβουλες ιστοσελίδες.

Norman Malware Cleaner

Πρόγραμμα ανίχνευσης και εξυγίανσης του υπολογιστή σας. Δεν πρόκειται για ασπίδα προστασίας σε πραγματικό χρόνο αλλά απευθύνεται ουσιαστικά στην ανάγκη καθαρισμού υπολογιστών που έχουν ήδη χτυπηθεί από κάποιο κακόβουλο λογισμικό. Προσφέρει ικανές δυνατότητες ανίχνευσης και καταπολέμησης.

Με Αγορά

ESET NOD32 Antivirus

Απολαύστε την πλήρη ισχύ του υπολογιστή σας. Παίξτε, εργαστείτε ή συνδεθείτε χωρίς καθυστερήσεις. Το λογισμικό μας τρέχει στο παρασκήνιο αφήνοντας πόρους για να

χρησιμοποιείτε τον υπολογιστή σας απρόσκοπτα. Εγκαταστήστε το και ρυθμίστε το. Απολαύστε κορυφαία προστασία με τις προεπιλεγμένες ρυθμίσεις. Εάν θέλετε, μπορείτε να ρυθμίσετε το πρόγραμμα μέχρι την παραμικρή λεπτομέρεια με περισσότερες από 150 ρυθμίσεις.

Norton Antivirus

Το **Norton AntiVirus** χρησιμοποιεί αποκλειστικά, πατενταρισμένα επίπεδα προστασίας που συνδυάζονται μεταξύ τους και εξουδετερώνουν ιούς, επικίνδυνες ιστοσελίδες και προσπάθειες εξαπάτησης στα κοινωνικά δίκτυα, ώστε να είστε προστατευμένοι από τις σημερινές αλλά και τις μελλοντικές online απειλές.

Kaspersky Antivirus

Οι νέες εκδόσεις διαθέτουν κορυφαίες τεχνολογίες προστασίας δεδομένων, ώστε να αντιμετωπίζουν τις εξελισσόμενες ηλεκτρονικές απειλές πιο γρήγορα και πιο αποτελεσματικά από ποτέ. Το **Kaspersky Anti-Virus 2014** παρέχει ένα ιδιαίτερα ασφαλές και φιλικό προς το χρήστη ψηφιακό περιβάλλον, είτε εργάζεται, είτε πραγματοποιεί τραπεζικές συναλλαγές και online αγορές, είτε απλά επικοινωνεί με τους φίλους και την οικογένεια του μέσα από ιστοσελίδες κοινωνικής δικτύωσης.

Κατηγορίες λογισμικών προστασίας

Anti-malware

Malwarebytes Anti-Malware

Είναι μια antimalware εφαρμογή που μπορεί να αφαιρέσει με επιτυχία ακόμη και τις πιο προηγμένες απειλές απο malware. Περιλαμβάνει μια σειρά από σύγχρονα χαρακτηριστικά. Μπλοκάρει κακόβουλες διαδικασίες προτού να αρχίσουν. Παρακολουθεί το σύστημά σας συνεχώς για να παραμείνει ασφαλές και σίγουρο.

Dr.Web CureIt

Εφαρμογή που θα σας βοηθήσει να σκανάρετε και να θεραπεύσετε γρήγορα τον υπολογιστή σας. Είναι ιδιαίτερα χρήσιμο οταν το antivirus που έχουμε εγκατεστημένο δεν μπορεί να αναγνωρίσει η να αφαιρέσει κάποιο ιό η spyware. Επειδή δεν χρειάζεται εγκατάσταση μπορείτε να το εκτελέσετε και από usb stick η cd.

Wormblaster Malware Protector

Σας βοηθάει να αναγνωρίσετε και να διαγράψετε μια ευρεία ποικιλία από απειλές, να βελτιώσετε την απόδοση του pc σας και να επιδιορθώσετε τα κενά στην registry που προκλήθηκαν από malware. Προσφέρει προστασία σε πραγματικό χρόνο, σκανάρισμα ιών, εμφάνιση διαδικασιών και πρόσφατες ενημερώσεις νέων απειλών.

Antispyware

SuperAntiSpyware Free

Εξαιρετική εφαρμογή για την αντιμετώπιση των spyware. Στην δωρεάν έκδοση της περιλαμβάνει χειρωνακτικό update, όχι όμως και προστασία σε πραγματικό χρόνο (real time protection). Ωστόσο το πρόγραμμα μπορεί να μας σώσει σε ΠΕΡΙΠΤΩΣΗ που ο υπολογιστής μας έχει ήδη προσβληθεί**.**

Spyware Terminator

Εγγυάται συνεχή προστασία του υπολογιστή σας από πιθανές απειλές που προέρχονται από πλοήγηση στο διαδίκτυο. Εξασφαλίζει τον εντοπισμό και την εξαφάνιση κάθε προγράμματος που βάζει σε κίνδυνο τον υπολογιστή σας ή απειλεί το απόρρητό σας συλλέγοντας δικές σας πληροφορίες.

Spybot - Search & Destroy

Εξαλείφει λογισμικά υποκλοπής, κακόβουλα λογισμικά και διαφημιστικά κάθε είδους που ενδέχεται να έχετε εγκαταστήσει στον υπολογιστή σας. Είναι εφαρμογή καταξιωμένη στο χώρο των antispyware, εύκολη στο χειρισμό της και ενημερώνεται μέσω αρχείων που κατεβάζει αυτόματα από το internet.

Antivirus

Avira Free Antivirus

Είναι απο τα κορυφαία δωρεάν προγράμματα προστασίας του pc σας γιατί είναι ικανό να εντοπίζει με επιτυχία όλους τους ιούς και όλες τις κακόβουλες απειλές. Γρήγορο, ικανό, αξιόπιστο είναι μερικά απο τα χαρακτηριστικά του. Εκτελείται αθόρυβα στο παρασκήνιο, καταναλώνει ελάχιστους πόρους και ενημερώνεται αυτόματα.

Avast Free Antivirus

Είναι ένα από τα πιο ισχυρά δωρεάν προγράμματα antivirus της αγοράς. Θα κρατήσει τον υπολογιστή σας σε τέλεια κατάσταση καθώς είναι ικανό να εντοπίζει τους περισσότερους ιούς, worms και trojans που υπάρχουν στο internet. Έχει ένα μόνιμο σύστημα ενημέρωσης το οποίο σας επιτρέπει να είστε πάντα ενημερωμένοι.

AVG Antivirus Free

Είναι ένα ισχυρό δωρεάν πρόγραμμα που προστατεύει το pc σας καθώς εντοπίζει και διαγράφει όλων των ειδών τις ηλεκτρονικές απειλές, τους ιούς και τα spyware. Διαθέτει εξελιγμένες και δυνατές μηχανές σκαναρίσματος και ενημερώνεται συνεχώς έτσι ώστε να έχετε πάντα τα πιο καινοτόμα και αξιόπιστα εργαλεία προστασίας.

FIREWALL

Τι είναι το τείχος προστασίας(firewall)

Ένα σύστημα που έχει σχεδιαστεί για να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση προς ή από ένα ιδιωτικό δίκτυο. Τα Firewalls μπορούν να εφαρμοστούν τόσο σε υλικό και λογισμικό, ή ένας συνδυασμός και των δύο. Τα Firewalls χρησιμοποιούνται συχνά για την αποτροπή μη εξουσιοδοτημένους χρήστες του Διαδικτύου από την πρόσβαση ιδιωτικών δικτύων που είναι συνδεδεμένα με το Διαδίκτυο, ιδιαίτερα intranets. Όλα τα μηνύματα που εισέρχονται ή εξέρχονται από το πέρασμα intranet μέσω του τείχους προστασίας, η οποία εξετάζει κάθε μήνυμα και μπλοκάρει εκείνα που δεν συναντούν τα καθορισμένα κριτήρια ασφαλείας.

Το Firewall δεν προστατεύει από ιούς! Αυτό που πετυχαίνει μέσα από τον έλεγχο της κυκλοφορίας των πληροφοριών είναι κυρίως την προστασία από προγράμματα τύπου backdoor που χρησιμοποιούν οι ερασιτέχνες hackers. Οι πραγματικά ικανοί εισβολείς ενός συστήματος βρίσκουν τρόπους να ξεγελάσουν το firewall οπότε δεν πρέπει να το αντιμετωπίζουμε σαν τη λύση για όλα τα προβλήματα ασφάλειας. Υπάρχουν μάλιστα και ορισμένοι φανατικοί υποστηρικτές της άποψης ότι το firewall είναι περιττό. Πέρα από κάθε φανατισμό όμως, είναι γενικότερα αποδεκτό ότι το firewall βοηθάει σημαντικά και επίσης μας προστατεύει από διάφορα σκουλήκια που μεταδίδονται μέσω του διαδικτύου.

Το τείχος προστασίας είναι πολύ σημαντικό να υπάρχει, μπορεί βέβαια να σας προβληματίσουν λίγο μερικά μηνύματα που θα σας στέλνει ζητώντας την άδειά σας για πρόσβαση των προγραμμάτων. Όταν δεν ξέρετε το πρόγραμμα, να του αρνείστε πάντα την πρόσβαση! Αν κάτι δε λειτουργεί σωστά και έχετε απαγορεύσει την είσοδο / έξοδο ενός σημαντικού προγράμματος του συστήματος μπορείτε ανά πάσα στιγμή να αλλάξετε την

εντολή. Πραγματικά δεν είναι τόσο πολύπλοκο όσο ακούγεται, απλά προσπαθώ να εξηγήσω εδώ κάπως αναλυτικά τι συμβαίνει. Κατά τη διάρκεια της λειτουργίας του firewall γίνονται αντιληπτά τα λεγόμενα port scans. Μπορούμε να φανταστούμε ότι ο Η/Υ έχει πολλές θύρες / πόρτες (ports) που χρησιμοποιούνται για την επικοινωνία με το διαδίκτυο. Υπάρχουν πολλοί λόγοι για τους οποίους μπορεί κάποιος ή κάτι να "χτυπήσει μια πόρτα" του υπολογιστή σας. Όταν όμως λειτουργεί το firewall δεν υπάρχει λόγος ανησυχίας το οποίο αυτόματα προστατεύει και είναι σπάνιο έως απίθανο να κρύβεται πίσω από όλα τα port scans ένας hacker!

Υπάρχουν διάφορα προγράμματα (τείχη προστασίας) συνιστάται το Sunbelt Personal Firewall για windows XP & Vista. Αυτό το πρόγραμμα ονομαζόταν Kerio πριν το αναλάβει η εταιρία Sunbelt. Δεν είναι πολύ φιλικό σε νέους και αρχάριους χρήστες, δίνει όμως πολλές επιλογές και έλεγχο σχετικά με τις εφαρμογές και τις διεργασίες που εκτελούνται στον υπολογιστή. Ανα πάσα στιγμή μπορεί ο χρήστης να δει σε ποιά προγράμματα έχει επιτραπεί η έξοδος ή η είσοδος στο τοπικό δίκτυο ή στο διαδίκτυο. Με τη χρήση της κοινής λογικής, μπορεί ακόμα και ένας νέος χρήστης να επιτρέπει ή να μπλοκάρει την πρόσβαση εφαρμοφών στο ίντερνετ. Παρόλαυτά, καθώς πλέον τα windows xp και vista περιλαμβάνουν και τείχος προστασίας, δεν είναι απαραίτητο να ύπάρχει πρόσθετο firewall στον υπολογιστή. Το τείχος προστασίας των windows αρκεί για να καλύψει τις ανάγκες ενός μέσου χρήστη.

Είδη Firewall

Online Armor Free

Θεωρείται ένα απο τα καλύτερα firewall σήμερα, το οποίο αν και free είναι πανίσχυρο. Αν ενδιαφέρεστε λοιπόν για την προστασία του υπολογιστή σας από κακόβουλες απειλές μέσω διαδικτύου το Online Armor Free είναι μια πολύ καλή πρόταση στον τομέα των firewalls.

Agnitum Outpost Firewall Free

Είναι ένα λογισμικό τείχους προστασίας που επίσης προστατεύει από ιούς και περιλαμβάνει πολλά ακόμα πρόσθετα. Όταν εγκατασταθεί θα σας προστατεύσει από επιθέσεις από το διαδίκτυο, ενώ θα παρακολουθεί και τις εξερχόμενες συνδέσεις σας. Αυτόματα δημιουργεί κανόνες για γνωστές ασφαλείς εφαρμογές.

Comodo Firewall

Το Comodo Firewall κατά πολλούς θεωρείται το καλύτερο από τα free και ανώτερο από τα περισσότερα εμπορικά firewalls. Είναι ελαφρύ, εύκολο στο setup και τη χρήση του και συνεχώς εξελισσόμενο. Αποτρέπει τους εισβολείς εμποδίζοντας την πρόσβαση χωρίς άδεια στον υπολογιστή σας.

ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ

Πως δημιουργώ αντίγραφα ασφαλείας και πόσο συχνά

Για να εξασφαλίσετε ότι δεν θα χάσετε τα αρχεία που δημιουργήσατε, τροποποιήσατε και αποθηκεύσατε στον υπολογιστή σας, πρέπει να δημιουργείτε αντίγραφα ασφαλείας ανά τακτά χρονικά διαστήματα. Μπορείτε να δημιουργήσετε αντίγραφα ασφαλείας με μη αυτόματο τρόπο οποιαδήποτε στιγμή ή μπορείτε να επιλέξετε την αυτόματη δημιουργία αντιγράφων ασφαλείας.

Σημείωση

Η δυνατότητα ρύθμισης αυτόματης δημιουργίας αντιγράφων ασφαλείας δεν περιλαμβάνεται στα Windows 7.

Ανοίξτε το Κέντρο αντιγράφων ασφαλείας και επαναφοράς κάνοντας κλικ στο κουμπί **Έναρξη** και στις επιλογές **Πίνακας Ελέγχου**, **Σύστημα και συντήρηση** και **Κέντρο αντιγράφων ασφαλείας και επαναφοράς**.

Κάντε κλικ στο κουμπί **Αντίγραφα ασφαλείας αρχείων** και μετά ακολουθήστε τα βήματα του οδηγού. Αν σας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση, πληκτρολογήστε τον κωδικό πρόσβασης ή παρέχετε την επιβεβαίωση.

Σημειώσεις

Μην δημιουργείτε αντίγραφα ασφαλείας των αρχείων σας στον ίδιο σκληρό δίσκο όπου είναι εγκατεστημένα τα Windows. Για παράδειγμα, μην δημιουργείτε αντίγραφα ασφαλείας των αρχείων σε ένα διαμέρισμα ανάκτησης.

Τα μέσα που χρησιμοποιείτε για την αποθήκευση αντιγράφων ασφαλείας (εξωτερικοί δίσκοι, DVD ή CD) πρέπει να τα διατηρείτε σε ασφαλή σημεία, όπου δεν θα έχουν πρόσβαση μη εξουσιοδοτημένα άτομα. Προτείνεται η αποθήκευση σε σημείο με πυροπροστασία, ξεχωριστά από τον υπολογιστή σας. Επίσης μπορεί να θέλετε να κρυπτογραφήσετε τα δεδομένα που υπάρχουν στα αντίγραφα ασφαλείας σας.

Εξαρτάται από τον αριθμό των αρχείων που δημιουργείτε και τη συχνότητα δημιουργίας τους. Εάν δημιουργείτε νέα αρχεία κάθε μέρα, τότε ίσως πρέπει να δημιουργείτε αντίγραφα ασφαλείας κάθε εβδομάδα ή και κάθε μέρα. Εάν δημιουργείτε πολλά αρχεία περιστασιακά, για παράδειγμα, όταν αποθηκεύετε πολλές ψηφιακές φωτογραφίες από ένα πάρτι γενεθλίων ή μια αποφοίτηση, τότε δημιουργήστε τα αντίγραφα ασφαλείας αμέσως. Καλύτερα είναι να προγραμματίσετε τακτική, αυτόματη δημιουργία αντιγράφων ασφαλείας έτσι ώστε να μην χρειάζεται καν να το σκεφτείτε. Μπορείτε να επιλέξετε την καθημερινή, εβδομαδιαία ή μηνιαία δημιουργία αντιγράφων ασφαλείας. Μπορείτε επίσης να δημιουργείτε αντίγραφα ασφαλείας με μη αυτόματο τρόπο, μεταξύ των αυτόματων αντιγράφων ασφαλείας.

ΕΠΑΝΑΦΟΡΑ ΑΡΧΕΙΩΝ

Με ποια διαδικασία εξασφαλίζουμε την επαναφορά των αρχείων

Η "Επαναφορά Συστήματος" σας βοηθά να επαναφέρετε τα αρχεία συστήματος του υπολογιστή σας σε ένα παλαιότερο χρονικό σημείο. Συνήθως, επιθυμείτε να κάνετε επαναφορά του υπολογιστή σας σε ένα σημείο επαναφοράς που δημιουργήθηκε αμέσως πριν την ημερομηνία και ώρα που αρχίσατε να παρατηρείτε προβλήματα. Οι περιγραφές των σημείων επαναφοράς που δημιουργούνται αυτόματα σχετίζονται με το όνομα ενός συμβάντος, όπως η εγκατάσταση μιας ενημέρωσης από το Windows Update. Η "Επαναφορά Συστήματος" επιστρέφει τον υπολογιστή σας στην κατάσταση στην οποία βρισκόταν πριν το σημείο επαναφοράς που επιλέγετε. Για να μάθετε περισσότερα σχετικά με τον τρόπο λειτουργίας της "Επαναφοράς Συστήματος", ανατρέξτε στο θέμα

Για επαναφορά αρχείων και ρυθμίσεων συστήματος χρησιμοποιώντας ένα προτεινόμενο σημείο επαναφοράς

Ανοίξτε την Επαναφορά Συστήματος κάνοντας κλικ στο κουμπί **Έναρξη**. Στο πλαίσιο αναζήτησης, πληκτρολογήστε **Επαναφορά Συστήματος** και, στη συνέχεια, στη λίστα των αποτελεσμάτων, κάντε κλικ στην επιλογή **Επαναφορά Συστήματος.** Αν σας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση, πληκτρολογήστε τον κωδικό πρόσβασης ή παρέχετε την επιβεβαίωση.

Κάντε κλικ στην επιλογή **Προτεινόμενη επαναφορά** και, στη συνέχεια, κάντε κλικ στο κουμπί **Επόμενο**.

Εάν δεν υπάρχει ένα προτεινόμενο σημείο επαναφοράς, ακολουθήστε τα παρακάτω βήματα για να επιλέξετε ένα συγκεκριμένο σημείο επαναφοράς.

Ελέγξτε το σημείο επαναφοράς και, στη συνέχεια, κάντε κλικ στο κουμπί **Τέλος**.

Για επαναφορά αρχείων και ρυθμίσεων συστήματος χρησιμοποιώντας ένα συγκεκριμένο σημείο επαναφοράς

Ανοίξτε την Επαναφορά Συστήματος κάνοντας κλικ στο κουμπί **Έναρξη**. Στο πλαίσιο αναζήτησης, πληκτρολογήστε **Επαναφορά Συστήματος** και, στη συνέχεια, στη λίστα των αποτελεσμάτων, κάντε κλικ στην επιλογή **Επαναφορά Συστήματος**. Αν σας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση, πληκτρολογήστε τον κωδικό πρόσβασης ή παρέχετε την επιβεβαίωση.

Κάντε ένα από τα παρακάτω:

1. Εάν υπάρχει ένα προτεινόμενο σημείο επαναφοράς, κάντε κλικ στην επιλογή **Επιλογή διαφορετικού σημείου επαναφοράς** και, στη συνέχεια, κάντε κλικ στο κουμπί **Επόμενο**.
2. Εάν δεν υπάρχει ένα προτεινόμενο σημείο επαναφοράς, κάντε κλικ στο κουμπί **Επόμενο**.
3. Επιλέξτε το σημείο επαναφοράς που θέλετε και, στη συνέχεια, κάντε κλικ στο κουμπί **Επόμενο**.
4. Για να προβάλετε τα προγράμματα και τα προγράμματα οδήγησης που επηρεάζονται (στα οποία θα μπορούσαν να περιλαμβάνονται προγράμματα που θα διαγραφούν), κάντε κλικ στην επιλογή **Σάρωση για προγράμματα που επηρεάστηκαν**.
5. Ελέγξτε το σημείο επαναφοράς και, στη συνέχεια, κάντε κλικ στο κουμπί **Τέλος**.

Πως κάνω ρυθμίσεις ασφαλείας στους φιλομετρητές μου

1. Κάντε κλικ στο μενού του Chrome  στη γραμμή εργαλείων του προγράμματος περιήγησης.
2. Επιλέξτε **Σύνδεση ως <τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας>** (θα πρέπει να έχετε συνδεθεί ήδη στο Chrome).
3. Στην ενότητα "Σύνδεση", κάντε κλικ στην επιλογή **Σύνθετες ρυθμίσεις συγχρονισμού** .
4. Ορίστε μια επιλογή κρυπτογράφησης:

Κρυπτογράφηση συγχρονισμένων κωδικών πρόσβασης με τα διαπιστευτήριά σας Google: Αυτή είναι η προεπιλεγμένη επιλογή. Οι αποθηκευμένοι σας κωδικοί πρόσβασης κρυπτογραφούνται στους διακομιστές της Google και προστατεύονται με τα διαπιστευτήρια του Λογαριασμού σας Google.

Κρυπτογράφηση όλων των συγχρονισμένων δεδομένων με τη δική σας φράση πρόσβασης συγχρονισμού: Ορίστε αυτήν την επιλογή, αν θέλετε να κρυπτογραφήσετε όλα τα δεδομένα που έχετε επιλέξει για συγχρονισμό. Μπορείτε να δώσετε τη δική σας φράση πρόσβασης, η οποία θα αποθηκευτεί μόνο στον υπολογιστή σας.

5. Κάντε κλικ στην επιλογή **OK**.

ΑΝΤΙΜΕΤΩΠΙΣΗ ΙΩΝ

Τι κάνουμε αν μολυνθεί ο υπολογιστής μας

Κοινά προβλήματα λογισμικού , όπως σφάλματα εκτέλεσης του προγράμματος και κατεστραμμένα αρχεία , μπορεί να δημιουργήσει συμπτώματα που φαίνεται να σχετίζονται με ιούς , έτσι είναι σημαντικό να γίνει διάκριση μεταξύ των συμπτωμάτων του ιού και εκείνων που προέρχονται από κατεστραμμένα αρχεία συστήματος . Θα πρέπει επίσης να αποκλείσει πιο συνήθη αίτια (π.χ. , που έχει πρόσφατα εγκατασταθεί το νέο λογισμικό) πριν υποψιάζεται έναν ιό .

Ωστόσο, αν ο υπολογιστής σας αρχίζει να ενεργεί παράξενα ή συμπεριφέρεται διαφορετικά από ό, τι στο παρελθόν , μπορεί να έχει μολυνθεί με έναν ιό . Συμπτώματα όπως οι μεγαλύτεροι από το κανονικό χρόνοι φόρτωσης του προγράμματος, απρόβλεπτη συμπεριφορά του προγράμματος , ανεξήγητες αλλαγές στο μέγεθος του αρχείου, η αδυναμία για την εκκίνηση , περίεργα γραφικά που εμφανίζονται στην οθόνη σας , ή ασυνήθιστους ήχους μπορεί να υποδεικνύει έναν ιό στο σύστημά σας .

Εάν δεν μπορείτε να εκκινήσετε τον υπολογιστή σας , επικοινωνήστε με το Κέντρο Υποστήριξης πανεπιστημιούπολη σας . Διαφορετικά , μπορείτε να προσπαθήσετε να αντιμετωπίσει το πρόβλημα με το λογισμικό ασφαλείας .

Αν είχατε μολυσμένα αρχεία , ίσως χρειαστεί να κάνετε πρόσθετες εργασίες επισκευής μετά το λογισμικό προστασίας από ιούς τους έχει καθαριστεί . Η ευκολότερη λύση είναι να ανοίξετε το αρχείο που θέλετε καθαρίσετε , επιλέξτε όλες τις πληροφορίες στο έγγραφο , και να αντιγράψετε και να επικολλήσετε σε ένα νέο έγγραφο .

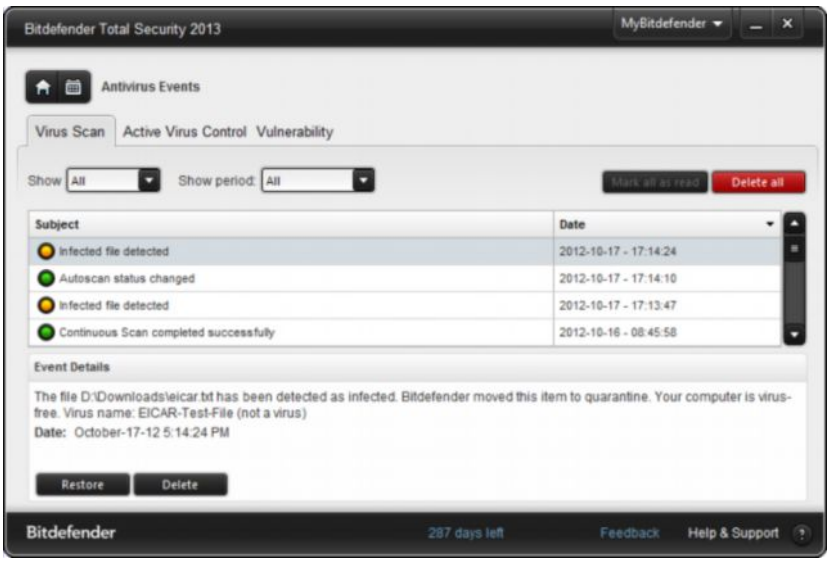
Σημείωση : Τα αρχεία που έχουν καθαριστεί μπορεί συχνά φαίνεται να έχουν κάποια καταστροφή του αρχείου που απομένει μετά την αφαίρεση του ιού και μακροεντολές . Αν τα σκουπίδια ή ανεπιθύμητες λέξεις έχουν εισαχθεί στα αρχεία σας , μπορείτε να είστε σε θέση να χρησιμοποιήσετε την αναζήτηση και να αντικαταστήσετε τη λειτουργία επεξεργασίας κειμένου σας ή την εφαρμογή λογιστικών φύλλων για την εξάλειψή τους .

Σημείωση : Με ορισμένες μολύνσεις σε επίπεδο συστήματος , λογισμικό προστασίας από ιούς δεν μπορεί να αφαιρέσει πλήρως προβλήματα και δεν μπορούν να ληφθούν υπόψη οι αλλαγές που μπορεί να έχουν γίνει κατά τη διάρκεια της λοίμωξης . Σε αυτές τις περιπτώσεις , θα πρέπει να εκτελέσετε μια καθαρή εγκατάσταση του λειτουργικού συστήματος .

ΠΕΡΙΠΤΩΣΗ 1η: Το Antivirus βρίσκει έναν ιο

Τα καλά νέα είναι πως το antivirus βρήκε έναν ιό. Και, γιατί είναι καλά αυτά τα νέα? Γιατί το πιθανότερο είναι πως το antivirus αφαίρεσε αυτόματα τον ιό, πριν προσβάλλει το σύστημά σας. Ίσως απλά είχατε κατεβάσει ένα μολυσμένο αρχείο και δεν το είχατε ακόμα τρέξει ή πήγατε να μπείτε σε μια μολυσμένη σελίδα, όμως το πιστό σας αντιβιοτικό σας κράτησε ασφαλή, και απλά αποφάσισε να σας χλιμιντρίσει για να σας ενημερώσει (μπορεί και από τη χαρά του).

Αυτό που μπορείτε να κάνετε (εκτός από το να κλείσετε τους ήχους του antivirus) είναι να ανοίξετε το antivirus, να βρείτε το κουμπί quarantine στο οποίο αποθηκεύονται όλα τα μολυσμένα αρχεία, και να αναλάβετε την κατάλληλη δράση (να επιχειρήσετε να καθαρίσετε το αρχείο ή απλά να το σβήσετε).



Προσοχή! Αν καθώς πλοηγείστε στο Internet σας πεταχτεί κάποιο παράθυρο διαφορετικό από αυτό του antivirus που σας λέει ότι το σύστημά σας είναι μολυσμένο, και σας ζητήσει να

κατεβάσετε οτιδήποτε, κλείστε το αμέσως! Ορισμένοι ιοί καμουφλάρονται σαν τέτοια προγράμματα

ΠΕΡΙΠΤΩΣΗ 2η: Δεν έχετε antivirus (ή δεν είναι ενημερωμένο)

Αν έχετε antivirus και δεν ανανεώνει τακτικά τα virus definitions.

Σε μια τέτοια ΠΕΡΙΠΤΩΣΗ, αν συμβαίνει οτιδήποτε από τα παρακάτω (ή σε συνδυασμό), υπάρχει σοβαρή πιθανότητα να έχετε ιό:

-Το σύστημα κολλάει και καθυστερεί

-Πετάγονται παράθυρα με διαφημίσεις ακόμα και όταν δεν έχετε ανοιχτό το browser και δεν πλοηγείστε στο Internet.

-Πετάγεται ένα captcha που πρέπει να συμπληρώσετε, χωρίς λόγο

-Αρχεία ή φάκελοι ανοίγουν από μόνα τους

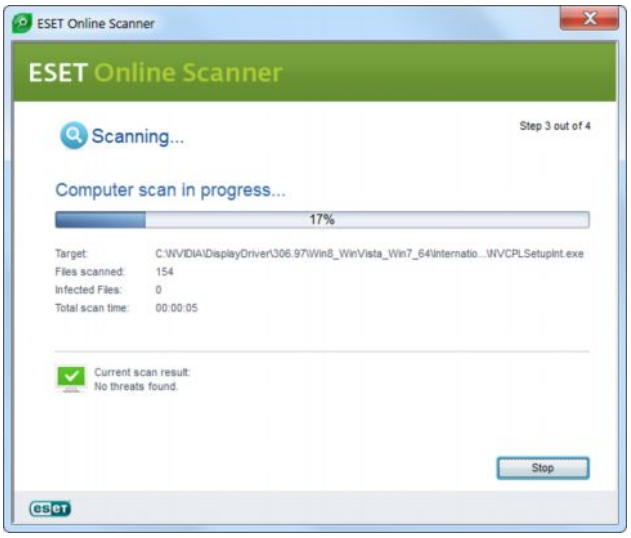
-Πάτε να μπείτε σε γνωστές σας σελίδες στο Internet, αλλά τελικά καταλήγετε σε σκοτεινά και άρρωστα sites.

Μια πρώτη κίνηση που μπορείτε να κάνετε είναι να κατεβάσετε ένα δωρεάν antivirus να το εγκαταστήσετε, να κατεβάσετε τις τελευταίες ενημερώσεις για ιούς και να κάνετε ένα πλήρες scan του υπολογιστή σας.

ΠΕΡΙΠΤΩΣΗ 3η: Έχετε ενημερωμένο Antivirus, αλλά δεν φτουράει

Κανένα antivirus δεν είναι τέλειο, με την έννοια να μην αφήνει κανέναν ιό να περάσει. Ακόμα και στα γνωστότερα ή τα ακριβότερα προγράμματα της αγοράς, υπάρχουν ιοί που αποφεύγουν κάθε εντοπισμό.

Υπάρχουν και antivirus τα οποία είναι one-time scanner. Για παράδειγμα, μπορείτε να κατεβάσετε τον Online Scanner της ESET ή το Hitman Pro της SurRight



Αφού κατεβάσετε και τρέξετε αυτά τα εργαλεία, θα ελέγξουν το σύστημά σας για ιούς χωρίς να χρειάζονται εγκατάσταση. Αν εντοπίσουν οτιδήποτε, θα μπορέσουν και να το αντιμετωπίσουν.

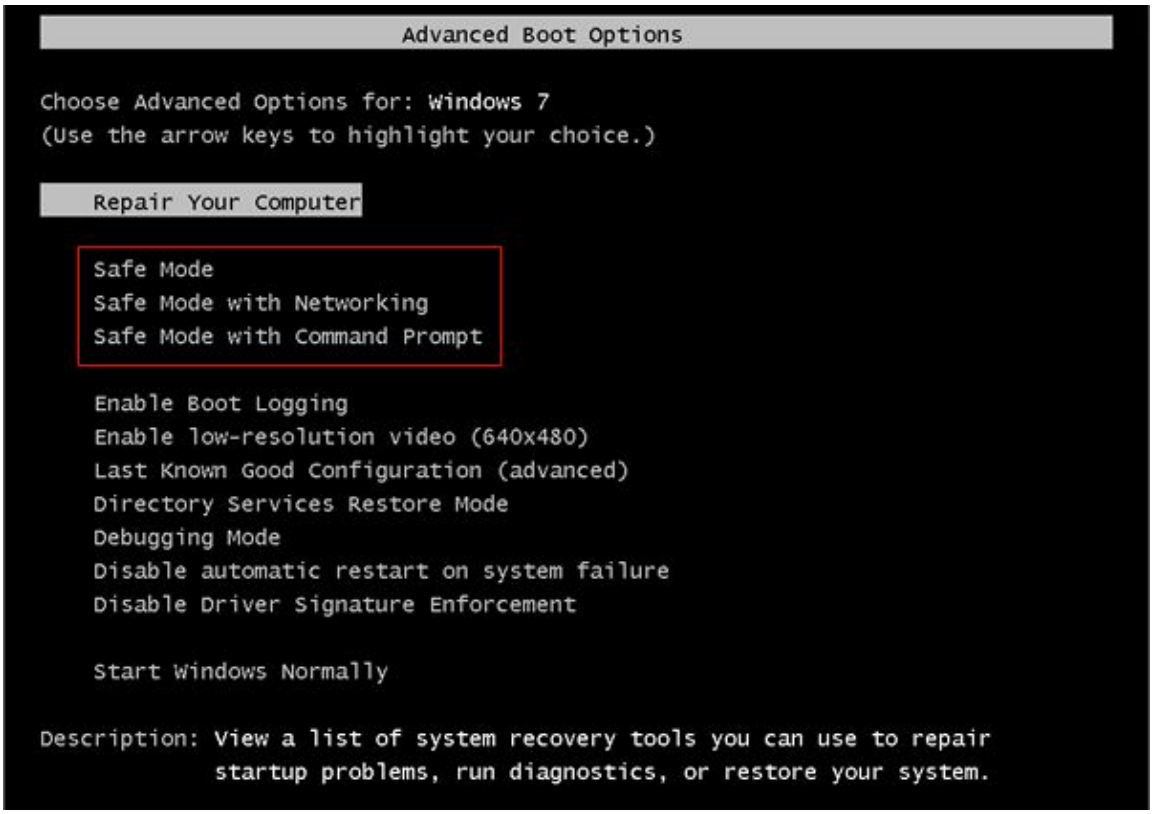
Σε καμία ΠΕΡΙΠΤΩΣΗ μην εγκαταστήσετε δύο διαφορετικά antivirus ταυτόχρονα στον ίδιο υπολογιστή. Τα εργαλεία που αναφέρουμε παραπάνω δεν είναι πλήρη antivirus που θα τρέχουν διαρκώς, ούτε παρέχουν οποιαδήποτε προστασία, απλά ελέγχουν το σύστημά μας όταν τα τρέχουμε και αντιμετωπίζουν τις μολύνσεις που θα εντοπίσουν.

Αν όντως κάποιος ιός ξέφυγε από το παλιό σας antivirus, μην είστε συναισθηματικοί. Αφού καθαρίσετε το σύστημά σας, διαγράψτε το παλιό antivirus και εγκαταστήστε κάποιο καινούριο.

ΠΕΡΙΠΤΩΣΗ 4η: Οι επίμονοι ιοί

Υπάρχουν ορισμένοι ιοί που διαγράφονται πολύ δύσκολα – ειδικά αν έχουν μολύνει το σύστημά μας πριν εγκαταστήσουμε ένα antivirus.

Μία λύση σε αυτή την ΠΕΡΙΠΤΩΣΗ είναι να μπούμε στα windows σε safe mode (ασφαλή λειτουργία). Για να το κάνουμε αυτό, πατάμε το κουμπί F8 καθώς φορτώνουν τα Windows (πριν όμως εμφανιστεί το desktop). Θα εμφανιστεί ένα μενού, από το ποίο επιλέγουμε Safe Mode (Ασφαλή Λειτουργία) ή Safe Mode with Networking, αν θέλετε να έχετε πρόσβαση στο Internet.



Σε αυτή την κατάσταση λειτουργίας, τα Windows δεν φορτώνουν καθόλου τρίτα προγράμματα (ούτε καν τους drivers), οπότε ίσως εμποδιστεί έτσι και ο ιός. Τρέξτε λοιπόν το full scan από το antivirus σε αυτό το mode λειτουργίας, και είναι πιθανό να έχετε καλύτερα αποτελέσματα.

Αν και το safe mode αποτύχει, τότε το επόμενο βήμα είναι να τρέξετε κάποιο rescue CD. Ουσιαστικά πρόκειται για Antivirus τα οποία έχουν το δικό τους λειτουργικό σύστημα και τρέχουν απ' ευθείας από το CD. Με αυτόν τον τρόπο, μπορούν να ελέγξουν το σύστημα χωρίς να έχουν φορτωθεί καθόλου τα windows ή ο ιός, και να τον αφαιρέσουν πολύ πιο εύκολα.

Ένα αρκετά αξιόπιστο rescue CD είναι αυτό της Bitdefender. Κατεβάζετε το αρχείο ISO, γράφετε το image σε ένα CD και κάνετε boot τον υπολογιστή από εκεί.

Αυτή η λύση θέλει προσοχή αν ο ιός έχει προσβάλλει αρχεία συστήματος των Windows. Αν τα σβήσετε από αυτό το περιβάλλον, τότε το πιθανότερο είναι πως τα Windows δεν θα φορτώνουν καθόλου

ΠΕΡΙΠΤΩΣΗ 5η: Ολική Επαναφορά

Αν και το rescue CD αποτύχει, δυστυχώς η μόνη λύση είναι η επαναφορά του συστήματος. Αρκετοί υπολογιστές έχουν επιλογές recovery, που επαναφέρουν το λειτουργικό σύστημα στην εργοστασιακή του κατάσταση (συμβουλευτείτε το manual του υπολογιστή σας αν έχει τέτοια δυνατότητα). Όμως όλα τα δεδομένα που είναι στο partition που βρίσκεται το λειτουργικό σύστημα θα χαθούν, έτσι θα χρειαστεί να κάνετε backup πριν την ξεκινήσετε.

