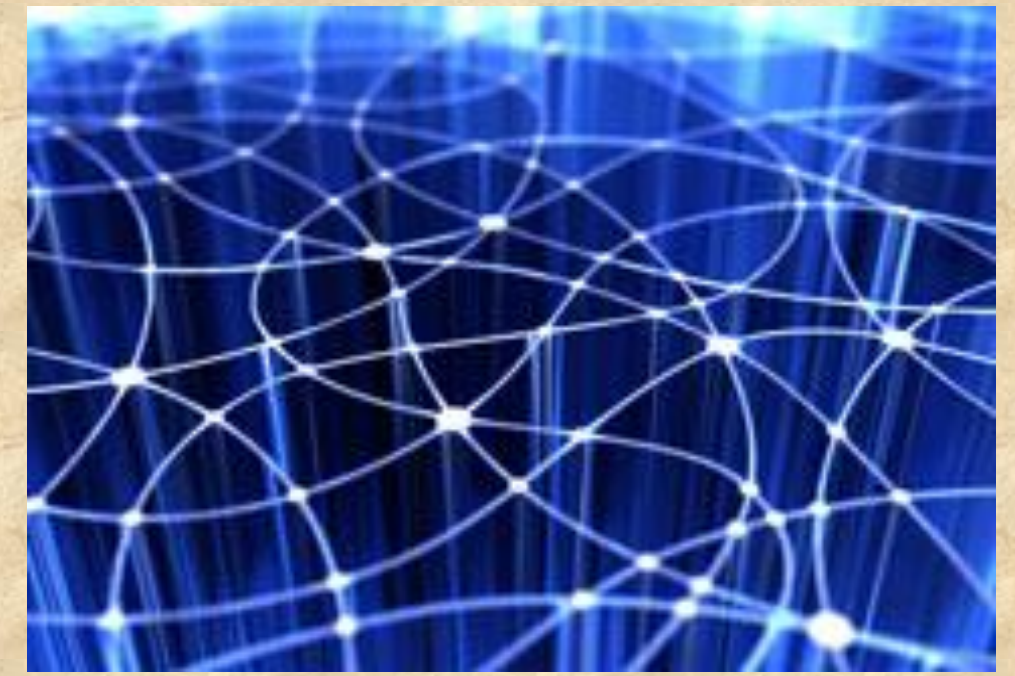
ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Δημητριάδης Ευάγγελος
Πληροφορικός - Φυσικός

Με τον όρο **<u>ασφάλεια στο Διαδίκτυο</u>** εννοούμε την, κατά το δυνατόν , αποτελεσματικότερη προστασία μας από τους ποικίλους κινδύνους όταν χρησιμοποιούμε το Διαδίκτυο.



Στοιχεία για την ασφάλεια στο Διαδίκτυο

1. Υπολογίζεται ότι υπάρχουν περίπου **150.000 ιοί** σε κυκλοφορία κάθε μέρα στους υπολογιστές, ενώ υπονομεύεται καθημερινά η λειτουργία **148.000 υπολογιστών**.
2. Σύμφωνα με το Παγκόσμιο Οικονομικό Φόρουμ, εκτιμάται ότι υπάρχει 10% πιθανότητα μείζονος κατάρρευσης υποδομών πληροφοριών ζωτικής σημασίας κατά την επόμενη δεκαετία, γεγονός που θα μπορούσε να προκαλέσει ζημία **250 δισεκατομμυρίων δολαρίων.**
3. Οι εγκληματικές δραστηριότητες στον κυβερνοχώρο ευθύνονται για μεγάλο ποσοστό των περιστατικών ασφάλειας στον κυβερνοχώρο, όπως εκτιμά η Symantec, τα θύματα εγκληματικών δραστηριοτήτων στον κυβερνοχώρο σε παγκόσμια κλίμακα χάνουν περίπου **290 δισ. ευρώ ετησίως**, ενώ μελέτη της McAfee υπολογίζει ότι οι εγκληματικές δραστηριότητες στον κυβερνοχώρο αποφέρουν κέρδη της τάξης των **750 δισ. ευρώ ετησίως**.
4. Στο μεταξύ, όπως φανερώνουν τα στοιχεία της Eurostat, έως τον Ιανουάριο του 2012 μόνο το 26% των επιχειρήσεων στην ΕΕ είχε επίσημα καθορισμένη πολιτική σε θέματα ασφάλειας των ΤΠΕ.

Οι σημαντικότεροι κίνδυνοι στο Διαδίκτυο είναι:

- Προσβολή από ανεπιθύμητα προγράμματα (ιούς)
- Κυβερνοεκφοβισμός (cyberbullying)
- Ηλεκτρονικές απάτες
- Παραβίαση προσωπικού απορρήτου

Ιοί και άλλα επιβλαβή προγράμματα υπολογιστών- Προστασία

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 περίπτωση 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.

ΤΡΟΠΟΙ ΜΕΤΑΔΟΣΗΣ - ΙΩΝ

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

ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ – ΑΠΟ ΙΟΥΣ

1.Επιλογή ενός καλού αντιβιοτικού προγράμματος
2. Τακτική ανίχνευση όλου του δίσκου με το αντιβιοτικό σας πρόγραμμα
3. Συνεχής ανανέωση (update) του αντιβιοτικού προγράμματος
4. Έλεγχος κάθε αποθηκευτικού μέσου με το αντιβιοτικό σας πρόγραμμα πριν το ανοίξετε.
5. Τήρηση αντιγράφων ασφαλείας (back up) όλων των αρχείων σας.
6. Συχνές επισκέψεις στην τοποθεσία των κρίσιμων ενημερώσεων των Windows όπου προσφέρονται δωρεάν προγράμματα (patches) διόρθωσης/κάλυψης των πιθανών ελλείψεων του λειτουργικού σας. Προτείνεται να ενεργοποιήσετε στον υπολογιστή σας την αυτόματη ενημέρωση των Windows.
7. Ανίχνευση μέσω του αντιβιοτικού κάθε νέου αρχείου που «κατεβάζετε» από το Internet.
8.Αν χρησιμοποιείτε irc chat, απενεργοποιείστε την επιλογή αυτόματης αποδοχής αρχείων και αυτόματης εκτέλεσης των αρχείων που σας στέλνουν.
9. 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.
10. Διατηρείτε και ανανεώνετε συχνά μια δισκέτα για αποκατάσταση ζημιών από ιούς, την οποία προσφέρουν συνήθως τα ίδια τα αντιβιοτικά προγράμματα.