Οδηγίες για εκκίνηση του υπολογιστή όταν έχει μολυνθεί από τον «Ιό της Αστυνομίας»

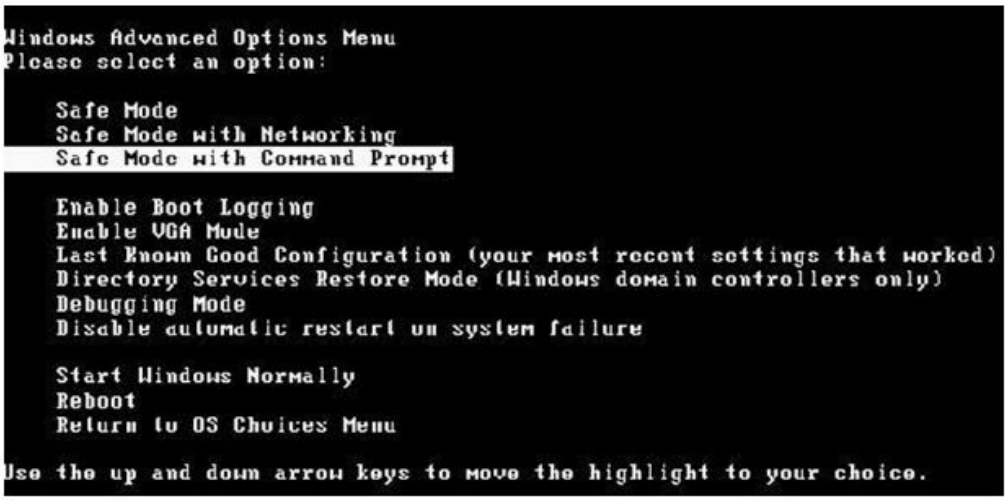
Ενδεικτικές οδηγίες για εκκίνηση του υπολογιστή όταν έχει μολυνθεί από το κακόβουλο λογισμικό “Ransomware”ή «ιός των 100 ευρώ»

Ακολουθούν δύο τρόποι για την εκκίνηση του υπολογιστή σας, όταν έχει μολυνθεί από το κακόβουλο λογισμικό “Ransomware”, ή αλλιώς «ιός των 100 ευρώ». Οι οδηγίες αυτές δεν είναι δεσμευτικές, καθώς οι πιο προχωρημένοι χρήστες μπορούν να κάνουν χρήση άλλων μεθόδων ή εργαλείων για την επιδιόρθωση του προβλήματος. Αν κανένας από τους δύο προτεινόμενους τρόπους δεν επιτύχει να επαναφέρει τον υπολογιστή σας, τότε συνίσταται η λήψη βοήθειας από εξειδικευμένο τεχνικό.

1ος Τρόπος (Επαναφορά συστήματος):

1. Επανεκκινούμε τον υπολογιστή (από το κουμπί power ή αποσυνδέοντας από το ρεύμα).

2. Κατά την επανεκκίνηση πατάμε επανειλημμένως το κουμπί F8 έως ότου εμφανιστεί μαύρη οθόνη με επιλογές “Advanced Options” ή “Επιλογές για προχωρημένους” αναλόγως με τη γλώσσα εγκατάστασης.



3. Από τις διαθέσιμες επιλογές επιλέγουμε αυτή που αναγράφει “Safe Mode with Command Prompt” ή “Ασφαλή Λειτουργία με γραμμή εντολών”.

4. Πραγματοποιούμε είσοδο (login) με τον χρήστη και τον κωδικό (αν έχουμε ορίσει κωδικό).

5. Εμφανίζεται ένα μαύρο παράθυρο εντολών.

6. Πληκτρολογούμε την παρακάτω εντολή ανάλογα με την έκδοση του λειτουργικού μας συστήματος:

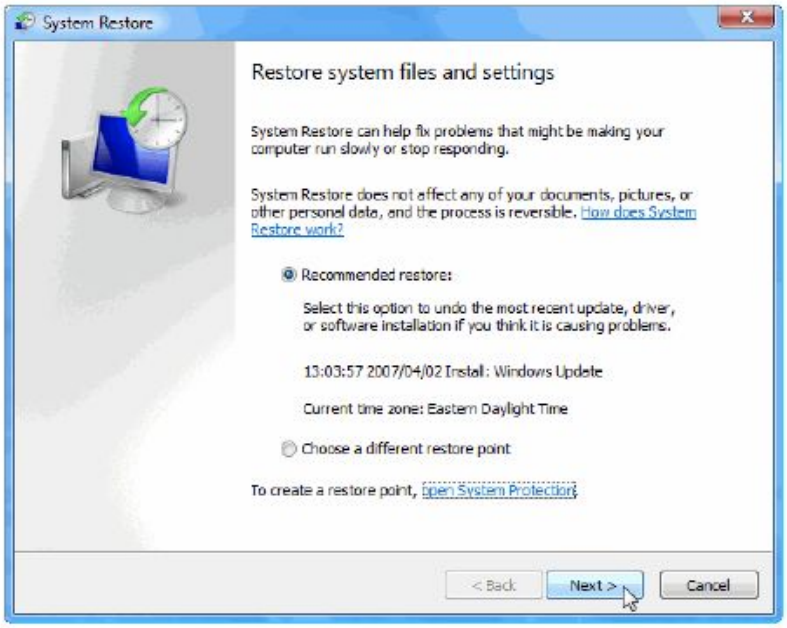
Windows 8: “C:\windows\system32\rstrui.exe”

Windows XP: “C:\windows\system32\restore\rstrui.exe”

Windows 7/vista: “C:\windows\system32\rstrui.exe”

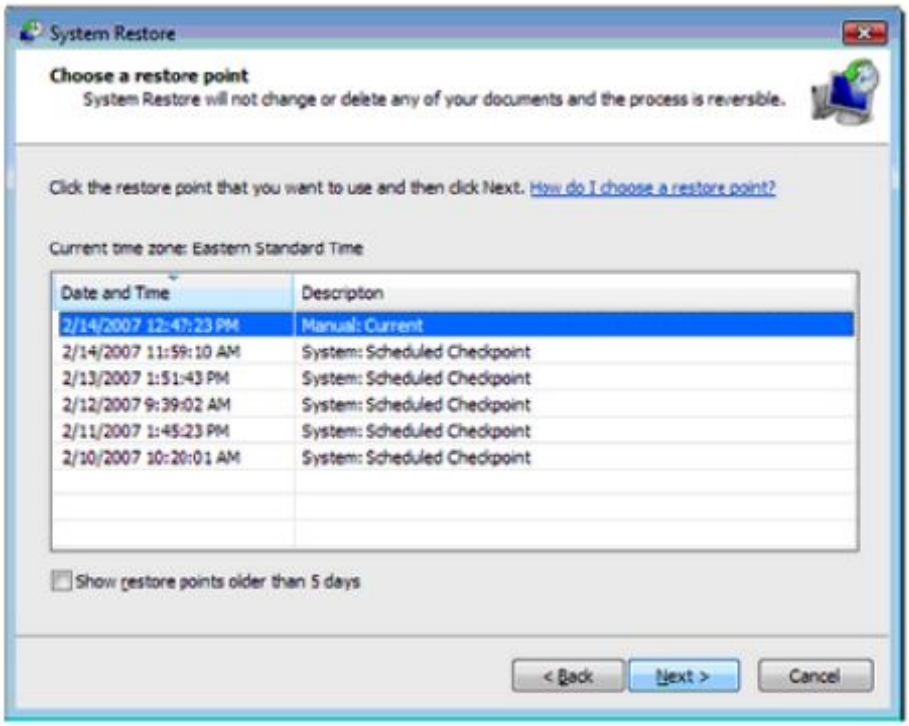
και πατάμε “enter”.

7. Εμφανίζεται ο οδηγός επαναφοράς συστήματος (Restore System Files and Settings).



Τα βήματα που ακολουθούν είναι ενδεικτικά και μπορεί να διαφέρουν ανάλογα με την έκδοση του λειτουργικού.

8. Στον οδηγό επιλέγουμε ένα σημείο επαναφοράς παλαιότερο από την ημερομηνία κατά την οποία μολύνθηκε ο υπολογιστής (εάν δεν είμαστε σίγουροι προτιμούμε μία παλαιότερη ημερομηνία κατά την οποία είμαστε σίγουροι ότι δεν είχε μολυνθεί το σύστημα).



9. Εκκινούμε τη διαδικασία και αφού ολοκληρωθεί επανεκκινούμε τον υπολογιστή εφόσον δεν έχει πραγματοποιήσει αυτόματη επανεκκίνηση.

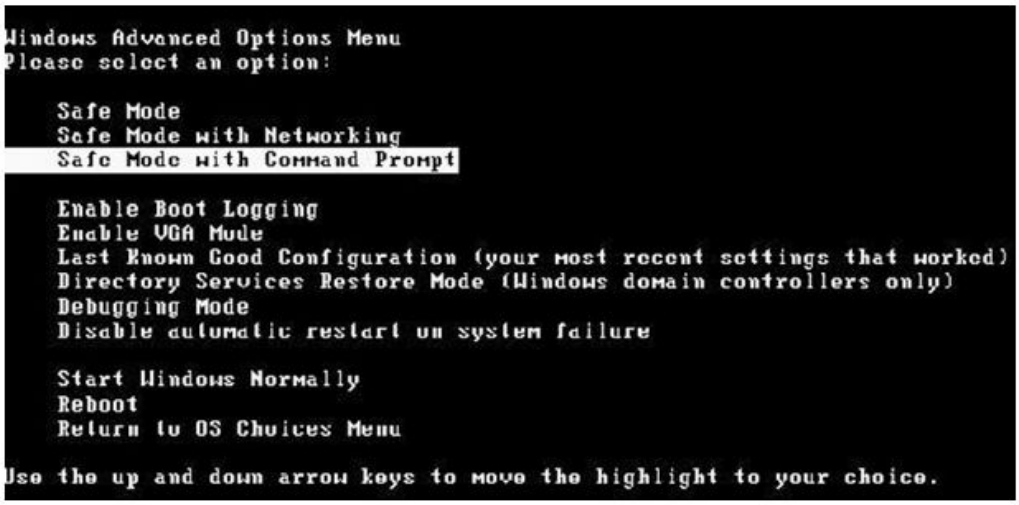
10. Ο υπολογιστής εκκινεί κανονικά (προαιρετικά μπορεί να γίνει και έλεγχος του συστήματος με πλήρως ενημερωμένο λογισμικό antivirus).

11. Σε κάθε ΠΕΡΙΠΤΩΣΗ και αφού αποθηκεύσουμε όλα τα αρχεία μας σε ασφαλές μέσο (εξωτερικό σκληρό δίσκο ή άλλο) προτείνεται και η επανεγκατάσταση του λειτουργικού.

2ος Τρόπος (Δημιουργία νέου χρήστη):

1. Επανεκκινούμε τον υπολογιστή (από το κουμπί)

2. Κατά την επανεκκίνηση πατάμε επανειλημμένως το κουμπί με επιλογές “Advanced Options εγκατάστασης.



3. Από τις διαθέσιμες επιλογές επιλέγουμε που αναγράφει “Safe Mode with

ή “Ασφαλή Λειτουργία με γραμμή εντολών”.

4. Πραγματοποιούμε είσοδο (Login) με τον χρήστη και τον κωδικό (αν έχουμε ορίσει κωδικό).

5. Εμφανίζεται ένα μαύρο παράθυρο εντολών.

6. Πληκτρολογούμε την εντολή ““C:/Windows/System32/control.exe”.

7. Εμφανίζεται ο οδηγός διαχείρισης του συστήματος

8. Στον οδηγό επιλέγουμε “Λογαριασμοί χρηστών και δημιουργούμε ένα νέο χρήστη.

Windows 7: “Διαχείριση ενός άλλου λογαριασμού” (“ manage another account account” και “δημιουργία νέου χρήστη” (“create new)

Windows XP: “Προσθήκη ννέου χρήστη: (“create new USER”).

9. Πληκτρολογούμε ένα όνομα, έναν κωδικό (αν ζητηθεί και ανάλογα με την έκδοση των Windows), επιλέγουμε δικαιώματα “διαχειριστή” (“administrator”) και δημιουργούμε το νέο χρήστη.

10. Επανεκκινούμε τον υπολογιστή κανονικά και όταν εμφανιστεί η οθόνη επιλογής χρήστη επιλέγουμε να εισέλθουμε με τον νέο χρήστη που δημιουργήσαμε στο βήμα (8).

11. Ο υπολογιστής εκκινεί κανονικά και εμφανίζεται η επιφάνεια εργασίας του νέου χρήστη.

12. Με τη χρήση λογισμικού antivirus της επιλογής μας, το οποίο ενημερώνουμε με τις τελευταίες ενημερώσεις εκτελούμε έλεγχο στο σύνολο των αρχείων του υπολογιστή και απομακρύνουμε το κακόβουλο λογισμικό.

13. Σε κάθε ΠΕΡΙΠΤΩΣΗ και αφού αποθηκεύσουμε όλα τα αρχεία μας σε ασφαλές μέσο (εξωτερικό σκληρό δίσκο ή άλλο) προτείνεται και η επανεγκατάσταση του λειτουργικού.

ΓΟΝΙΚΟΣ ΈΛΕΓΧΟΣ

Ρυθμίσεις γονικού έλεγχου

Εάν ο υπολογιστής σας είναι συνδεδεμένος σε έναν τομέα, ο γονικός έλεγχος δεν θα είναι διαθέσιμος.

Μπορείτε να χρησιμοποιήσετε το Γονικό έλεγχο για να διαχειριστείτε καλύτερα τον τρόπο, με τον οποίο τα παιδιά σας χρησιμοποιούν τον υπολογιστή. Για παράδειγμα, μπορείτε να θέσετε όρια στην πρόσβαση των παιδιών στο Web, στις ώρες κατά τις οποίες μπορούν να συνδεθούν με τον υπολογιστή, στα παιχνίδια που μπορούν να παίζουν και στα προγράμματα που μπορούν να εκτελούν.

Όταν ο Γονικός έλεγχος αποκλείει την πρόσβαση σε μια ιστοσελίδα ή σε ένα παιχνίδι, εμφανίζεται μια ειδοποίηση για τον αποκλεισμό της ιστοσελίδας ή του προγράμματος. Το παιδί μπορεί να κάνει κλικ σε μια σύνδεση στην ειδοποίηση, με την οποία αιτείται την εκχώρηση δικαιωμάτων πρόσβασης σε αυτή την ιστοσελίδα ή το πρόγραμμα. Μπορείτε να επιτρέψετε την πρόσβαση εισάγοντας τις πληροφορίες του λογαριασμού σας.

Πριν ξεκινήσετε, βεβαιωθείτε ότι όλα τα παιδιά, για τα οποία θέλετε να ρυθμίσετε το Γονικό έλεγχο, διαθέτουν έναν τυπικό λογαριασμό χρήστη, καθώς ο Γονικός έλεγχος εφαρμόζεται

μόνον σε τυπικούς λογαριασμούς χρήστη. Για να ρυθμίσετε το Γονικό έλεγχο για το παιδί σας, θα χρειαστείτε ένα λογαριασμό διαχειριστή. Ο Γονικός έλεγχος δεν είναι δυνατό να εφαρμοστεί σε έναν λογαριασμό διαχειριστή.

Για να ενεργοποιήσετε το Γονικό έλεγχο για έναν τυπικό λογαριασμό χρήστη

Ανοίξτε τον Γονικό έλεγχο κάνοντας κλικ στο κουμπί **Έναρξη**, έπειτα κάντε κλικ στον **Πίνακα ελέγχου** και, στη συνέχεια, στην επιλογή **Λογαριασμοί χρήστη**, επιλέξτε **Ρύθμιση γονικού ελέγχου**. Αν σας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση, πληκτρολογήστε τον κωδικό πρόσβασης ή παρέχετε την επιβεβαίωση.

Κάντε κλικ στον τυπικό λογαριασμό χρήστη, για τον οποίο θέλετε να ρυθμίσετε το Γονικό έλεγχο.

Στην περιοχή **Γονικός έλεγχος**, κάντε κλικ στην επιλογή **Ενεργός**.

Αφού ενεργοποιήσετε το Γονικό έλεγχο για τον τυπικό λογαριασμό χρήστη του παιδιού σας, μπορείτε να προσαρμόσετε τις μεμονωμένες ρυθμίσεις, τις οποίες θέλετε να ελέγξετε. Μπορείτε να ελέγξετε τις ακόλουθες περιοχές:

Περιορισμοί Web. Μπορείτε να περιορίσετε τις τοποθεσίες Web, τις οποίες θα μπορούν να επισκέπτονται τα παιδιά σας, να εξασφαλίσετε ότι τα παιδιά σας θα επισκέπτονται μόνον τοποθεσίες που είναι κατάλληλες για την ηλικία τους, να δηλώσετε εάν θέλετε να επιτρέπεται η λήψη αρχείων και να καθορίσετε το περιεχόμενο, το οποίο θα αποκλείουν ή θα επιτρέπουν τα φίλτρα περιεχομένου. Μπορείτε επίσης να αποκλείσετε ή να επιτρέψετε συγκεκριμένες τοποθεσίες Web. Για περισσότερες πληροφορίες, ανατρέξτε στο θέμα **Περιορισμός του περιεχομένου που μπορούν να προβάλουν τα παιδιά στο Web**.

Χρονικά όρια. Μπορείτε να ρυθμίσετε χρονικά όρια, ώστε να ελέγχετε πότε επιτρέπεται στα παιδιά να συνδεθούν ως χρήστες στον υπολογιστή. Τα χρονικά όρια εμποδίζουν τα παιδιά να συνδέονται ως χρήστες κατά τις προκαθορισμένες ώρες και, εάν είναι ήδη συνδεδεμένα, τα αποσυνδέουν αυτόματα. Μπορείτε να καθορίσετε διάφορες ώρες σύνδεσης για κάθε ημέρα της εβδομάδας. Για περισσότερες πληροφορίες, ανατρέξτε στο θέμα **Έλεγχος του χρόνου χρήσης του υπολογιστή από τα παιδιά**.

Παιχνίδια. Μπορείτε να ελέγξετε την πρόσβαση σε παιχνίδια, να επιλέξετε ένα επίπεδο ηλικιακού χαρακτηρισμού, να επιλέξετε τον τύπο περιεχομένου που θέλετε να αποκλειστεί και να καθορίσετε εάν θέλετε να επιτρέψετε ή να αποκλείσετε μη χαρακτηρισμένα ή συγκεκριμένα παιχνίδια. Για περισσότερες πληροφορίες, ανατρέξτε στο θέμα **Καθορισμός των παιχνιδιών που θα μπορούν να παίξουν παιδιά**.

Να επιτρέπονται ή να αποκλείονται συγκεκριμένα προγράμματα. Μπορείτε να εμποδίσετε τα παιδιά σας να εκτελούν μη επιθυμητά προγράμματα. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα **Αποτροπή της χρήσης ορισμένων προγραμμάτων από παιδιά**.

Windows Family Safety

Διατηρήστε την ασφάλεια των παιδιών σας. Όταν τα παιδιά είναι στο internet και εσείς είστε απασχολημένοι, το Family Safety είναι εκεί για να βοηθήσει. Χρησιμοποιήστε τις αναφορές δραστηριότητας για να παρακολουθήσετε τη δραστηριότητα των παιδιών σας στον υπολογιστή, επιλέξτε τοποθεσίες web, παιχνίδια κα.

K9 Web Protection

Το πρόγραμμα K9 Web Protection είναι σχεδιασμένο για γονείς και οικογένειες. Είναι ένα πολύ ικανό πρόγραμμα γονικού ελέγχου που μας προστατεύει από ανεπιθύμητα ή επικίνδυνα sites. Μια δυνατή δωρεάν λύση για να προστατεύσετε τα παιδιά σας από τις ιστοσελίδες ακατάλληλου περιεχομένου.

ParetoLogic PGsurfer

Είναι ένα δωρεάν πρόγραμμα λογισμικού με σκοπό να βοηθήσει τους γονείς να κρατήσουν τα παιδιά τους σε ασφαλή σύνδεση. Παρέχει αρκετές προηγμένες και αποτελεσματικές δυνατότητες. Φιλτράρει το περιεχόμενο των ιστοσελίδων, τα chat rooms, τα instant messaging, τα emails, τις p2p εφαρμογές και άλλα.

Σύμφωνα με την έρευνα που έγινε στο http://internet-filter-review.toptenreviews.com βγάζουμε το συμπέρασμα ότι το καλύτερο πρόγραμμα γονικού έλεγχου είναι το Net Nanny Parental Controls

Το οποίο υπερηχε στα χαρακτηριστικά, στην ευκολία χρήσης, στην ευκολία εγκατάστασης και στην αποτελεσματικότητα του φιλτραρίσματος.

Εικόνα 1

ΠΑΡΑΝΟΜΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Ποιά είναι τα Προσωπικά δεδομένα;

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

Πώς χρησιμοποιούνται τα προσωπικά μου δεδομένα;

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.

Είναι δυνατόν τα προσωπικά μου δεδομένα να χρησιμοποιηθούν... εναντίον μου;

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 θέλεις 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.

Πότε επιτρέπεται κάποιος να χρησιμοποιεί τα προσωπικά μου δεδομένα;

Στην Ελλάδα, όπως και στις υπόλοιπες χώρες της Ευρωπαϊκής Ένωσης, υπάρχει ειδική νομοθεσία που προστατεύει τα άτομα από την ανεξέλεγκτη χρήση των προσωπικών τους δεδομένων. Η Αρχή Προστασίας Δεδομένων είναι ο αρμόδιος φορέας για την εφαρμογή αυτής της νομοθεσίας (νόμοι 2472/1997 και 3471/2006).Ως βασικός κανόνας ισχύει ότι για να χρησιμοποιήσει κάποιος τα προσωπικά σου δεδομένα για έναν συγκεκριμένο σκοπό πρέπει να έχει εξασφαλίσει την συγκατάθεσή σου και, σε αρκετές περιπτώσεις, τη συναίνεση των γονιών σου. Με αυτό εννοούμε ότι, αφού προηγουμένως έχεις ενημερωθεί ακριβώς για το ποιος είναι αυτός που θέλει να χρησιμοποιήσει τα δεδομένα σου, για ποιον λόγο θέλει να τα χρησιμοποιήσει, ποια στοιχεία σου θέλει να πάρει και με ποιους θα τα μοιραστεί, έχεις δεχθεί και έχεις πει με σαφή τρόπο ότι συμφωνείς.Η συγκατάθεση είναι ο γενικός κανόνας, αλλά υπάρχουν και εξαιρέσεις. Για παράδειγμα κάποιοι οργανισμοί, όπως π.χ. ο δήμος ή το σχολείο σου, μπορούν να επεξεργάζονται συγκεκριμένα προσωπικά δεδομένα χωρίς τη συγκατάθεσή σου. Αυτό συμβαίνει γιατί τα δεδομένα σου είναι απαραίτητα για να εκτελέσουν το έργο τους και αυτό συνήθως ορίζεται σε κάποιο νόμο.

Ποια είναι τα δικαιώματα μου σε σχέση με τα προσωπικά μου δεδομένα;

Όταν κάποιος σου ζητά να του δώσεις προσωπικά σου δεδομένα, έχεις το δικαίωμα να γνωρίζεις ακριβώς την ταυτότητά του, τον σκοπό για τον οποίο χρειάζεται τα δεδομένα σου, σε ποιους θα τα στείλει, καθώς και ποιοι θα έχουν πρόσβαση σε αυτά.Έχεις το δικαίωμα να γνωρίζεις ποια δεδομένα τηρούν οι άλλοι (οργανισμοί ή άτομα) για σένα και μπορείς να τους ζητάς να σε ενημερώνουν για αυτό.Έχεις το δικαίωμα να ζητάς τη διαγραφή ή τη διόρθωση των προσωπικών σου δεδομένων, όταν θεωρείς ότι η πληροφορία αυτή σε θίγει ή είναι λανθασμένη ή όταν διαφωνείς με την επεξεργασία αυτών των δεδομένων.

Πώς μπορώ να προστατεύσω την ιδιωτική μου ζωή στο Διαδίκτυο;

Μπορείτε εύκολα να προστατεύσετε την ιδιωτική σας ζωή με το να μη δημοσιεύετε ποτέ προσωπικά σας δεδομένα, όπως το πραγματικό σας όνομα, τη διεύθυνσή σας, τον αριθμό τηλεφώνου, το όνομα του σχολείου (αν είστε ανήλικος), ή στοιχεία που αφορούν φίλους και οικογένεια. Όταν κάνετε chat, χρησιμοποιήστε ψευδώνυμο και αποφύγετε να μπαίνετε σε προσωπικές λεπτομέρειες, αν δεν γνωρίζετε προσωπικά το άτομο με το οποίο συνομιλείτε. Όταν επισκέπτεστε ιστοσελίδες που ζητούν τις προσωπικές σας πληροφορίες, σιγουρευτείτε ότι η

σελίδα είναι αξιόπιστη και πριν καταχωρήσετε τα στοιχεία σας, ρωτήστε για ποιο λόγο τα χρειάζονται. Πάντα να συμβουλεύεστε τους όρους και προϋποθέσεις (terms and conditions) και την πολιτική απορρήτου (privacy statement) της εταιρίας που διαχειρίζεται τον ιστοχώρο.

Αν κάποιος φίλος ζητήσει τον κωδικό της σύνδεσής μου στο Διαδίκτυο, να του τον δώσω;

Μην δίνετε τον κωδικό σας γιατί εσείς θα είστε υπεύθυνος για ότι δραστηριότητα κάνει ο φίλος ή η φίλη σας στο Διαδίκτυο. Γενικά δεν πρέπει ποτέ να αποκαλύπτετε τον κωδικό σας. Αν πιστεύετε ότι κάποιος ανακάλυψε τον κωδικό σας πρέπει να τον αλλάξετε άμεσα. Να χρησιμοποιείτε πάντα κωδικούς πρόσβασης που είναι δύσκολο να φανταστεί κανείς. Για παράδειγμα, να αποφεύγετε να χρησιμοποιείτε το όνομά σας, το επίθετό σας, ή ονόματα φίλων, κατοικίδιων και ημερομηνίες γενεθλίων

Είμαι ορατός στο Διαδίκτυο;

Όλοι οι χρήστες του Διαδικτύου, αφήνουν πάντα ίχνη, τα αποκαλούμενα «cybertrails» όταν είναι συνδεδεμένοι σε αυτό. Αυτό στην πραγματικότητα είναι καλό: αν κάποιοι διαπράττουν εγκλήματα στο Διαδίκτυο, η αστυνομία και άλλες αρχές μπορούν να εντοπίσουν τα αποδεικτικά στοιχεία και να τους πιάσουν.

Ένας ηλεκτρονικός φίλος μου ζήτησε να του στείλω μια φωτογραφία μου. Τι να κάνω;

Το να στέλνετε φωτογραφίες σε ηλεκτρονικούς φίλους δεν είναι και τόσο καλή ιδέα. Έτσι, λοιπόν αποφύγετε να στέλνετε δικές σας φωτογραφίες σε άτομα που γνωρίσατε μέσω Διαδικτύου και δεν γνωρίζετε προσωπικά.

Μια δική σας φωτογραφία θα κάνει πιο εύκολο τον εντοπισμό σας στον πραγματικό κόσμο. Επίσης να θυμάστε ότι μια ψηφιακή φωτογραφία σας μπορεί να υπάρχει για πάντα και αν κάποιος ηλεκτρονικός σας φίλος την έχει κρατήσει, μπορεί κάποια μέρα να συναντήσετε την επίμαχη φωτογραφία στο Διαδίκτυο και υπάρχει ΠΕΡΙΠΤΩΣΗ να μην μοιάζει καθόλου με το πρωτότυπο, καθότι η επεξεργασία μιας φωτογραφίας είναι με τα σημερινά μέσα απίστευτα εύκολη. Να θυμάστε πάντα ότι από τη στιγμή που ανεβάζετε μια φωτογραφία σας στο Διαδίκτυο, παύει πια να είναι προσωπική και δεν μπορείτε να ελέγξετε που θα δημοσιευθεί και από ποιόν θα χρησιμοποιηθεί.

Απόφαση για τα Προσωπικά Δεδομένα στο Facebook

Το Μονομελές Πρωτοδικείο Θεσσαλονίκης εξέδωσε την πρώτη στην Ελλάδα απόφαση για τα προσωπικά δεδομένα στο Facebook. Πρόκειται για την αίτηση ασφαλιστικών μέτρων που κατέθεσε διδάσκουσα σε πανεπιστημιακό τμήμα εναντίον ανθυποψηφίου της για θέση ΔΕΠ, ο οποίος ανήρτησε έγγραφα σχετικά με τις σπουδές της και την επαγγελματική της εξέλιξη -τα οποία εκείνη τού είχε χορηγήσει- σε συγκεκριμένο προφίλ στο Facebook, σχολιάζοντάς τα αρνητικά. Το δικαστήριο έκρινε ότι αυτό αποτελεί προσβολή της προσωπικότητάς της, είναι παράνομη πράξη και επέβαλε ποινή 1.000 ευρώ για κάθε περαιτέρω σχετική παράβαση (δημοσίευση και άλλων τέτοιων στοιχείων).

Ειδικότερα, όπως δέχθηκαν οι δικαστές στην απόφαση 16790/2009, ο έτερος υποψήφιος για την προκηρυχθείσα θέση και επίκουρος καθηγητής πανεπιστημιακού τμήματος, δημιούργησε στο Facebook ψεύτικο προφίλ στο οποίο δημοσίευσε τα εν λόγω έγγραφα (σχετικά με την ακαδημαϊκή, δημοσιογραφική και επαγγελματική πορεία της αιτούσας), χρησιμοποιώντας συκοφαντικούς χαρακτηρισμούς, αμφισβητώντας τους τίτλους της, κατηγορώντας την ότι έχει διασυνδέσεις με πολιτικά πρόσωπα κλπ.

Στη συνέχεια, φέρεται τα συγκεκριμένα κείμενα να εστάλησαν σε λίστα 300 περίπου ηλεκτρονικών διευθύνσεων από τον ακαδημαϊκό, πολιτικό και δημοσιογραφικό χώρο. Το δικαστήριο πιθανολόγησε ότι, μολονότι τα στοιχεία αναρτήθηκαν υπό ψευδώνυμο, πίσω από τη συγκεκριμένη πράξη ήταν ο εν λόγω διδάσκων, μιας και ήταν το μόνο πρόσωπο που είχε λάβει

κατά τον επίμαχο χρόνο τα αντίγραφα (του τα είχε προσκομίσει έπειτα από δικό του αίτημα η αιτούσα προς ενημέρωσή του).

Αξίζει να σημειωθεί ότι στις αναρτήσεις αυτές μπορούσε να έχει πρόσβαση ο οποιοσδήποτε (δεν ήταν «κλειστό» το προφίλ). Μεταξύ άλλων, φαίνεται ότι το ελληνικό δικαστήριο έλαβε υπόψη απόφαση του Δικαστηρίου των Ευρωπαϊκών Κοινοτήτων, σύμφωνα με την οποία η ανάρτηση προσωπικών δεδομένων σε δημόσια προσβάσιμη ιστοσελίδα αποτελεί «επεξεργασία» αυτών. Επιπλέον, όπως σχολιάζουν εμπλεκόμενοι στη δίκη, με την απόφαση αυτή αποδεικνύεται ότι, ακόμη και χωρίς άρση του απορρήτου, είναι δυνατόν να δοθεί δικαστική προστασία των προσωπικών δεδομένων από την ελληνική δικαιοσύνη.

Η Προστασία των Προσωπικών Δεδομένων

Καιρός ήταν να πάρει και η χώρα μας μια πρωτιά σ' ό,τι αφορά τη χρήση του Internet. Σύμφωνα με την ετήσια έκθεση των οργανισμών *Privacy International* και *Electronic Privacy Information Center* για το έτος 2007, η Ελλάδα παρείχε την καλύτερη προστασία στα προσωπικά δεδομένα των πολιτών της (προστασία του ιδιωτικού απορρήτου) από τις 47 χώρες που κάλυψε η σχετική έρευνα. Η χώρα μας αναγνωρίστηκε ως η μοναδική που λαμβάνει ικανοποιητικά μέτρα ασφαλείας κατά της κατάχρησης των προσωπικών δεδομένων. Εκείνο που επισημάνθηκε στην έκθεση ήταν ότι η προστασία του ιδιωτικού απορρήτου στο Διαδίκτυο επιδεινώθηκε σημαντικά κατά το έτος 2007, κυρίως στις προηγμένες δυτικές χώρες, από τις προσπάθειες των κυβερνήσεων και των μεγάλων επιχειρηματικών ομίλων να αποκτήσουν έλεγχο στα προσωπικά δεδομένα των πολιτών τα οποία διακινούνται online.

Η κατάσταση αναμένεται να επιδεινωθεί τα επόμενα χρόνια και από μια σειρά νέων μέτρων παρακολούθησης των πολιτών, όπως είναι οι νέες ταυτότητες και οι κάμερες παρακολούθησης. Μεγάλες χώρες, όπως η ΗΠΑ, η Ρωσία και η Κίνα, ανήκουν στον αντίποδα της λίστας, ασκούν δηλαδή μεγαλύτερο έλεγχο στα προσωπικά δεδομένα των πολιτών τους, και αυτό για δύο κυρίως λόγους όπως επισημαίνουν οι ειδικοί : για λόγους εθνικής ασφαλείας και για την καταγραφή των δεδομένων για επιχειρηματικούς σκοπούς. Πάντως, τον Μάρτιο του 2008 γερμανικό δικαστήριο απαγόρευσε την πρόσβαση στα προσωπικά δεδομένα των πολιτών που αφορούν τις τηλεφωνικές επικοινωνίες και τη χρήση του Internet. Το δικαστήριο έκρινε ότι οι διωκτικές αρχές μπορούν να έχουν πρόσβαση σ' αυτά τα δεδομένα μόνο σε περιπτώσεις ιδιαίτερα σοβαρών εγκλημάτων και μετά από δικαστική απόφαση.

Οι εταιρείες τηλεπικοινωνιών θα έχουν την υποχρέωση διατήρησης των τεχνικών δεδομένων των τηλεφωνικών συνδιαλέξεων και της πρόσβασης στο Internet για ένα εξάμηνο, όπως προβλέπει σχετικός νόμος που ψηφίσθηκε τον Ιανουάριο του 2008, αλλά θα υποχρεούνται να τα παραδίδουν στις διωκτικές αρχές μόνο σε πολύ σοβαρές περιπτώσεις. Σχετικός νόμος για την ηλεκτρονική παρακολούθηση των διαδικτυακών και τηλεφωνικών επικοινωνιών των πολιτών ψηφίστηκε στη Σουηδία τον Μάιο του 2008 και προβλέπει ότι όλες οι διακινούμενες πληροφορίες θα περνούν μέσα από φίλτρα για τον εντοπισμό τυχόν κρυπτογραφημένων μηνυμάτων ή συνθηματικών λέξεων. Η αντίδραση ενάντια στον νόμο ήταν άμεση από μεγάλη μερίδα Σουηδών πολιτών, οι οποίοι τονίζουν ότι θα πρέπει να ελέγχονται και οι αρχές και όχι μόνο οι απλοί πολίτες.

Έναν ανάλογο νόμο σκέφτεται να εφαρμόσει η κυβέρνηση της Μεγάλης Βρετανίας, κάνοντας μια σχετική ανακοίνωση τον Οκτώβριο του 2008. Στο πλαίσιο της καταπολέμησης της τρομοκρατίας, προτίθεται να δημιουργήσει μια τεράστια βάση δεδομένων όπου θα καταγράφονται όλα τα τηλεφωνήματα, τα e-mails αλλά και οι πληροφορίες που διακινούνται στο Διαδίκτυο, αλλά όχι και το περιεχόμενο των επικοινωνιών. Και στην ΠΕΡΙΠΤΩΣΗ της Μεγάλης Βρετανίας έντονες υπήρξαν οι αντιδράσεις από τα κόμματα της αντιπολίτευσης αλλά και από οργανώσεις ανθρωπίνων δικαιωμάτων.

Σύμφωνα με το νόμο περί διατήρησης των τηλεπικοινωνιακών δεδομένων (data retention), ο οποίος εφαρμόζεται ήδη στις ΗΠΑ και σε πολλά κράτη-μέλη της ΕΕ, οι πάροχοι τηλεπικοινωνιακών υπηρεσιών υποχρεούνται να διατηρούν για έξι μήνες τα στοιχεία από τις επικοινωνίες των πελατών τους, όπως είναι η πηγή και ο αποδέκτης κάθε τηλεφωνικής κλήσης,

γραπτού μηνύματος (sms) αλλά και μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail) καθώς και την ώρα της επικοινωνίας, αλλά όχι το περιεχόμενό της.

Πάντως, είναι γεγονός ότι από τότε που άρχισε να ισχύει ο νόμος αυτός, έχει αλλάξει ριζικά η τηλεπικοινωνιακή συμπεριφορά των πολιτών, καθώς ένα μεγάλο ποσοστό δηλώνει ότι έχει ήδη περιορίσει σημαντικά τις εμπιστευτικές του συνομιλίες με τα ηλεκτρονικά μέσα ή σκοπεύει να το κάνει πολύ σύντομα. Σύμφωνα με νομοσχέδιο που κατατέθηκε από το ελληνικό υπουργείο Δικαιοσύνης τον Μάιο του 2008 στη Βουλή προβλέπεται να αντιμετωπίζεται ως κακούργημα η μαγνητοφώνηση ή η μαγνητοσκόπηση τηλεφωνικών ή προφορικών συνομιλιών. Το υλικό αυτό δεν θα μπορεί να χρησιμοποιηθεί ως αποδεικτικό στα δικαστήρια εκτός από τις περιπτώσεις τέλεσης ιδιαίτερα σοβαρών εγκλημάτων ή θεμάτων που έχουν να κάνουν με τη δημόσια ασφάλεια.

Στη χώρα μας, σχετικός είναι ο Ν. 3471/2006 *«Προστασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών»*, όπου αναφέρεται ότι οποιαδήποτε επεξεργασία προσωπικών δεδομένων πρέπει να γίνεται με τη συγκατάθεση του πολίτη. Για να επικοινωνήσει μια εταιρεία τηλεφωνικά μ' έναν συνδρομητή για καθαρά διαφημιστικό σκοπό, θα πρέπει να έχει λάβει προηγουμένως τη συγκατάθεσή του. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα τηρεί ένα μητρώο με τα στοιχεία όσων πολιτών δεν επιθυμούν να λαμβάνουν διαφημιστικό υλικό και οι υπεύθυνοι επεξεργασίας των σχετικών αρχείων είναι υποχρεωμένοι να συμβουλεύονται αυτό το μητρώο πριν από κάθε επεξεργασία στοιχείων, ώστε να μην στέλνουν διαφημιστικό υλικό σε άτομα που δεν το επιθυμούν.