Εδώ πρέπει να επισημανθεί πως όσο πιο αυστηρές ρυθμίσεις ασφαλείας ενεργοποιείτε στον υπολογιστή σας, τόσο πιο δύσκολα έχετε πρόσβαση σε σελίδες του Διαδικτύου. Η συνήθης ρύθμιση ασφαλείας στους φυλλομετρητές είναι η «μεσαία».

ΑΝΤΙΜΕΤΩΠΙΣΗ ΜΟΛΥΝΣΗΣ – ΑΠΟ ΙΟ

- Αν έχετε μολυνθεί από ιό και έχετε εγκατεστημένο αντιβιοτικό πρόγραμμα, βάλτε το να κάνει πλήρη έλεγχο όλου του σκληρού σας δίσκου (full system scan). Αν βρει τον ιό, θα προβεί αυτόματα στις κατάλληλες ενέργειες, είτε διαγράφοντάς τον, είτε απομονώνοντάς τον από το υπόλοιπο σύστημα.
- Σε περίπτωση που το αντιβιοτικό σας αδυνατεί να αποκαταστήσει τη ζημιά, μη διαγράψετε κανένα μολυσμένο αρχείο. Επανελέγξτε τα μολυσμένα αρχεία με κάποιο άλλο πρόγραμμα, ίσως αυτό να έχει δυνατότητα αποκατάστασης που δεν έχει το πρώτο πρόγραμμα.
- Προσπαθήστε να βρείτε από το Διαδίκτυο το πρόγραμμα απομάκρυνσης του ιού (virus removal tool) επισκεπτόμενοι τις κατάλληλες διευθύνσεις (εδώ πρέπει να γνωρίζετε την ακριβή ονομασία του ιού, προκειμένου να βρείτε το κατάλληλο για αυτόν πρόγραμμα) και, αφού το κατεβάσετε σε μια «καθαρή» δισκέτα, τρέξτε το στον υπολογιστή σας πάνω από μία φορά.
- Σε περίπτωση που ούτε το αντιβιοτικό σας, ούτε το ειδικό πρόγραμμα απομάκρυνσης μπορεί να «καθαρίσει» τον υπολογιστή σας, μπορεί να χρειαστεί να κάνετε format. Σε αυτήν την περίπτωση είναι καλό να έχετε κρατήσει αντίγραφα όλων των προγραμμάτων που υπάρχουν στον υπολογιστή σας, για να μπορέσετε μετά το format να τα ξαναπεράσετε.
- Γνωστές εταιρείες προσφέρουν τη δυνατότητα ελέγχου και απομάκρυνσης των ιών του υπολογιστή σας on-line.

Ενοχλητική αλληλογραφία (spam mail)

Το λεγόμενο spam ή junk mail είναι μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Στο spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς επίσης και διάφοροι άλλοι τύποι e-mail (π.χ. ανεπιθύμητα newsletters).Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Internet και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Internet και κινδυνεύει η ασφάλεια των δικτύων.

Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα να μην απαντάει σε μηνύματα τέτοιου είδους, ούτε και σε αυτά με την ένδειξη "remove me from the mailing list", τα οποία αντί να αποσύρουν την ηλεκτρονική του διεύθυνση, όπως υπόσχονται, επιβεβαιώνουν ότι είναι ενεργή και συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα.

Ο χρήστης μπορεί να χρησιμοποιήσει τα φίλτρα που του προσφέρουν τα περισσότερα web mail για να διαγράφει τα μηνύματα αυτά, ή να ρυθμίσει κατάλληλα το πρόγραμμα διαχείρισης αλληλογραφίας του υπολογιστή του (συνηθέστερα το outlook express), μέσω των επιλογών που δίνονται από τις καρτέλες στο μενού του προγράμματος.

Επίσης, στο Διαδίκτυο υπάρχουν προγράμματα καταπολέμησης των spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη.

Μηνύματα απατηλού περιεχομένου (hoaxes)

Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου:
1. «Προειδοποιητικά»: είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες, είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή για το σύστημα

2. «Συμπαράστασης»: παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται

3. «Εκφοβισμού» : οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες.
Ο ουσιαστικός κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοσή τους και, κατά συνέπεια, η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. Εκτός αυτού, δημοσιοποιούνται ευρέως και πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου, καθιστώντας τους ιδιοκτήτες τους ευκολότερα θύματα κάθε τέτοιου είδους ενοχλήσεως.
Τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από την τυποποιημένη φράση «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε» ("send this to everyone you know"). Στην περίπτωση των «προειδοποιητικών» μηνυμάτων εμφανίζονται ως αποστολείς μεγάλες και γνωστές εταιρείες, με σκοπό να ξεγελάσουν το χρήστη και να τον κάνουν να εμπιστευτεί το περιεχόμενο του μηνύματος.
Ο χρήστης πρέπει να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του και προκαλεί άνευ λόγου πανικό. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες που ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

Κυβερνοεκφοβισμός (cyberbullying)

Cyber Bullying
(Διαδικτυακή Παρενόχληση)

Η παρενόχληση στον κυβερνοχώρο προκύπτει όταν παιδιά ή έφηβοι παρενοχλούνται μεταξύ τους μέσω του Διαδικτύου

Cyber Bullying

Πρόκειται για μια εξελισσόμενη μόδα και περιλαμβάνει:

- Αποστολή e-mail, ή άμεσων μηνυμάτων με κακό περιεχόμενο.
- Δημοσίευση δυσάρεστων φωτογραφιών ή μηνυμάτων για άλλους σε ιστολόγια (blogs) ή άλλες ιστοσελίδες.
- Χρήση του ονόματος ξένου χρήστη με σκοπό τη διάδοση φημών και ψεμάτων για κάποιον τρίτο (κλοπή ταυτότητας).
- Προσβλητικά μηνύματα. Μερικές φορές προσβλητικά γραπτά μηνύματα προς κινητά τηλέφωνα στέλνονται μέσω ιστοσελίδων χρησιμοποιώντας ονόματα και τηλέφωνα ανθρώπων που δεν έχουν καμία σχέση με το μήνυμα αυτό, αλλά καταλήγουν να κατηγορούνται ότι το έστειλαν οι ίδιοι.
- Η δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας άλλους να δημοσιεύσουν μηνύματα μίσους.