ΗΛΕΚΤΡΟΝΙΚΟΣ ΕΚΦΟΒΙΣΜΟΣ

Τι είναι Ηλεκτρονικός Εκφοβισμός

Ένα από τα πιο σοβαρά νομικά θέματα του Internet, του οποίου η αντιμετώπιση φαντάζει από δύσκολη έως αδύνατη και το οποίο καθημερινά λαμβάνει μεγάλες διαστάσεις, είναι αυτό του ηλεκτρονικού εκφοβισμού (cyberbullying), με θύματα κυρίως εφήβους και κατά πλειοψηφία αγόρια, ενώ τα κορίτσια δείχνουν ότι ξέρουν να προφυλάσσονται καλύτερα και να μην παρασύρονται εύκολα από τις ψηφιακές παρέες. Με το φαινόμενο ηλεκτρονικού εκφοβισμού (Cyberbullying) αναφερόμαστε στην ενδο και εξωσχολική βία που εκδηλώνεται μέσω ηλεκτρονικών συσκευών. Περιλαμβάνει την επαναλαμβανόμενη αποστολή ηλεκτρονικών ή τηλεφωνικών μηνυμάτων με απειλητικό, ρατσιστικό ή σεξιστικό περιεχόμενο, δημιουργία προφίλ διαδικτυακά με ψευδή στοιχεία, ανάρτηση ψεύτικων ειδήσεων, προσωπικών πληροφοριών, φωτογραφιών, βιντεοσκοπημένου υλικού καθώς και την υποκίνηση ενός ατόμου να λάβει μέρος σε μια ομάδα που έχει σκοπό την άσκηση βίας.Η τεχνολογία προσφέρει μια ανωνυμία που οδηγεί ορισμένους να συμπεριφέρονται καταχρηστικά online, με τρόπους που ποτέ δεν θα εξετάζαμε στον πραγματικό κόσμο. Κακόβουλο ή δυσφημιστικό περιεχόμενο μπορεί να κυκλοφορήσει με ευκολία και να το δει ένα ευρύτερο ακροατήριο. Το περιεχόμενο μπορεί ενδεχομένως να υπάρχει για πάντα, παρά τις καλύτερες προσπάθειες για την αφαίρεσή του.Ένα θύμα ηλεκτρονικής παρενόχλησης είναι δυνητικά ευάλωτο 24 ώρες το 24ωρο και δεν έχει πλέον ένα ασφαλές καταφύγιο μακριά από αυτόν που τον φοβερίζει.Η κυρία ***Βασιλική Γκουντσίδου***, που είναι μέλος της διοικούσας επιτροπής του Ευρωπαϊκού Προγράμματος E-Cost για το

cyberbullying, αναφέρει ότι ο ηλεκτρονικός εκφοβισμός συνιστά απειλή που εξαπλώνεται συνεχώς και η επίθεση μπορεί να γίνει με μηνύματα SMS, με κάμερες κινητών τηλεφώνων, με e-mail, μέσω chat room και γενικά μέσω του συνδυασμού των τεχνολογιών της κινητής τηλεφωνίας και του Internet.Ο ηλεκτρονικός εκφοβισμός μπορεί να σημαίνει βιντεοσκόπηση προσωπικών στιγμών και απειλή για ανάρτηση του σχετικού βίντεο στο Διαδίκτυο, παρενόχληση, δυσφήμηση, χρήση του προσωπικού λογαριασμού, δημοσιοποίηση προσωπικών στοιχείων και απόψεων κ.ά. Η κυρία Βασιλική Γκουντσίδου επισημαίνει ότι τα πιθανά συμπτώματα που πρέπει να ανησυχήσουν τους γονείς στην ΠΕΡΙΠΤΩΣΗ που το παιδί τους έχει πέσει θύμα ηλεκτρονικού εκφοβισμού είναι το ότι γίνεται αντικοινωνικό, παρουσιάζει διαταραχές ύπνου, μείωση του ενδιαφέροντος για το σχολείο και σε ακραίες περιπτώσεις τάσεις αυτοκτονίας. Επίσης, αποφεύγει να συζητά για τον υπολογιστή και το Internet, δείχνει ανήσυχο όταν λαμβάνει ηλεκτρονικά μηνύματα, είναι ευερέθιστο, παρουσιάζει συμπτώματα κατάθλιψης μετά τη χρήση υπολογιστή. Ανησυχητικές διαστάσεις λαμβάνει τελευταία το φαινόμενο του ηλεκτρονικού εκφοβισμού και στη χώρα μας, γνωστό με το όρο cyberbullying, καθώς μέσω του Διαδικτύου ή των νέων τεχνολογιών όλο και περισσότεροι νέοι δέχονται απειλές. Πρόσφατη μελέτη στο Λονδίνο σε μαθητές Γυμνασίου έδειξε ότι το 46% υπήρξαν θύματα επιθετικότητας με μηνύματα, με κάμερες κινητών τηλεφώνων, με e-mail, μέσω chat room ή και μέσω χρήσης Διαδικτύου, με τους θύτες να είναι συνήθως άτομα μεγαλύτερης ηλικίας.Ως bullying θεωρείται ο επαναλαμβανόμενος εκφοβισμός ατόμων με πραγματική ή απειλούμενη μαρτυρική ποινή φυσικής, προφορικής, γραπτής ή συναισθηματικής κακομεταχείρισής τους ή της αρπαγής της περιουσίας τους και συμπεριλαμβάνει και τις περιπτώσεις ύβρεων κατά της εθνικότητας, φυλής ή ιδιαιτερότητας κάποιου. Η καινούργια μορφή του εκφοβισμού και της παρενόχλησης μέσω του Διαδικτύου και των κινητών τηλεφώνων διαφέρει σε αρκετά σημεία από την κλασική, με το σημαντικότερο ότι το θύμα δεν μπορεί πλέον να νιώσει ασφάλεια ούτε μέσα στο ίδιο του το σπίτι.

Υπάρχει σχετική νομοθεσία προστασίας μας από φαινόμενα cyberbulling;

Ελληνική Νομοθεσία

Η Ελληνική νομοθεσία για την προστασία του απορρήτου και της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, αποτελεί έναν συνδυασμό διεθνών συνθηκών, συνταγματικών διατάξεων, διατάξεων του κοινού ποινικού δικαίου και νόμων που έχουν εκδοθεί βάσει κοινοτικών οδηγιών.

Στο Σύνταγμα της Ελλάδος, περιλαμβάνονται μια σειρά από διατάξεις, για την προστασία της ιδιωτικής σφαίρας του ατόμου. Η θεμελιώδης διάταξη του άρθρου 2 παρ. 1, αναφέρει ότι «ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν πρωταρχική υποχρέωση της πολιτείας». Σημαντικές διατάξεις περιλαμβάνονται στα άρθρα 9 και 19. Στο άρθρο 9, αναφέρεται ότι «η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη» διάταξη που απαγορεύει τη δημοσιοποίηση της ζωής του ατόμου. Το άρθρο 19 προστατεύει το απόρρητο των επιστολών και την ελεύθερη ανταπόκριση και επικοινωνία. Βασικό στοιχείο της επικοινωνίας αποτελεί η μυστικότητα του περιεχομένου της.

Στον Ποινικό Κώδικα, η προστασία του απορρήτου προβλέπεται από τα άρθρα 370, 370Α,370Β και 370Γ. Τα άρθρα 370 και 370Α αναφέρονται στην προστασία των επιστολών και την παραβίαση του απορρήτου των τηλεφωνημάτων και της προσωπικής συνομιλίας, αντίστοιχα. Η ανάλογη εφαρμογή των διατάξεων αυτών στο χώρο του Διαδικτύου, έχει προκαλέσει έντονο προβληματισμό στους νομικούς κύκλους, ιδιαίτερα όσον αφορά το άρθρο 370Α, το οποίο κατά πολλούς, θεωρείται ότι δεν μπορεί να τύχει εφαρμογής στο Διαδίκτυο, αν και η σύνδεση γίνεται μέσω μισθωμένης τηλεφωνικής γραμμής (Καράκωστας, 2001). Το άρθρο 370Β, παρέχει ικανοποιητική προστασία μόνο όμως για κρατικά, επιστημονικά και επαγγελματικά απόρρητα, αποκλείοντας τα ιδιωτικά απόρρητα. Η πιο ουσιαστική διάταξη, όσον αφορά το χώρο του Διαδικτύου, περιλαμβάνεται στο άρθρο 370Γ, που τιμωρεί τη χωρίς άδεια πρόσβαση σε δεδομένα αποθηκευμένα σε Η/Υ. Το απόρρητο στην ΠΕΡΙΠΤΩΣΗ αυτή προστατεύεται υπό μία ευρεία έννοια. Δεν περιλαμβάνει μόνο δεδομένα τα οποία χαρακτηρίζονται από τη φύση τους απόρρητα, αλλά προστατεύεται το δικαίωμα του νομίμου

κατόχου των δεδομένων να αποκλείει σε άλλους την πρόσβαση σε όλα τα δεδομένα, που είναι αποθηκευμένα στον υπολογιστή του. Τα παραπάνω άρθρα του Ποινικού Κώδικα δεν είναι αρκετά για να καλύψουν τις ανάγκες δίωξης της ηλεκτρονικής εγκληματικότητας, η οποία παράλληλα πάντα με τις τεχνολογικές εξελίξεις εμφανίζεται με νέες μορφές. Άλλωστε στα συγκεκριμένα άρθρα δεν έχει προβλεφθεί η ύπαρξη του διαδικτύου το οποίο πλέον δίνει νέες διαστάσεις στο ζήτημα. Αδικήματα όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης δεν μπορούν να τιμωρηθούν με βάση την ισχύουσα στην Ελλάδα νομοθεσία. Αυτό το κενό βέβαια αντιμετωπίζεται με την υπάρχουσα νομοθεσία για τα συμβατικά εγκλήματα, εφόσον ο εικονικός κόσμος του διαδικτύου θεωρηθεί απλά ως ένα ακόμα μέσο για τη διάπραξη εγκλημάτων. Ακόμα, διατάξεις που σχετίζονται με το ηλεκτρονικό έγκλημα περιλαμβάνονται στο Π.Δ. 131/2003 που αναφέρεται στην ανεπιθύμητη αλληλογραφία (spamming) και στην ευθύνη των παρόχων υπηρεσιών διαδικτύου για πράξεις των χρηστών που είναι συνδρομητές τους. Το συγκεκριμένο Π.Δ. θεσπίστηκε σε εφαρμογή της κοινοτικής οδηγίας για το ηλεκτρονικό εμπόριο. Επίσης ο Ν.2867/2000 για την «οργάνωση και λειτουργία του τομέα των Τηλεπικοινωνιών», οι Ν.2774/1999 και Ν.2472/1997 «περί προσωπικών δεδομένων» και ο Ν.2225/1994 για την «προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας» σχετίζονται με κάποιες πτυχές του ηλεκτρονικού εγκλήματος..

Τι πρέπει να κάνει ένας έφηβος όταν πέσει θύμα cyberbulling;

1. Ενδεικτικοί τρόποι αντιμετώπισης του παραπάνω διαδικτυακού κινδύνου επισημαίνονται παρακάτω:
2. Εάν πέσουμε θύμα εκφοβισμού, σταματάμε αμέσως την επικοινωνία με το θύτη.
3. Εμπιστευόμαστε στους γονείς μας ή σε κάποιο ενήλικα τον εκφοβισμό που έχουμε δεχθεί.
4. Δεν προωθούμε εκφοβιστικά μηνύματα.
5. Αν γνωρίζουμε κάποιο φίλο που είναι θύτης τον συμβουλεύουμε να σταματήσει.
6. Φιλτράρουμε ηλεκτρονικά μηνύματα από άτομα που μάς παρενοχλούν και μπλοκάρουμε την πρόσβασή τους σε προσωπικούς δικτυακούς χώρους (π.χ., ιστολόγιο).

Είναι χρήσιμο να επισημανθεί ότι στην ηλεκτρονική διεύθυνση http://www.antibullying.eu παρουσιάζεται η Ευρωπαϊκή καμπάνια κατά του σχολικού εκφοβισμού σε όλες του τις μορφές (π.χ., διαδικτυακός εκφοβισμός) που υλοποιείται στα πλαίσια του κοινοτικού προγράμματος Daphne III[1]. Ο στόχος του συγκεκριμένου προγράμματος συνίσταται στη δημιουργία μιας ενιαίας πολιτικής στην καταγραφή και διαχείριση του σχολικού εκφοβισμού και την δημιουργία μιας Ευρωπαϊκής πλατφόρμας για την ενημέρωση των παιδιών, γονέων, εκπαιδευτικών και κάθε άμεσα ενδιαφερόμενου για το συγκεκριμένο πρόβλημα.

GROOMING: ΣΕΞΟΥΑΛΙΚΗ ΑΠΟΠΛΑΝΗΣΗ

Τι σημαίνει ο όρος Grooming

Ο όρος **Grooming** αναφέρεται στην αποπλάνηση και συμβαίνει όταν άγνωστοι εκμεταλλεύονται κακόβουλα το στοιχείο της ανωνυμίας στο Διαδίκτυο για να προσεγγίσουν ανήλικους με στόχο τη σεξουαλική παρενόχληση. Γενικά, στο Διαδίκτυο ποτέ δεν μπορούμε να είμαστε σίγουροι ποιος είναι ο συνομιλητής μας στις ηλεκτρονικές μας επικοινωνίες, ακόμα και αν βλέπουμε τη φωτογραφία του ή αν χρησιμοποιούμε ψηφιακή κάμερα. Έτσι, πολλοί επιτήδειοι εκμεταλλεύονται το γεγονός αυτό, δίνουν ψεύτικα στοιχεία (π.χ., ηλικία) και ξεκινούν συζητήσεις με τα πιθανά θύματά τους με στόχο να αναπτύξουν φιλική σχέση και να αποσπάσουν όσο το δυνατό περισσότερες πληροφορίες (π.χ., τόπο διαμονής, τα ενδιαφέροντά τους, τις σεξουαλικές τους εμπειρίες κλπ). Το Grooming αποτελεί ένα είδος ψυχολογικού χειρισμού και για το λόγο αυτό είναι σημαντικό **να εξηγήσουμε στους γονείς** πως οφείλουν να είναι ενημερωμένοι για τις

διαδικτυακές γνωριμίες των παιδιών τους ώστε, όταν παρατηρήσουν κάτι ύποπτο, να μπορέσουν να τα συμβουλέψουν αποτελεσματικά και να δράσουν άμεσα.

ΠΑΙΔΙΚΗ ΠΟΡΝΟΓΡΑΦΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Παιδιά και Πορνογραφία

Σύμφωνα με στοιχεία του Ευρωβαρόμετρου, το 74% των παιδιών ηλικίας 12-15 ετών χρησιμοποιεί 3 ώρες τουλάχιστον καθημερινά το Internet και είναι επίσης διαπιστωμένο ότι όλα σχεδόν τα παιδιά εκτίθενται τυχαία σε υλικό πορνογραφικού περιεχομένου κατά την περιήγησή τους στο Διαδίκτυο. Από άλλες έρευνες προκύπτει ότι υπάρχει μια αύξηση κατά 16% της πορνογραφικής παρουσίασης παιδιών στο Internet και υπολογίζονται σε περισσότερες από 500.000 οι φωτογραφίες πορνογραφικού περιεχομένου με πρωταγωνιστές παιδιά και σε περισσότερα από 20.000 τα παιδιά που συμμετέχουν στο κύκλωμα.

Με βάση τα παραπάνω, το Ευρωπαϊκό Κοινοβούλιο ενέκρινε τον Νοέμβριο του 2008 τη θέσπιση ενός πολυετούς προγράμματος για την προστασία των παιδιών που είναι χρήστες του Internet. Συντάκτης της γνωμοδότησης σχετικά με την ενδυνάμωση της ασφάλειας και των θεμελιωδών ελευθεριών στο Διαδίκτυο ορίστηκε ο Έλληνας ευρωβουλευτής Μανώλης Μαυρομμάτης.

Η Παιδοφιλία στα ChatRooms

Είναι γεγονός ότι το Internet έχει εξελιχθεί στον πλέον κατάλληλο χώρο όπου μπορούν να δράσουν οι παιδόφιλοι, οι οποίοι χρησιμοποιούν κατά κόρο τα λεγόμενα chat rooms (δωμάτια ανοικτής επικοινωνίας) που επιτρέπουν τη διατήρηση της ανωνυμίας των χρηστών και της απόλυτης ελευθερίας εκφράσεων. Οι ειδικοί μάς ενημερώνουν ότι ως σύνδρομο η παιδοφιλία δεν έχει αλλάξει από αρχαιοτάτων χρόνων και αυτό που αλλάζει είναι το μέσο καθώς το Διαδίκτυο διευκολύνει έναν ενήλικο να γνωρίσει και να παγιδεύσει έναν ανήλικο με όπλο την ανωνυμία και τη δυσκολία εντοπισμού του.

Ο επίκουρος καθηγητής του Τμήματος Κοινωνιολογίας του Πανεπιστημίου Αιγαίου κ. Ευστράτιος Παπάνης με μια ομάδα φοιτητών δημιούργησαν δύο εικονικά προφίλ ανηλίκων σ' ένα chat room με στόχο την καταγραφή των κοινωνικών και ψυχολογικών χαρακτηριστικών των ατόμων που έρχονται σε επαφή με ανήλικα παιδιά, τη θεματολογία της συνομιλίας και τον βαθμό διακίνησης πορνογραφικού υλικού. Τα συμπεράσματά τους μετά από μια εξάμηνη έρευνα είναι αποκαλυπτικά. Οι χρήστες που προσέγγισαν τους δύο υποτιθέμενους ανήλικους ήταν εκατοντάδες αλλά περίπου 50 ήταν αυτοί που επέμεναν να επικοινωνήσουν μαζί τους με περισσότερες λεπτομέρειες παρά το υποτιθέμενο νεαρό της ηλικίας των συνομιλητών τους.

Αποδείχθηκε ότι το 16% των 50 αυτών χρηστών εμφάνισαν παιδοφιλικά χαρακτηριστικά, οι οποίοι ενώ ξεκινούσαν συνήθως με ευγενικές εκφράσεις στη συνέχεια γινόντουσαν χυδαίοι και άσεμνοι και ζητούσαν επιμόνως τη χρήση web κάμερας. Συνέχιζαν με ερωτήσεις σεξουαλικού περιεχομένου και με αποστολή πορνογραφικού υλικού παρά το ότι ήταν ενήμεροι για την ηλικία του συνομιλητή τους. Η ηλικία των χρηστών ήταν 20-27 ετών και ήταν κυρίως κάτοικοι αστικών περιοχών.

Πάντως, είναι ενθαρρυντικό το γεγονός ότι το 84% των συνομιλητών που προσέγγισαν τους δύο υποτιθέμενους ανηλίκους είχαν φυσιολογική συμπεριφορά καθώς διέκοψαν τη συνομιλία αμέσως και μάλιστα 3 απ' αυτούς προέτρεψαν τους ανηλίκους να βγουν από το chat room και 2 τούς παρότρυναν να ενημερώσουν τους γονείς τους. Φαίνεται ότι έχει πιάσει τόπο η εκστρατεία που έχει ξεκινήσει η πολιτεία μέσω των προγραμμάτων SaferInternet και SafeLine αλλά και άλλων.

Ζωντανοί Βιασμοί Ανηλίκων

Μια ιδιαίτερη ΠΕΡΙΠΤΩΣΗ παιδικής πορνογραφίας απασχόλησε το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής τον Μάρτιο του 2009 καθώς εντοπίστηκαν ένας Σκοτσέζος στο Ηράκλειο Κρήτης και ένας επιχειρηματίας στην Αθήνα να συμμετέχουν σε κύκλωμα όπου παρουσιάζονταν ζωντανές μεταδόσεις βιασμού και σεξουαλικής κακοποίησης μικρών παιδιών.

Οδηγίες και συμβουλές προς γονείς και παιδιά

Σε ότι αφορά την προστασία των ανηλίκων από το φαινόμενο του grooming πρέπει να δοθεί ιδιαίτερη έμφαση στα παρακάτω: Το παιδί πρέπει να κατανοήσει ότι σε χώρους όπως τα chat room δεν μπορούμε ποτέ να είμαστε σίγουροι για την ταυτότητα του άλλου. Επομένως πρέπει να αντιμετωπίζει τις διαδικτυακές γνωριμίες με αρκετή επιφυλακτικότητα, καθώς ακόμη και άτομα που έχουν κερδίσει την εμπιστοσύνη του μπορεί να έχουν σκοπό να το βλάψουν. Υπάρχει η δυνατότητα αποθήκευσης των συνομιλιών που πραγματοποιείτε στα chat room. Κάτι τέτοιο είναι ιδιαίτερα χρήσιμο για να μπορέσετε να κάνετε κάποια καταγγελία στην ΠΕΡΙΠΤΩΣΗ που κάποιος προσπαθεί να παρενοχλήσει το παιδί. Δεν είναι ασφαλές να δίνετε τα προσωπικά στοιχεία επικοινωνίας σε ένα chat room. Άλλωστε αν κάποιος επιτήδειος γνωρίζει το κινητό τηλέφωνο, τη διεύθυνση κατοικίας και το σχολείο, ακόμη και αν το παιδί αποφασίσει να αποφύγει τη διαδικτυακή επικοινωνία, μπορεί εύκολα να εντοπιστεί στον φυσικό κόσμο.Οι γονείς οφείλουν να είναι ενημερωμένοι για τις διαδικτυακές γνωριμίες των παιδιών τους ώστε όταν παρατηρήσουν κάτι ύποπτο να μπορέσουν να τα συμβουλέψουν αποτελεσματικά.

Υπάρχει σχετική νομοθεσία για την παιδική πορνογραφία;

Με αφορμή τη μεγάλη επιχείρηση, η οποία πραγματοποιήθηκε τον τελευταίο μήνα (25-6 έως 26-7/2012), από στελέχη του Σώματος Δίωξης Ηλεκτρονικού Εγκλήματος, για την αντιμετώπιση του φαινομένου της κατοχής και διακίνησης ψηφιακού υλικού παιδικής πορνογραφίας, παραθέτουμε σχετικά την ισχύουσα νομοθεσία στη χώρα μας.

Στην κορωνίδα του άμεσου ποινικού ενδιαφέροντος βρίσκονται όλες εκείνες οι εγκληματικές πράξεις που μπορούν να βλάψουν τα παιδιά είτε θίγοντας τη γενετήσια αξιοπρέπειά τους είτε βλάπτοντας την ψυχική και σωματική τους υγεία. Εδώ εντάσσεται η διακίνηση παιδικής πορνογραφίας, η προσέλκυση παιδιών για γενετήσιους λόγους, η σεξουαλική παρενόχληση και η προσβολή της γενετήσιας αξιοπρέπειας, περιπτώσεις οι οποίες αναλύονται εκτενέστερα στο αρχείο παρακάτω. Στα εγκλήματα κατά των ανηλίκων χρηστών εντάσσεται επίσης η προτροπή σε αυτοκτονία, φαινόμενο ιδιαίτερα συχνό στο χώρο του Διαδικτύου, καθώς επίσης και ο λεγόμενος κυβερνοεκφοβισμός (cyber bullying).

Ειδικότερα, στελέχη της Δίωξης Ηλεκτρονικού Εγκλήματος, μετά από αστυνομική διαδικτυακή έρευνα, πραγματοποίησαν τον τελευταίο μήνα παράλληλες επιχειρήσεις σε Αττική, Θεσσαλονίκη, Ροδόπη, Ηράκλειο και Χανιά, όπου διαπιστώθηκε ότι 15 κατηγορούμενοι κατείχαν σε ψηφιακή μορφή «σκληρό» υλικό παιδικής πορνογραφίας.

Από την περαιτέρω ψηφιακή ανάλυση των ηλεκτρονικών ιχνών, προέκυψε ότι δύο από τους κατηγορούμενους προσέλκυαν ανήλικους, μέσω forums, chat-rooms και των social media καθώς προφασιζόμενοι ότι είναι συνομήλικοι τους, αποσπούσαν ερωτικές τους φωτογραφίες και βίντεο και στη συνέχεια τους εκβίαζαν για να συνευρεθούν ερωτικά μαζί τους. Επιπλέον διαπιστώθηκε ότι διαμοίραζαν υλικό παιδικής πορνογραφίας σε άλλους χρήστες του διαδικτύου, ενώ ακόμα επιδίωκαν την ανταλλαγή και την πώληση του υλικού αυτού.

Στο πλαίσιο της συνεργασίας με τις αντίστοιχες Υπηρεσίες της Interpol και της Europol, διαπιστώθηκε ότι πέντε (5) από τους συλληφθέντες είχαν καταβάλλει μεγάλα χρηματικά ποσά, είτε για την αγορά ψηφιακού υλικού παιδικής πορνογραφίας, είτε για την απευθείας παρακολούθηση υλικού κακοποίησης ανηλίκων, από «κρυφή» ιστοσελίδα του εξωτερικού. Παράλληλα διαμοίραζαν αυτό το υλικό σε άλλους χρήστες του διαδικτύου, μέσω ιστοσελίδων και προγραμμάτων ανταλλαγής αρχείων (Peer to Peer).

Σχετική νομοθεσία: Ν. 3064/2002 (για πρώτη φορά εισήχθη στον Ελληνικό Ποινικό Κώδικα το άρθρο 348Α, το οποίο μεταξύ άλλων αφορούσε στη «διακίνηση παιδικής πορνογραφίας μέσω Διαδικτύου»), Ν. 3625/2007 και Ν. 3666/2008 ο οποίος και συμπεριέλαβε το έγκλημα του 348Α στις περιπτώσεις άρσης του απορρήτου των επικοινωνιών.

Πέρα όμως από τη διακίνηση παιδικής πορνογραφίας, οι ανήλικοι χρήστες έρχονται να αντιμετωπίσουν και άλλων παράνομες πράξεις όπως είναι η προσβολή της γενετήσιας αξιοπρέπειας. Αυτού του είδους η πράξη ποινικοποιείται βάσει του 337 άρθρο του Ποινικού Κώδικα και δυστυχώς λαμβάνει χώρα καθημερινά. Σύμφωνα με όσα ορίζει η διάταξη στην παράγραφο 3 που προστέθηκε με το Ν. 3727/2008:

«Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο που δεν συμπλήρωσε τα 15 έτη και, με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του ανηλίκου στο πεδίο της γενετήσιας ζωής του, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση, ο ενήλικος τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.» Ο νομοθέτης εδώ, με τον όρο «ή άλλου επικοινωνιακού μέσου».

Αντιθέτως, όταν ο ενήλικος πέραν της επικοινωνίας με την/ον ανήλικο, προσποιείται επιπλέον τον ανήλικο με σκοπό να τον προσεγγίσει ευκολότερα και εν τέλει να έρθει σε σεξουαλική επαφή μαζί του στον πραγματικό κόσμο, τότε γίνεται λόγος για το φαινόμενο “Grooming”. Παρά το γεγονός ότι δεν υπάρχει ο όρος “grooming” στον ελληνικό ποινικό κώδικα, εν τούτοις αυτή η πράξη τιμωρείται βάσει του άρθρου 348Β Π.Κ., όπως αυτό προστέθηκε με το Ν. 3727/2008. Κύριο στοιχείο της αντικειμενικής υπόστασης του 348 Π.Κ. είναι ο ενήλικας μέσω της τεχνολογίας πληροφόρησης και επικοινωνίας να αποσκοπεί στην αποπλάνηση του παιδιού (339 Π.Κ.) και στο φυσικό κόσμο

Παραδείγματα διακίνησης πορνογραφικού υλικού στην Ελλάδα και στην Ευρώπη

Μια ιδιαίτερη ΠΕΡΙΠΤΩΣΗ παιδικής πορνογραφίας απασχόλησε το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής τον Μάρτιο του 2009 καθώς εντοπίστηκαν ένας Σκοτσέζος στο Ηράκλειο Κρήτης και ένας επιχειρηματίας στην Αθήνα να συμμετέχουν σε κύκλωμα όπου παρουσιάζονταν ζωντανές μεταδόσεις βιασμού και σεξουαλικής κακοποίησης μικρών παιδιών.

Εξάρθρωση Κυκλώματος Παιδικής Πορνογραφίας

Οι υπηρεσίες δίωξης ηλεκτρονικού εγκλήματος στην Αθήνα και τη Θεσσαλονίκη εξάρθρωσαν τον Ιανουάριο του 2009 μεγάλο κύκλωμα παιδικής πορνογραφίας στο οποίο συμμετείχαν 24 Έλληνες χρήστες από διάφορες περιοχές της χώρας, όλοι υπεράνω πάσης υποψίας και ανάμεσά τους κληρικοί, γιατροί, στρατιωτικοί και επιχειρηματίες. Η υπόθεση άρχισε να ερευνάται από την Μητροπολιτική Αστυνομία του Λονδίνου, η οποία εντόπισε κύκλωμα διακίνησης υλικού παιδικής πορνογραφίας στο Διαδίκτυο για VIPs και βρέθηκαν ψηφιακά ίχνη και στην Ελλάδα. Έγινε άρση απορρήτου από την εισαγγελία, εντοπίστηκαν 137 ηλεκτρονικά ίχνη Ελλήνων χρηστών και η έρευνα κατέληξε στον εντοπισμό 24 ατόμων, από τους οποίους συνελήφθησαν οι 11 στο πλαίσιο του αυτοφώρου.

Στους 4 από τους συλληφθέντες ασκήθηκε ποινική δίωξη για πορνογραφία ανηλίκων με χρήση του Διαδικτύου κατ’ εξακολούθηση και από συνήθεια, που διώκεται σε βαθμό κακουργήματος σύμφωνα με τη νέα νομοθεσία. Για τις συλλήψεις των χρηστών οργανώθηκε επιχείρηση από την αστυνομία με την κωδική ονομασία Myosis. Όμως, τα στοιχεία της ΕΛ.ΑΣ. από την εξάρθρωση των κυκλωμάτων διακίνησης υλικού παιδικής πορνογραφίας προκαλούν

σκεπτικισμό καθώς από το καλοκαίρι του 2004 που άρχισε να δραστηριοποιείται και να σημειώνει επιτυχίες το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος, 219 υποθέσεις παιδικής πορνογραφίας την έχουν απασχολήσει, 220 πολίτες έχουν κατηγορηθεί, 107 έχουν συλληφθεί, 31 έχουν προφυλακισθεί και σχεδόν κανένας δεν έχει καταδικαστεί.

Αντίθετα, πολίτες που έχουν συλληφθεί για το αδίκημα αυτό, έχουν αθωωθεί και αξιώνουν μεγάλες αποζημιώσεις από το Ελληνικό Δημόσιο για τις ημέρες της κράτησής τους συνεκτιμώντας την ηθική και περιουσιακή βλάβη που υπέστησαν και την καταστροφή της ζωής τους. Οι συλληφθέντες από τις δύο πρόσφατες επιχειρήσεις της ΕΛ.ΑΣ. με τις ονομασίες «Καρουσέλ» και «Μύοσις» προβλέπεται να δικαστούν με βάση τον νέο νόμο, ο οποίος τιμωρεί ως κακούργημα ακόμα και την κατοχή υλικού παιδικής πορνογραφίας, αλλά η δημοσιοποίηση των ονομάτων όσων έχουν συλληφθεί ή κατηγορηθεί χωρίς ακόμα να έχουν καν δικαστεί, έχει προκαλέσει αντιδράσεις και προβληματισμό σε έγκριτους νομικούς κύκλους.

SEXTING

Το **sexting** ορίζεται ως η πράξη αποστολής, λήψης και διατήρησης μηνυμάτων σεξουαλικού περιεχομένου με φωτογραφικό ή οπτικοακουστικό υλικό μέσω κινητού τηλεφώνου ή άλλου μέσου ψηφιακής τεχνολογίας. Τυπικά το sexting, στα πλαίσια του σχολείου, εμφανίζεται περισσότερο μέσα από τη χρήση κινητών τηλεφώνων, ωστόσο με τις αυξημένες δυνατότητες διαδικτυακής πρόσβασης των σύγχρονων συσκευών (κινητά τηλέφωνα, notebooks, tablets κλπ), τα υβριδικά μηνύματα πορνογραφικού περιεχομένου (**sexts**) δύναται να μεταδίδονται μέσω e-mail, μέσω ιστοτόπων κοινωνικής δικτύωσης κλπ. Μια επιφανειακή προσέγγιση του sexting καθιστά προφανές το γεγονός ότι οι εμπλεκόμενοι μαθητές δεν κατανοούν πλήρως όλες τις πτυχές και τους κινδύνους του συγκεκριμένου φαινομένου. Οι εμπλεκόμενοι έφηβοι, συχνά δεν μπορούν να διανοηθούν ότι ένα sext μπορεί να προωθηθεί σε πολλαπλούς αποδέκτες καθώς και ότι κάτι που προορίζονταν στα πλαίσια μιας ιδιαίτερα προσωπικής επικοινωνίας, δύναται να έχει διανεμηθεί σε πολλαπλούς παραλήπτες. Επίσης, οι περισσότεροι έφηβοι αγνοούν ότι η αποστολή ή προώθηση υλικού που απεικονίζει ανήλικο σε γυμνή ή ημίγυμνη φωτογραφία εμπίπτει σε νομικές διατάξεις παιδικής πορνογραφίας

Που μπορώ να καταγγείλω ύποπτες σελίδες;

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 δέχεται καταγγελίες για ιστοχώρους (websites) ή υπηρεσίες νέων (newsgroups) που περιέχουν:

1. Εικόνες κακομεταχείρισης των παιδιών, οπουδήποτε στον κόσμο.

2. Ρατσιστικό και ξενοφοβικό περιεχόμενο που, κατά την άποψή σας, παραβαίνει την Ελληνική νομοθεσία.

3. Άλλο περιεχόμενο, παράνομο, κατά την άποψή σας.

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 της Ευρωπαϊκής Ένωσης των hotlines INHOPE.

ΚΙΝΔΥΝΟΙ ΑΠΟ ΤΗ ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΓΙΑ ΕΝΑΝ ΠΑΙΔΙ-ΕΦΗΒΟ

PHISHING

Τι ονομάζεται phishing- οικονομική εξαπάτηση;

Πρόκειται για μια ιδιαίτερα διαδεδομένη τεχνική οικονομικής εξαπάτησης μέσω του «ψαρέματος» προσωπικών δεδομένων και ειδικότερα στοιχείων που αφορούν οικονομικές συναλλαγές (αριθμό λογαριασμού, κωδικό πιστωτικής κάρτας κ.λπ.).

Από πού προέρχεται ο όρος phishing;

Ο όρος είναι μια παραλλαγή της αλιείας, πιθανώς επηρεασμένος από phreaking, και παραπέμπει στο «δόλωμα». Χρησιμοποιείται με την ελπίδα ότι το ενδεχόμενο θύμα θα "δαγκώνει" κάνοντας κλικ σε ένα κακόβουλο link ή το άνοιγμα ενός κακόβουλου αρχείου, προγραμματισμένου να αντιγράψει οικονομικά στοιχεία ή και κωδικούς πρόσβασης.

Η έκφραση “phishing” προέρχεται από την συνήθεια των hackers να χαρακτηρίζουν τους ηλεκτρονικούς τόπους στους οποίους έχουν πρόσβαση “phish”.

Πώς μπορείτε να εντοπίσετε ένα μήνυμα ψαρέματος;

Οι επιτήδειοι της ηλεκτρονικής απάτης σας πλησιάζουν με ψεύτικα προσχήματα. Οι απάτες ψαρέματος μπορεί να γίνουν αυτοπροσώπως ή μέσω τηλεφώνου ενώ διακινούνται μέσω ανεπιθύμητων ηλεκτρονικών μηνυμάτων, pop up windows ή άμεσων μηνυμάτων (Instant messaging). Μια κοινή τεχνική ψαρέματος είναι το άνοιγμα ενός ψεύτικου αναδυόμενου παραθύρου όταν κάποιος κάνει κλικ σε ένα ηλεκτρονικό μήνυμα ψαρέματος. Μπορεί να φαίνεται πολύ πειστικό ή μπορεί να εμφανίζεται πάνω από ένα παράθυρο που εμπιστεύεστε. Ακόμη και εάν το αναδυόμενο παράθυρο φαίνεται πολύ επίσημο ή διακηρύσσει πως είναι ασφαλές, θα πρέπει να αποφεύγετε να εισάγετε ευαίσθητα προσωπικά δεδομένα γιατί δεν υπάρχει τρόπος να ελέγξετε την πιστοποίηση ασφάλειας.

Παρά την πιστή αντιγραφή γνήσιων και νόμιμων μηνυμάτων τα phishing emails είναι εύκολο να τα διακρίνετε από τα ακόλουθα σημεία:

Η προσφώνηση είναι γενική και δεν αναφέρει το όνομα του παραλήπτη, όπως π.χ. "Αγαπητέ πελάτη"

Ενδέχεται το κείμενο να μην είναι ορθό συντακτικά επειδή είναι προϊόν αυτόματης μετάφρασης στα Ελληνικά από άλλη γλώσσα.

Η πλειοψηφία των phishing μηνυμάτων επικαλείται κάποιο πρόβλημα, κάποια ενέργεια αναβάθμισης υπηρεσίας ή κάποια "μοναδική ευκαιρία" και δηλώνοντας ως επείγουσα την ενέργεια που πρέπει να γίνει από τον παραλήπτη.

Συνήθως ζητείται ο παραλήπτης να απαντήσει δίνοντας προσωπικά στοιχεία ή να επισκεφθεί συγκεκριμένη ιστοσελίδα, μέσα από σύνδεσμο (link) που περιλαμβάνεται στο κείμενο, η οποία προσομοιάζει ή και αντιγράφει ακριβώς τις οικείες ιστοσελίδες των πραγματικών εταιρειών με τις οποίες ο παραλήπτης μπορεί να έχει συναλλακτική σχέση. Τα

στοιχεία που ζητούνται ενδέχεται να αφορούν τραπεζικούς λογαριασμούς, πιστωτικές κάρτες ή όνομα χρήστη (username) και κωδικό πρόσβασης (password).

Η εκτέλεση λογισμικού προστασίας από ιούς μπορεί να βοηθήσει στην προστασία σας από απάτες ψαρέματος. Αληθεύει;

Αν και το λογισμικό προστασίας από ιούς δεν μπορεί να σας αποτρέψει να ανοίξετε ένα πλαστό ηλεκτρονικό μήνυμα ή να κάνετε κλικ σε επικίνδυνους συνδέσμους, μπορεί εντούτοις να σταματήσει ιούς ή λογισμικό υποκλοπής που θα προέλθει από τέτοιες ενέργειες. Κάποιο πλαστό ηλεκτρονικό μήνυμα μπορεί να σας οδηγήσει σε τοποθεσίες Web που εγκαθιστούν στον υπολογιστή σας λογισμικό το οποίο συνεχίζει να καταγράφει τις πληροφορίες που εισάγετε όπως τον κωδικό πρόσβασης, πληροφορίες σύνδεσης και δεδομένα του λογαριασμού. Αυτού του είδους το ανεπιθύμητο λογισμικό συχνά καλείται spyware (λογισμικό υποκλοπής) ενώ μπορεί να περιέχει ακόμη και ιό.

Τι πρέπει να κάνουμε όταν λαμβάνουμε ένα μήνυμα phishing;

Αποφύγετε την κοινοποίηση προσωπικών και ευαίσθητων στοιχείων σας μέσω τηλεφώνου, e-mail ή/και ηλεκτρονικής φόρμας, εφόσον δεν έχετε επιβεβαιώσει ότι το αίτημα έχει προέλθει από την ίδια την εταιρεία με την οποία συνεργάζεστε και η οποία παρουσιάζεται ως αποστολέας.

Βεβαιωθείτε ότι ο τομέας της διεύθυνσης URL στη συγκεκριμένη σελίδα είναι σωστός και κάντε κλικ σε οποιεσδήποτε εικόνες ή συνδέσμους, για να επαληθεύσετε ότι σας οδηγούν στις σωστές σελίδες μέσα στον ιστότοπο.

Αναζητάτε πάντοτε το εικονίδιο με το κλειστό λουκέτο στη γραμμή κατάστασης που βρίσκεται στο κάτω μέρος του παραθύρου του προγράμματος περιήγησής σας κάθε φορά που πληκτρολογείτε προσωπικά στοιχεία, όπως ο κωδικός πρόσβασής σας.

Ελέγχετε τις κεφαλίδες των μηνυμάτων. Το πεδίο "Από:" παραποιείται εύκολα ώστε να εμφανίζει ένα παραπλανητικό όνομα αποστολέα.

Εάν εξακολουθείτε να έχετε αμφιβολίες, επικοινωνήστε με τον οργανισμό από τον οποίο εμφανίζεται ότι έχει αποσταλεί το μήνυμα. Μη χρησιμοποιήσετε τη διεύθυνση απάντησης που δίνεται στο μήνυμα, καθώς μπορεί να είναι πλαστογραφημένη. Αντίθετα, επισκεφθείτε τον επίσημο ιστότοπο της συγκεκριμένης εταιρείας και αναζητήστε μια διαφορετική διεύθυνση επικοινωνίας.

Στην ΠΕΡΙΠΤΩΣΗ που δηλώσατε τον λογαριασμό σας ή προσωπικά σας στοιχεία απαντώντας σε κάποιο πλαστογραφημένο μήνυμα ή σε μήνυμα ηλεκτρονικού "ψαρέματος" (phishing), θα πρέπει να δράσετε άμεσα. Στείλτε ένα αντίγραφο της κεφαλίδας και του πλήρους κειμένου του μηνύματος στην εταιρεία που σας παρέχει το ηλεκτρονικό ταχυδρομείο. Στην ΠΕΡΙΠΤΩΣΗ που δηλώσατε αριθμούς πιστωτικής κάρτας ή τραπεζικού λογαριασμού, επικοινωνήστε με την τράπεζά σας. Στην ΠΕΡΙΠΤΩΣΗ που θεωρείτε ότι έχετε πέσει θύμα κλοπής ταυτότητας, επικοινωνήστε με την τοπική αστυνομία**.**

Ποιες είναι οι τακτικές «ψαρέματος»

Το Phishing επιχειρείται συνήθως με τη αποστολή κάποιου spam email, το οποίο ισχυρίζεται –ψευδώς- ότι αποστέλλεται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κλπ.), σε μία προσπάθεια να παραπλανήσει τον παραλήπτη και να του αποσπάσει απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, τα στοιχεία αυτά θα χρησιμοποιηθούν από τους εγκέφαλους της απάτης για την πραγματοποίηση μή εξουσιοδοτημένων/παράνομων οικονομικών συναλλαγών.

Τα email αυτά ισχυρίζονται ότι ο παραλήπτης απαιτείται να ενημερώσει ή να επαληθεύσει άμεσα κάποια προσωπικά στοιχεία του για λόγους ασφαλείας, και τον οδηγούν μέσω συνδέσμων σε πλαστά web sites, τα οποία μιμούνται πολύ πειστικά τους διαδικτυακούς τόπους υπαρκτών και αξιόπιστων οργανισμών. Σε κάποιες περιπτώσεις η αντιγραφή είναι τόσο καλή που και ο ίδιος ο internet browser «ξεγελιέται» και δείχνει στην γραμμή θέματος την αναμενόμενη διεύθυνση και όχι την πραγματική διεύθυνση της πλαστής διαδικτυακής τοποθεσίας.

Σε μία προσπάθεια να μειώσουν τον χρόνο αντίδρασης του ανυποψίαστου παραλήπτη, ορισμένα μηνύματα απειλούν ότι εάν δεν προβεί στις απαιτούμενες ενέργειες (ενημέρωση, επαλήθευση στοιχείων) εντός του υποδεικνυόμενου –σύντομου- χρονικού διαστήματος ο λογαριασμός του θα μπλοκαριστεί και δεν θα μπορεί να πραγματοποιήσει περαιτέρω συναλλαγές. Σκοπός τους είναι να εξαναγκάσουν τον παραλήπτη να αποκαλύψει τις πληροφορίες που του ζητείται χωρίς καν να προλάβει να εξετάσει την γνησιότητα του μηνύματος.

SPAM EMAIL

Τι είναι τα spam email;

Η ανεπιθύμητη αλληλογραφία ή spamming είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων ηλεκτρονικού ταχυδρομείου που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς αυτοί να έχουν προκαλέσει συνειδητά την αλληλογραφία με τον εν λόγω αποστολέα. Παρά το γεγονός ότι ο όρος spamming αναφέρεται περισσότερο στην αποστολή μεγάλων ποσοτήτων μηνυμάτων διαφημιστικού ή ενημερωτικού περιεχομένου, χρησιμοποιείται επιπρόσθετα για να καταδείξει την αποστολή οποιουδήποτε μηνύματος που μπορεί να χαρακτηριστεί ως «ενοχλητικό» για αυτόν που το λαμβάνει. Η αλληλογραφία αυτή θα μπορούσε να χαρακτηριστεί «απρόκλητη» καθώς άτομα χωρίς προηγούμενη έμπρακτη εκδήλωση ενδιαφέροντος, γίνονται αποδέκτες διαφημίσεων από εταιρίες που απέκτησαν με νόμιμο ή παράνομο τρόπο τις διευθύνσεις της ηλεκτρονικής τους αλληλογραφίας.

Από πού προέρχεται ο όρος spam;

Ο όρος spam προέρχεται από το εμπορικό όνομα αμερικανικού προϊόντος κρέατος σε κονσέρβα στη δεκαετία του 1960 το οποίο εισαγόταν στη Μεγάλη Βρετανία σε μεγάλες ποσότητες. Το 1970, οι Μόντυ Πάιθονς έγραψαν το σκετς Σπαμ ως μέρος της εκπομπής Το ιπτάμενο τσίρκο των Μόντυ Πάιθονς όπου μια ομάδα Βίκινγκς επαναλάμβαναν δυνατά ένα τραγούδι με μόνα λόγια το «σπαμ σπαμ σπαμ...ωραίο σπαμ...εξαίρετο σπαμ». Στη συνέχεια, στη δεκαετία του 1980 οι εταιρείες αποστολής τέτοιων μηνυμάτων τα ονόμαζαν SPAM ως ακρωνύμιο του Sales Promotion and Marketing (Προώθηση Πωλήσεων και Μάρκετιν). Αργότερα η χρήση του επεκτάθηκε και το 1998 το New Oxford Dictionary of English το περιέλαβε με την έννοια των «ασχέτων ή μη αποδεκτών μηνυμάτων που στέλνονται στο Ίντερνετ σε μεγάλο αριθμό ομάδων ειδήσεων ή χρηστών»

Ποιο είναι συνήθως το περιεχόμενό των spam;

Παρακάτω αναφέρονται τα κυριότερα χαρακτηριστικά του spamming :

• **Απρόκλητο**: Δεν υπάρχει κάποια σχέση μεταξύ παραλήπτη και αποστολέα η οποία θα δικαιολογούσε ή θα προκαλούσε τη σχέση αυτή.

• **Εμπορικό:** Το spamming αφορά την αποστολή μηνυμάτων με εμπορικό σκοπό κατά κύριο λόγο, σκοπεύοντας την προβολή και διαφήμιση προϊόντων και υπηρεσιών και εν συνεχεία διεύρυνση πελατολογίου και πραγματοποίηση πωλήσεων.

• **Μαζικό**: Το spamming συνίσταται στη μαζική αποστολή μεγάλων ποσοτήτων μηνυμάτων από τον αποστολέα σε ένα πλήθος παραληπτών.

Για να προστατευτεί ο χρήστης που λαμβάνει ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου πρέπει μόλις το εντοπίσει στο φάκελο των εισερχομένων μηνυμάτων του, να το διαγράψει αμέσως χωρίς να προσπαθήσει να το ανοίξει και να το διαβάσει, και αυτό γιατί υπάρχει πιθανότητα να εμπεριέχει απάτη ή να «μολύνει» με κακόβουλο λογισμικό τον ηλεκτρονικό υπολογιστή του. Κρίνεται σκόπιμο κάθε χρήστης να εγκαταστήσει στον Η/Υ ενημερωμένα φίλτρα κατά των ανεπιθύμητων μηνυμάτων όπως επίσης να αποφεύγει να δίνει την ηλεκτρονική του διεύθυνση σε οποιονδήποτε τη ζητήσει.

Πώς να αποφύγετε τα spam email;

Μη δημοσιεύετε την διεύθυνση ηλεκτρονικού ταχυδρομείου σας. Μη δίνετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας, σε οργανισμούς που δεν εμπιστεύεστε. Μην απαντάτε στο spam. Αναφέρετε κάθε μήνυμα Spam που λαμβάνετε. Διαδώστε την γνώση σας και την εμπειρία σας σε σχέση με το Spam .Ελέγξτε τα συστήματα σας ώστε να είναι σωστά διαμορφωμένα και ασφαλή.

HOAXES

Τι είναι τα μηνύματα απατηλού περιεχομένου (hoaxes);

Ο όρος Hoax χρησιμοποιείται στα αγγλικά για να περιγράψει μια απάτη ή κάτι ψεύτικο και φαίνεται ότι προέρχεται από τις μαγικές λέξεις Hocus Pocus (κάτι σαν το δικό μας άμπρα Κατάμπρα). Πιο ακριβής πάντως είναι ο όρος Urban Legend (Αστικός Θρύλος) μια και ένα Hoax είναι στην πραγματικότητα μια φήμη, δηλαδή ένας θρύλος ο οποίος "περιφέρεται" μέσα στο δίκτυο. Τα Hoaxes διακινούνται στο δίκτυο μέσω του ηλεκτρονικού ταχυδρομείου και η δημοφιλέστερη κατηγορία τους είναι τα προειδοποιητικά μηνύματα σχετικά με ιούς (π.χ. μη διαβάσετε email με το subject "Good Times" διότι θα καταστραφεί ο Η/Υ σας).

ΕΘΙΣΜΟ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Ποιοι είναι οι παράγοντες που οδηγούν τους νέους σε εθισμό στο διαδίκτυο και ποιες οι συνέπειες ;

Το Ίντερνετ 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, πολλές φορές, 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).

Επίσης, ο εθισμός των εφήβων στο διαδίκτυο μπορεί, επίσης να είναι το αποτέλεσμα άλλων ψυχικών διαταραχών, όπως κατάθλιψη, αγχώδεις διαταραχές, διαταραχές προσωπικότητας, υπερκινητικότητα και κοινωνική φοβία. Συμπτώματα συνδρόμου απόσυρσης,

όπως ψυχοκινητική διέγερση, εκούσια ή ακούσια κίνηση δακτυλογράφησης των δακτύλων του χεριού, άγχος, έμμονη σκέψη για το διαδίκτυο και όνειρα για το διαδίκτυο.

Συμπτώματα εθισμού στο διαδίκτυο

Όπως χαρακτηριστικά περιγράφει ο γιατρός «Αρχίζουν σταδιακά να χάνουν ή να αποφεύγουν να κάνουν τα απαραίτητα πράγματα για την επιβίωση ακόμα και στο πρωταρχικό επίπεδο της αυτοσυντήρησης. Καθυστερούν να φάνε ή ξεχνούν να φάνε και να πιούν νερό, αργούν να πάνε για ύπνο, χάνουν τα ραντεβού του και καθυστερούν να πάνε στη δουλειά ή στο σχολείο». Αναλυτικά

1. Κατανάλωση υπερβολικού χρόνου ή και χρήματος σε δραστηριότητες σχετικές με το διαδίκτυο (λογισμικοί, σκληροί δίσκοι κ.λ.π)
2. Μείωση λειτουργικότητας του ατόμου σε κοινωνικό, οικογενειακό αλλά και προσωπικό επίπεδο.
3. Μειωμένη επίδοση στο σχολείο λόγω των πολλών ωρών που περνάει ο έφηβος στο διαδίκτυο ή διακοπή του σχολείου.
4. Σε προχωρημένες περιπτώσεις ο έφηβος δεν κοιμάται,
5. Παραμελεί την προσωπική του υγιεινή, μπορεί να σταματήσει ακόμα και το σχολείο.
6. Απομονώνεται από την οικογένεια και τους φίλους τους, γίνονται επιθετικοί, μπορεί να κλέβουν χρήματα από τους γονείς για να παίζουν.
7. Τέλος, φτάνουν σε σημείο να μην τρώνε ή και το αντίθετο (να παχύνουν πολύ).
8. Απουσία για ημέρες από το σπίτι (π.χ. σε internet café)
9. Αδυναμία περιορισμού της χρήσης, παρά την γνώση των προβλημάτων που μπορούν να δημιουργηθούν
10. Δεν συνειδητοποιούν την κατάσταση, ώστε να αναζητήσουν ή να δεχθούν βοήθεια

Το φαινόμενο αυτό, μπορεί να εμφανιστεί σε εφήβους κατά την πρώιμη εφηβεία (10-14 ετών) ή και σε μικρότερη ακόμη ηλικία. Είναι πιο συχνό κατά την μέση εφηβεία (15-17 ετών), κατά την οποία οι έφηβοι πειραματίζονται και σταδιακά αυτονομούνται, καθώς και κατά την όψιμη εφηβεία

Η υπερβολική χρήση του διαδικτύου οδηγεί τους νέους σε κατάθλιψη λένε οι έρευνες;

Κατάθλιψη, απομόνωση, εσωστρέφεια, κοινωνική φοβία, διαταραχή ελέγχου των παρορμήσεων και διαταραχή ελλειμματικής προσοχής συνοδεύουν πολύ συχνά τα περιστατικά εθισμού στο Διαδίκτυο. Ειδικά στην κυρίως ομάδα εθισμένων αγοριών εφηβικής ηλικίας, η κατάθλιψη αποτελεί τον σημαντικότερο παράγοντα πρόγνωσης του εθισμού, όπως ανέφερε ο πρόεδρος της Ελληνικής Εταιρείας Μελέτης Διαταραχών Εθισμού στο Διαδίκτυο, ψυχίατρος, Κωνσταντίνος Σιώμος, στο πλαίσιο του 23ου Πανελλήνιου Συνεδρίου της Ελληνικής Εταιρείας Κοινωνικής Παιδιατρικής και Προαγωγής Υγείας που πραγματοποιήθηκε στη Θεσσαλονίκη. Με δεδομένη την ταχύτατη εξάπλωση του Διαδικτύου σε παγκόσμιο επίπεδο και ιδιαίτερα στους εφηβικούς πληθυσμούς, οι ψυχίατροι παιδιών και εφήβων οφείλουν να εξετάζουν σε βάθος τη σχέση των νέων με το Διαδίκτυο και πώς αυτή αλληλεπιδρά με ψυχικές διαταραχές, για την παροχή ποιοτικότερης και αποτελεσματικότερης φροντίδας υγείας, ανέφερε ο κ. Σιώμος, ο οποίος επικαλέστηκε στοιχεία ξένων μελετών, σύμφωνα με τα οποία το 54% όσων πληρούσαν τα κριτήρια για τον εθισμό στο Διαδίκτυο είχαν ένα προηγούμενο ιστορικό κατάθλιψης, ενώ άλλοι είχαν για χρόνια χαμηλή αυτοεκτίμηση.

Σύμφωνα με πρόσφατη έρευνα, από τον περασμένο Δεκέμβριο περισσότεροι από ένα δισεκατομμύριο άνθρωποι χρησιμοποιούν το Facebook και πάνω από 500.000 το Twitter . Καθημερινά γίνονται 500 εκατομμύρια likes στο Facebook και περίπου 340 εκατομμύρια Tweets. Το πιο εντυπωσιακό ωστόσο είναι πως περισσότεροι από 350 εκατομμύρια χρήστες

υποφέρουν από το σύνδρομο εθισμού στο Facebook. Για να αντιληφθούμε το μέγεθος του προβλήματος είναι ενδεικτικές κάποιες απαντήσεις στους δρόμους του Λονδίνου. «Όλο το 24ωρο χρησιμοποιώ το Facebook και το Twitter», είπαν γελώντας αρκετοί. Ίσως και δέκα φορές την ημέρα, 4 με 6 φορές την ημέρα. Όταν τους λένε πως μπορεί να είναι εθισμένοι στο Διαδίκτυο λένε πως δεν εκπλήσσονται. Μελέτη του Πανεπιστημίου του Σικάγου, την περασμένη χρονιά, καταδεικνύει τον τρόπο με τον οποίο τα μέσα κοινωνικής δικτύωσης έχουν εισβάλλει στις ζωές των ανθρώπων από κάθε σημείο του πλανήτη. Τα πορίσματα αποκαλύπτουν πως οι χρήστες επιθυμούν να μπαίνουν στο Facebook και στο Twitter περισσότερο από το να κάνουν σεξ, να πιούν αλκοόλ ή να καπνίσουν τσιγάρα. Σύμφωνα με την μελέτη, οι χρήστες δείχνουν μεγαλύτερη λαχτάρα όταν προσπαθούν να αντισταθούν στην επιθυμία τους για συγκεκριμένα πράγματα. Υπήρχαν πολλοί που απάντησαν πως δεν ήθελαν να σπαταλούν το χρόνο τους μπαίνοντας σε σελίδες κοινωνικής δικτύωσης καθώς αυτό θα τους αποσπούσε από τη δουλειά τους ή γιατί το θεωρούσαν χάσιμο χρόνου. Ωστόσο το βρήκαν πολύ δύσκολο να αντισταθούν στα όσα τους προσέφεραν οι χώροι κοινωνικής δικτύωσης.

Η έρευνα έδειξε ότι τμήματα του Facebook και του Twitter, όπως τα likes και τα re-tweets, δίνουν στους χρήστες μια δόση πρόσθετης ουσίας ντοπαμίνης που επηρεάζει τα νεύρα ενώ έλλειψή της προκαλεί ζήλια και άγχος .Σημάδι εθισμού αποτελεί και το να ξοδεύεις περισσότερες από πέντε ώρες τη ημέρα σε ιστότοπο κοινωνικής δικτύωσης.Η κλινική Τάβιστοκ και Πόρτμαν στο Λονδίνο θεραπεύει μεταξύ άλλων και τον εθισμό στα social media. Ο δόκτωρ Ρίτσαρντ Γκράχαμ βλέπει περισσότερους από 100 ασθενείς το χρόνο με παρόμοια συμπτώματα που συνδέονται με τον εθισμό στο τζόγο και στο Διαδίκτυο. Στους ασθενείς του περιλαμβάνονται ενήλικοι 35 ετών αλλά και παιδιά.

ΨΕΥΤΙΚΑ PROFIL

Τι είναι τα ψεύτικα profil σε site κοινωνικής δικτύωσης;

Νέα αναστάτωση στο χώρο του facebook από τη νέα τάση της εποχής κατά την οποία hackers δημιουργούν ψεύτικα προφίλ τρίτων προσώπων και εμφανίζονται σαν να ήσαν εκείνοι. Αποθηκεύουν μερικές φωτογραφίες των θυμάτων τους, δημιουργούν προφίλ με αυτές τις φωτογραφίες και αρχίζουν να κάνουν νέα αιτήματα σε φίλους. Στη συνέχεια γράφουν κ δημοσιεύουν πράγματα που εκθέτουν τους εμφανιζόμενους ως κατόχους των προφίλ, ενώ στην πραγματικότητα αυτοί δεν έχουν ιδέα. Γι τον λόγο αυτό ίσως να έχετε εκπλαγεί το τελευταίο διάστημα έχοντας ανακαλύψει πως κάποιος φίλος ή φίλη σας διαθέτει όχι ένα, αλλά δύο ίσως και περισσότερα προφίλ. Στην πραγματικότητα, μόνο ένα έχει ο συγκεκριμένος. Απλώς κάποιοι επιτήδειοι έχουν δημιουργήσει τα υπόλοιπα εν αγνοία του..

Υπολογίζεται ότι **περίπου το 5% των προφίλ, είναι ψεύτικα**. Έτσι λοιπόν, είναι αρκετά πιθανό, να βρείτε όχι 1 αλλά πολλά τέτοια, μέσα στο λογαριασμό σας.

Ποιος ο σκοπός των δημιουργών τους;

Αρκετοί δημιουργούν προφίλ για διαφημιστικούς σκοπούς. Ανεβάζουν τη φωτογραφία μιας οποιαδήποτε κοπέλας στη κεντρική φωτογραφία του προφίλ τους και απλά αναρτούν είτε το προϊόν τους, είτε το site που διαφημίζουν....

Ορισμένοι άνδρες δεν ανεβάζουν φωτογραφίες δικές τους, αλλά ανεβάζουν γλυκές φωτογραφίες από σκυλιά, λιοντάρια, έξυπνες παροιμίες κτλ με σκοπό να επικεντρωθούν στον συναισθηματικό τομέα μιας κοπέλας. Και αυτά τα προφίλ είναι συνήθως ψεύτικα και δεν αντιπροσωπεύουν το όνομα που έχουν δώσει στο συγκεκριμένο προφίλ.

Τα ψεύτικα προφίλ είναι πολυάριθμα στους χώρους κοινωνικής δικτύωσης και ειδικά στον χώρο του facebook. Πίσω από την ανωνυμία των χρηστών, κρύβεται η προώθηση ενός διαφημιστικού υλικού ή προϊόντος. Σε άλλες περιπτώσεις, τα κίνητρα είναι διαφορετικά και σχετίζονται με τον εκφοβισμό (**cyber bulling**), την ηλεκτρονική απάτη κ.α.

Πώς μπορείτε να καταλάβετε αν ένα προφίλ είναι ψεύτικο;

Τα **ψεύτικα προφίλ** που δημιουργούνται είναι πάρα πολλά και δυστυχώς οι επιτήδειοι ξέρουν τον τρόπο να τα παρουσιάζουν ως αληθινά.

Υπάρχει όμως τρόπος να ανακαλύψετε ποιοι λογαριασμοί είναι ψεύτικοι. **Αρκεί να ακολουθήσετε τα παρακάτω βήματα:**

1) Κοιτάξτε τις φωτογραφίες του/της. Έχει πολλές φωτογραφίες; Ανεβάζει φωτογραφίες με φίλους ή φίλες; Επίσης, τις ανανεώνει ή έχει την ίδια φωτογραφία εδώ και χρόνια; Στα περισσότερα αυθεντικά προφίλ υπάρχουν πολλές φωτογραφίες του ατόμου στο οποίο ανήκει το προφίλ.

2) Πολύ σημαντικό είναι να κοιτάτε τα σχόλια στις αναρτήσεις και στις φωτογραφίες. Αν φαίνεται ότι σχολιάζουν πολλά διαφορετικά άτομα τα οποία δείχνουν να γνωρίζουν το άτομο, τότε πιθανότατα το προφίλ δεν είναι ψεύτικο. Όσο λιγότερα σχόλια υπάρχουν, τόσο αυξάνεται η πιθανότητα το προφίλ να είναι ψεύτικο.

3) Τα περισσότερα ψεύτικα προφίλ δημιουργούνται από άνδρες που το... παίζουν γυναίκες. Μια γυναίκα θα κάνει πιο εύκολα αποδοχή φιλίας σε μια άγνωστη γυναίκα, παρά σε έναν άγνωστο άνδρα. Αυτό το γνωρίζουν οι άνδρες, με αποτέλεσμα να δημιουργούν ψεύτικα, γυναικεία προφίλ με την ελπίδα να δημιουργήσουν φιλίες με κοπέλες. Αν βλέπετε γυναικεία προφίλ με φωτογραφίες με λίγα ρούχα, σώματα στην παραλία και με σχόλια σεξουαλικού περιεχομένου, τότε μάλλον κάτι δεν πάει καλά...

4) Δείτε αν ανανεώνει το προφίλ του/της συχνά. Αν έχει ελάχιστες αναρτήσεις και μάλιστα με σπάνια ανανέωση, τότε κι αυτό είναι ύποπτο.

5) Υπάρχουν ορισμένοι που ανεβάζουν πολλές φωτογραφίες που βρίσκουν είτε από το google, είτε από άλλα ξένα προφίλ στο facebook. Συνήθως, οι φωτογραφίες αυτές είναι τραβηγμένες στο εξωτερικό και αρκετές φορές αυτό μπορείτε να το διακρίνετε...

Χαρακτηριστικά των ψεύτικων προφίλ

Φωτογραφικό υλικό: δεν υπάρχουν φωτογραφίες του χρήστη από προσωπικές ή κοινωνικές δράσεις του. Αντί αυτών υπάρχουν 2 – 3 φωτογραφίες με αφηρημένο και γενικό περιεχόμενο (π.χ. ηλιοβασίλεμα, θάλασσα, **κατοικίδια** κ.α.). Αυτές συνήθως έχουν αλιευθεί από τις μηχανές αναζητήσεις (π.χ. google)

Σχόλια: δεν υπάρχουν σχόλια από πολλά άτομα, κάτω από τις φωτογραφίες ή τις αναρτήσεις του χρήστη. Ακόμα, τα σχόλια που υπάρχουν δεν έχουν φιλικό ύφος και αυτό δηλώνει ότι οι **φίλοι** του χρήστη δεν είναι «πραγματικοί».
Αλλαγή φύλου: ο χρήστης προσπαθώντας να αποπροσανατολίσει και να μην γίνει αντιληπτός, αλλάζει φύλο. Έτσι λοιπόν, ένας άντρας επιλέγει το γυναικείο φύλο με αποτέλεσμα να προσεγγίζει ευκολότερα άλλες άγνωστες γυναίκες.

Προκλητικό φωτογραφικό υλικό: τα γυναικεία προφίλ που έχουν φωτογραφίες με ημι-γυμνό περιεχόμενο, προκλητικά ρούχα κ.α. μάλλον είναι ψεύτικα.
Το όνομα του χρήστη: δεν παραπέμπει στο πραγματικό ονοματεπώνυμο του χρήστη ή στην ιδιότητα του (π.χ. δάσκαλος).

Οι αναρτήσεις - δημοσιεύσεις: δεν αποκαλύπτουν προσωπικά στοιχεία του χρήστη (π.χ. ενδιαφέροντα, εργασία κ.α.).

Ιδανική εικόνα: κοιτώντας τις προσωπικές πληροφορίες – όπου υπάρχουν – του χρήστη, θα δούμε ότι είναι μορφωμένος, εργάζεται σε κάποια γνωστή εταιρεία και έχει πολλά ενδιαφέροντα και χόμπι. Πίσω λοιπόν, από την ανωνυμία και την μπλε μάσκα του facebook, κρύβεται ένας ιδανικός εαυτός, ο οποίος όμως απέχει πολύ από την πραγματικότητα.

Πώς μπορείτε να προφυλαχθείτε από τα ψεύτικα profil;

1) Μην κλείσετε ραντεβού με κάποιον άγνωστο χρήστη του διαδικτύου.
2) Εάν εμπιστευτείτε κάποιον άγνωστο χρήστη, το ραντεβού φροντίστε να είναι σε δημόσιο χώρο, στον οποίο θα νιώθετε και θα είστε ασφαλής.

3) Ψάξτε και **διαγράψτε** τα ψεύτικα προφίλ από τους φίλους σας, ειδικά αν προσπαθούν να σας προσεγγίσουν.

4) Χρησιμοποιήστε τις λειτουργίες **block** (δεν μπορεί να δει το προφίλ σας) και **report** (αναφορά ψεύτικου προφίλ στο facebook), ανάλογα με την εκάστοτε ΠΕΡΙΠΤΩΣΗ.

5) Να αναφέρεις ελάχιστα στοιχεία σχετικά με τα **προσωπικά σου δεδομένα** (π.χ. πολιτικές απόψεις).

6) Ακολουθήσετε την παρακάτω διαδικασία, που περιγράφεται στο βίντεο και ανακαλύψετε αν μια φωτογραφία είναι αληθινή ή κατεβασμένη από το google.

ΔΙΑΔΙΚΤΥΑΚΑ ΠΑΙΧΝΙΔΙΑ

Τι είναι τα διαδικτυακά παιχνίδια;

Τα διαδικτυακά παιχνίδια είναι δισδιάστατα ή τρισδιάστατα παιχνίδια που παίζονται στον ηλεκτρονικό υπολογιστή ή στις παιχνιδομηχανές (π.χ. Playstation) και, μέσω του διαδικτύου, ο χρήστης μπορεί να παίζει και να αλληλεπιδρά με χρήστες από διάφορες χώρες, πολύ συχνά, σε έναν ενιαίο, εικονικό κόσμο. Η θεματολογία τους ποικίλει, όμως τα περισσότερα και πιο διαδεδομένα διαδικτυακά παιχνίδια είναι παιχνίδια ρόλων και παρουσιάζουν ένα πλαίσιο Ηρωικής Φαντασίας . Σε μερικά ηλεκτρονικά παιχνίδια μπορούν να παίξουν παραπάνω από ένας παίχτες που μοιράζονται την ίδια περιοχή του παιχνιδιού. Οι παίχτες μπορούν είτε να δημιουργήσουν ομάδες που παίζουν μεταξύ τους είτε απλά να βλέπουν ποιος μεμονωμένος παίχτης είναι ο καλύτερος.Κάποια αρκετά διαδεδομένα παιχνίδια μπορεί να παίζονται διαδικτυακά, αλλά δεν είναι αμιγώς διαδικτυακά, μπορούν να παιχτούν και σε ατομικό υπολογιστή ή τοπικό δίκτυο (LAN). Παιχνίδια που παίζονται όχι αποκλειστικά διαδικτυακά, αλλά είναι ιδιαίτερα δημοφιλή είναι τα Warcraft, Counter Strike, DoTA κ.α. Φυσικά υπάρχουν διαδικτυακά παιχνίδια που δεν ανήκουν στις παραπάνω κατηγορίες, όπως το Second Life.

Ποιες είναι οι διαφορές τους με τα μη διαδικτυακά παιχνίδια και για ποιο λόγο είναι τόσο δημοφιλή;

Τα διαδικτυακά παιχνίδια έχουν κάποια χαρακτηριστικά γνωρίσματα, τα οποία τα διαφοροποιούν από τα υπόλοιπα παιχνίδια. Πρώτον, ο κόσμος που περιγράφουν δεν σταματά ποτέ και υφίσταται ακόμα και όταν ο παίκτης δεν είναι συνδεδεμένος. Ως εκ τούτου, ο παίκτης παύει να είναι ο πρωταγωνιστής και γίνεται απλά ένα μέρος του κόσμου. Δεύτερον, οι διαδικτυακές δυνατότητες επιτρέπουν την ταυτόχρονη επικοινωνία χιλιάδων παικτών, από διαφορετικές χώρες και πολιτισμικό υπόβαθρο, και την αλληλεπίδραση τους. Αν στα δύο παραπάνω χαρακτηριστικά προσθέσει κανείς ένα ισχυρότατο σύστημα συνεχών ανταμοιβών/ενισχύσεων (ολοκληρώνω μια αποστολή, παίρνω ένα βραβείο και πηγαίνω για την επόμενη αποστολή και το επόμενο βραβείο), μέσα σε έναν κόσμο που συνεχώς εξελίσσεται και εμπλουτίζεται για να κρατάει τους παίκτες σε εγρήγορση ή και ανταγωνισμό, είναι ξεκάθαρο ότι τα διαδικτυακά παιχνίδια είναι σχεδιασμένα για να προσελκύουν μεγάλους αριθμούς παικτών και ότι τα τελευταία χρόνια αποτελούν μια ξεχωριστή μόδα για τους νέους (και όχι μόνο) ανθρώπους. Άλλωστε, δεν θα πρέπει να παραβλέπει κανείς την κατεξοχήν κοινωνική φύση του διαδικτύου, η οποία παίζει πάρα πολύ μεγάλο ρόλο στην εξάπλωση των περισσότερων διαδικτυακών δραστηριοτήτων.

Τι είναι online gambling?

Ο συστηματικός τζόγος περιλαμβάνει τη συνάντηση δύο ή περισσότερων ατόμων με σκοπό την ανταλλαγή στοιχημάτων ή/και την ίδια την δραστηριότητα για την οποία γίνονται τα στοιχήματα, αν αυτό είναι δυνατό. Αυτό γίνεται είτε με φυσική παρουσία είτε με μεσάζοντες όπως τα παραδοσιακά γραφεία στοιχημάτων. Το Διαδίκτυο έχει κάνει τη συνάντηση αυτών των τζογαδόρων πολύ πιο εύκολη, είτε πρόκειται για απλό στοίχημα είτε για πόκερ, τάβλι, και σκάκι. Δεν είναι απαραίτητο να συναντήσει κανείς τους υπόλοιπους παίχτες. Για παράδειγμα, στο πόκερ οι παίχτες παίζουν σε πραγματικό χρόνο σε ένα κοινό ηλεκτρονικό περιβάλλον το οποίο ο κάθε παίκτης βλέπει στην οθόνη του.

Ποιες είναι οι διαφορές ανάμεσα στα παιχνίδια και τον τζόγο;

Τα παιχνίδια και ο τζόγος είναι δύο εντελώς διαφορετικοί όροι. Ενώ το παιχνίδι έχει μια μη πραγματική προσέγγιση με μόνο φανταστικούς δεσμούς με τον φυσικό κόσμο, ο τζόγος περιλαμβάνει το ρίσκο της πραγματικής οικονομικής απώλειας ή του κέρδους. Ψυχολογικά, αυτό οδηγεί σε δυο πολύ διαφορετικούς τρόπους παιχνιδιού: Αν κάποιος χάσει ένα γύρο στο αγαπημένο του παιχνίδι, μπορεί πάντα να θεωρήσει ότι είχε «απλά μια κακή ημέρα» και να επιστρέψει για ρεβάνς την επομένη, ενώ ο φόβος του να χάσει κανείς τα χρήματά του εξαιτίας μιας λανθασμένης κρίσης σε ένα γύρο πόκερ ξυπνά ένα εντελώς διαφορετικό είδος συναισθημάτων.

Ποιά είναι η διαφορά ανάμεσα στις τοποθεσίες παιχνιδιών και τις τοποθεσίες τυχερών παιχνιδιών;

Οι κυριότερες διαφορές μεταξύ των τύπων των ιστοσελίδων είναι οι εξής:

Οι τοποθεσίες παιχνιδιών συνήθως περιέχουν παιχνίδια με κάρτες, πίνακες, λέξεις, arcade ή παζλ, με αυτόματη παρακολούθηση και προβολή του σκορ.

Δεν γίνεται ανταλλαγή χρημάτων, αληθινών ή ψεύτικων. Οι τοποθεσίες τυχερών παιχνιδιών μπορούν να περιέχουν σενάρια, στα οποία οι άνθρωποι κερδίζουν ή χάνουν κάποιο τεχνητό νόμισμα. Οι τοποθεσίες Τζόγου συνήθως αφορούν το κέρδος ή την απώλεια αληθινών χρημάτων.

Βοηθήστε τα παιδιά σας να αποφύγουν το διαδικτυακό τζόγο

Οι γονείς θα πρέπει να αποφασίσουν ποιοί τύποι παιχνιδιών ή τοποθεσιών παιχνιδιών είναι κατάλληλοι για τα παιδιά τους. Για παράδειγμα, μπορείτε να βασίσετε τα κριτήριά σας στον τύπο του παιχνιδιού (μόνον παιχνίδια με κάρτες και πίνακα ή μόνον παιχνίδια στρατηγικής και φαντασίας), καθώς και στο εάν το παιχνίδι παίζεται διαδραστικά με άλλους στο Διαδίκτυο, εάν η τοποθεσία προσφέρει το παιχνίδι δωρεάν ή και κατά ΠΕΡΙΠΤΩΣΗ

Είναι ωφέλιμο να παίζει ένα παιδί ή έφηβος διαδικτυακά παιχνίδια;

Οι κίνδυνοι του διαδικτύου και των διαδικτυακών παιχνιδιών δεν θα πρέπει να αποτελούν αποτρεπτικό παράγοντα για τη χρήση τους. Άλλωστε, η μεγάλη πλειοψηφία των παικτών δεν παρουσιάζουν εθισμό. Η χρήση διαδικτυακών παιχνιδιών έχει συσχετιστεί με πολλά οφέλη για τους χρήστες, πέραν της ψυχαγωγίας. Οι κύριες κατηγορίες που εντοπίζονται τα οφέλη είναι η κοινωνικοποίηση, αφού τα άτομα αλληλεπιδρούν με εκατοντάδες χρήστες, η βελτίωση αισθητηριακών χαρακτηριστικών (π.χ. όραση, χρόνος αντίδρασης) και το πεδίο της μάθησης, καθώς τα παιχνίδια είναι ένα εξαιρετικό εργαλείο εκμάθησης γνώσεων και δεξιοτήτων και για το λόγο αυτό, τα τελευταία χρόνια, σχεδιάζονται ειδικά παιχνίδια. Σχετικά με την

κοινωνικοποίηση, στα διαδικτυακά παιχνίδια βρίσκουν «καταφύγιο» πολλοί παίκτες με κάποια σωματική ή ψυχική αναπηρία και με διάφορες κοινωνικές δυσκολίες (π.χ. κοινωνική φοβία). Τέλος, να σημειωθεί, ότι τα διαδικτυακά παιχνίδια μπορούν να χρησιμοποιηθούν και για θεραπευτικούς σκοπούς από τους ειδικούς ψυχικής υγείας.