Cyber Bullying

- Η σχετική ανωνυμία στο Διαδίκτυο προσφέρει το έδαφος καθώς ενισχύει τον φόβο και κάνει τον εντοπισμό δυσκολότερο
- Η έλλειψη προσωπικής επαφής με το θύμα κάνει το δράστη σκληρότερο
- Η ευρύτητα της πληροφορίας και η ευρύτητα του «κοινού» καθιστά το Cyber Bullying πιο αποτελεσματικό για τον δράστη και σκληρότερο για το θύμα σε σχέση με τις παραδοσιακές μεθόδους

Προστασία από το Cyber Bullying

- Προστασία προσωπικών δεδομένων από ιστοσελίδες κοινωνικής δικτύωσης.
- Περιορίζοντας τις διαθέσιμες πληροφορίες για τον εαυτό μας η την οικογένειά μας μειώνουμε τις πιθανότητες να πέσουμε θύματα αγνώστων δραστών και διευκολυνόμαστε στο να αναγνωρίσουμε τον πιθανό δράστη.
- Αποφεύγουμε να απαντήσουμε στις απειλές του δράστη. Απαντώντας επιθετικά φέρνουμε νέες απειλές και την ικανοποίηση στον δράστη ότι η παρενόχληση λειτουργεί.

Προστασία από το Cyber Bullying

- Αλλάζουμε email ή «κατεβάζουμε» την σελίδα δικτύωσης και δημιουργούμε νέους λογαριασμούς αν αυτό είναι εφικτό.
- Κρατάμε αποδεικτικά της δράσης συμπεριλαμβάνοντας όσα περισσότερα στοιχεία μπορούμε όπως ημερομηνίες και ώρες, λογαριασμούς ηλεκτρονικού ταχυδρομείου και λοιπά. Καλό θα είναι τα στοιχεία αυτά να υπάρχουν και σε μορφή εκτύπωσης.
- Επικοινωνούμε με τις αρμόδιες αρχές όσο το δυνατόν συντομότερα για να αποφευχθεί κλιμάκωση της παρενόχλησης.

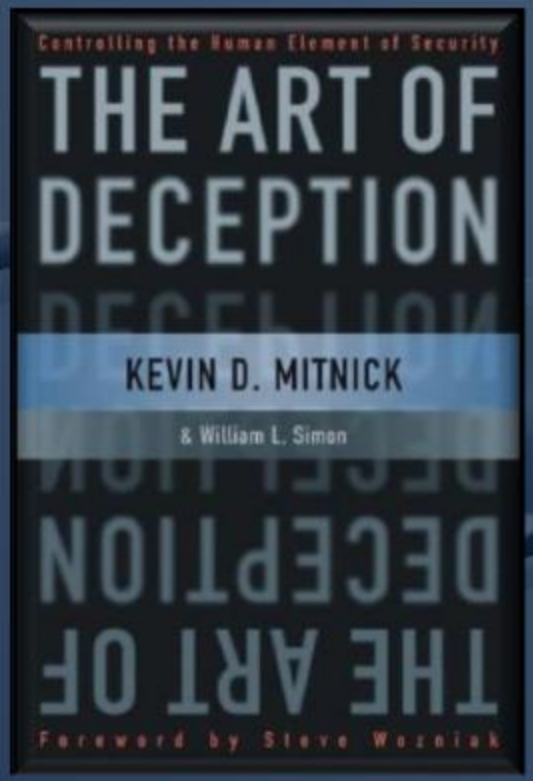
ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

Απάτες μέσω διαδικτύου

- Social Engineering
- Phishing
- Νιγηριανές απάτες
- Ισπανικό Λόττο

Απάτη μέσω διαδικτύου Social Engineering

Ο επιτιθέμενος χρησιμοποιεί την προσωπική επαφή και επικοινωνία με το θύμα ώστε να αποσπάσει προσωπικές πληροφορίες του θύματος.



Απάτη μέσω διαδικτύου Phishing

Είδος social engineering

- Αυτές οι επιθέσεις χρησιμοποιούν email και διάφορα websites ώστε να αποκτήσουν πληροφορίες των θυμάτων. Ο επιτιθέμενος στέλνει email υποστηρίζοντας ότι είναι μία τράπεζα ή ένας οικονομικός οργανισμός και ζητάει τραπεζικούς κωδικούς λόγω ύπαρξης κάποιου προβλήματος. Το θύμα πολλές φορές στέλνει τα προσωπικά του στοιχεία.

Απάτη μέσω διαδικτύου Phishing

- Διαδεδομένη είναι η μορφή του «ψαρέματος» τραπεζικών δεδομένων μέσα από ιστοσελίδες με εμφάνιση όμοια με την επίσημη τραπεζική ιστοσελίδα
- Η τράπεζα ποτέ δεν θα σου ζητήσει επιβεβαίωση προσωπικού κωδικού μέσω ηλεκτρονικού ταχυδρομείου

Απάτη μέσω διαδικτύου
Νιγηριανές απάτες

- Με τον όρο «νιγηριανή απάτη» περιγράφουμε την περίπτωση στην οποία αποστέλλονται mail τα οποία ενημερώνουν τον χρήστη είτε ότι είναι αποδέκτης κάποιας μεγάλης κληρονομιάς είτε ότι μπορεί να γίνει συνεργάτης κάποιας ξένης εταιρείας για την μεταφορά κεφαλαίων.

- Από τον χρήστη ζητούνται τα προσωπικά τραπεζικά στοιχεία τα οποία και στην συνέχεια χρησιμοποιούνται από τους επιτήδειους.

Απάτη μέσω διαδικτύου
Ισπανικό Λόττο

Ο χρήστης λαμβάνει email ότι κέρδισε ένα πολύ μεγάλο χρηματικό ποσό σε μια διεθνή λοταρία και ότι για να πάρει τα κέρδη πρέπει να δώσει κάποια χρήματα για να καλύψει τα έξοδα μεταφοράς των χρημάτων

Τρόποι Προστασίας από Απάτες μέσω Διαδικτύου

Ο χρήστης πρέπει να:

- Είναι υποψιασμένος σε ανώνυμες κλήσεις ή email που παρέχουν θέσεις εργασίας έναντι αδράς αμοιβής
- Μη δίνει προσωπικά στοιχεία σχετικά με την εταιρεία στην οποία εργάζεται, συμπεριλαμβανομένης της εσωτερικής δομής του δικτύου της εταιρείας, εκτός αν είναι σίγουρος ότι πρόκειται για εξουσιοδοτημένο εκπρόσωπο
- Μην αποκαλύπτει προσωπική ή οικονομική πληροφορία σε email και να μην ανταποκρίνεται σε ανώνυμα email σχετικά με τέτοιες πληροφορίες και να μην συνδέεται στα links που περιέχονται στα email αυτά
- Ταυτοποιεί τα στοιχεία οποιουδήποτε αγνώστου που υποστηρίζει ότι εκπροσωπεί νόμιμο οργανισμό, κατευθείαν με τον οργανισμό