Πώς επηρεάζουν την συμπεριφορά παιδιών και εφήβων όταν γίνεται κατάχρηση των διαδικτυακών παιχνιδιών;

Τα παιχνίδια αυτά δημιουργούν εξάρτηση. Οι έρευνες δείχνουν ότι η συντριπτική πλειοψηφία των χρηστών του διαδικτύου που παρουσιάζουν υπερενασχόληση ή εθισμό σε αυτό, είναι παίκτες διαδικτυακών παιχνιδιών. Πράγματι, τα χαρακτηριστικά των παιχνιδιών και των κινήτρων για τα οποία παίζει κανείς, έχουν ταυτιστεί με τον εθισμό στο διαδίκτυο, αφού στα παιχνίδια συγκεντρώνονται τόσο διαδικτυακές, όσο διαδραστικές-κοινωνικές συνθήκες, που αυξάνουν πολύ τις πιθανότητες για ανάπτυξη εθισμού. Στη διαδικασία αυτή συμβάλλουν και τα παιχνίδια, καθώς αν θέλει κανείς να διακριθεί σε αυτά, χρειάζεται να δαπανήσει αρκετές ώρες την εβδομάδα. Συγκεκριμένα, προτείνεται ότι αν κάποιος παίζει 40 ώρες την εβδομάδα, είναι σίγουρο ότι θα έχει αρνητικές επιπτώσεις στην καθημερινότητα του και θεωρείται εθισμένος. Σε κάθε ΠΕΡΙΠΤΩΣΗ πρέπει να γίνεται σαφής διάκριση μεταξύ ενασχόλησης, εντατικής ενασχόλησης και εξάρτησης.

Με τι είδους δυσκολίες συνδέεται η κατάχρηση των παιχνιδιών;

Τα άτομα που παρουσιάζουν εθισμό στα παιχνίδια έχουν πολλά προβλήματα στην καθημερινότητα τους και τη ψυχική τους διάθεση. Επηρεάζεται η εργασία τους (για τους ενήλικες), η ακαδημαϊκή πορεία ή επίδοση στο σχολείο, οι σχέσεις τους με γονείς και συνομηλίκους, αφού το παιχνίδι γίνεται, όχι απλά η κύρια ασχολία, αλλά το μοναδικό πράγμα που απασχολεί τη σκέψη τους και τη συμπεριφορά τους. Σε επίπεδο ψυχικής υγείας και λειτουργίας, ο εθισμός στα παιχνίδια συσχετίζεται με Διαταραχή Ελλειμματικής Προσοχής, με αισθήματα μοναξιάς και κενού, Κατάθλιψη, νευρωτισμό, αποφευκτική συμπεριφορά και άλλα προβλήματα που δεν αργούν να γίνουν εμφανή στο άτομο. Σε επίπεδο συμπεριφοράς, πολύ συχνά είναι τα ξεσπάσματα θυμού, τα οποία μπορούν να λάβουν και ακραίες μορφές (σωματική επίθεση στους γονείς, αυτοτραυματισμοί), συνήθως, σε ΠΕΡΙΠΤΩΣΗ βίαιης διακοπής του διαδικτύου. Τα παραπάνω φαινόμενα, να σημειωθεί, αποτελούν αρκετά σπάνια περιστατικά.

Ποιες ακατάλληλες συμπεριφορές μπορεί κανείς να συναντήσει σε έναν εικονικό κόσμο παιχνιδιού;

Όπως προαναφέρθηκε, η κοινωνία του παιχνιδιού είναι μια μικρογραφία της κοινωνίας, με όλες τις πιθανές συμπεριφορές να είναι δυνατόν να εμφανιστούν. Τις περισσότερες φορές, η συμπεριφορά ενός παίκτη δεν είναι κατεξοχήν αρνητική, έχει τόσο αρνητικά, όσο και θετικά στοιχεία. Κάποιες φορές, όμως, οι παίκτες παρουσιάζουν μια αποκλίνουσα συμπεριφορά, η οποία τους χαρακτηρίζει, ιδίως στη σχέση τους με τους άλλους παίκτες. Οι συμπεριφορές κυμαίνονται από άκρως εγωκεντρική θέαση του παιχνιδιού, δυναστευτική συμπεριφορά, υπερβολική καχυποψία, ρατσισμό, συναισθηματική εξάρτηση από το παιχνίδι και υπερβολική επένδυση σε αυτό, καταναγκαστική συμπεριφορά κ.α. Είναι σημαντικό να έχει κανείς κατά νου ότι οι παραπάνω συμπεριφορές επηρεάζουν τόσο τους παίκτες που τις παρουσιάζουν, όσο και τους άλλους, οι οποίοι είναι οι τελικοί αποδέκτες.

SOCIAL MEDIA

Ποιοι κίνδυνοι κρύβονται για τους εφήβους από τη χρήση social media;

Κίνδυνοι αρχίζουν να εμφανίζονται όταν οι χρήστες δίνουν τα προσωπικά τους στοιχεία σε αγνώστους. Ο διαδικτυακός κόσμος είναι πολύ διαφορετικός από τον πραγματικό. Νέοι μπαίνουν σε πειρασμό να κάνουν και να λένε πράγματα που δε θα διανοούνταν να κάνουν και να πουν σε κάποιον έχοντας τον μπροστά τους. Κάτι τέτοιο περιλαμβάνει και το να εμπιστεύονται προσωπικές πληροφορίες όπως για παράδειγμα αριθμούς κινητών τηλεφώνων

ή φωτογραφίες. Εάν συνομιλούν με κάποιον συνομήλικό τους, τότε υπάρχει κίνδυνος να χρησιμοποιήσουν πληροφορίες απρόσεχτα. Για παράδειγμα, στέλνοντας προσβλητικά μηνύματα, ή ανεβάζοντας κάποια εικόνα σε μια ιστοσελίδα. Όμως, ο κίνδυνος είναι φανερά μεγαλύτερος εάν το άτομο με το οποίο συνομιλούν είναι ενήλικας. Δυστυχώς, παιδόφιλοι ενήλικες που επιθυμούν να γνωρίσουν νέους για να ικανοποιήσουν τις σεξουαλικές τους ανάγκες- χρησιμοποιούν το Διαδίκτυο για να τον προσεγγίσουν ενδεχομένως με τελικό σκοπό μια συνάντηση στον πραγματικό κόσμο. Οι νέοι άνθρωποι μπορεί να επιδείξουν αφέλεια μπροστά σε τέτοιους κινδύνους και συνήθως νιώθουν αόρατοι ή ότι «θα το καταλάβαιναν αν κάποιος έλεγε <<ψέματα>>. Οι νέοι άνθρωποι ανταλλάσσουν φίλους μέσω υπηρεσιών άμεσων μηνυμάτων και με τον τρόπο αυτό συνομιλούν με αγνώστους, τους οποίους νοιώθουν ότι μπορούν να εμπιστευτούν επειδή «ένας φίλος ενός φίλου» τους γνωρίζει. Οι υπηρεσίες άμεσων μηνυμάτων είναι μια πολύ προσωπική μέθοδος επικοινωνίας περισσότερο από ένα δωμάτιο συνομιλίας με πολλούς συμμετέχοντες- και έτσι οι παιδόφιλοι χρησιμοποιούν αυτό το μέσο για να αποσπάσουν πληροφορίες από ένα νεαρό άτομο.

Ένας ακόμα κίνδυνος που κρύβουν τα μέσα κοινωνικής δικτύωσης είναι η υποκλοπή προσωπικών στοιχείων ενός ατόμου. Μία από τις "πονηρές" προσπάθειες υποκλοπής των στοιχείων μας είναι το "στήσιμο" μιας απομίμησης του πραγματικού site που θέλουμε να επισκεφθούμε. Αυτός μπορεί να είναι ένας ιστότοπος κοινωνικής δικτύωσης ή ακόμα και μια ιστοσελίδα τραπεζικού οργανισμού. Αν κάνουμε το λάθος και παραχωρήσουμε τους κωδικούς μας σε μια τέτοια ΠΕΡΙΠΤΩΣΗ, τότε οι επιτήδειοι που ελέγχουν αυτά τα υποτιθέμενα site θα το εκμεταλλευτούν ανάλογα. Έχοντας ο επιτιθέμενος τον έλεγχο του λογαριασμού μπορεί να προβεί σε διάφορες ενέργειες όπως να στείλει μηνύματα στους "φίλους" που υποτίθεται ότι προέρχονται από το θύμα, ενώ μπορεί ακόμα να προωθήσει διάφορα links τα οποία θα παραπέμπουν σε κάτι "ενδιαφέρον" ή "αξιόπιστο" αλλά στην πραγματικότητα θα παραπέμπουν σε κάποιο κακόβουλο αρχείο ή πρόγραμμα ή ακόμα να κάνει εισαγωγή σε άλλο phising site. Χάνοντας τους κωδικούς μας χωρίς να γίνουμε θύματα "ψαρέματος".

Ένας άλλος τύπος απειλής είναι κακόβουλα προγράμματα που αποκαλούνται "κλέφτες κωδικών πρόσβασης" (password stealers). Αυτά τα προγράμματα έχουν την δυνατότητα να εισάγουν κακόβουλο κώδικα στο πρόγραμμα περιήγησης μας (π.χ. Internet Explorer ή Mozilla Firefox). Αυτά τα προγράμματα έχουν την ικανότητα να υποκλέπτουν τα δεδομένα μας πριν καν συνδεθούμε στο αντίστοιχο site! Επειδή τα προγράμματα αυτά αποτελούν είδος κακόβουλου λογισμικού (malware), μπορούν να αντιμετωπιστούν αποτελεσματικά με ένα ενημερωμένο αντιβιοτικό. Ιστοσελίδες όπως το Facebook επιτρέπουν σε τρίτους κατασκευαστές λογισμικού να δημιουργούν εφαρμογές (applications) μέσω των οποίων οι δημιουργοί αυτοί αποκτούν πρόσβαση στα προφίλ και τις πληροφορίες των λογαριασμών μας. Βέβαια, εταιρίες όπως το Facebook χρησιμοποιούν πολλές χιλιάδες από αυτές τις εφαρμογές και φυσικά δεν υπάρχει εγγύηση για την ασφάλεια τους. Αυτό που μπορεί να μας βοηθήσει είναι ένα ενημερωμένο αντιβιοτικό αλλά και η προσοχή σε κάθε είδους τέτοια "παγίδα'.

Αποτελέσματα έρευνας σχετικά με τους κινδύνους που κρύβονται για τους εφήβους από τη χρήση social media

Οι κίνδυνοι στο facebook και η χρήση των social networks είναι από τα μεγαλύτερα θέματα συζήτησης των ημερών. Τα δίκτυα κοινωνικής δικτύωσης (social network) γοητεύουν τους μαθητές, που βρίσκουν ότι η ηλεκτρονική κοινωνική δικτύωση είναι ο βολικότερος τρόπος επικοινωνίας. Σε έρευνες που έγιναν για τη χρήση του facebook από μαθητές διαπιστώθηκαν

- Οι πολύωροι χρήστες του Facebook έχουν συνήθως γονείς που είναι απόφοιτοι της Τριτοβάθμιας Εκπαίδευσης. Όσο υψηλότερο είναι το επίπεδο γνώσεων των γονέων σχετικά με τον Η/Υ, τόσο περισσότερο ασχολούνται τα παιδιά τους με το διαδίκτυο και την κοινωνική δικτύωση μέσω Η/Υ.
- Πολλοί θεώρησαν ότι η ηλεκτρονική κοινωνική δικτύωση είναι ο βολικότερος τρόπος επικοινωνίας, που θα αντικαταστήσει το email και τις πιο συμβατικές μορφές διάδρασης. Κανόνιζαν τα ραντεβού τους μέσω του Facebook αντί να τηλεφωνήσουν, συζητούσαν γι' αυτό με τους φίλους τους και χρησιμοποιούσαν την ηλεκτρονική ιδιόλεκτο (αργκώ).
- Πολλοί άνοιξαν λογαριασμό στο Facebook, επειδή είναι μόδα.
- Οι χρήστες με μεγαλύτερη εξάρτηση από το Facebook, παρουσίαζαν την ίδια νοσηρή σχέση και με τα ηλεκτρονικά παιχνίδια και τον υπολογιστή γενικότερα.
- Το γλωσσικό επίπεδο των χρηστών του Facebook πολλές φορές κατρακυλάει σε ύβρεις και χυδαιολογίες, ενώ η ελληνική ορθογραφία παραχαράσσεται. Η γλώσσα είναι ένα συνονθύλευμα αγγλικών συντμήσεων και ελληνικών. Συχνή είναι η χρήση emoticons που όμως γίνονται δύσκολα στην αποκρυπτογράφησή τους και δυσχεραίνουν τη φόρτωση της σελίδας.
- Σε χρήστες μικρότερης ηλικίας αναπτύσσεται ανταγωνισμός για το ποιος θα προσελκύσει περισσότερους φίλους, κυρίως του αντιθέτου φύλου.

Υπηρεσίες Κοινωνικής Δικτύωσης και Μαθητές

Σύμφωνα με μία άλλη έρευνα, ένα στα δυο παιδιά στην Ελλάδα δηλώνει ότι παρέχει πολλές προσωπικές πληροφορίες στο Διαδίκτυο και συγκεκριμένα στους ιδιαίτερα δημοφιλείς ιστοχώρους κοινωνικής δικτύωσης, όπως το Facebook (http://www.facebook.com). Επίσης, θεωρούν ότι η ηλεκτρονική κοινωνική δικτύωση είναι ο βολικότερος τρόπος επικοινωνίας, που θα αντικαταστήσει συμβατικές μορφές επικοινωνίας και διάδρασης (π.χ., email). Κανονίζουν τα ραντεβού τους μέσω του Facebook αντί να τηλεφωνήσουν, συζητούν γι' αυτό με τους φίλους τους και χρησιμοποιούν την ηλεκτρονική ιδιόλεκτο (αργκό). Επιπλέον, πολλοί μαθητές

δήλωσαν ότι αυτό που τους συναρπάζει στο Facebook είναι ότι γνωρίζουν άτομα που μοιράζονται τα ίδια ενδιαφέροντα, ότι έχουν πρόσβαση σε πληροφορίες που τους ενδιαφέρουν, ακόμη και ότι συγκροτούν ομάδες μελέτης για διάφορες εκπαιδευτικές δραστηριότητες.

Από τα παραπάνω γίνεται αντιληπτό ότι οι εκπαιδευτικοί θα πρέπει να συζητούν με τους μαθητές και να τους προστατεύουν σε ότι σχετίζεται με τις καθημερινές τους δραστηριότητες σε ιστοχώρους κοινωνικής δικτύωσης. Τα παιδιά πρέπει να αντιληφθούν ότι οι άνθρωποι στο Διαδίκτυο, ακόμα και αυτοί με τους οποίους αλληλογραφούν ή συνομιλούν, ακόμα και για πολύ καιρό, αλλά δεν τους γνωρίζουν στο φυσικό κόσμο, δεν είναι πάντοτε αυτοί που φαίνεται ότι είναι. Οι άνθρωποι δεν λένε πάντοτε την αλήθεια στο Διαδίκτυο, οπότε πρέπει να αντιμετωπίζονται με τη δέουσα προσοχή και να υιοθετείται μια κριτική στάση στην διαδικτυακή τους συμπεριφορά.

Πρέπει οι μαθητές να βεβαιωθούν ότι δεν θα συναντήσουν κάποιο άτομο που γνωρίζουν μόνο μέσω του Διαδικτύου. Ακόμα και αν τα παιδιά επιμένουν ότι έχουν δει φωτογραφία του ατόμου αυτού, εξηγήστε τους ότι η φωτογραφία αυτή μπορεί να είναι πλαστή, για να τα παραπλανήσει και να επιτύχει ευκολότερα να συναντηθεί μαζί τους. Ακόμα και αν δουν κάποιον μέσω web κάμερας, πάλι διατρέχουν τον ίδιο κίνδυνο από πιθανά παιδοφιλικά ή άλλα κυκλώματα, τα οποία, ενδεχομένως, να έχουν επιστρατεύσει και ανήλικα παιδιά με σκοπό να προσελκύσουν άλλα παιδιά.

Πως καταλαβαίνω ότι η σελίδα είναι ασφαλής?

Πάντα, όταν επισκεπτόμαστε μια ιστοσελίδα που χρησιμοποιεί SSL certificate, υπάρχουν συγκεκριμένα στοιχεία, που αποδεικνύουν ότι βρισκόμαστε υπό ασφαλή σύνδεση. Κάποια από αυτά είναι ένα μικρό εικονίδιο με λουκέτο, το πρόθεμα https που εμφανίζεται μπροστά από την διεύθυνση της ιστοσελίδας, καθώς και το σύμβολο της εταιρίας η οποία παρέχει το πιστοποιητικό και εγγυάται την ασφαλή ανταλλαγή δεδομένων αλλά και την ταυτότητα της ιστοσελίδας.

Ποιος τρόπος υπάρχει να διαπιστώσετε εάν μία τοποθεσία Web προσφέρει ασφάλεια για να προστατέψετε τα ευαίσθητα προσωπικά σας δεδομένα;

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

ΑΣΦΑΛΕΙΣ ΟΙΚΟΝΟΜΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

Τι είναι το Ακρωνυμιο SSL;

SSL είναι το ακρωνύμιο για τις λέξεις **Secure Socket Layers**. Αλλιώς γνωστό και ως **Ηλεκτρονικό Πιστοποιητικό**, το πρωτόκολλο SSL δημιουργεί μια ασφαλή σύνδεση μεταξύ της εκάστοτε ιστοσελίδας και του φυλλομετρητή (browser) του χρήστη. Τα SSL πιστοποιητικά εξασφαλίζουν την **ασφαλή ανταλλαγή δεδομένων ανάμεσα στις δύο πλευρές**, **αποτρέποντας** κακόβουλους χρήστες από την **υποκλοπή δεδομένων**.

Ειδη πιστοποιητικων SSL :

Υπάρχουν 3 βασικές κατηγορίες πιστοποιητικών:

τα Domain Validation SSL **Certificates** (DV SSL),

τα Organization Validation SSL **Certificates** (OV SSL)

τα Extended Validation SSL **Certificates** (EV SSL).

Ας δούμε λίγο αναλυτικότερα τι είναι το καθένα από αυτά.

Τα **DV SSL** χρησιμοποιούνται για κωδικοποίηση της πληροφορίας και την ταυτοποίηση των στοιχείων του καταχωρητή και του ονόματος χώρου της ιστοσελίδας (domain). Με αυτόν τον τρόπο ο χρήστης μπορεί να είναι σίγουρος ότι η διεύθυνση της ιστοσελίδας είναι σωστή και παραπέμπει στο σωστό εξυπηρετητή.

Τα **OV SSL** χρησιμοποιούνται για κωδικοποίηση της πληροφορίας και την ταυτοποίηση της ιστοσελίδας και της εταιρίας που βρίσκεται πίσω από αυτήν. Πριν οι Αρχές Πιστοποιητικών εκδώσουν το πιστοποιητικό, ακολουθούν μια διαδικασία ταυτοποίησης της εταιρίας, των στοιχείων της διεύθυνσής της, καθώς και της ιδιοκτησίας του Domain Name.

Τέλος, τα **EV SSL** είναι τα πιο πλήρη και πιο ασφαλή πιστοποιητικά που μπορεί να παρέχει μια ιστοσελίδα στους χρήστες της σήμερα. Η αδειοδότηση και έκδοση των πιστοποιητικών αυτών απαιτεί διεξοδικές διαδικασίες, μέσα από τις οποίες οι Αρχές Πιστοποίησης ελέγχουν σχεδόν όλες τις πτυχές μιας εταιρίας και της ιστοσελίδας. Ο τρόπος για να καταλάβετε ότι βρίσκεστε σε μια ιστοσελίδα που καλύπτεται από αυτού του είδους το πιστοποιητικό, είναι ο πράσινος χρωματισμός της μπάρας διεύθυνσης της ιστοσελίδας σε συνδυασμό με το εικονίδιο του λουκέτου και το πρόθεμα https.

Ποιοι παρέχουν τα SSL;

Τα SSL πιστοποιητικά παρέχονται από εταιρίες προστασίας δεδομένων και έκδοσης πιστοποιητικών, οι οποίες ονομάζονται **Αρχές Πιστοποιητικών** (**Certificate Authorities**). Οι εταιρίες αυτές αναλαμβάνουν την ταυτοποίηση των στοιχείων της ιστοσελίδας καθώς και την ασφαλή μεταφορά δεδομένων μεταξύ των ιστοσελίδων αυτών και των χρηστών τους.

Πώς λειτουργούν τα SSL;

Τα SSL εξυπηρετούν τις εξής δύο διαδικασίες:

Ασφαλή μεταφορά δεδομένων μεταξύ ενός εξυπηρετητή και ενός υπολογιστή.

Πιστοποίηση και ταυτοποίηση, βοηθώντας τον χρήστη να επιβεβαιώσει την ταυτότητα της ιστοσελίδας με την οποία συναλλάσσεται.

Μόλις ξεκινήσει η διαδικασία που ενεργοποιεί τα SSL, όπως είναι για παράδειγμα η online παραγγελία ενός προϊόντος μέσω μίας ιστοσελίδας, τότε πραγματοποιείται μία ακολουθία από 4 βήματα, ώστε να εξασφαλιστεί η ασφαλής σύνδεση μεταξύ ιστοσελίδας και χρήστη:

Ο φυλλομετρητής ελέγχει το SSL Certificate, για να διαπιστώσει αν είναι έγκυρο και να πιστοποιήσει την ταυτότητα της ιστοσελίδας.

Ο εξυπηρετητής επικοινωνεί με τον φυλλομετρητή, και ενεργοποιείται η κρυπτογράφηση δεδομένων σε συγκεκριμένα bit (συνήθως **128bit** ή **256bit**).

Ο εξυπηρετητής και ο φυλλομετρητής ανταλλάσσουν μοναδικούς κωδικούς αποκρυπτογράφησης, ώστε να τους χρησιμοποιήσουν στην αποκρυπτογράφηση που πραγματοποιείται με την ολοκλήρωση της ανταλλαγής δεδομένων.

Η διαδικασία ανταλλαγής δεδομένων ξεκινάει, το εικονίδιο ασφαλούς μεταφοράς δεδομένων SSL εμφανίζεται δίπλα από την γραμμή διεύθυνσης της ιστοσελίδας και η συναλλαγή είναι πλέον ασφαλής.

Οι κωδικοί πρόσβασης είναι σημαντικό στοιχείο στη χρήση του Διαδικτύου και οι επιτήδειοι έχουν γίνει πολύ καλοί στο να τους μαντεύουν. Ποιοι είναι οι Συχνοί κίνδυνοι που σχετίζονται με τους κωδικούς πρόσβασης;

Ένας μεγάλος παράγοντας κινδύνου στο διαδίκτυο είναι οι κωδικοί πρόσβασης. Συχνά οι κωδικοί που χρησιμοποιούνται δεν έχουν τα απαραίτητα στοιχειά ασφαλείας και έτσι πέφτουν θύματα επιτηδείων. Οι οποίοι παραβιάζουν τις προσωπικές τους σελίδες στο διαδίκτυο και αποσπούν απόρρητα δεδομένα του χρηστή !! Ο σκοπός τους άλλοτε είναι επαγγελματικός και

άλλοτε για να περάσουν τον ελεύθερο χρόνο τους !! Οι χρηστές πρέπει να είναι προσεκτικοί και να ακολουθούν όλες τις προϋποθέσεις για ένα ασφαλές «σερφάρισμα» στην σελίδα τους και στα social media γενικότερα !

ΠΩΣ ΝΑ ΠΡΟΣΤΑΤΕΨΩ ΤΟΝ ΕΑΥΤΟ ΜΟΥ

ΒΑΣΙΚΟΙ ΚΑΝΟΝΕΣ ΧΡΗΣΗΣ ΔΙΑΔΙΚΤΥΟΥ

Ποιοί είναι Βασικοί κανόνες χρήσης Διαδικτύου από τους εφήβους; (κοινωνικά δίκτυα, ηλεκτρονικό ταχυδρομείο κτλ.)

Οι γενικοί κανόνες καλής συμπεριφοράς που δημιουργήθηκαν από τις ιδιαιτερότητες του δικτύου είναι:

Μ**ετριοπάθεια** Όποια άποψη και αν υποστηρίζουμε πάντα θα υπάρχει κάποιος που έχει σοβαρούς λόγους, ή νομίζει πως έχει σοβαρούς λόγους, να υποστηρίζει το αντίθετο. Γι' αυτό αντί να πούμε: «Ο Αρμαγεδδών ήταν απαίσια ταινία» καλύτερο είναι να γράψουμε: « Εμένα ο Αρμαγεδδών δεν μου άρεσε». Όσο πιο απόλυτη η δήλωσή σας τόσο πιο πιθανό είναι να αρχίσετε να λαμβάνετε flames (επιθετικά μηνύματα από τρίτους).

Ε**υγένεια** Μη ξεχνάτε πως υπάρχουν λέξεις και εκφράσεις που μπορούν να ερμηνευτούν με πολλούς διαφορετικούς τρόπους (ειδικά αν δεν γράφετε στη μητρική σας γλώσσα). Προσπαθήστε να είστε πολύ περισσότερο ευγενικοί απ' ότι σε μια συνηθισμένη ζωντανή «συζήτηση» αφού η απουσία άλλων στοιχείων (τόνος φωνής, έκφραση προσώπου κλπ.) οδηγεί πολύ εύκολα σε παρανοήσεις (κάποτε έστειλα ένα email επαινώντας κάποιον και νόμιζε πως τον κορόιδευα).

Π**ερίσκεψη** Ξαναδιαβάστε αυτό που γράψατε πριν το στείλετε και αυτό που σας έστειλαν πριν απαντήσετε. Ένας απίστευτος αριθμός καυγάδων ξεκινούν κυριολεκτικά άνευ λόγου και αιτίας (από παρανοήσεις όπου ο ένας έγραψε το Χ και ο άλλος κατάλαβε το Ψ).

Π**ροσαρμοστικότητα** Κάθε χώρος, mailing list, Usenet group ή chat room έχει τις δικές του ιδιαιτερότητες. Υπάρχουν συζητήσεις που μπορεί να είναι απόλυτα αποδεκτές σε ένα χώρο αλλά απαράδεκτες σε ένα άλλο. Γι' αυτό, κάθε φορά που συμμετέχετε σε ένα νέο χώρο, προτιμήστε να περάσετε λίγο χρόνο παρακολουθώντας τους άλλους για να καταλάβετε το πνεύμα των συζητήσεων.

Μ**ετριοφροσύνη** Δεν ξέρετε πόσο πιο ειδικός από σας μπορεί να είναι αυτός με τον οποίο μιλάτε. Μπορεί να είστε συγγενής καρδιοπαθή, άρα ξέρετε κάποια πράγματα, και να βρεθείτε να συζητάτε με ένα γιατρό, που μάλλον ξέρει περισσότερα.

Ι**εραρχία** Ο list ή group owner και ο moderator είναι οι αδιαμφισβήτητοι αρχηγοί και σπανιότατα θα σας υποστηρίξει κανείς αν τους πάτε κόντρα.

Θ**άρρος** Όχι για να τσακωθείτε, αλλά για να παραδεχθείτε τα λάθη σας. Όσο πιο έντονα υποστηρίζετε κάποιο λάθος σας τόσο πιο ανόητος φαίνεστε.

Κατανόηση Η κοινωνία μας χρειάστηκε αιώνες για να βρει και να καθιερώσει τους σημερινούς κανόνες καλής συμπεριφοράς. Είναι φυσιολογικό στο δίκτυο να υπάρχουν πολλοί άνθρωποι που ακόμη πως πρέπει να συμπεριφέρονται. Θεωρείστε τους κακότροπους ανθρώπους όχι σαν αγενείς αλλά σαν αρχάριους και προσπαθήστε να τους βοηθήσετε να μάθουν να ξεχωρίζουν το σωστό από το λάθος, χωρίς βέβαια να κάνετε τους έξυπνους.

Συναδελφικότητα Οι χρήστες του Internet εξερευνούν ένα καινούριο χώρο που εξακολουθεί να έχει μυστικά ακόμη και για τους πιο πεπειραμένους. Αυτή η αίσθηση του «νέου συνόρου» φέρνει μαζί τους ανθρώπους του δικτύου πιο κοντά και τους κάνει πιο δεκτικούς στην επικοινωνία. Στο δίκτυο μπορείτε να ζητήσετε βοήθεια από έναν άγνωστο ακριβώς όπως μπορείτε να σταματήσετε κάποιον άγνωστο στο δρόμο και να τον ρωτήσετε που βρίσκεται η οδός Χ. Για να διατηρήσουμε αυτό το όμορφο πνεύμα προσπαθήστε να μην κάνετε κατάχρηση της καλής διάθεσης των άλλων, ζητώντας συνέχεια βοήθεια για ότι σας απασχολεί, και προσπαθήστε να μην παίρνετε αλλά να δίνετε κιόλας βοηθώντας κι εσείς με τη σειρά σας όσους μπορείτε.

Προσωπική Επαφή Μη τσακώνεστε ποτέ μέσω δικτύου. Τα γραπτά αποθηκεύονται σε σκληρούς δίσκους και μένουν για καιρό να μας θυμίζουν τα σκληρά λόγια που γράψαμε ή μας έγραψαν. Αφού τελειώσει η διαμάχη, διαγράψτε ότι σας είπαν για να μην δηλητηριάσει τις σχέσεις σας στο μέλλον. Και, αν πρέπει οπωσδήποτε να καυγαδίσετε, φροντίστε να το κάνετε από το τηλέφωνο. Τα λόγια χάνονται και δεν θα στοιχειώσουν τις σχέσεις σας στο μέλλον.

Συγκεκριμένα στα κοινωνικά δίκτυα

Δεν θα πρέπει να δίνετε σε κανέναν τον κωδικό πρόσβασης στο εικονικό προφίλ σας. Όποιος αποκτά πρόσβαση στο προφίλ σας μπορεί να διαχειριστεί πλήρως τα δεδομένα που εμφανίζονται σε αυτό.

Πριν εγγραφείτε σε μια ιστοσελίδα κοινωνικής δικτύωσης αναζητήστε τη δήλωση περί απορρήτου και κατανοήστε πλήρως με ποιον τρόπο θα χρησιμοποιούνται από την Ιστοσελίδα τα προσωπικά σας δεδομένα.

Μην ανεβάζετε στο προφίλ σας φωτογραφίες όπου φαίνεται καθαρά η τοποθεσία στην οποία βρίσκεστε, ειδικότερα αν πρόκειται για το σπίτι σας, το σχολείο ή μέρη που συχνάζετε. Έτσι θα μειώσετε τις πιθανότητες εντοπισμού σας στον φυσικό κόσμο.

Αν δεχθείτε ένα προσβλητικό ή ανεπιθύμητο μήνυμα, χρησιμοποιήστε την ενσωματωμένη μέθοδο καταγγελιών της ιστοσελίδας κοινωνικής δικτύωσης που χρησιμοποιείτε. Συνήθως αναφέρεται με τη λέξη «report».

Να έχετε πάντα υπόψη σας ότι οι πληροφορίες που δημοσιεύετε στις ιστοσελίδες κοινωνικής δικτύωσης είναι δημόσια προσπελάσιμες, επομένως, καλό θα ήταν να μη δημοσιεύετε στοιχεία και φωτογραφίες που θα σας έφερναν σε δύσκολη θέση. Ακόμα και όταν διαγράψετε το προφίλ σας πολλές πληροφορίες δεν αφαιρούνται και ενδέχεται επίσης να τις συναντήσετε και αλλού στο Διαδίκτυο.

Να γνωρίζετε ότι από τη στιγμή που προσθέτετε στη λίστα των φίλων σας κάποιο άτομο (αποδοχή friend request), αυτό αποκτά πρόσβαση στα προσωπικά δεδομένα που εμφανίζονται στο προφίλ σας, μεταξύ των οποίων οι φωτογραφίες και τα στοιχεία επικοινωνίας σας.

Από τη στιγμή που δημιουργείτε το εικονικό σας προφίλ, θα πρέπει να πάτε στο μενού των ρυθμίσεων για τη διαχείριση των προσωπικών σας δεδομένων (συνηθέστερα θα το βρείτε στα αγγλικά **ως privacy settings**) και να αλλάξετε τις προεπιλεγμένες ρυθμίσεις.

Στο μενού αυτό μπορείτε μεταξύ άλλων:

- Να επιλέξετε αν οι επισκέπτες του προφίλ σας μπορούν να δουν αν είστε on-line ή όχι.

- Να καθορίσετε ποιοι θα μπορούν να βλέπουν το εικονικό σας προφίλ ή συγκεκριμένα στοιχεία που περιλαμβάνονται σε αυτό (ημερομηνία γέννησης, φωτογραφία, κ.ά.).

- Να μπλοκάρετε την πρόσβαση συγκεκριμένων ατόμων στο προφίλ σας.

- Να ρυθμίσετε από ποιους χρήστες μπορείτε να λαμβάνετε προσωπικά μηνύματα και σχόλια.

- Να ρυθμίσετε αν θα εμφανίζεται το προφίλ σας στα αποτελέσματα αναζήτησης μέσω της Ιστοσελίδας καθώς και τη μορφή που θα έχει (αν θα φαίνεται η φωτογραφία, τα στοιχεία επικοινωνίας, κ.ά.).

Ποια είναι η σωστή συμπεριφοράς του χρήστη όταν κάνει αναζήτηση πληροφοριών, έτσι ώστε να αποφεύγει να προσπελάσει ακατάλληλο υλικό;

Συμβουλές για παιδιά/εφήβους

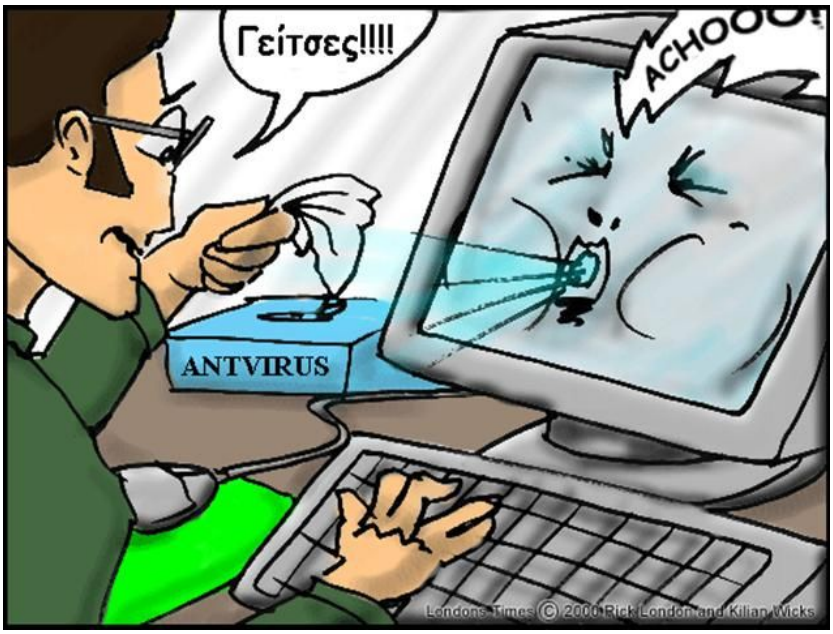
Ακατάλληλη ή κακή συμπεριφορά από κάποιον ή ακατάλληλο περιεχόμενο δεν είναι ποτέ εντάξει. Εάν συμβεί κάτι τέτοιο, **μπλοκάρουμε την πρόσβαση αυτού του χρήστη και το λέμε στους γονείς μας ή σε έναν ενήλικα που εμπιστευόμαστε.**

Είναι σημαντικό να **χρησιμοποιούμε πάντα ιστοσελίδες και ιστοχώρους που είναι κατάλληλα για την ηλικία μας.**

Τα **φίλτρα γονικού ελέγχου** μπορούν να μειώσουν αυτό τον κίνδυνο.

Θα πρέπει **να ενθαρρύνουμε** τα παιδιά να μας μιλάνε σε ΠΕΡΙΠΤΩΣΗ που έχουν έρθει αντιμέτωπα στο διαδίκτυο με κάτι που τα κάνει να αισθάνονται άβολα.

Επίσης, είναι σημαντικό **να καταγγείλουμε** τις περιπτώσεις που θεωρούμε ότι το συγκεκριμένο υλικό είναι παράνομο (όπως για παράδειγμα σεξουαλικό υλικό με πρωταγωνιστές παιδιά).



FACEBOOK

Πώς να αποφύγουμε κακόβουλο λογισμικό μέσω Facebook;

1. Μάθετε τι να αναζητάτε: οι Facebook spammers γίνονται όλο και πιο δημιουργικοί και μπορούν να σας κάνουν να την πατήσετε για κάτι επιβλαβές και πιο ασαφές όσον αφορά τον εντοπισμό τους. Εάν παρατηρήσετε οποιοδήποτε από τα ακόλουθα χαρακτηριστικά για μια ανάρτησε σε τοίχο, ομάδα, σελίδα, κλπ., συνιστάται να μην κάνετε κλικ.