Τρόποι Προστασίας από Απάτες μέσω Διαδικτύου

Ο χρήστης πρέπει να:

- Μην στέλνει ευαίσθητα δεδομένα στο διαδίκτυο πριν ελέγξει την ασφάλεια ενός website
- Δίνει έμφαση στο URL του website. Κακόβουλα websites μπορεί να φαίνονται ίδια με νόμιμα site, αλλά το URL μπορεί να διαφοροποιείται από το επίσημο είτε λεκτικά είτε ως προς το domain (.com, .net)
- Εγκαθιστά και συντηρεί αντι-ιικά προγράμματα, firewalls, και email φίλτρα ώστε να μειωθεί η διακίνηση κακόβουλων μηνυμάτων
- Εκμεταλλευτεί anti-phishing λειτουργίες που παρέχονται σε email και web browser

Αντίδραση σε Περίπτωση Απάτης

- Εάν πιστεύετε ότι οι οικονομικοί σας λογαριασμοί διακυβεύονται, επικοινωνήστε με τους τραπεζικούς οργανισμούς άμεσα και κλείστε κάθε λογαριασμό που είναι σε κίνδυνο. Παρακολουθείστε για ανεξήγητες χρεώσεις του λογαριασμού σας.
- Αλλάξτε άμεσα κάθε password που μπορεί να έχει αποκαλυφθεί. Εάν χρησιμοποιείτε το ίδιο password για διαφορετικές περιπτώσεις αλλάξτε το για κάθε λογαριασμό και μην το χρησιμοποιήσετε στο μέλλον.
- Παρακολουθείτε για σημάδια κλοπής στοιχείων ταυτότητας.
- Αναφέρετε την επίθεση στην Υπηρεσία μας.

Παιδική Πορνογραφία

- Οργιάζουν καθημερινά σε όλο τον κόσμο τα κυκλώματα παιδικής πορνογραφίας.
- Στην Ελλάδα τιμωρείται η κατοχή αρχείων παιδικής πορνογραφίας.

Παιδική Πορνογραφία

Πως λειτουργούν τα κυκλώματα:

Πρόκειται για «κλειστές ομάδες» οι οποίες επικοινωνούν μέσω ομάδων συζήτησης (newsgroups), είτε μέσω δωματίων επικοινωνίας (chat rooms), είτε μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (email)

Εκτιμάται ότι πάνω από ένα εκατομμύριο εικόνες παιδιών που υποβάλλονται σε σεξουαλική κακοποίηση και εκμετάλλευση βρίσκονται σήμερα στο Διαδίκτυο. Σύμφωνα με το Γραφείο του ΟΗΕ για τα Ναρκωτικά και το Έγκλημα (UNODC), 50.000 νέες εικόνες κακοποίησης παιδιών αναρτώνται στο Διαδίκτυο κάθε χρόνο.

Καμία χώρα δεν μπορεί να καταπολεμήσει μόνη της αυτό το φρικτό φαινόμενο, καθώς τα εγκληματικά κυκλώματα που βρίσκονται πίσω του δεν γνωρίζουν σύνορα και εκμεταλλεύονται την έλλειψη αλληλοενημέρωσης και τα νομικά κενά που υπάρχουν σε εθνικό και διεθνές επίπεδο. Αυτός είναι ο λόγος για τον οποίο η διεθνής συνεργασία είναι ζωτικής σημασίας για την αποτελεσματική διερεύνηση των κρουσμάτων σεξουαλικής κακοποίησης παιδιών στο Διαδίκτυο και για τον καλύτερο εντοπισμό και τη δίωξη των δραστών.

Παραβίαση προσωπικού απορρήτου

Επίθεση από hackers-crackers

Οι βασικοί λόγοι για τους για τους οποίους hacker μπορεί να θέλει να αποκτήσει πρόσβαση στον υπολογιστή ενός χρήστη είναι δύο.

Ο πρώτος αφορά την άντληση πληροφοριών, όπως passwords και αριθμοί πιστωτικών καρτών, από τον υπολογιστή του χρήστη για να αγοράσει κάτι on-line, ή να χρησιμοποιήσει τις πληροφορίες που αποθηκεύονται στα log files για να χρησιμοποιηθούν για τον ISP ,για παράνομη δραστηριότητα, όπως διανομή της παιδικής πορνογραφίας.

Ο δεύτερος αφορά τη χρησιμοποίηση του υπολογιστή σε επιθέσεις για να προκληθεί διανεμητική άρνηση της υπηρεσίας, οι λεγόμενες επιθέσεις DDoS (distributive denial of service). Σε μια επίθεση DDoS, ο υπολογιστής πελάτης (client) διατάζει όλους τους κεντρικούς υπολογιστές (servers) που βρίσκονται σε μεμονωμένα PCs να επιτεθούν σε έναν ενιαίο ιστοχώρο. Χιλιάδες μεμονωμένα PCs μπορούν να διαταχθούν να έχουν πρόσβαση σε έναν ιστοχώρο όπως eBay ή Yahoo συγχρόνως, με αποστολή τεράστιου αριθμού αιτήσεων, με αποτέλεσμα να φράξουν το εύρος ζώνης (site's bandwidth) της περιοχής και να προκληθεί διακοπή της υπηρεσίας και οι πραγματικοί επισκέπτες να μην μπορούν να χρησιμοποιήσουν τις υπηρεσίες του Site.

Ποιο είδος πληροφοριών μπορεί ένας hacker να κλέψει από τον υπολογιστή σας.

Οι προσωπικές πληροφορίες, η διεύθυνση ονομάτων, οι οικονομικές πληροφορίες, ακόμη και οι πληροφορίες του λογαριασμού σας για τον ISP σας και οι κωδικοί πρόσβασης, και γενικά οτιδήποτε που έχει αποθηκευτεί στον υπολογιστή σας μπορούν να ληφθούν από τον hacker. Το πρόγραμμα Trojan μπορεί ακόμη και να είναι σε θέση να καταγράψει κάθε πληκτρολόγηση που κάνετε, να αποθηκεύσει τις πληροφορίες σε ένα κρυφό αρχείο (hidden file)και έπειτα όταν συνδεθείτε on-line το αρχείο θα φορτωθεί στον υπολογιστή του hacker. Αυτό σημαίνει ότι ακόμα κι αν δεν κρατάτε τις προσωπικές σας πληροφορίες ή τους κωδικούς πρόσβασης αποθηκευμένους στον υπολογιστή σας , ο hacker μπορεί ακόμα να τα λάβει από το αρχείο καταγραφής πληκτρολόγησης (log file).