Μπορεί να δείτε μια ανάρτηση σε τοίχο από έναν φίλο με τον οποίο ποτέ δεν αλληλεπιδράτε. Σχεδόν πάντα αποτελείται από ένα αισθητά αυτοματοποιημένο χαιρετισμό με έναν άγνωστο σύνδεσμο στο τέλος. Τα παραδείγματα περιλαμβάνουν "Γεια σου Χαρά, δεν θα το πιστέψεις, αλλά αυτή η δίαιτα λειτουργεί πραγματικά [σύνδεσμος σε ιστοσελίδα]!" ή "Χάρη δεν θα το πιστέψεις, αλλά μόλις παρέλαβα

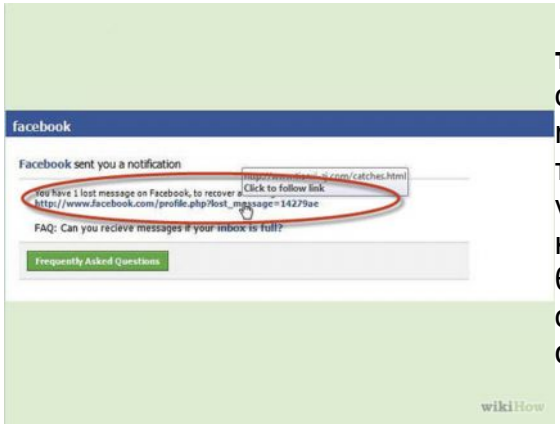
δωρεάν ένα iPad στην πόρτα μου, κάνε κλικ εδώ -! [σύνδεσμος σε ιστοσελίδα]"

Μπορεί να δείτε μια ανάρτηση σε τοίχο από έναν φίλο να σας ζητά να παρακολουθήσετε ένα βίντεο από το YouTube στο οποίο υποτίθεται ότι απεικονίζεστε. Αυτό μπορεί να προηγηθεί από ένα αυτοματοποιημένο χαιρετισμό, όπως "Θεέ μου Χάρη, τι κάνεις σε αυτό το βίντεο; LOL!"

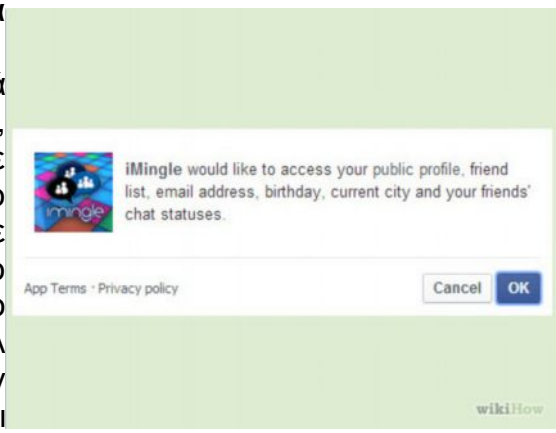
Έχετε προσκληθεί σε μια ομάδα ή ένα γεγονός που έχει να κάνει με δωρεάν ηλεκτρονικά ή παραχώρηση ρούχων, συχνά με τα πρώτα 50.000 άτομα που συμμετέχουν ή υποτίθεται μετά την ολοκλήρωση μια μακράς έρευνας.

Θέλετε να αρχίσετε να παίζετε ένα παιχνίδι στο Facebook ή να χρησιμοποιήσετε μια εφαρμογή, και προτού ξεκινήσετε, σας ζητείται να εξιουσιοδοτήσετε το πρόγραμμα για να δημοσιεύσει στον τοίχο σας, στους τοίχους των φίλων σας, πρόσβαση σε όλες τις προσωπικές σας πληροφορίες, κλπ.

2. Μην ξεγελιέστε από τα σύντομα links: οι Facebook spammers σχεδόν πάντα αποκρύπτουν τις συνδέσεις με επιβλαβείς ιστοσελίδες σε υπολογιστή χρησιμοποιώντας μια υπηρεσία URL συντόμευσης, η οποία μπορεί να σας παραπλανήσει και να νομίζετε ότι κάνετε κλικ πάνω σε ένα νόμιμο άρθρο ή blog. Στην πραγματικότητα, αυτοί οι σύνδεσμοι οδηγούν σε ιστοσελίδες που μπορούν να εγκαταστήσουν κακόβουλο λογισμικό, spyware, και άλλους ιούς στον υπολογιστή σας.



3. Αποφεύγετε να εξουσιοδοτείτε αναξιόπιστα παιχνίδια και εφαρμογές: Αν σας ζητηθεί να επιτρέψετε σε ένα πρόγραμμα Facebook να δημοσιεύει στο δικό σας ή/και στους τοίχους των φίλων σας, να αποκτήσει πρόσβαση σε ιδιωτικές πληροφορίες και τα δίκτυα σας, να έχει πρόσβαση στα δεδομένα σας ανά πάσα στιγμή, κλπ., κλείστε το παιχνίδι ή την εφαρμογή. Σκεφτείτε το - θα παραχωρούσατε στην πραγματική ζωή πρόσβαση σε όλες αυτές τις πληροφορίες σε ένα παντελώς άγνωστο άτομο;



4. Ψάξτε για αποκαλυπτικά σημάδια του spam: Αν δείτε ένα φίλο να αναρτά πολλαπλές συνδέσεις ή βίντεο σε τοίχους πολλών φίλων, είναι πολύ πιθανό να είναι το έργο ενός spammer. Αν δείτε μια ανάρτηση σε τοίχο φίλου που ισχυρίζεται ότι το Facebook προσφέρει επιτέλους έναν τρόπο για να δείτε ποιος βλέπει το προφίλ σας, για παράδειγμα, μην το πιστέψετε και προπαντός αποφύγετε να κάνετε κλικ στο σύνδεσμο spam "Ενεργοποίηση Ειδοποιήσεων Προφίλ Viewer". Επιπλέον, οι σελίδες που προειδοποιούν ότι δεν έχουν εγκριθεί από το Facebook θα μπορούσαν (αν και όχι πάντα) να είναι επιβλαβείς για τον υπολογιστή σας.

5. Ενεργήστε το ταχύτερο δυνατό αν πέσατε θύμα spam συνδέσμου ή σελίδας. Υπάρχουν μερικοί τρόποι που μπορείτε να χειριστείτε την κατάσταση, αν καταλάβατε ότι έχετε ανεπιθύμητα μηνύματα ή κάνετε spamming σε άλλους.

Αφαιρέστε τις spam αναρτήσεις στον τοίχο, είτε κάνοντας κλικ στο "X" στα δεξιά της ανάρτησης, ή επισημαίνοντας την ως spam μέσω του ίδιου αναπτυσσόμενου μενού.

Απαλλαγείτε από τα παιχνίδια που μπορεί να είναι spam με τη μετάβαση σε «Ρυθμίσεις λογαριασμού», και στη συνέχεια "Διαχείριση Εφαρμογών". Έτσι θα είστε σε θέση να

επεξεργαστείτε και να καταργήσετε τα δικαιώματα.

Αλλάξτε τον κωδικό πρόσβασης στο Facebook! Ένας συνδυασμός από σύμβολα, γράμματα και αριθμούς αποτελεί ένα ισχυρό και καλό κωδικό. Συμβουλές για passwords στο άρθρο Ανάγκη για ουσιαστική προστασία της διαδικτυακής μας ταυτότητας.

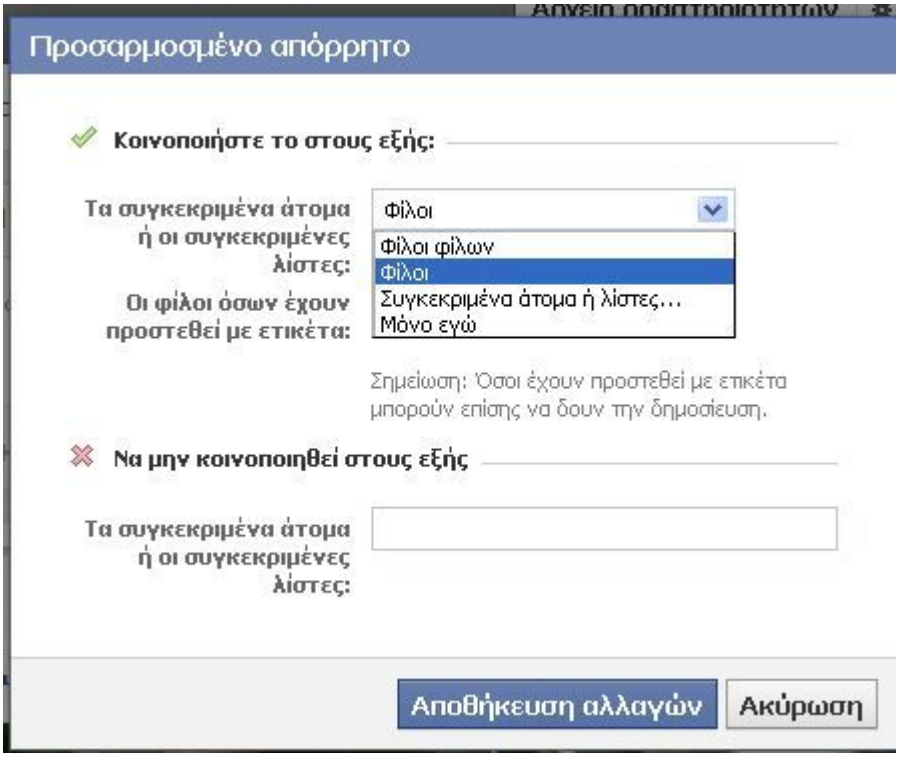
Σκεφθείτε να επιτρέψετε την ασφαλή πλοήγηση μέσω του Facebook μέσα από τις Ρυθμίσεις ασφαλείας. Επίσης, σπεύσατε για λήψη δωρεάν και αξιόπιστου προγράμματος ανίχνευσης ιών (ή αγορά μιας πιο προηγμένης έκδοσης λογισμικού) για να ελέξγετε την ασφάλεια στον υπολογιστή σας. Όσο νωρίτερα γίνει αυτό, τόσο το καλύτερο.

Πώς μπορώ να έχω το προφίλ μου στο Facebook ασφαλές;

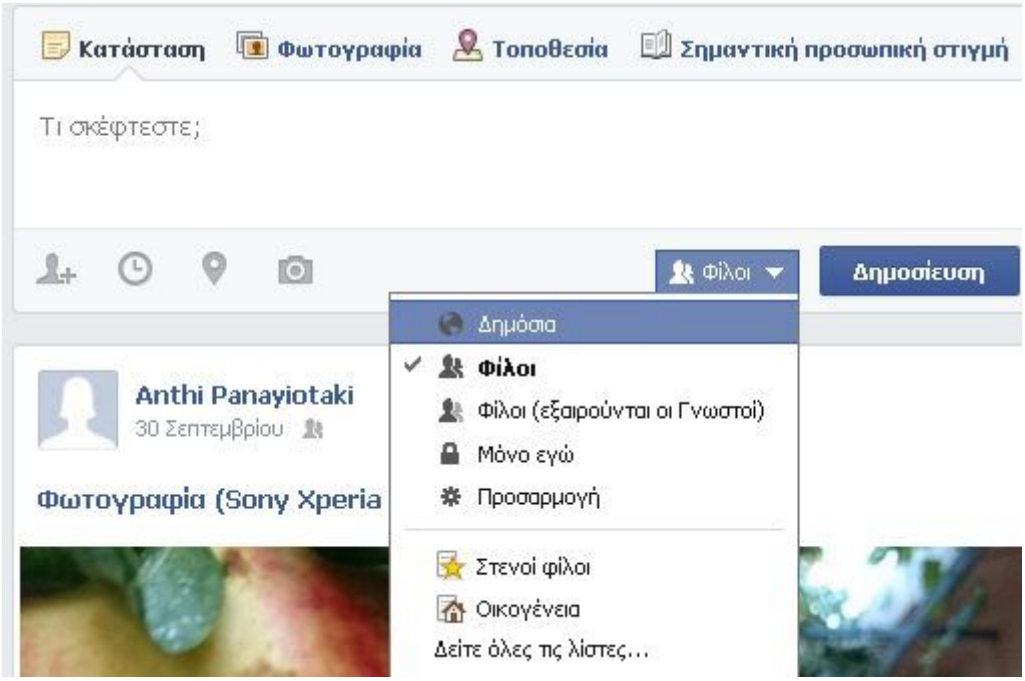
Δεν υπάρχουν απόρρητα ονόματα στο Facebook

Το μεγαλύτερο σάιτ κοινωνικής δικτύωσης που στεγάζει πάνω από 1 δισεκατομμύριο χρήστες του Διαδικτύου παύει οριστικά να τους παρέχει την δυνατότητα να ορίσουν ως απόρρητη την συμμετοχή τους σε αυτό. Στο εξής, όλα τα μέλη του Facebook εντοπίζονται όταν γίνεται αναζήτηση του ονόματός τους στο κοινωνικό δίκτυο.

Η υπηρεσία αναφέρεται στην δυνατότητα ως κάτι από το παρελθόν, τότε που το Facebook δεν ήταν τίποτα περισσότερο από ένας διαδικτυακός κατάλογος με ανθρώπινα προφίλ. Η απενεργοποίηση της δυνατότητας καταχώρησης ως απόρρητου του ονόματος είχε ξεκινήσει πριν από έναν χρόνο για εκείνους που δεν το χρησιμοποίησαν, αναφέρει στην σχετική ανακοίνωση το Facebook και ο εκπρόσωπός του Μάικλ Ρίχτερ επισημαίνει πως είναι μικρό το ποσοστό των μελών του που είχε δηλώσει ως απόρρητο το όνομά του και «ζούσε» στο Facebook μόνο με τον στενό κύκλο των φίλων του. Τονίζει δε, πως έτσι κι αλλιώς, το απόρρητο όνομά τους εμφανιζόταν στις Ενημερώσεις από το προφίλ του ή στις Ενημερώσεις ενός κοινού φίλου, οπότε το έβλεπαν και μπορούσαν να κάνουν κλικ τρίτα πρόσωπα.



Το Facebook συστήνει σε όσους θέλουν να κρύβονται, να αναθεωρούν τις επιλογές τους σε καθετί που γράφουν: σε κάθε post, σε κάθε φωτογραφία, σε κάθε ετικέτα, σε κάθε δήλωση τοποθεσίας πρέπει και μπορούν να διαλέγουν ή να προσαρμόζουν το κοινό (μπορεί κανείς και να αποκλείσει αποδέκτες) ή να ορίσουν εκ προοιμίου το κοινό για όλα όσα γράφουν.



Δημόσια μία ανάρτηση σήμερα, δημόσιες όλες αύριο;

Μάλλον ανησυχητικό είναι ότι εάν γράψετε κάτι Δημόσιο σήμερα στο πλαίσιο δημοσίευσης, το Facebook θυμάται αυτή την επιλογή και οι μελλοντικές σας δημοσιεύσεις θα είναι εκ προοιμίου όλες δημόσιες. Ομοίως, εξίσου ενοχλητικό μπορεί να αποδειχτεί ότι εάν γράψετε κάτι μόνο για τους Φίλους (εξαιρούνται οι Γνωστοί), τότε το κοινό θα είναι περιορισμένο και στις επόμενες αναρτήσεις σας.

«Μπορείτε να διαχειριστείτε το απόρρητο όσων κοινοποιείτε, με το εργαλείο επιλογής κοινού στο πλαίσιο δημοσίευσης. Το εργαλείο απομνημονεύει την επιλογή σας, η οποία ισχύει και για τις επόμενες δημοσιεύσεις σας, μέχρι να την ξαναλλάξετε», μεταφέρει το σχετικό μήνυμα της υπηρεσίας.

Αυτό σημαίνει ότι εάν εσείς έχετε επιλέξει να βλέπουν τις αναρτήσεις μόνο οι φίλοι σας, εάν αλλάξετε την ρύθμιση για μια μόνο ανάρτηση, η αλλαγή θα ισχύει (αυθαίρετα) και για το μέλλον, παρακάμπτοντας την συνολική ρύθμιση του απορρήτου σας στις Ρυθμίσεις Απορρήτου.

Κρύψτε μαζικά τις παλαιότερες δημοσιεύσεις σας

Σε ότι αφορά τις δημοσιεύσεις που έχουν κάνει τα μέλη στο παρελθόν και θέλουν πλέον να περιορίσουν την εμφάνισή τους μαζικά με ένα κλικ, το Facebook παραπέμπει στις ρυθμίσεις απορρήτου. Προειδοποιεί όμως τα μέλη του πως εάν το κάνουν μαζικά για τις παλαιότερες δημοσιεύσεις τους χωρίς να τις δουν μια προς μια από το λεγόμενο Αρχείο δραστηριοτήτων, και μετά το μετανιώσουν, θα πρέπει να τις αναθεωρήσουν μια προς μια και να κάνουν πάλι ορατές όσες θέλουν να απευθύνονται σε ευρύτερο κοινό (π.χ. μια δημόσια φωτογραφία που περιορίστηκε μόνο στους φίλους). Βεβαίως, το απόρρητό σας δεν εξαρτάται μόνο από τις δικές σας επιλογές, αλλά και από τις επιλογές που έκαναν οι φίλοι σας για εσάς (π.χ. προσθέτοντας το όνομά σας ως ετικέτα σε μια δημόσια φωτογραφία που το βλέπουν οι πιθανά άγνωστοι φίλοι τους -αν και μπορείτε να ζητήσετε να αφαιρεθεί το tag ή προσωπικά ή με «αναφορά»).

Επισκεφτείτε τις δικές σας ρυθμίσεις απορρήτου

Από τις ρυθμίσεις απορρήτου μπορείτε επίσης να ορίσετε εάν θα εμφανίζεται περιεχόμενο από ό,τι είναι δημόσιο στο προφίλ σας στο Facebook όταν κάποιος κάνει μια σχετική αναζήτηση στις μηχανές αναζήτησης, εκτός Facebook.

Πάντως, η ανακοίνωση για την κατάργηση της δυνατότητας ορισμού απορρήτου ονόματος στο Facebook μπορεί να έχει πολλαπλές συνέπειες τις οποίες θα διερευνήσουμε.

Προφανώς, στο εξής εάν δεν εμφανίζονται αποτελέσματα για ένα πρόσωπο αυτό σημαίνει είτε ότι δεν έχει λογαριασμό στην υπηρεσία ή την χρησιμοποιεί με άλλο όνομα.Ο μόνος τρόπος για να κρυφτείτε από κάποιον στο Facebook είναι **να τον μπλοκάρετε.**

Χρήσιμο tip: Εάν θέλετε να δείτε πως εμφανίζεται το Χρονολόγιό σας Δημόσια ή τι βλέπει για εσάς ένα συγκεκριμένο πρόσωπο που είναι φίλος σας (δεν θα δείτε βέβαια τι βλέπει κάποιος άγνωστος, με τον οποίο έχετε τουλάχιστον έναν κοινό φίλο) επιλέξτε «Προβολή ως» από το βελάκι που ενεργοποιεί ένα αναδυόμενο μενού δίπλα στο κουμπί για το Αρχείο Δραστηριοτήτων:

Τι επιτρέπεται και τι όχι να αναρτάται στο facebook;

Τα παρακάτω είναι μερικά από τα είδη περιεχομένου που απαγορεύονται στο Facebook. Για να δείτε την πλήρη λίστα και να μάθετε περισσότερα σχετικά με τις πολιτικές μας, διαβάστε τους Όρους της κοινότητας:

- Περιεχόμενο με γυμνό ή σεξουαλικά υπονοούμενα
- Ρητορική μίσους, βάσιμες απειλές ή ευθείες επιθέσεις σε άτομα ή ομάδες
- Περιεχόμενο με σκηνές αυτοτραυματισμού ή σκληρής βίας
- Ψεύτικα ή παραπλανητικά Χρονολόγια
- Ανεπιθύμητο περιεχόμενο (σπαμ)

Γιατί το Facebook δεν είναι κατάλληλο για παιδιά κάτω των 13 ετών;

1. Τα παιδιά αποτελούν μέρος της πιο επεκτατικής προσωπικής συλλογής δεδομένων και προφίλ στο πιο ισχυρό κοινωνικό μέσο του Διαδικτύου.
2. Τα παιδιά εκτίθενται σε μια νέα γενιά εξαιρετικά πειστικών και χειραγωγίσιμων ψηφιακών πρακτικών μάρκετινγκ.
3. Οι πρακτικές μάρκετινγκ του Facebook επωφελούνται από τα γνωστικό-κοινωνικά και συναισθηματικά ευάλωτα σημεία των παιδιών.
4. Τα παιδιά υποβάλλονται σε μια επίθεση ανθυγιεινής εμπορίας τροφίμων – ακριβώς σε μια εποχή που η παιδική παχυσαρκία έχει γίνει μια μεγάλη κρίση.
5. Δεν υπάρχουν εγγυήσεις που να προστατεύουν επαρκώς τα παιδιά από την επιθετικές και τις επιβλαβείς πρακτικές μάρκετινγκ συλλογής δεδομένων του Facebook.

ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ

Πώς μπορώ να δημιουργήσω ασφαλέστερους κωδικούς πρόσβασης ;

1. Χρησιμοποιείτε δυνατούς κωδικούς και όχι απλούς

Ένας κωδικός μπορεί να είναι ο εξής: **olympiacos**. Πολύ κοινός και εύκολος να τον σκεφτεί

κανείς. Ένας άλλος κωδικός μπορεί να είναι ο εξής: **!OlympiaC0s**. Μάλλον όχι και τόσο εύκολος κωδικός για να τον βρει κανείς.

Γενικά, να θυμάστε πως σε έναν κωδικό καλό είναι να χρησιμοποιείτε τουλάχιστον ένα **σύμβολο**, **γράμμα** (κεφαλαίο και μικρό) και **αριθμό**. Ο συνδυασμός των προηγουμένων μπορεί να δημιουργήσει έναν **ισχυρό κωδικό**. Φυσικά, αποφεύγετε ονόματα, ημερομηνίες γεννήσεις κλπ, τα οποία χαρακτηρίζουν εσάς.

2. Μη χρησιμοποιείτε τον ίδιο κωδικό παντού

Ξέρω πως είναι δύσκολο να χρησιμοποιείτε διαφορετικό κωδικό σε κάθε Κοινωνικό Δίκτυο, καθώς ένα μυαλό το έχετε και δεν το χρειάζεστε μόνο για τους κωδικούς. Παρόλα αυτά, δε θέλετε κάποιος να βρει τον κωδικό σας στο Facebook και ύστερα να αποκτήσει πρόσβαση σε Twitter, Foursquare κλπ.

Τουλάχιστον, προσέξτε ώστε **ο κωδικός για το email που δηλώνετε στα Κοινωνικά Δίκτυα να είναι μοναδικός**. Αν κάποιος μπορεί να διαχειριστεί το email σας, τότε μπορεί να διαχειριστεί και να αλλάξει όλους τους κωδικούς σας. Να το θυμάστε αυτό. Μοναδικός **κωδικός για το email λοιπόν.**

3. Μη μοιράζεστε τους κωδικούς σας με φίλους

Δε θα ήθελα να φανώ απόλυτος, υπάρχουν περιπτώσεις όπου κάποιος μπορεί να μοιραστεί έναν κωδικό του με φίλο του, αν και δε θα το συνιστούσα. **Αποφεύγετε να δίνετε κωδικούς** σας σε άτομα χωρίς να υπάρχει ιδιαίτερος λόγος. Κι αν το έχετε κάνει και το μετανιώσατε, ποτέ δεν είναι αργά να αλλάξετε τον κωδικό σας. ;)

4. Αλλάζετε τον κωδικό σας συχνά

Όχι κάθε μέρα, προς Θεού. Μην τον αφήνετε όμως και χρόνια ίδιο, καθώς υπάρχει πιθανότητα κάποιος άλλος να έχει βρει και να χρησιμοποιεί το λογαριασμό σας και να μην το έχετε πάρει χαμπάρι εσείς. Καλό είναι **κάθε τόσο**, ας πούμε εξάμηνο ή όσο νομίζει ο καθένας σας, **να αλλάζετε τον κωδικό σας**, ειδικά αν έχετε υποψίες ότι κάτι δεν πάει καλά με το λογαριασμό σας...

5. Μη χρησιμοποιείτε τον κωδικό σας σε ιστοσελίδες μη ασφαλείς ή σε δημόσιους υπολογιστές

Αν θέλετε να συνδεθείτε στο Facebook ή το Twitter, **σιγουρευτείτε πως βρίσκεστε στις επίσημες ιστοσελίδες** τους και όχι σε κάποια άλλη ιστοσελίδα. Μην εμπιστεύεστε πλαίσια για σύνδεση σε κάποιο Κοινωνικό Δίκτυο, τα οποία δε βρίσκονται στις επίσημες ιστοσελίδες των Κοινωνικών Δικτύων. Κατά πάσα πιθανότητα μπορείτε να πέσετε θύμα μιας επίθεσης phising.

Όσον αφορά τους **δημόσιους υπολογιστές**, όπως για παράδειγμα τον υπολογιστή στη βιβλιοθήκη της σχολής ή στο ίντερνετ καφέ, **ποτέ μην τους εμπιστεύεστε**, καθώς πολλά χέρια πιάνουν το πληκτρολόγιο τους και πολλά ύποπτα προγράμματα μπορούν να τρέχουν στο παρασκήνιο. Αν δεν υπάρχει απόλυτη ανάγκη για ρίσκο, τότε μη συνδεθείτε με τα στοιχεία σας.

6. Χρησιμοποιείτε το πρωτόκολλο https όπου αυτό είναι δυνατό να συμβεί

Στο browser που χρησιμοποιείτε για να συνδεθείτε στο ίντερνετ, π.χ. Internet Explorer, Google Chrome, Mozilla Firefox κλπ, θα έχετε παρατηρήσει κάποιες ιστοσελίδες όπου ο σύνδεσμος ξεκινά με **https** και όχι με http. Συνήθως το https είναι και με πράσινο χρώμα ή έχει το εικονίδιο μιας κλειδαριάς.

Με το https στέλνετε κρυπτογραφημένους τους κωδικούς σας και είναι πολύ πιο δύσκολο να σας τους κλέψουν. Για το λόγο αυτό, ρίξτε μια ματιά στις ρυθμίσεις του Κοινωνικού Δικτύου που χρησιμοποιείτε και **ενεργοποιήστε την επιλογή για σύνδεση με πρωτόκολλο https** αν αυτή υπάρχει και αν δεν είναι ενεργοποιημένη ήδη.

ΗΛΕΚΤΡΟΝΙΚΗ ΕΞΑΠΑΤΗΣΗ

Πώς να προστατευτείτε από την ηλεκτρονική εξαπάτηση;

Βέλτιστες πρακτικές για να προστατευτείτε από την ηλεκτρονική εξαπάτηση

Μην απαντάτε ποτέ σε μηνύματα ηλεκτρονικού ταχυδρομείου που σας ζητούν τα προσωπικά σας στοιχεία Πρέπει να είστε καχύποπτοι αν λάβετε μήνυμα από εταιρεία ή άτομο που σας ζητάει τα προσωπικά σας στοιχεία — ή που σας στέλνει προσωπικά στοιχεία ζητώντας σας να τα επαληθεύσετε. Αντί για αυτό, χρησιμοποιήστε τον αριθμό τηλεφώνου από το τραπεζικό έντυπο για να τηλεφωνήσετε. Μην τηλεφωνήσετε στον αριθμό που μπορεί να περιλαμβάνεται στο μήνυμα. Ομοίως, δεν πρέπει να δίνετε ποτέ οικειοθελώς τα στοιχεία σας σε όποιον σας τηλεφωνεί χωρίς να γνωρίζετε ποιος είναι.

Μην κάνετε κλικ σε ύποπτες συνδέσεις Μην κάνετε κλικ σε συνδέσεις που περιλαμβάνονται σε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου. Η σύνδεση μπορεί να μην είναι αξιόπιστη. Αντί για αυτό, επισκεφτείτε τις τοποθεσίες Web πληκτρολογώντας τη σχετική διεύθυνση URL στο πρόγραμμα περιήγησης ή χρησιμοποιώντας τη σύνδεση Αγαπημένα.

Χρησιμοποιείτε δυναμικούς κωδικούς πρόσβασης και αλλάζετέ τους συχνά Αν ο λογαριασμός τους επιτρέπει, οι δυναμικοί κωδικοί πρόσβασης συνδυάζουν πεζά και κεφαλαία γράμματα, αριθμούς και σύμβολα ώστε να είναι ακόμα ποιο δύσκολοι να σπάσουν. Μην χρησιμοποιείτε πραγματικές λέξεις. Χρησιμοποιείτε διαφορετικούς κωδικούς πρόσβασης για κάθε λογαριασμό και αλλάζετέ τους συχνά. Είναι δύσκολο να θυμάστε τόσους κωδικούς

πρόσβασης και μπορεί να τους χάσετε εύκολα, συνεπώς βεβαιωθείτε ότι τους έχετε σημειώσει κάπου ή αποθηκεύστε τους στη συσκευή ως διακριτικό USB. Βεβαιωθείτε ότι τους φυλάσσετε σε κλειδωμένη τοποθεσία! Για περισσότερες συμβολές σχετικά με τη δημιουργία δυναμικών κωδικών πρόσβασης καθώς και πώς μπορείτε να θυμάστε και να αποθηκεύσετε με ασφάλεια τους κωδικούς πρόσβασης, δείτε την ενότητα Δημιουργία δυναμικών κωδικών πρόσβασης (Στα Αγγλικά).

Μην στέλνετε προσωπικά στοιχεία σε τυπικά μηνύματα ηλεκτρονικού ταχυδρομείου Τα συνηθισμένα μηνύματα ηλεκτρονικού ταχυδρομείου δεν είναι κρυπτογραφημένα, είναι σαν να στέλνετε μια απλή καρτ ποστάλ. Αν είναι ανάγκη να χρησιμοποιήσετε μηνύματα ηλεκτρονικού ταχυδρομείου για τις προσωπικές συναλλαγές σας, χρησιμοποιήστε το Outlook για να υπογράψετε ψηφιακά και να κρυπτογραφήσετε τα μηνύματα με ασφάλεια S/MIME. Τα MSN®, Hotmail®, Outlook Express, Microsoft Office Outlook Web Access, Lotus Notes, Netscape και Eudora υποστηρίζουν την ασφάλεια S/MIME.

Συνεργαστείτε με εταιρείες που γνωρίζετε και εμπιστεύεστε Χρησιμοποιείτε γνωστές, καθιερωμένες εταιρείες με φήμη για παροχή ποιοτικών υπηρεσιών. Μια επαγγελματική τοποθεσία Web πρέπει να συνοδεύεται πάντα από δήλωση προστασίας του ιδιωτικού απορρήτου η οποία αναφέρει συγκεκριμένα ότι η εταιρεία δεν πρόκειται να διαβιβάσει το όνομα και τα στοιχεία σας σε τρίτους.

Βεβαιωθείτε ότι η τοποθεσία Web χρησιμοποιεί κρυπτογράφηση Της διεύθυνσης Web πρέπει να προηγείται η έκφραση https:// αντί για το συνηθισμένο http:// στη γραμμή διευθύνσεων. Επίσης, κάντε διπλό κλικ στο εικονίδιο κλειδαριάς από τη γραμμή κατάστασης του προγράμματος περιήγησης για να εμφανιστεί το ψηφιακό πιστοποιητικό για την τοποθεσία. Το όνομα μετά από το στοιχείο **Εκδόθηκε σε** στο πιστοποιητικό πρέπει να αντιστοιχεί στην τοποθεσία που πιστεύετε ότι έχετε επισκεφτεί. Αν υποψιάζεστε ότι η τοποθεσία Web δεν είναι αυτή που θα έπρεπε, βγείτε αμέσως και αναφέρετέ την. Μην ακολουθήσετε καμία από τις συμπεριλαμβανόμενες οδηγίες.

Προστατεύστε τον υπολογιστή σας Η χρήση τείχους προστασίας είναι σημαντική, όπως επίσης η ενημέρωση του υπολογιστή και η χρήση λογισμικού αντιμετώπισης ιών. Για πληροφορίες σχετικά με το πώς μπορείτε να το κάνετε, επισκεφτείτε την ενότητα Προστατέψτε τον υπολογιστή σας. Η προστασία το υπολογιστή είναι ιδιαίτερα σημαντική αν συνδέεστε στο Internet με καλώδιο μόντεμ ή με μόντεμ DSL. Για περισσότερες πληροφορίες σχετικά με την προστασία από ιούς, δείτε την ενότητα Βέλτιστες πρακτικές για προστασία από ιούς και Βέλτιστες πρακτικές για την αποτροπή ανεπιθύμητης αλληλογραφίας.

Παρακολουθείτε τις συναλλαγές Εξετάστε τις επιβεβαιώσεις των παραγγελιών σας, τις δηλώσεις της πιστωτικής κάρτας και του τραπεζικού σας λογαριασμού μόλις τις λάβετε για να βεβαιωθείτε ότι έχετε χρεωθεί μόνο για τις συναλλαγές που πραγματοποιήσατε. Πρέπει να κάνετε αναφορά χωρίς καθυστέρηση αν προκύψουν προβλήματα με το λογαριασμό σας. Καλέστε τον αριθμό που αναγράφεται στη δήλωση του τραπεζικού λογαριασμού. Χρησιμοποιείτε μόνο μία πιστωτική κάρτα για τις ηλεκτρονικές αγορές σας ώστε να παρακολουθείτε πιο εύκολα τις συναλλαγές.

Χρήση πιστωτικών καρτών για συναλλαγές στο Internet Στις περισσότερες χώρες, η προσωπική σας ευθύνη σε ΠΕΡΙΠΤΩΣΗ που κάποιος χρησιμοποιήσει την πιστωτική σας κάρτα χωρίς άδεια περιορίζεται σημαντικά. Σε αντίθεση, αν χρησιμοποιείτε απευθείας χρέωση από τον τραπεζικό λογαριασμό ή την κάρτα σας, η προσωπική σας ευθύνη είναι συχνά το υπόλοιπο στον τραπεζικό λογαριασμό σας. Επιπλέον, μια πιστωτική κάρτα με μικρότερο πιστωτικό όριο προτιμάται για χρήση στο Internet επειδή περιορίζει το χρηματικό ποσό που μπορεί να κλέψει κάποιος σε ΠΕΡΙΠΤΩΣΗ που υπάρξει παραβίαση της κάρτας. Ακόμα καλύτερα, πολλές εταιρείες έκδοσης πιστωτικών καρτών προσφέρουν στους πελάτες τους την επιλογή ηλεκτρονικών αγορών με εικονικούς αριθμούς πιστωτικών καρτών μίας χρήσεως που λήγουν μετά από έναν ή δύο μήνες. Για περισσότερες λεπτομέρειες, ρωτήστε την εταιρεία σας για πληροφορίες σχετικά με τους αναλώσιμους αριθμούς πιστωτικών καρτών.

ΣΩΣΤΗ ΣΤΑΣΗ ΤΟΥ ΣΩΜΑΤΟΣ

Ποια είναι η σωστή στάση του σώματος όταν είμαστε μπροστά σε έναν υπολογιστή;

ΕΘΙΣΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Πώς αντιμετωπίζεται το πρόβλημα του εθισμού στο διαδίκτυο;

• Να βάλεις τα απαραίτητα ΟΡΙΑ και να απολαμβάνεις τα θετικά της τεχνολογίας χωρίς αρνητικές συνέπειες

• Να αναζητήσεις βοήθεια εάν χρειαστείς

• Να ενημερώσεις τους φίλους σου εάν ΔΕΝ βάζουν όρια ή χρειάζονται βοήθεια

• Να μην παραμελείς τις δραστηριότητές σου, τον ύπνο σου, τους φίλους σου και την οικογένειά σου λόγω διαδικτυακών δραστηριοτήτων (π.χ. παιχνίδια, facebook)Έχε υπόψη σου ότι:

• Εάν το πρόβλημα αναγνωριστεί σε αρχικό στάδιο, είναι πολύ πιο εύκολο να αντιμετωπισθεί

• Όταν παίζεις ηλεκτρονικά παιχνίδια μετά την επιστροφή σου από το σχολείο η απόδοσή σου στις άλλες δραστηριότητες (διάβασμα, αθλητισμός κλπ) μπορεί **να επηρεαστεί**

ΓΟΝΕΙΣ – ΠΑΙΔΙΑ- ΔΙΑΔΙΚΤΥΟ

Ποια είναι η σωστή στάση των γονέων απέναντι στα παιδιά τους ώστε να είναι ασφαλείς στο διαδίκτυο;

Εξοικειωθείτε με το περιβάλλον των παιδιών σας και γνωρίστε τους φίλους τους, τους γονείς των φίλων τους, τους δασκάλους και τους συμμαθητές τους.

• Συχνά τα παιδιά αποφεύγουν να αναφέρουν τα δυσάρεστα που συναντούν στο Διαδίκτυο ή μέσω του κινητού τους. Γι' αυτό είναι βασικό να τους εξηγήσετε ότι, αν τους συμβεί κάτι δυσάρεστο, δε φταίνε αυτά και θα πρέπει να το αναφέρουν άμεσα σε εσάς.

• Μάθετε στα παιδιά σας να μην απαντούν ποτέ σε πρόστυχα ή προσβλητικά μηνύματα. Εάν λάβουν τέτοια μηνύματα ή μηνύματα που δεν κατανοούν, αν δουν απρεπείς εικόνες στο Διαδίκτυο, αν λάβουν τέτοιες εικόνες στο κινητό τους τηλέφωνο, ή αν παρενοχληθούν, πρέπει πάντοτε να σας το λένε.

Συνοπτικός οδηγός για μπαμπάδες και μαμάδες, για παππούδες και γιαγιάδες

• Εάν τα παιδιά σας παρενοχλούνται, ερευνήστε εάν ο δράστης βρίσκεται στο κοντινό σας περιβάλλον. Συχνά ο θύτης είναι συμμαθητής ή φίλος, που για κάποιο λόγο θέλει να παρενοχλήσει γελοιοποιήσει / εκφοβίσει το παιδί σας ή που απλά το κάνει «για πλάκα» μην έχοντας συναίσθηση των πιθανών συνεπειών. Σε μια τέτοια ΠΕΡΙΠΤΩΣΗ μιλήστε άμεσα με τους γονείς του θύτη καθώς και με τη διεύθυνση του σχολείου.

• Για τέτοια προβλήματα μπορείτε να επικοινωνείτε με τη Γραμμή Βοηθείας ΥποΣΤΗΡΙΖΩ του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου, στο τηλέφωνο χωρίς χρέωση 800 11 800 15, ή στην ηλεκτρονική διεύθυνση help@saferinternet.gr. Η Γραμμή υλοποιείται από τη Μονάδα Εφηβικής Υγείας της Β' Παιδιατρικής Κλινικής του Πανεπιστημίου Αθηνών και είναι ανοιχτή Δευτέρα - Παρασκευή, ώρες 9:00 – 15:00.