Προστασία από hackers

Firewall: Τοίχος Φωτιάς -Αντιπυρική προστασία.

Μπορεί να είναι είτε Hardware είτε Software και έχει τη δυνατότητα να μπλοκάρει την είσοδο και έξοδο πληροφοριών από το δίκτυο. Λειτουργεί με τη λογική των rules - Κανόνων, τα οποία ορίζει ο ίδιος ο χρήστης.

Το Firewall αναλαμβάνει να κλείσει όλα τα ανοιχτά ports, από τα οποία μπορούν να περάσουν οι εντολές ενός Hacker . Ένα Trojan πρόγραμμα συνήθως έρχεται ως συνημμένο αρχείο σε e-mail ή ως ένα χρήσιμο πρόγραμμα που θα σας βοηθήσει να λύσετε προβλήματα, ενώ στην πραγματικότητα απλά θα ανοίξει την πόρτα στους hackers . Το Firewall μπορεί επίσης να συλλέξει ορισμένα στοιχεία για τον επιτιθέμενο. Επισημαίνουμε τα προγράμματα Firewall δεν προσφέρουν απόλυτη προστασία απέναντι σε κάποιον αποφασισμένο hacker. Επισημαίνουμε επίσης ότι το Firewall δεν θα απεγκαταστήσει ένα πιθανό Trojan που έχει εισβάλει στον υπολογιστή σας αλλά απλά δεν θα του επιτρέπει να επικοινωνεί με κάποιον client (υπολογιστή πελάτη). Για να επεγκαταστήσετε ένα Trojan χρειάζεστε κάποιο άλλο ειδικό πρόγραμμα.

CLOUD COMPUTING-ΑΠΟΘΗΚΕΥΣΗ ΣΤΟ ΣΥΝΝΕΦΟ (facebook-twitter-youtube-googledocs

Η απειλή που στοιχειοθετεί για την ιδιωτική ζωή το λεγόμενο **"cloud computing"** δεν έχει αξιολογηθεί επαρκώς, ίσως μάλιστα έχει αγνοηθεί εντελώς, προειδοποιεί μελέτη του ΕΚ καθώς προχωρεί η διαδικασία αναθεώρησης της απαρχαιωμένης οδηγίας του 1995 για την προστασία των δεδομένων. Σήμερα η Ευρώπη εορτάζει την Ημέρα Προστασίας των Δεδομένων, που είναι προσπάθεια αφύπνισης των πολιτών για το πώς σχεδόν ότι κάνουν στο Διαδίκτυο συλλέγεται και "αξιοποιείται".

Μυστικά μάτια στο "σύννεφο"

Σύμφωνα με μελέτη που δημοσίευσε το ΕΚ στο τέλος του 2012, "η πρόκληση που στοιχειοθετεί το "could computing" δεν έχει αξιολογηθεί επαρκώς, ίσως μάλιστα έχει αγνοηθεί εντελώς". Η μεγαλύτερη ανησυχία είναι η αυξανόμενη χρήση του cloud computing, της αποθήκευσης δεδομένων όχι πια στον προσωπικό υπολογιστή (ή τηλέφωνο ή άλλη συσκευή) του καθ' ενός αλλά σε κεντρικούς σέρβερ κάπου... Αυτή η "ανησυχία" που εκφράζει η μελέτη αφορά φυσικά τη δυνατότητα τρίτων να αποκτούν πρόσβαση στα στοιχεία αυτά.

Όπως μάλιστα επισημαίνει, η πραγματική ανησυχία εν προκειμένω δεν είναι τόσο το ενδεχόμενο απάτης ή κυβερνοεγκλήματος: ο πραγματικός κίνδυνος είναι η πλήρης απώλεια ελέγχου από τους πολίτες στα πιο προσωπικά δεδομένα τους.

Ο παράγοντας ΗΠΑ

Η ίδια έκθεση επισημαίνει ότι οι αμερικανικές αρχές έχουν δικαίωμα, βάσει νόμου, να επιτηρούν το "σύννεφο" και να εισέρχονται στα στοιχεία οποιουδήποτε απ' όπου κι αν προέρχεται. Στο ερώτημα αν αυτό σημαίνει ότι η CIA κοιτά τα πάντα στο "σύννεφο" ή κατά πόσον η μάχη κατά της τρομοκρατίας υπονομεύει βασικά δικαιώματά μας η έκθεση σημειώνει ότι αυτό δεν είναι θέμα που αγγίζει η προτεινόμενη μεταρρύθμιση αλλά θα μπορούσε να αντιμετωπισθεί με μια μελλοντική συμφωνία ΕΕ-ΗΠΑ.

Έφηβοι και online φήμη

Η online φήμη (Online reputation) είναι οι πληροφορίες που είναι διαθέσιμες online παρέχοντας σε άλλους χρήστες μια εικόνα για την επαγγελματική και κυρίως την προσωπική ζωή μας. Μπορεί να θεωρηθεί ως ένα ψηφιακό αποτύπωμα του μονοπατιού ή του ίχνους πληροφοριών που ένα άτομο μπορεί να αφήσει στο διαδίκτυο. Αυτό μπορεί να κυμαίνεται από φωτογραφίες και σχόλια σε ιστοσελίδες κοινωνικής δικτύωσης ως τα δεδομένα που αποθηκεύονται στον υπολογιστή (cookies) μετά την περιήγηση στο διαδίκτυο. Όσο μεγαλύτερη αλληλεπίδραση ένα άτομο έχει σε ένα ψηφιακό περιβάλλον, τόσο μεγαλύτερο είναι το ψηφιακό αποτύπωμα του.

Γιατί χρειάζεται όμως να ανησυχούμε για το ψηφιακό μας αποτύπωμα;

Όσο περισσότερες δραστηριότητες κοινοποιούνται πλέον oline, οφείλουμε να γνωρίζουμε ότι το υλικό μπορεί να ενσωματωθεί στο διαδίκτυο και άλλοι μπορεί να είναι σε θέση να έχουν πρόσβαση σε αυτό. Οι περισσότεροι που χρησιμοποιούν το διαδίκτυο σωστά δεν θα πρέπει να ανησυχούν σχετικά με τη διαδικτυακή φήμη τους. Αλλά οι έφηβοι πρέπει να επανεξετάσουν με ποιον τρόπο ανόητα ή επιπόλαια σχόλια, που πραγματοποιήθηκαν χωρίς δεύτερη σκέψη, θα μπορούσαν ακόμα να είναι διαθέσιμα όταν ενδεχομένως υποβάλλουν αίτηση για θέσεις εργασίας στο μέλλον.

Μία αρνητική online φήμη όπως προκύπτει από ένα ακατάλληλο σχόλιο ή μία φωτογραφία μπορεί να έχει καταστροφικές συνέπειες. Δείτε λοιπόν τη θεματική παρουσίαση η οποία απευθύνεται κυρίως στους εφήβους με αφορμή την **επετειακή 10η Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου** (5/2/2013)

Ασφαλής χρήση σελίδων κοινωνικής δικτύωσης facebook, twitter

11. Ο δεκάλογος της ασφαλούς χρήσης ιστοχώρων κοινωνικής δικτύωσης

Συνοψίζοντας τα παραπάνω, παραθέτουμε εδώ τα πιο σημαντικά σημεία σχετικά με την ασφαλή χρήση ιστοχώρων κοινωνικής δικτύωσης που θα προστατεύσουν την ιδιωτική μας ζωή και θα μας επιτρέψουν να επικοινωνούμε και να διασκεδάζουμε σε αυτούς τους ιστοχώρους με ασφάλεια:

1. Πριν εγγραφούμε σε έναν ιστοχώρο κοινωνικής δικτύωσης αναζητούμε την πολιτική απορρήτου και τους όρους χρήσης και βεβαιωνόμαστε ότι **κατανοούμε πλήρως** με ποιον τρόπο θα χρησιμοποιούνται από τον ιστοχώρο τα προσωπικά μας δεδομένα.

2. Από τη στιγμή που θα δημιουργήσουμε λογαριασμό θα πρέπει να **αλλάξουμε τις προεπιλεγμένες ρυθμίσεις** στο μενού *Απόρρητο/Privacy*.

3. **Περιορίζουμε την πρόσβαση στο λογαριασμό μας** μειώνοντας τις πιθανότητες άντλησης πολλών έγκυρων προσωπικών δεδομένων και πληροφοριών από επιτήδειους, οι οποίοι τα χρησιμοποιούν για εξειδικευμένη επίθεση ηρηέhing» μέσω των ιστοχώρων κοινωνικής δικτύωσης.

4. Δε δίνουμε σε κανέναν τον κωδικό πρόσβασης στο λογαριασμό μας. Κάποιος, γνωρίζοντας τον κωδικό μας, αποκτά **πρόσβαση στο λογαριασμό μας** και μπορεί να διαχειριστεί **πλήρως** τα δεδομένα που συνδέονται με αυτόν.

5. Δεν ανεβάζουμε **φωτογραφίες όπου φαίνεται καθαρά η τοποθεσία στην οποία βρισκόμαστε**, ειδικότερα αν πρόκειται για το σπίτι μας, το σχολείο, ή μέρη που συχνάζουμε. Έτσι θα προστατευθούμε καλύτερα από την πιθανότητα εντοπισμού μας στον φυσικό κόσμο.

6. Αν δεχθούμε ένα προσβλητικό ή ανεπιθύμητο μήνυμα, χρησιμοποιούμε **την ενσωματωμένη μέθοδο καταγγελιών** του ιστοχώρου κοινωνικής δικτύωσης που χρησιμοποιούμε. Συνήθως την εντοπίζουμε ως «Αναφορά / Report».

7. Έχουμε πάντα υπόψη ότι οι πληροφορίες που δημοσιεύουμε στους ιστοχώρους κοινωνικής δικτύωσης είναι δημόσια προσπελάσιμες, επομένως, καλό θα ήταν να μη δημοσιεύουμε στοιχεία και φωτογραφίες που θα μας έφερναν σε δύσκολη θέση. Ακόμα και αν απενεργοποιήσουμε/ακυρώσουμε το λογαριασμό μας, **πολλές πληροφορίες δεν αφαιρούνται** και ενδέχεται, επίσης, να τις συναντήσουμε και αλλού στο Διαδίκτυο.

8. Γνωρίζουμε ότι από τη στιγμή που προσθέτουμε στη λίστα των φίλων μας κάποιο άτομο (αποδοχή: *friend request*), αυτό **αποκτά πρόσβαση στα προσωπικά δεδομένα που εμφανίζονται στη σελίδα μας**, μεταξύ των οποίων οι φωτογραφίες και τα στοιχεία επικοινωνίας μας. Γι' αυτό, σκεφτόμαστε πολύ προσεχτικά ποια άτομα θα προσθέσουμε στη λίστα αυτή.

9. Γνωρίζουμε ότι οι ιστοχώροι κοινωνικής δικτύωσης προσφέρουν πολλές εφαρμογές (παιχνίδια, κουίζ, κ.λπ.), τα οποία **δεν υπόκεινται πάντα στην ίδια πολιτική απορρήτου** και, επομένως, μπορούν να διαχειριστούν τα προσωπικά μας δεδομένα με διαφορετικό τρόπο.

10. Έχουμε πάντα υπόψη ότι στον ψηφιακό κόσμο είναι εύκολο να δημιουργήσει κανείς μια **ψεύτικη ταυτότητα** και να **παραπλανήσει άλλους χρήστες**. Επομένως, θα πρέπει να είμαστε επιφυλακτικοί με τους εικονικούς φίλους.