• Προωθείστε μέσα στην οικογένεια ένα περιβάλλον που δεν ανέχεται την παρενόχληση. Διδάξτε στα παιδιά σας ότι ανωνυμία στο Διαδίκτυο δε σημαίνει ανεύθυνη συμπεριφορά. Όλοι μας αφήνουμε ηλεκτρονικά ίχνη στο Διαδίκτυο, συνεπώς πρέπει να συμπεριφερόμαστε ευγενικά, με κανόνες και με ηθική, όπως και στον πραγματικό κόσμο. Θυμηθείτε ότι ακόμη και τα ίδια σας τα παιδιά δεν είναι πάντα αγγελούδια!

• Τα παιδιά πρέπει να γνωρίζουν τα δικαιώματα και τις υποχρεώσεις τους και πώς να σέβονται τα δικαιώματα των άλλων. Διατηρείτε συνεχώς ανοικτό διάλογο μαζί με τα παιδιά σας, ώστε να σας εμπιστεύονται τις όποιες ανησυχίες τους. Οι διαδραστικές τεχνολογίες, όπως το Διαδίκτυο και η κινητή τηλεφωνία, μπορούν να σας προσφέρουν εξαιρετικές ευκαιρίες για συζήτηση και προβληματισμό!

• Αφιερώστε χρόνο και διάθεση, ώστε να ασχολείστε με το διαδίκτυο MAZI με τα παιδιά σας

• Το διαδίκτυο προσφέρει σε εσάς τους γονείς την ευκαιρία να διδάξετε στο παιδί την προσωπική ευθύνη και να προσφέρετε εμπειρία ζωής όπως και στο φυσικό κόσμο

• Ενθαρρύνετέ τα παιδιά να αναπτύξουν το κριτικό πνεύμα και να αξιολογούν το περιεχόμενο της κάθε πληροφορίας

• Η ενημέρωση των παιδιών για το φαινόμενο διαδικτυακού εκφοβισμού είναι σημαντική

• Συζητήστε και συμφωνήστε με τους εφήβους τα χρονικά ΟΡΙΑ καθημερινής ενασχόλησης με το διαδίκτυο (προσπαθήστε να μην ξεπερνάτε τις 10 ώρες / εβδομάδα)

σημαντική

• Χρήση φίλτρων για επιβλαβείς ιστοσελίδες και συμμετοχή στις επιλογές του εφήβου (χωρίς υπερβολές ή/και παράλογες απαγορεύσεις), συμβάλλουν σε ένα θετικό αποτέλεσμα

• Εάν παρατηρήσετε υπερβολική χρήση ή και συμπεριφορές εθισμού (σελ 4 και 5), αναζητήστε ΑΜΕΣΩΣ βοήθεια.

Ποια πρέπει να είναι η αντιμετώπιση των παιδιών από τους γονείς τους σε ΠΕΡΙΠΤΩΣΗ που καθηλώνονται στα ηλεκτρονικά διαδικτυακά παιχνίδια

Καταρχήν, ο γονέας δεν πρέπει να πανικοβληθεί. Θεωρητικά θα πρέπει να έχει δει τα σημάδια στη συμπεριφορά του παιδιού και να επιληφθεί της κατάστασης πριν φτάσει σε επίπεδα δύσκολο να αντιμετωπισθούν. Η αντιμετώπιση έχει τρεις βασικούς άξονες: επικοινωνία με τον έφηβο/παιδί, επικοινωνία μεταξύ των ατόμων που φροντίζουν τον έφηβο/ παιδί και συνεργασία με ειδικό ψυχικής υγείας, ο οποίος να γνωρίζει τη συγκεκριμένη κατηγορία συμπεριφορών. Η επικοινωνία με το παιδί είναι ο ακρογωνιαίος λίθος της εμπιστοσύνης που πρέπει να υπάρχει, η οποία θα φέρει τους γονείς συμμάχους στην προσπάθεια για απεγκλωβισμό από τον διαδικτυακό κόσμο. Οι γονείς θα πρέπει να έχουν τακτική επαφή με τους καθηγητές και αλλά σημαντικά πρόσωπα φροντίδας, προκειμένου να τηρείται μια κοινή γραμμή σε κάποια βασικά θέματα συμπεριφοράς και τη θέσπιση ορίων και κανόνων, καθώς επίσης και για να παρατηρείται η συμπεριφορά του παιδιού/ εφήβου σε διαφορετικά πλαίσια. Τέλος, ο εξειδικευμένος ειδικός ψυχικής υγείας, θα αξιολογήσει την κατάσταση και θα εφαρμόσει συγκεκριμένες τεχνικές προκειμένου να καταφέρει το ίδιο το άτομο να επαναπροσδιορίσει την εμπλοκή του με τα διαδικτυακά παιχνίδια και να ελαττώσει, σταδιακά, τις ώρες παιχνιδιού. Για να γίνει αυτό, θα πρέπει να έχει σύμμαχους, τόσο το συγγενικό περιβάλλον, όσο και τους δασκάλους/ καθηγητές

Συμπληρωματικές Οδηγίες προς τους μαθητές για την Ασφαλή Χρήση του Διαδικτύου

Συμβουλές ασφαλούς χρήσης του Διαδικτύου

Παρακάτω παρουσιάζονται χρήσιμες πρακτικές για την ασφαλή πλοήγηση στο Διαδίκτυο:

1. Μη δίνετε ποτέ προσωπικά σας στοιχεία καθώς και ψηφιακό υλικό (π.χ., φωτογραφίες) σε άλλους χρήστες του Διαδικτύου. Επιπλέον, μη παρέχετε πληροφορίες που αφορούν τους φίλους σας, την οικογένεια σας καθώς και το σχολείο σας.
2. Μη γνωστοποιείτε μέσω του Διαδικτύου τα στοιχεία επικοινωνίας σας σε αγνώστους.
3. Μην αποκαλύπτετε τους κωδικούς πρόσβασης (password) που χρησιμοποιείτε σε κρίσιμες διαδικτυακές υπηρεσίες (π.χ., Webmail, τραπεζικοί λογαριασμοί, ιστότοποι δημόσιων υπηρεσιών, κλπ).
4. Μην επιχειρείτε συναλλαγές (π.χ., χρήση πιστωτικής κάρτας) μέσω του Διαδικτύου από άγνωστους ή τυχαίους ιστοτόπους για την αγορά προϊόντων. Αντίθετα, αναζητήστε διαδεδομένους ιστοτόπους που παρέχουν τους κατάλληλους μηχανισμούς για ασφαλείς διαδικτυακές αγορές, τμήμα εξυπηρέτησης πελατών, προβλεπόμενη διαδικασία επιστροφής προϊόντος κλπ. Για την πρώτη σας διαδικτυακή συναλλαγή είναι ιδιαιτέρως χρήσιμη η φυσική παρουσία και καθοδήγηση κάποιου χρήστη με μεγαλύτερη εμπειρία.
5. Κατά την επίσκεψή σας σε τυχαίους δικτυακούς τόπους μη συμπληρώνετε φόρμες με τα προσωπικά σας στοιχεία.
6. Τα άτομα που γνωρίζετε στο Διαδίκτυο δεν είναι πάντοτε αυτά που ισχυρίζονται ότι είναι, ενδεχομένως να λένε ψέματα για να κερδίσουν την εμπιστοσύνη σας και να αποσπάσουν χρήσιμες πληροφορίες.
7. Μη συναντάτε μόνοι σας άτομα που γνωρίσατε από το Διαδίκτυο.
8. Να συζητάτε με τους δασκάλους σας, τους γονείς σας καθώς και με πρόσωπα που εμπιστεύεστε για τις δραστηριότητες σας στο Διαδίκτυο, ιδιαίτερα αν αντιμετωπίσετε οποιαδήποτε περίεργη ή ασυνήθιστη κατάσταση.
9. Να έχετε πάντα υπόψη σας ότι τα προϊόντα της πνευματικής δημιουργίας/ιδιοκτησίας (μουσική, λογοτεχνία, κινηματογράφος, λογισμικό κλπ) προστατεύονται από τη σχετική νομοθεσία και η διανομή τους μέσω του Διαδικτύου είναι παράνομη πράξη. Έργα (π.χ., λογοτεχνία, μουσική) και προϊόντα (π.χ., λογισμικό) που υπόκεινται σε καθεστώς πνευματικής ιδιοκτησίας (copyright), προστατεύονται από τη σχετική νομοθεσία και η διανομή τους μέσω Διαδικτύου θεωρείται παράνομη πράξη.
10. Όπως επισημαίνεται παραπάνω, παράνομη πράξη θεωρείται και η διακίνηση εφαρμογών λογισμικού (software) εκτός και αν ανήκουν στην κατηγορία του Ελεύθερου Λογισμικού (open source software). Σε κάθε ΠΕΡΙΠΤΩΣΗ θα πρέπει να έχετε κατανοήσει τους όρους χρήσης και τις προϋποθέσεις για την τροποποίηση και την ελεύθερη διακίνησή τους. Σχετικές πληροφορίες μπορείτε να αντλήσετε στην ακόλουθη ηλεκτρονική διεύθυνση http://opensource.org/.
11. Μη χρησιμοποιείτε άκριτα οποιοδήποτε πρόγραμμα βρίσκεται στο Διαδίκτυο ακόμη και αν αποτελεί κάποιο παιχνίδι, διότι μπορεί να περιέχει κακόβουλο λογισμικό (π.χ., trojan horse) και να επιφέρει σημαντικές δυσλειτουργίες στο υπολογιστικό σύστημα (π.χ., διαγραφή αρχείων, απενεργοποίηση firewall, επανεκκίνηση ή τερματισμός Η/Υ κλπ).
12. Μην ανοίγετε e-mail από άγνωστους αποστολείς με τα ακόλουθα χαρακτηριστικά: (α) χωρίς θέμα (subject), (β) με περίεργο θέμα και (γ) περιέχουν επισυναπτόμενο/α αρχείο/α (π.χ., σε εκτελέσιμη μορφή, αρχείο/α .zip κλπ), διότι είναι πολύ πιθανό να περιέχουν κακόβουλο λογισμικό ή να αποτελούν μέρος στοχευμένης προσπάθειας Phishing (βλ. παραπάνω).

Πέρα από τις παραπάνω συμβουλές επισημαίνονται ακολούθως και βασικές οδηγίες καλής χρήσης του Διαδικτύου σχετικά με τα μηνύματα Ηλεκτρονικού Ταχυδρομείου και τις πληροφορίες που αποστέλλουν οι μαθητές με οποιοδήποτε τρόπο σε χρήστες ή ομάδες χρηστών του Πανελλήνιου Σχολικού Δικτύου καθώς και του Διαδικτύου γενικότερα:

Το περιεχόμενο των πληροφοριών **δεν** πρέπει:

- να προσβάλλει άλλους χρήστες του Διαδικτύου, αλλά να ακολουθεί τους νόμους, τα χρηστά ήθη και τα ήθη χρήσης του Διαδικτύου.
- να προσβάλλει τα ανθρώπινα δικαιώματα και τις διάφορες μειονότητες.
- να σχετίζεται με παράνομες πράξεις (π.χ., τυχερά παιχνίδια, διακίνηση εμπορικού λογισμικού κλπ).
- να έχει υβριστικό χαρακτήρα ή διαφημιστική χροιά (παρά μόνο ενημερωτική).

Μην διακινείτε πληροφορίες και **μην προωθείτε ή προβάλλετε** δικτυακούς τόπους που:

προπαγανδίζουν την βίαιη και επιθετική συμπεριφορά, το μίσος και το ρατσισμό.

προωθούν τα ναρκωτικά, το αλκοόλ και τα τυχερά παιχνίδια.

περιέχουν πορνογραφικό περιεχόμενο.

αναφέρονται σε παραβιάσεις ασφάλειας διαφόρων υπολογιστικών συστημάτων ή και εφαρμογών.

αφορούν στην παράνομη διανομή λογισμικού, ταινιών ή μουσικής.

περιέχουν οπτικοακουστικό υλικό που αποτελεί προϊόν πνευματικής δημιουργίας.

αφορούν σε υλικό με διαφημιστικά banners.

Επιπλέον, θα πρέπει να ελέγχετε το περιεχόμενο των ηλεκτρονικών μηνυμάτων σας για την πιθανή απομάκρυνση ιών ή άλλων κακόβουλων τμημάτων λογισμικού που μπορούν εν δυνάμει να βλάψουν άλλους χρήστες. Για το λόγο αυτό, προτείνεται στο υπολογιστικό σύστημα να υπάρχει εγκατεστημένο **λογισμικό προστασίας** από ιούς (antivirus) και κακόβουλο λογισμικό, το οποίο να είναι **ενεργό** και να ανανεώνεται **αυτόματα** από τον κατασκευαστή του με τις πληροφορίες για νέους ιούς ή απειλές.

Μελέτη Περιπτώσεων

ΠΕΡΙΠΤΩΣΗ 1

Η Ζέτα είναι επίσκεψη σε μια φίλη που εγγράφεται σε μια υπηρεσία τσατ. Η φίλη της συμπληρώνει το προφίλ της με όλα τα προσωπικά της στοιχεία. Η Ζέτα, η οποία έχει μάθει πώς να δημιουργεί ένα ασφαλές προφίλ με την Αθηνά, πιστεύει ότι η φίλη της θα πρέπει να το δημιουργήσει διαφορετικά.

Τι νομίζεις ότι θα συμβουλεύσει η Ζέτα τη φίλη της;

Νομίζω ότι πρέπει να συμβουλεύσει η Ζέτα την Αθηνά το προφίλ της να μην συμπληρώνει με όλα τα προσωπικά της τα στοιχεία. Γιατί μπορούν να πάρουν όλα τα στοιχεία της και μπορούν να δημιουργήσουν ψεύτικο προφίλ. Καλό είναι τα προσωπικά στοιχεί της να τα εμπιστεύεται σε άτομα που γνωρίζει καλά εκτός διαδικτύου.

ΠΕΡΙΠΤΩΣΗ 2

Ο φίλος του Αλέξη, ο Μιχάλης, είχε έναν καυγά με έναν στενό του φίλο και αμέσως μετά οι συμμαθητές του έλαβαν άσχημα μηνύματα από τον Μιχάλη. Ο Μιχάλης είναι συντετριμμένος και ορκίζεται ότι δεν έχει στείλει τα μηνύματα. Ο Αλέξης νομίζει ότι ξέρει τι έχει συμβεί. Μπορείς να μαντέψεις;

Όχι δεν νομίζω ότι έκανε ο Μιχάλης, γιατί με κάποια προγράμματα μπορεί να στέλνει μηνύματα κάποιος χωρίς να φαίνεται ποιος είναι επίσης αν δώσουμε το κωδικό μας μπορεί να χρησιμοποιήσει αντί για εμάς . Γιατί η τεχνολογία προχώρησε πάρα πολύ.

ΠΕΡΙΠΤΩΣΗ 3

Η Ζέτα συνομιλεί εδώ και μερικές εβδομάδες με μέλη από το φαν κλαμπ του αγαπημένου της καλλιτέχνη. Ένας από αυτούς τους φίλους της πρότεινε να συναντηθούν στον «πραγματικό κόσμο». Η Ζέτα δεν ξέρει τι να κάνει. Μπορείς να της δώσεις κάποια καλή συμβουλή;

Αν δεν γνωρίζεις κάποιον στη πραγματικότητα να μην συναντηθείς. Γιατί δεν τον γνωρίζεις και μπορεί να μην σου φερθεί καλά! Αν συμβεί κάτι τέτοιο είναι καλό να ξέρει και οι γονείς της .

ΠΕΡΙΠΤΩΣΗ 4

Ο Αλέξης έλαβε ένα κινητό τηλέφωνο ως δώρο Χριστουγέννων και το χρησιμοποιεί για να επικοινωνεί με την οικογένεια και τους φίλους του. Μια μέρα λαμβάνει από ένα φίλο ένα βιντεάκι που δείχνει ένα αγόρι να ξυλοκοπείται. Νιώθει πολύ άσχημα και δεν ξέρει τι να κάνει. Τι λες; Θα πρέπει να στείλει και αυτός το μήνυμα και σε άλλους;

Να μην στέλνει σε κανέναν μηνύματα που μπορούν να πληγώσουν κάποιον, να φέρεστε σε άλλους όπως θέλετε να σας φερθούν και να πάει στην αστυνομία.

ΠΕΡΙΠΤΩΣΗ 5

Ένας φίλος του Αλέξη είναι πολύ λυπημένος. Κάποιος του στέλνει άσεμνα μηνύματα. Ο Αλέξης πιστεύει ότι αυτή είναι απαράδεκτη συμπεριφορά και θέλει να βοηθήσει τον φίλο του. Τι μπορεί να κάνει;

Να μην απαντήσουν στα μηνύματα και να το πουν στους γονείς τους.

ΠΕΡΙΠΤΩΣΗ 6

Στην τάξη της Ζέτας μαθαίνουν για τη σημασία της σωστής μεταχείρισης των άλλων. Η δασκάλα της αναφέρεται στην παρενόχληση και ζητάει από την τάξη να σκεφτεί κανόνες συμπεριφοράς. Η Ζέτα θέλει να πρωτοτυπήσει και αποφασίζει να γράψει για το «netiquette» ως μέσο πρόληψης από την ηλεκτρονική παρενόχληση. Μπορείς να τη βοηθήσεις με κάποιες ιδέες;

Εάν κάποιος την ενοχλεί στο fb κ.τ.λ. να τον διαγράψει από τους φίλους.

ΠΕΡΙΠΤΩΣΗ 7

Ο Αλέξης παίζει ένα παιχνίδι στο Διαδίκτυο, στο οποίο είναι σε άμεση επαφή με άλλους παίκτες. Είναι πραγματικά διασκεδαστικό. Μερικές φορές κάνει τσατ με τους συμπαίκτες του. Τι συμβουλές μπορείς να του δώσεις για την ασφάλειά του;

Να μην δώσει τα προσωπικά του στοιχεία σε αυτό παιχνίδι που παίζει στο διαδίκτυο

ΔΗΜΟΣΚΟΠΙΚΗ ΕΡΕΥΝΑ - ΠΑΡΟΥΣΙΑΣΗ ΚΑΙ ΑΝΑΛΥΣΗ ΤΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ ΕΡΩΤΗΜΑΤΟΛΟΓΙΩΝ

Ερωτηματολογιο Για Μαθητες

1. Φύλο

□ Κορίτσι □ Αγόρι

2. Έχετε Πρόσβαση στο Διαδίκτυο?

□ Ναι □ Όχι

3. Πόσες Ώρες έχετε Πρόσβαση στο Διαδίκτυο Την Ημέρα?

□ 0-1 □ 1-3 □ 3-5 □ 5+

4. Από που Έχετε Πρόσβαση Στο Διαδίκτυο?

□ Σπίτι

□ Σχολείο

□ Ιντερνετ Καφέ

5. Για ποιο λόγο μπαίνετε στο Διαδίκτυο?

□ Διασκέδαση (Μουσική, Βίντεο)

□ Πληροφορίες Για Σχολικές Εργασίες

□ Ενημέρωση

□ Μέσα Κοινωνικής Δικτυωτής (Facebook, Twitter..)

□ Παιχνίδια

6. Ποιους Θεωρείτε ποιο Σοβαρούς Κινδύνους Του Διαδικτύου?

□ Ιοί Υπολογιστών-Κακόβουλα Προγράμματα

□ Παραβίαση Προσωπικών Δεδομένων

□ Εθισμός Στο Διαδίκτυο

□ Σελίδες Ανάρμοστου Περιεχομένου

□ Παρενόχληση (Cyber Bulling, Λεκτικη, Σεξουαλικη)

7. Από πού έχετε ενημερωθεί για τους κινδύνους?

□ Σχολείο

□ Φίλους

□ Συγγενείς

□ Μόνος μου

8. Έχετε «κολλήσει» Ποτέ Ιό στον Υπολογιστή σας?

□ Ναι □ Όχι

9. Πως Θα Αντιμετωπίζατε Μια Ενδεχόμενη Μόλυνση Του Υπολογιστή σας Από Ιό?

□ Βοήθεια Από Τεχνικό

□ Μόνος Μου (Anti-Virus)

□ Βοήθεια από φίλο

□ Θα έψαχνα λύση στο ίντερνετ

10. Έχετε Προφίλ Σε Site Κοινωνικής Δικτυωτής ?

□ Ναι □ Όχι

11. Αν Ναι Σε Ποια Site?

□ Facebook □ Twitter □ My Space □ Instagram

12. Γιατί Χρησιμοποιείτε Site Κοινωνικής Δικτυωτής ?

□ Επικοινωνία Με Φίλους

□ Γνωριμία Νέων Φιλών □

□ Παιχνίδια

□ Άλλο……..

13. Έχετε Δεχθεί Κάποια Παρενόχληση (Υβριστική, Σεξουαλικη, …..)

□ Ναι □ Όχι

14. Πως θα το Αντιμετώπιζες?

□ Θα μιλούσα στους γονείς μου-συγγενή

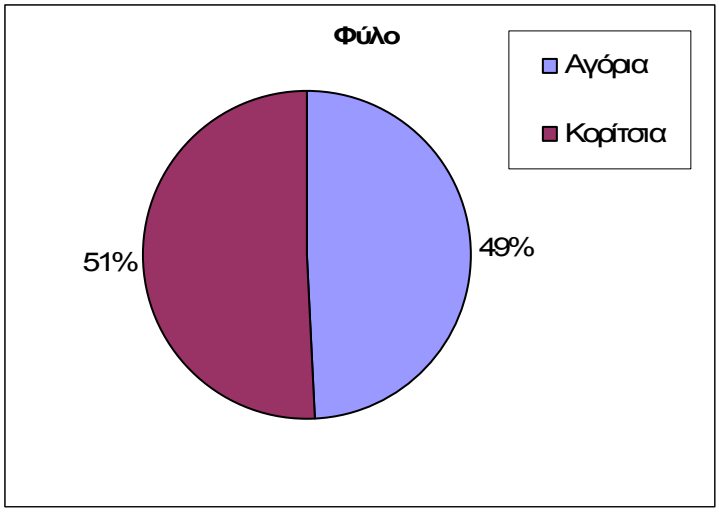
□ Θα μιλούσα σε κάποιον φίλο μου

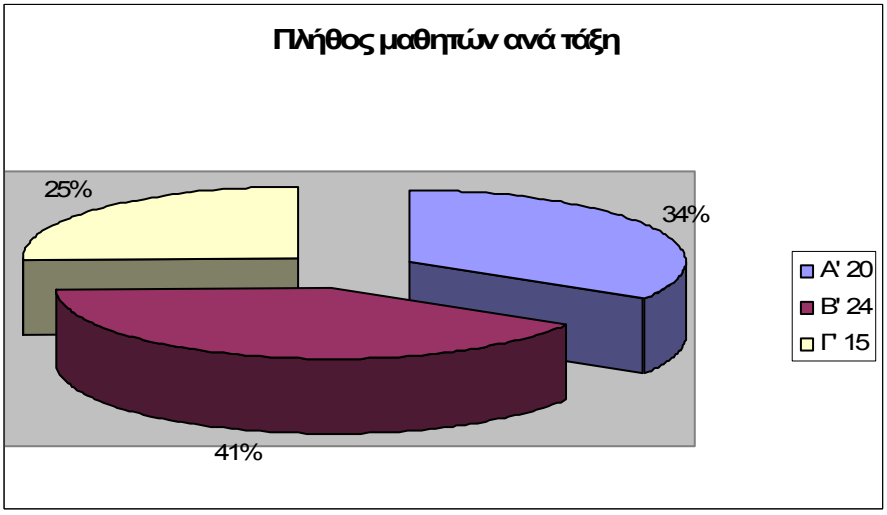
□ Θα επικοινωνούσα με τον admin του site

□ Δεν θα έκανα τίποτα

ΣΧΟΛΙΑΣΜΟΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

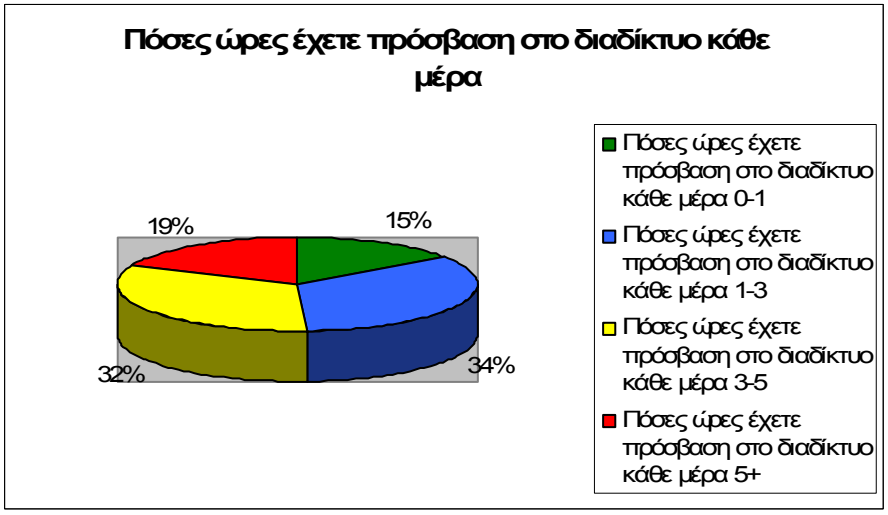
Από την έρευνα που κάναμε για την ασφάλεια στο διαδίκτυο στο σχολείο μας το 51% ήταν κορίτσια και το 49% αγόρια.



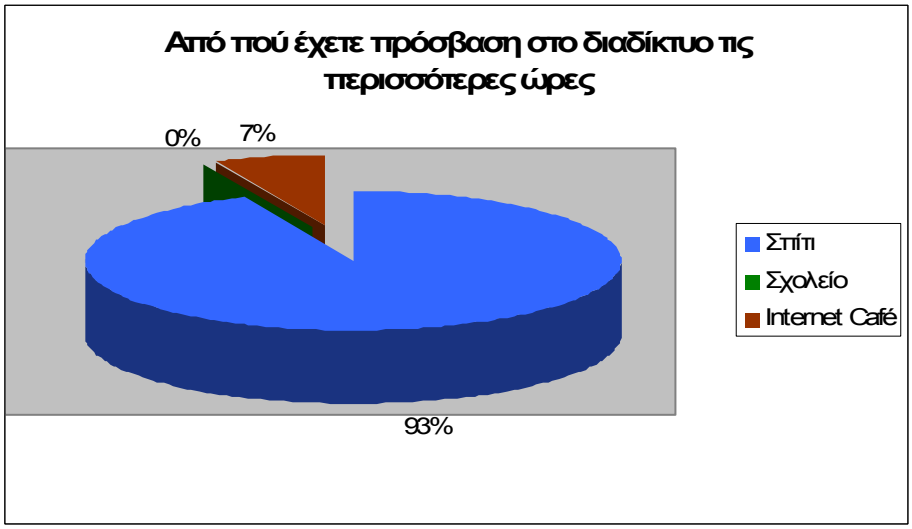


Από αυτά το 34% ήταν στην Ά τάξη, το 41% ήταν στην ‘Β και το 25% ήταν της ‘Γ.

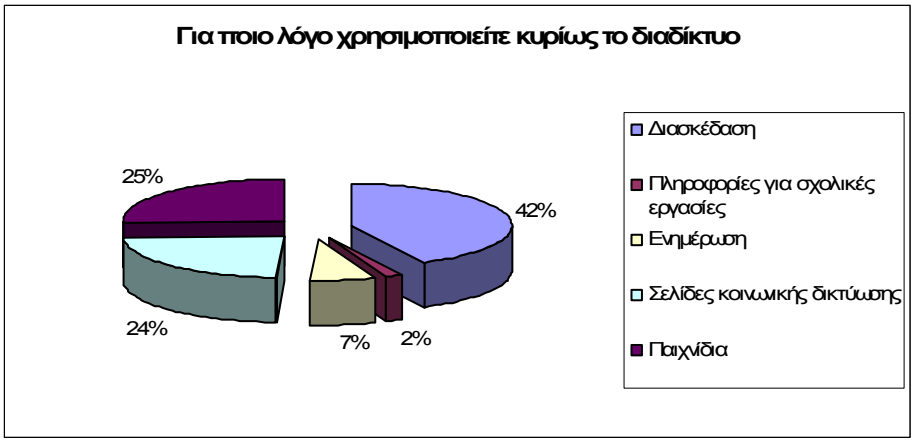
Το 100% των μαθητών που ερωτήθηκαν έχουν πρόσβαση στο διαδίκτυο.



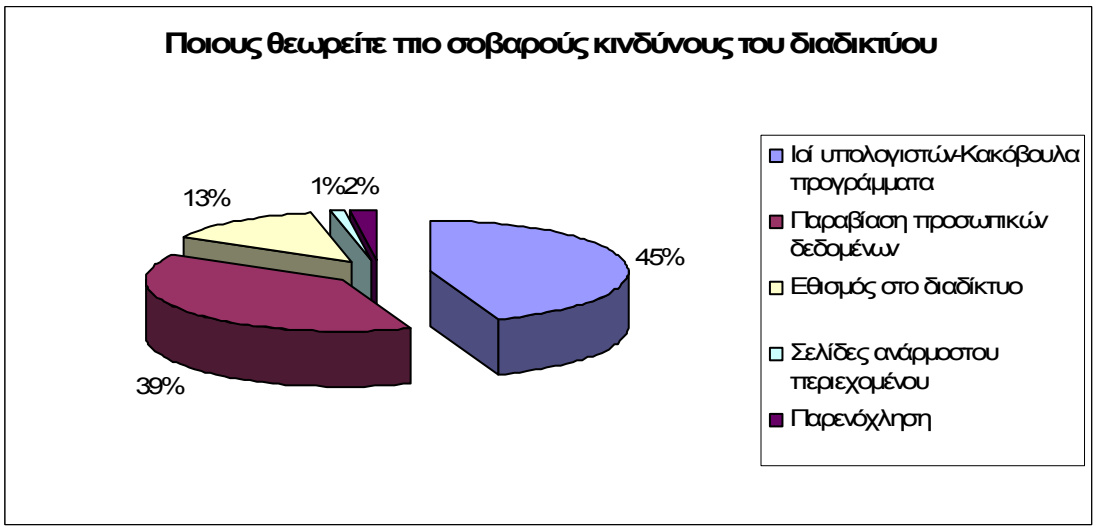
Το 66% χρησιμοποιούν το διαδίκτυο 1 με 5 ώρες και το 15% χρησιμοποιεί το ίντερνετ 0 με 1 ώρα κάθε μέρα, ενώ το υπόλοιπο 19% χρησιμοποιεί καθημερινά το διαδίκτυο πάνω από 5 ώρες.



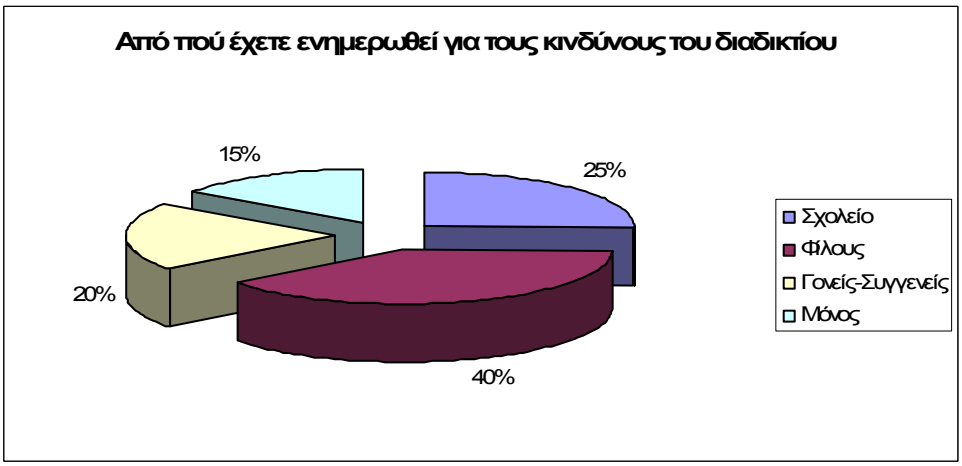
Η συντριπτική πλειοψηφία 93% τις περισσότερες ώρες έχουν πρόσβαση στο διαδίκτυο από το σπίτι. Μόνο 7% χρησιμοποιούν το ίντερνετ τις περισσότερες ώρες από internet café. Κανένας δεν έχει πρόσβαση τις περισσότερες ώρες από το σχολείο.



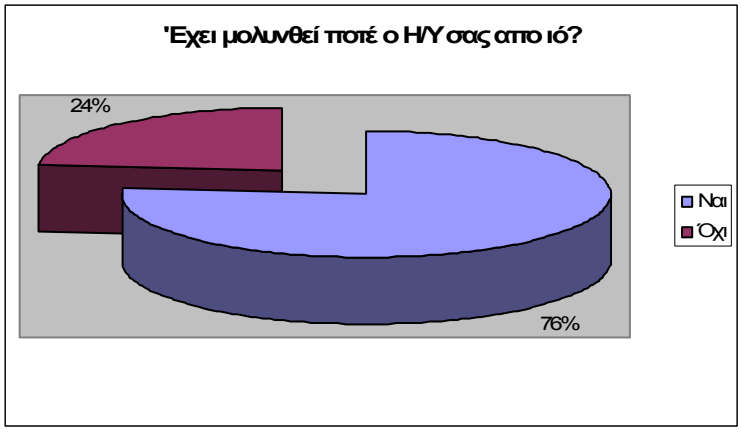
Το 42% χρησιμοποιούν το διαδίκτυο για διασκέδαση. Για παιχνίδια και σελίδες κοινωνικής δικτύωσης το χρησιμοποιούν το 49%. Μόνο το 2% μπαίνει στο διαδίκτυο για σχολικές εργασίες και το 7% για ενημέρωση. Γενικά μπορούμε να συμπεράνουμε ότι οι νέοι χρησιμοποιούν το ίντερνετ για διασκέδαση και ψυχαγωγία αντί για ενημέρωση κλπ.



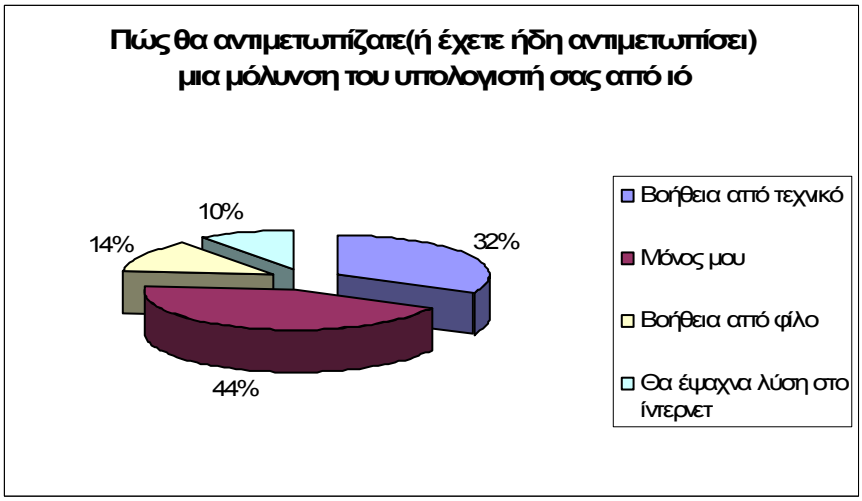
Σύμφωνα με τους μαθητές οι μεγαλύτεροι κίνδυνοι είναι οι ιοί υπολογιστών-κακόβουλα προγράμματα(45%), οι παραβιάσεις προσωπικών δεδομένων(39%), ο εθισμός στο διαδίκτυο(13%), οι σελίδες ανάρμοστου περιεχομένου(1%) και η παρενόχληση που μπορεί να υποστούμε(2%).



Στην ερώτηση «Από πού έχετε ενημερωθεί για τους κινδύνους του διαδικτύου» η πλειοψηφία απάντησε από φίλους(40%),το 25% απάντησε από το σχολείο, το 20% απάντησε από γονείς και συγγενείς και το υπόλοιπο 15% απάντησε μόνο του. Συμπεραίνουμε λοιπόν ότι η πλειοψηφία έχει εμπειρία μόλυνσης του Η/Υ από ιό.

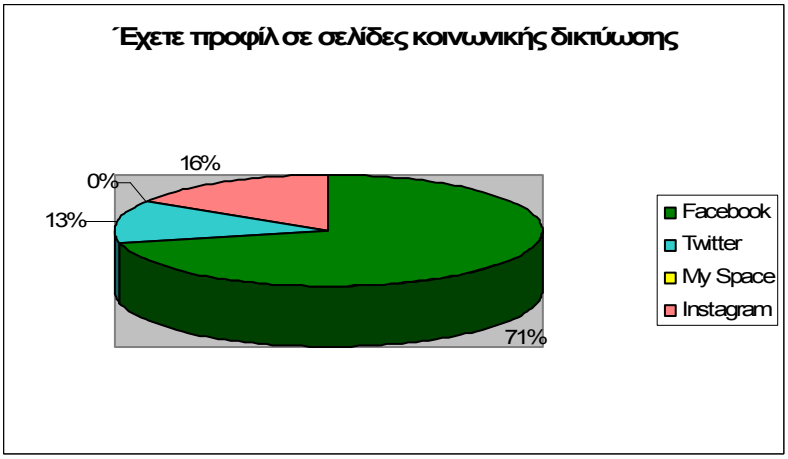


Στην ερώτηση «Έχετε μολυνθεί ποτέ ο υπολογιστής σας από ιό» το 76% απάντησε ΝΑΙ και το άλλο 24% απάντησε ΟΧΙ.

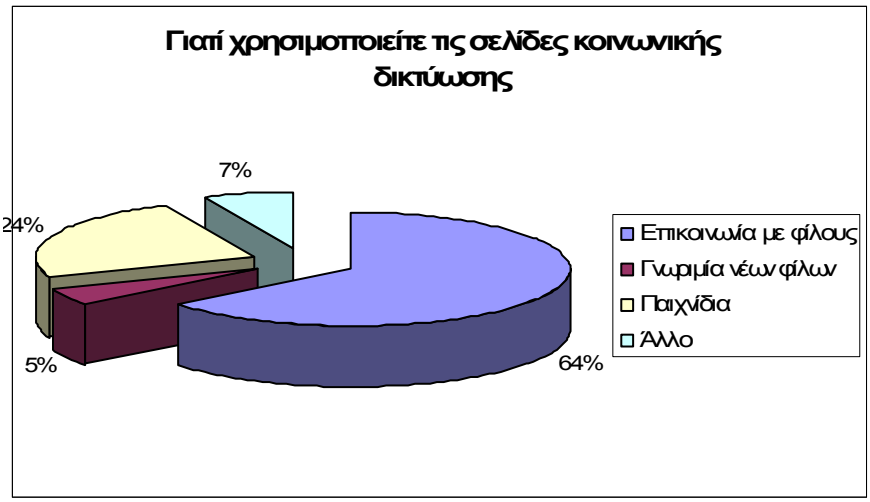


Το 44% θα αντιμετώπιζε ένα πρόβλημα του υπολογιστή μόνος του, ενώ το 32% θα ζητούσε βοήθεια από τεχνικό, το 14% από φίλο και το 10% θα έψαχνε για βοήθεια στο ίντερνετ.

Από το σύνολο των μαθητών το 95% έχει προφίλ σε σελίδες κοινωνικής δικτύωσης ενώ το υπόλοιπο 5%δεν έχει.

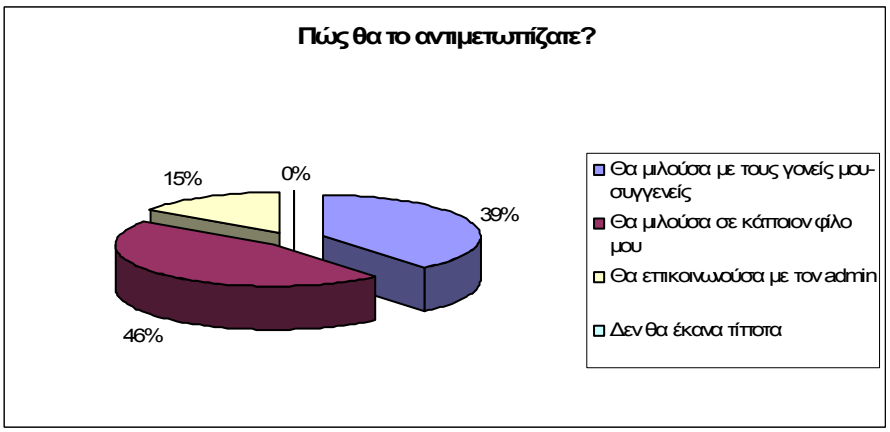


Το 71% αυτών έχουν προφίλ στο Facebook, το 16% στο Instagram, το 13% στο Twitter, ενώ κανένας από τους μαθητές δεν έχει προφίλ στο My Space. Άρα η πλειοψηφία έχει προφίλ σε σελίδες κοινωνικής δικτύωσης. Άρα το πιο διαδεδομένο μέσο κοινωνικής δικτύωσης είναι το Facebook.



Επίσης το 64% χρησιμοποιεί το Ίντερνετ για να επικοινωνεί με τους φίλους του, το 24% για παιχνίδια, το 5% για γνωριμία φίλων και το 7% για κάτι άλλο.

΄Υστερα το 63% των ατόμων που απάντησαν στο ερωτηματολόγιο έχουν δεχθεί προσέγγιση από άτομα που δεν ήξεραν, ενώ το υπόλοιπο 37% δεν έχει δεχθεί.



Από το σύνολο των μαθητών που δέχθηκαν προσέγγιση από αγνώστους στο διαδίκτυο, η πλειοψηφία(46%) θα μιλούσε σε ένα φίλο για αυτό, το 39% θα το συζητούσε με τους γονείς του για την εύρεση λύσης στο πρόβλημα, το 15% θα μιλούσε με τον διαχειριστή της ιστοσελίδας για την διόρθωση του προβλήματος, ενώ κανένας από τους μαθητές δεν θα αντιμετώπιζε το πρόβλημα με το να μην κάνει τίποτα. Συμπεραίνουμε λοιπόν ότι οι περισσότεροι από τους μαθητές θα εμπιστεύονταν τους φίλους τους ή τους γονείς τους για ένα πρόβλημα τέτοιας φύσης.

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ ΓΙΑ ΓΟΝΕΙΣ ΜΑΘΗΤΏΝ & ΚΑΘΗΓΗΤΕΣ

Παρακαλούμε σημειώστε Χ στα αριστερά για την επιλογή σας.

1. Φύλο
   - □ Άντρας
   - □ Γυναίκα
2. Ηλικία
   - □ 30-40
   - □ 40-50
   - □ πάνω από 50
3. Έχετε πρόσβαση στο διαδίκτυο;
   - □ Ναι
   - □ Όχι

Πόσες ώρες την ημέρα;

- □ καθόλου
- □ λιγότερο από 1 ώρα ημερησίως
- □ 1-2 ώρες ημερησίως
- □ 2-4 ώρες ημερησίως
- □ πάνω από 4 ώρες ημερησίως

4. Πως χαρακτηρίζετε τις γνώσεις σας για τον Η/Υ και το διαδίκτυο;
   - □ Καθόλου καλές
   - □ Ελάχιστες
   - □ Μέτριες
   - □ Πολύ καλές
5. Πόσες ώρες χρησιμοποιεί το παιδί σας το διαδίκτυο την ημέρα (είτε στο σπίτι είτε εκτός σπιτιού);
   - □ 1-2
   - □ 2-4
   - □ Πάνω από 4
   - □ Δε γνωρίζω
6. Γνωρίζετε τι είδους ιστοσελίδες επισκέπτεται το παιδί σας;
   - □ Ναι
   - □ Όχι
   - □ Δεν ασχολούμαι
7. Θα επιτρέπατε στα παιδιά σας να χρησιμοποιούν site κοινωνικής δικτύωσης (π.χ. facebook ,twitter)
   - □ Ναι
   - □ Όχι
8. Θεωρείτε πως υπάρχουν κίνδυνοι στο διαδίκτυο;

□ Ναι

□ Όχι

9. Ποια από τα παρακάτω αναγνωρίζετε ως κινδύνους του διαδικτύου; (μπορείτε να επιλέξτε πάνω από ένα)

□ Ιοί-Κακόβουλο λογισμικό

□ Ηλεκτρονικός τζόγος

□ Κλοπή προσωπικών δεδομένων

□ Παρενόχληση (λεκτική/σεξουαλική, παιδοφιλία -παιδεραστία)

□ Εθισμός

□ Spam email (ενοχλητικά μηνύματα)

10. Έχετε υποψιαστεί αν το παιδί σας έχει πέσει ποτέ θύμα σε κάποιον από τους παραπάνω κινδύνους

□ Ναι

□ Όχι

11. Έχετε αναγκαστεί να πάρετε ακραία μέτρα ώστε να προστατεύσετε το παιδί σας όταν χρησιμοποιεί το διαδίκτυο;

□ Ναι

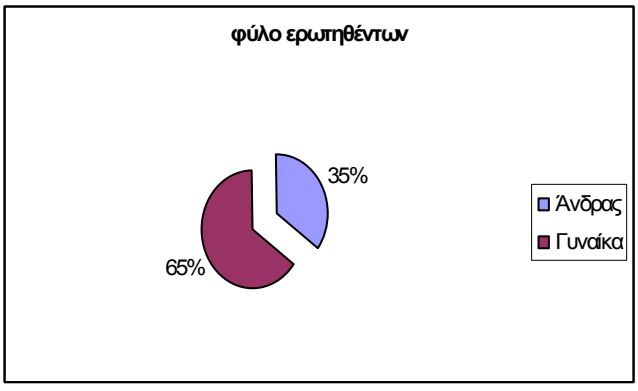
□ Όχι

12. Θα επιτρέπατε στα παιδιά σας να χρησιμοποιούν site κοινωνικής δικτύωσης (π.χ. facebook ,twitter)

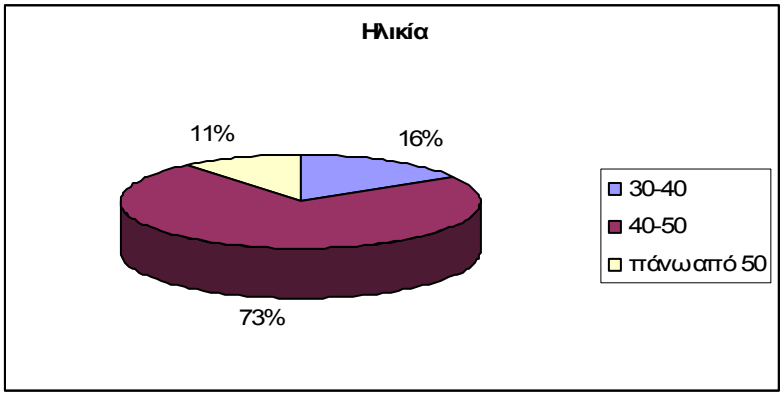
□ Ναι

□ Όχι

ΣΧΟΛΙΑΣΜΟΣ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟΥ

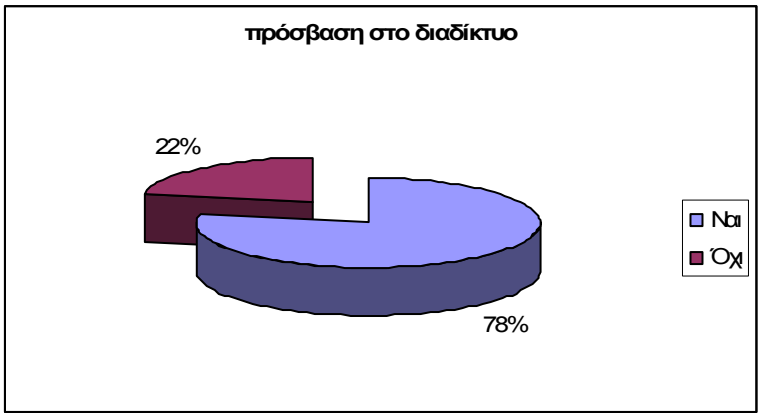


Από το σύνολο των γονέων το 65% είναι γυναίκες και το 35% είναι άνδρες.

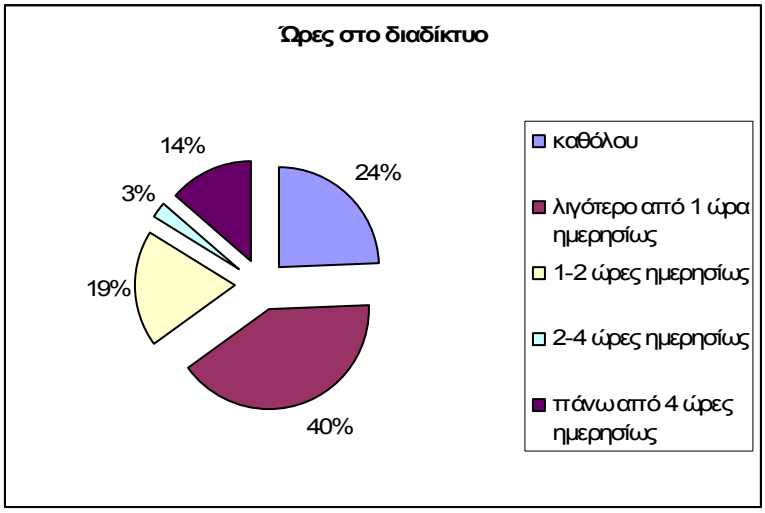


Οι περισσότεροι γονείς βρίσκονται στην ηλικία 40-50 και αυτό είναι φυσιολογικό καθώς

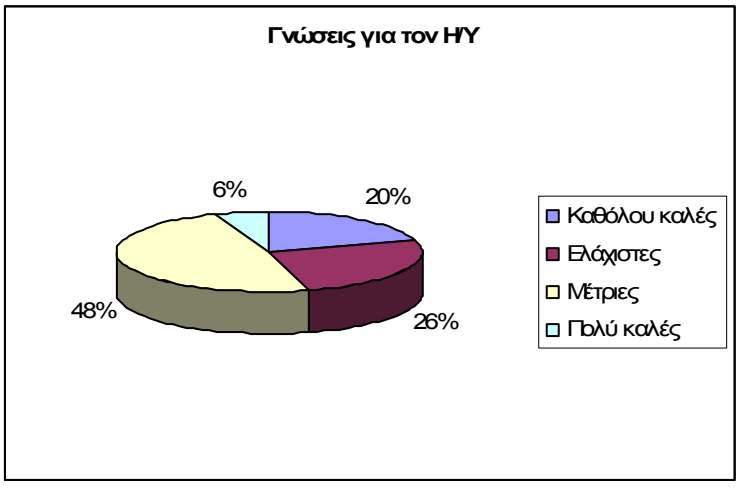
είναι γονείς παιδιών Λυκείου. Το ποσοστό των γονέων που βρίσκονται στην ηλικία των 30-40 και πάνω από 50 είναι λιγότερο.



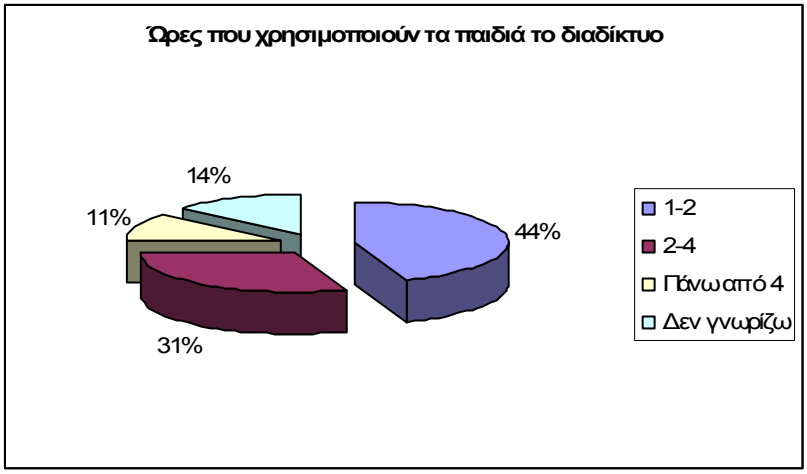
Στη μεγάλη τους πλειοψηφία οι γονείς χρησιμοποιούν το διαδίκτυο. Το 78% ναι και το 22% όχι.



Οι περισσότεροι γονείς χρησιμοποιούν το διαδίκτυο λιγότερο από 1 ώρα ημερησίως ενώ μόλις το 3% χρησιμοποιεί μόλις 2-4 ώρες ημερησίως.



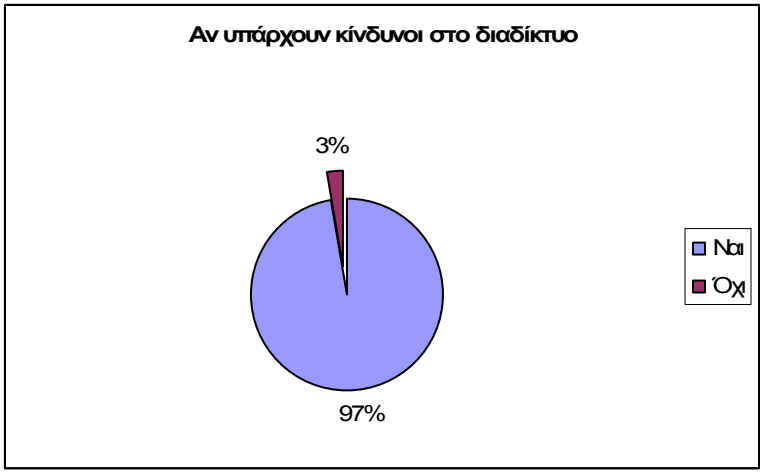
Στις μέρες μας οι πιο πολλοί γονείς έχουν μέτριες γνώσεις σχετικά με το διαδίκτυο. Δυστυχώς μόνο το 6% έχει πολύ καλές γνώσεις .Το 20% δεν θεωρείτε υψηλό ποσοστό, όμως δεν παύει να υπάρχει.



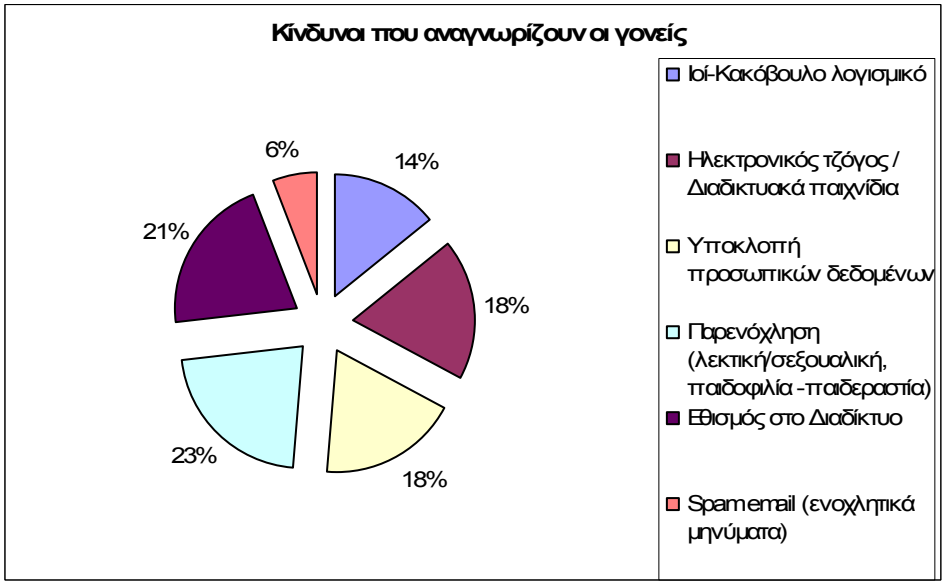
Οι γονείς γνωρίζουν πως τα παιδιά τους χρησιμοποιούν το διαδίκτυο 2-4 ωρες την ημερα ενώ το 11% δηλώνει πως τα παιδιά τους απασχολούνται με το διαδίκτυο πάνω από 4 ώρες.Το 14% βρίσκεται στην άγνοια.

Το 56% γνωρίζει τι είδους ιστοσελίδες επισκέπτονται τα παιδιά τους. Μόλις το 3% δεν γνωρίζει ενώ το 41% δεν γνωρίζει.

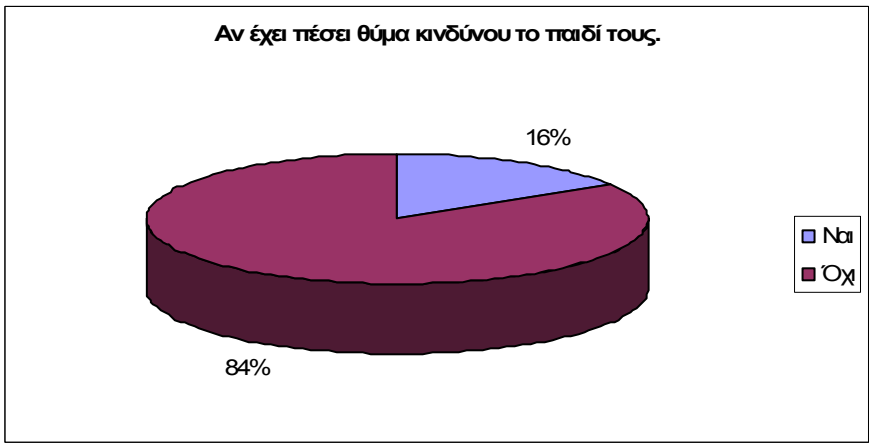
Οι περισσότεροι γονείς , το 84% επιτρέπουν στα παιδιά τους να χρησιμοποιούν site κοινωνικής δικτύωσης (π.χ. facebook ,twitter κλπ) .



Ευτυχώς το 97% ,ποσό αρκετά ικανοποιητικό γνωρίζει πως υπάρχουν κίνδυνοι στο διαδίκτυο .Το 3% δεν γνωρίζει , ποσοστό που δεν υπερβαίνει ούτε το 50%.



Οι περισσότεροι γονείς έχουν επίγνωση ότι οι περισσότεροι κίνδυνοι έχουν να κάνουν με παρενόχληση λεκτική ή σεξουαλική όπως παιδοφιλία-παιδεραστία. Αμέσως μετά ακολουθεί ο εθισμός στο Διαδίκτυο και τέλος το spam ermail.

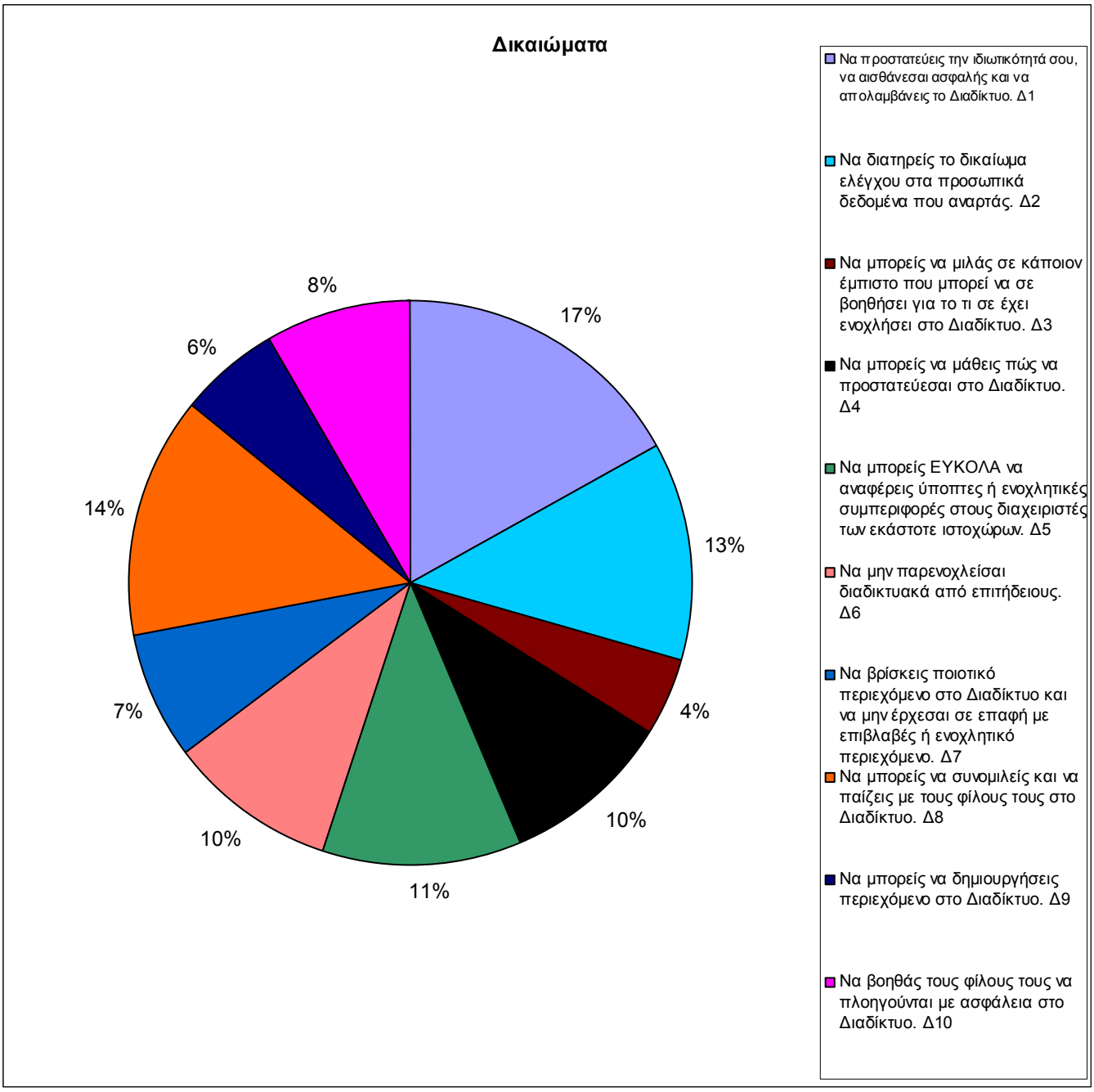


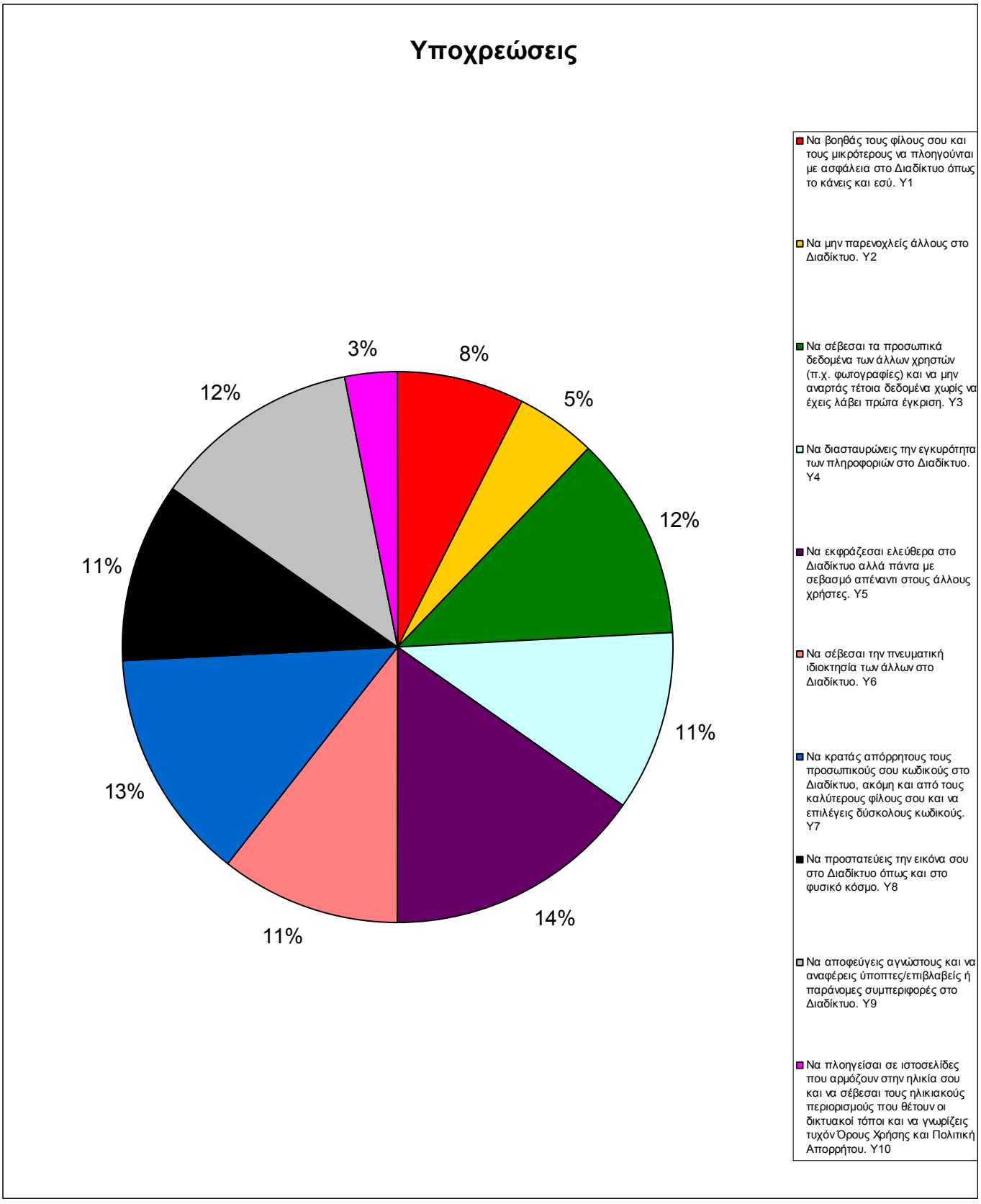
Τα περισσότερα παιδιά δεν έχουν πέσει θύμα κινδύνου διότι ενημερώνονται και δεν βρίσκονται σε άγνοια.

Επειδή τα παιδιά πλέον είναι ενημερωμένα οι γονείς δεν χρειάζεται να πάρουν ακραία μέτρα για την προστασία τους.

ΥΠΟΧΡΕΩΣΕΙΣ ΚΑΙ ΔΙΚΑΙΩΜΑΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Οι μαθητές επέλεξαν 5 πιο σημαντικά γι αυτούς δικαιώματα και 5 υποχρεώσεις τους όταν πλοηγούνται στο διαδίκτυο. Τα αποτελέσματα φαίνονται στα ακόλουθα γραφήματα.


Δικαιώματα
17%
13%
4%
10%
11%
10%
7%
14%
6%
8%
Να προστατεύεις την ιδιωτικότητά σου, να αισθάνεσαι ασφαλής και να απολαμβάνεις το Διαδίκτυο. Δ1
Να διατηρείς το δικαίωμα ελέγχου στα προσωπικά δεδομένα που αναρτάς. Δ2
Να μπορείς να μιλάς σε κάποιον έμπιστο που μπορεί να σε βοηθήσει για το τι σε έχει ενοχλήσει στο Διαδίκτυο. Δ3
Να μπορείς να μάθεις πώς να προστατεύεσαι στο Διαδίκτυο. Δ4
Να μπορείς ΕΥΚΟΛΑ να αναφέρεις ύποπτες ή ενοχλητικές συμπεριφορές στους διαχειριστές των εκάστοτε ιστοχώρων. Δ5
Να μην παρενοχλείσαι διαδικτυακά από επιτήδειους. Δ6
Να βρίσκεις ποιοτικό περιεχόμενο στο Διαδίκτυο και να μην έρχεσαι σε επαφή με επιβλαβές ή ενοχλητικό περιεχόμενο. Δ7
Να μπορείς να συνομιλείς και να παίζεις με τους φίλους τους στο Διαδίκτυο. Δ8
Να μπορείς να δημιουργήσεις περιεχόμενο στο Διαδίκτυο. Δ9
Να βοηθάς τους φίλους τους να πλοηγούνται με ασφάλεια στο Διαδίκτυο. Δ10



ΕΠΙΛΟΓΟΣ

Συνοψίζοντας καταλαβαίνουμε πως το διαδίκτυο αν και κρύβει πολλούς κινδύνους είναι ένα χρήσιμο εργαλείο στις μέρες μας, το οποίο μας δίνει την δυνατότητα να επικοινωνούμε και να ασχολούμαστε με τις χιλιάδες εφαρμογές του. Από την έρευνα που κάναμε γι'αυτό είμαστε ικανοποιημένοι αφού μάθαμε πολλές πληροφορίες και χρήσιμες συμβουλές για να το χρησιμοποιούμε σωστά.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Πώς να προστατέψω τον Η/Υ μου

http://www.zougla.gr/file.ashx?fid=1051520

http://www.e-crime.gr/security_tips.htm

http://www.pcsteps.gr/1329-ti-na-kanete-an-o-ypologistis-sas-molynthei-apo-io-5-periptoseis/

http://windows.microsoft.com

http:/ /www.e-yliko.gr/htmls/pc_use/publish/html/etusivu.htm

http://www.pi.ac.cy/InternetSafety/PROLOGOS.htmL

http://sxoleio.eu

http://sxoleio.eu/Firewalls.php

http://www.itsecurity.gr/firewall.html

http://windows.microsoft.com

http://internet-filter-review.toptenreviews.com

Κίνδυνοι από τη χρήση του Διαδικτύου για έναν παιδί-έφηβο

http://www.newsbomb.gr/technologia/story/300229/deite-pos-mporeite-na-anakalypsete-ta-pseytika-profil-sto-facebook

http://www.e-istos.gr/home/2009-11-02-09-18-29/8699-hackers-----facebook.html

http://www.apodoxi.gr/alphanualphakappaalphalambda973psiepsilontauepsilon-taualpha-psiepsilon973tauiotakappaalpha-pirhoomicronphi943lambda.html

http://www.saferinternet.gr/

http://www.tophost.gr/learningcenter/%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%B1-ssl-certficates/

http://www.youtube.com/watch?feature=player_embedded&v=DJqz2eUHMHg#t=128

http://www.gnet.gr/gr/press/warning-about-facebook.html

www.tophost.gr

http://dotsub.com/view/41ffcc22-6609-4780-bf9d-5bcf88d3197d

http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-LawAndInternet2008.html

http://artemis.cslab.ntua.gr/el_thesis/artemis.ntua.ece/DT2013-0020/DT2013-0020.pdf

http://efivoidimosiografoi.pbworks.com/w/page/36345627/%CE%9A%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%BA%CE%AC%20%CE%94%CE%AF%CE%BA%CF%84%CF%85%CE%B1

http://www.youth-health.gr/gr/documents/praktika_2nd_seminar.pdf

http://odysonline.gr

www.youth-health.gr

www.pentapostagma.gr

www.diadiktio.wikispaces.com

Δημοκρίτειο Πανεπιστήμιο Θράκης

Interbiz news letter

Πανελλήνιο σχολικό δίκτυο – http://www.sch.gr

Βικιπαίδεια www.wikipedia.gr

http://windows.microsoft.com

Κίνδυνοι από τη χρήση του Διαδικτύου για τους Υπολογιστές

http://www.ianswer4u.com/2011/05/peer-to-peer-network-p2p-advantages-and.html#axzz2kWWEu8Sb

http://netforbeginners.about.com/od/peersharing/a/torrent_search.htm

http://www.ianswer4u.com/2011/05/peer-to-peer-network-p2p-advantages-and.html # ixzz2kWWOG35F

www.wikipedia.gr

www.astynomia.gr

http://www2.e-yliko.gr/htmls/safety/svirus.aspx

http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-Hackers-Crackers.html

http://www.noc.ntua.gr/index.php?module=contentexpress&func=display&ceid=174

http://www.itsecurity.gr/viruses.html

http://artemis.cslab.ntua.gr/el_thesis/artemis.ntua.ece/DT2013-0020/ DT2013-0020.pdf

Πώς να προστατέψω τον εαυτό μου

http://www.techne.gr/threads/8873-%CE%93%CE%B5%CE%BD%CE%B9%CE%BA%CE%BF%CE%AF-%CE%BA%CE%B1%CE%BD%CF%8C%CE%BD%CE%B5%CF%82-%CE%BA%CE%B1%CE%BB%CE%AE%CF%82-%CF%83%CF%85%CE%BC%CF%80%CE%B5%CF%81%CE%B9%CF%86%CE%BF%CF%81%CE%AC%CF%82-%CF%83%CF%84%CE%BF-%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

http://www.sch.gr/96-announces/1057-8242old

http://www.saferinternet.gr/index.php?objId=Category291&childobjId=Category294&parentobjId=Page187

http://www.saferinternet.gr/index.php?objId=Category291&childobjId=Category293&parentobjId=Page187

http://internet-safety.sch.gr/index.php/articles/parents/item/244-fbmal

http://tech.in.gr/news/article/?aid=1231268774

https://www.facebook.com/help/www/212826392083694

http://internet-safety.sch.gr/index.php/articles/teach/item/249-allvsfb2

http://www.socialmedialife.gr/99231/social-media-kai-asfaleia-passwords/

http://office.microsoft.com/el-gr/outlook-help/HA001140002.aspx

http://www.minedu.gov.gr/

http://www.physio-aid.gr/index.php?view=article&catid=4%3A2009-05-10-09-25-22&id=87%3A2009-09-30-07-46-14&format=phocapdf&option=com_content&Itemid=13.

http://www.e-yliko.gr/htmls/pc_use/fylladio_INTERNET_NEW_9-2012.pdf

http://www.slideshare.net/dourvas/saferinternet-gr-sinoptikosodigosgiagoneisprosonlinexrisi

http://blogs.sch.gr/internet-safety/archives/374

http://training.sch.gr/notes/ea22_safe/EA22_eBook.doc.

http://www.schoolessons.gr/data-general/internet-1/pdfs/safety.swf

Παράνομες Δραστηριότητες στο Διαδίκτυο

www.wikipedia

www.saferinternet.gr

www.cnc.uom.gr

http://greece-salonika.blogspot.com/2009/06/facebook.html
http://www.dpa.gr

ΠΑΡΑΡΤΗΜΑ

Σύννεφα Λέξεων

Στο παράρτημα παραθέτουμε τις εικόνες με τα σύννεφα λέξεων που φτιάξαμε

Ομάδα 1

Ομάδα 2

Ομάδα 3


hackers
MALWARE
INSTAGRAM
MYSPACE
VIRUS
CRACKERS
SPYWARE
TWITTER
ANTI
Λογισμικό
Αρχεία
Favorite Buy
UPLOAD
SECURITY
BLOCK
Blog
Share
PHISING
DISAGREE
Report
Password
SERVER
LICENSE
PIRACY
Page
OPEN
Spam
PICTURE
AGREEMENT
Ads
MAIL
ROOTKIT
Torrent
Stream
WEB
AGREE
WHITEHAT
THUMBNAILS
UPLOAD
YOUTUBE
ROOTKIT
Text
Post
Chat
PROXIES
Comment
PASSWORD
WINDOW
INFECT
AGREEMENT
USERNAME
KOOBFACE
ICON
ADRESS
FOLLOW
INTERNET
Ιός

Ομάδα 4


ΜΕΤΡΙΟΠΑΘΕΙΑ
ΠΡΟΣΩΠΙΚΗ
ΕΥΓΕΝΕΙΑ
ΜΕΤΡΙΟΦΡΟΣΥΝΗ
ΚΑΤΑΝΟΗΣΗ
ΕΠΑΦΗ
ΠΩΣ
ΝΑ
ΜΠΟΡΩ
ΠΡΟΣΤΑΤΕΥΤΩ
ΣΥΝΑΔΕΛΦΙΚΟΤΗΤΑ

Ομάδα 5


phising
grooming
grooming
phising
cyberbulling
sexting
phising
grooming
grooming
phising
grooming
phising
phising
cyberbulling
sexting
grooming
phising
cyberbulling
grooming
phising
sexting
phising
sexting
phising
sexting
sexting
grooming
cyberbulling
cyberbulling
phising
cyberbulling
sexting
phising
cyberbulling
grooming
sexting
grooming
phising
cyberbulling
phising
cyberbulling
sexting
sexting
cyberbulling
grooming
grooming
grooming
phising
sexting
sexting
grooming
grooming
phising
cyberbulling
sexting
grooming
cyberbulling
cyberbulling
sexting
grooming
cyberbulling
cyberbulling
cyberbulling
cyberbulling
cyberbulling
sexting
grooming
cyberbulling
grooming
sexting
cyberbulling
grooming
grooming
cyberbulling
sexting
grooming
cyberbulling
sexting
grooming
phising
phising
phising
cyberbulling
sexting
phising
phising
sexting
cyberbulling
cyberbulling
sexting
cyberbulling
sexting
grooming
sexting
phising
sexting
phising
grooming
phising