ΣΗΜΑΝΤΙΚΟ

Το Facebook δε θα ζητήσει ποτέ μέσω e-mail τα προσωπικά μας στοιχεία σύνδεσης. Επίσης, δε θα μας ζητήσει ποτέ να συνδεθούμε περισσότερες από μια φορά στο λογαριασμό μας κατά τη διάρκεια μιας συγκεκριμένης σύνδεσής μας με τον ιστοχώρο. Αν μας ζητηθεί κάτι τέτοιο, τότε ο ιστοχώρος στον οποίο βρισκόμαστε **δεν είναι ο γνήσιος του Facebook.**

Ενημερώνουμε σε τακτά χρονικά διαστήματα τον πλοηγό μας (browser), καθώς έτσι μας παρέχονται σε συνεχή βάση οι ενημερωμένες λειτουργίες ασφάλειας και αποτροπής απατηλών δραστηριοτήτων.

s@ferinternet.gr

Γραμμή Βοηθείας

ΥΠΟ.ΣΤΗΡΙ.ΖΟ

800 11 800 15

Εάν το Διαδίκτυο δυσκολεύει τη ζωή του παιδιού σας ζητήστε βοήθεια

safeline

www.safeline.gr

Καταγγείλετε παράνομο περιεχόμενο στο Διαδίκτυο

WWW

Ασφαλής χρήση του Διαδικτύου

Συνοπτικός οδηγός για τους μαθητές

Στο πλαίσιο του Μνημονίου Συνεργασίας

Ελληνικό Κέντρο Ασφαλούς Διαδικτύου
Δράση Ενημέρωσης
s@ferInternet.gr
το δίκτυο ασφαλέστερο ειδικά για σένα

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ
ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ

ΜΟΝΑΔΑ ΕΦΗΒΙΚΗΣ ΥΓΕΙΑΣ (Μ.Ε.Υ.)
Β΄ ΠΑΙΔΙΑΤΡΙΚΗ ΚΛΙΝΙΚΗ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΑΘΗΝΩΝ
ΝΟΣΟΚΟΜΕΙΟ ΠΑΙΔΩΝ "Π. & Α. ΚΥΡΙΑΚΟΥ"

Υπό την αιγίδα της Ευρωπαϊκής Επιτροπής

- Ο χρόνος που μένω στον υπολογιστή και το Διαδίκτυο δεν πρέπει να μου στερεί ούτε ένα λεπτό από το παιχνίδι μου, τα χόμπι μου, τους φίλους μου, το διάβασμά μου και τον ύπνο μου.
- Μπορώ να διασκεδάζω στον εικονικό κόσμο του Διαδικτύου, όμως πάντα **αναγνωρίζω ότι διαφέρει από τον πραγματικό κόσμο**.

s@ferinternet.gr

Το Διαδίκτυο: **ένας καταπληκτικός κόσμος**

Το Διαδίκτυο είναι ένας καταπληκτικός κόσμος μάθησης, επικοινωνίας και διασκέδασης, είναι όμως και ένα κόσμος ανοιχτός σε όλους, καλούς και κακούς! Με μερικά απλά τρικ λοιπόν που δίνονται στον οδηγό αυτό, όλοι εμείς μπορούμε να απολαμβάνουμε τα πολλά οφέλη του Διαδικτύου με ασφάλεια και να αποφεύγουμε τους πιθανούς κινδύνους. Σας καλούμε να τα διαβάσετε με προσοχή!

- **Δεν αποκαλύπτω ποτέ προσωπικές λεπτομέρειες στο Διαδίκτυο,** όπως το πραγματικό μου όνομα, τη διεύθυνση της κατοικίας μου, το όνομα του σχολείου μου, το τηλέφωνό μου, ή την φωτογραφία μου, γιατί ποτέ δεν μπορώ να ξέρω που μπορούν να καταλήξουν. Αντίστοιχα, δεν ζητώ από άλλους να αποκαλύψουν προσωπικές τους πληροφορίες, όσο είμαι μαθητής- ανήλικος.

Σκέψου πριν δημοσιεύσεις! Προστάτευσε την ιδιωτική ζωή, τη δική σου, της οικογένειάς σου, των φίλων σου.

- **Δεν αποκαλύπτω σε κανέναν, ούτε και στους καλύτερούς μου φίλους, τον κωδικό πρόσβασης του λογαριασμού που έχω στο Διαδίκτυο.** Κάποιο άλλο άτομο θα μπορούσε να προφασιστεί ότι είμαι εγώ στο Διαδίκτυο, να διαβάσει το ηλεκτρονικό μου ταχυδρομείο, να αναρτήσει λανθασμένες ή κακές πληροφορίες, να παρενοχλήσει άλλα άτομα ή να διαδώσει ψέματα για τρίτους, χρησιμοποιώντας τον κωδικό αυτό.

- Γνωρίζω ότι οποιαδήποτε προσωπική πληροφορία δημοσιεύσω στο Διαδίκτυο, **εκείνη τη στιγμή παύει να είναι προσωπική και γίνεται δημοσίως προσβάσιμη, παντού στον κόσμο.** Για αυτό το λόγο, πρέπει πάντα να σκέφτομαι πριν δημοσιεύω οτιδήποτε στο Διαδίκτυο.

s@ferinternet.gr

- **Σβήνω αμέσως e-mail που έχω λάβει από αποστολείς που δεν γνωρίζω,** ή ακόμα και από φίλους, από τους οποίους όμως δεν αναμένω ηλεκτρονική αλληλογραφία. Σε καμία περίπτωση δεν ενεργοποιώ τους συνδέσμους του Διαδικτύου που υπάρχουν σε αυτά τα ηλεκτρονικά μηνύματα ούτε ανοίγω τυχόν προσαρτήματα. Το ίδιο ισχύει και για την λήψη αρχείων από κόμβους του Διαδικτύου, γιατί έτσι πιθανόν να μεταδοθεί ιός στον υπολογιστή μου που θα μπορούσε να τον βλάψει ή να τον καταστρέψει.

- **Δεν κάνω ποτέ αγορές από το Διαδίκτυο αν δεν είναι δίπλα μου ένας γονέας.** Αποφεύγω ιστοχώρους που δεν γνωρίζω εάν είναι έγκυροι. Πληκτρολογώ πάντα εγώ την διεύθυνση της ιστοσελίδας, για να είμαι σίγουρος/η ότι θα μεταβώ στην γνήσια και όχι σε άλλη, πλαστή.

- Κάνω **τακτικά διαλείμματα** όταν είμαι στον υπολογιστή, για να ξεκουράζονται τα μάτια μου.

Μην ξεχνάς να ζεις στον πραγματικό κόσμο για χάρη του Διαδικτύου

Σέρφαρε ηθικά και με κριτική σκέψη

- **Αντιμετωπίζω τους άλλους χρήστες** του Διαδικτύου **με τον ίδιο τρόπο που θα ήθελα να μου φέρονται αυτοί**. Δεν κατηγορώ ούτε προσβάλλω κάποιον στο Διαδίκτυο θεωρώντας ότι αστειεύομαι, γιατί το αστείο μου μπορεί να μη γίνει αποδεκτό και να πληγώσει το άτομο αυτό.

- Γνωρίζω ότι **το κατέβασμα φωτογραφιών, μουσικής ή βίντεο μπορεί να είναι παράνομο**. Για αυτό το λόγο ελέγχω εάν μπορώ να το κάνω αυτό στην ιστοσελίδα ή εάν πρέπει να πληρώσω για την υπηρεσία αυτή. Υπάρχουν πολλές ιστοσελίδες που παρέχουν δωρεάν υλικό στους χρήστες τους.

- **Δεν αντιγράφω έτσι απλώς κείμενα από υλικό του Διαδικτύου** για τις εργασίες μου, γιατί είναι σαν να κλέβω. Η αντιγραφή από το Διαδίκτυο μπορεί να είναι παράνομη και δεν βοηθάει καθόλου στην ανάπτυξη των γνωστικών μου δεξιοτήτων και της κριτικής μου ικανότητας, προσόντα που θα χρειαστώ στο μέλλον μου.

- **Δεν προωθώ e-mail** που έλαβα και που βρίσκω απαράδεκτο, γιατί είναι σαν να προωθώ ανεπιθύμητη αλληλογραφία.

s@ferinternet.gr

Δεν είμαστε ανώνυμοι στο Διαδίκτυο. Όλοι αφήνουμε ηλεκτρονικά ίχνη!

- Όλοι αφήνουμε ηλεκτρονικά ίχνη στο Διαδίκτυο! Συνεπώς, πρέπει να συμπεριφέρομαι με κανόνες και με ηθική, όπως το κάνω και στον πραγματικό κόσμο. Θυμάμαι, ότι αν παραβώ κάποιους συγκεκριμένους κανόνες που συνεπάγονται κυρώσεις, τότε μέσα από τα ηλεκτρονικά μου ίχνη θα μπορώ να εντοπιστώ, οπουδήποτε στον κόσμο.

- Ενημερώνω τους γονείς ή τους δασκάλους μου στην περίπτωση που διαβάσω **στο Διαδίκτυο κάτι που με ενοχλεί ή που με κάνει να νοιώθω άβολα**, δίχως να διστάσω. Ακόμα και αν πιστεύω ότι γνωρίζω πολύ καλύτερα το Διαδίκτυο από τους γονείς ή τους δασκάλους μου, δεν ξεχνάω ότι εκείνοι μπορούν να με προστατεύσουν από κακοτοπιές μέσα από την γνώση και την εμπειρία τους.

Ό,τι ανεβαίνει στο Διαδίκτυο, παραμένει εκεί για πάντα!

- Ποτέ **δεν συναντώ στο φυσικό κόσμο φίλους που γνώρισα στο Διαδίκτυο** και που δεν γνωρίζω στον πραγματικό κόσμο. Τα άτομα αυτά δεν είναι πάντοτε αυτά που ισχυρίζονται ότι είναι, ακόμα και αν αλληλογραφώ ή επικοινωνώ μαζί τους για πολύ καιρό, ή μου έχουν στείλει φωτογραφία τους ή τους έχω δει με web κάμερα. Ακόμα και η φωτογραφία ή το βίντεο μπορεί να είναι πλαστά.

- Εάν κάποιος διαδικτυακός φίλος μου ζητήσει να κρατήσω **τη φιλία μας μυστική, τότε κάτι δεν πάει καλά**. Ποιος αληθινός φίλος θα το ζητούσε αυτό; Πρέπει αμέσως να ενημερώσω τους γονείς μου ή τους δασκάλους μου.

Οι φίλοι που γνωρίζουμε μόνο μέσα από το Διαδίκτυο παραμένουν άγνωστοι!

- Εάν κάποιος μου στείλει ένα απρεπές μήνυμα ή μια απρεπή εικόνα ή με παρενοχλεί στο Διαδίκτυο, πρέπει να σταματήσω αμέσως την επικοινωνία μαζί του και να αναφέρω το γεγονός στους γονείς μου ή στους δασκάλους μου για να με βοηθήσουν. Μπορώ, επίσης, να καλέσω το τηλέφωνο **800 11 800 15** χωρίς χρέωση για να ζητήσω ανώνυμα βοήθεια από ειδικούς του **Ελληνικού Κέντρου Ασφαλούς Διαδικτύου**.

- **Εάν κάποιος μου προσφέρει κάτι στο Διαδίκτυο που μου φαίνεται υπερβολικό** για να είναι αλήθεια, όπως π.χ. δώρα για συμμετοχή σε διαγωνισμό ή κουίζ, τότε πιθανώς, όντως να μην είναι αληθινό και να πρόκειται για κάποιο τέχνασμα! Καλό θα είναι λοιπόν να αποφεύγω τέτοιου είδους επαφές ή ιστοσελίδες.

- **Δεν ενδιαφέρομαι για υλικό που απευθύνεται σε ενηλίκους**, αναζητώ ιστοσελίδες που έχουν δημιουργηθεί για παιδιά της ηλικίας μου.

- **Εάν βρω κάποια ιστοσελίδα που με τρομάζει**, μου φαίνεται περίεργη, ή περιέχει ρατσιστικό / εξτρεμιστικό ή άλλο ύποπτο περιεχόμενο, το αναφέρω αμέσως στους γονείς μου ή στους δασκάλους μου.

Έλεγξε την εγκυρότητα της πληροφορίας στο Διαδίκτυο

- **Διασταυρώνω πάντα το υλικό που βρίσκω στο Διαδίκτυο** με άλλες πηγές, όπως βιβλία, εφημερίδες, περιοδικά, ρωτώ επίσης τους δασκάλους και τους γονείς μου. Όλοι εμείς μπορούμε να είμαστε συγγραφείς του Διαδικτύου, και δεν είναι όλοι οι άνθρωποι επιστήμονες ή ειδικοί!

Συμβουλές για τους γονείς

Προτιμήστε να τοποθετήσετε τον Η/Υ σας σε χώρους, όπως είναι το σαλόνι και όχι σε υπνοδωμάτια. Έτσι θα έχετε τη δυνατότητα να επιβλέπετε το παιδί σας, χωρίς το ίδιο να αισθάνεται ότι ελέγχεται.

Κάντε την πλοήγηση στο Internet μία οικογενειακή δραστηριότητα. Χρησιμοποιείστε τον Η/Υ μαζί με τα παιδιά σας.

Ενημερώστε τα παιδιά σας για τους κινδύνους που υπάρχουν όταν συνομιλούν με αγνώστους μέσω chatrooms.

Συζητήστε με τα παιδιά σας για θέματα ασφάλειας (επικοινωνία με επικίνδυνα άτομα, πρόσβαση σε sites με βλαβερό περιεχόμενο) που προκύπτουν από την πλοήγηση στο διαδίκτυο.

Διδάξτε τους να μην δίνουν προσωπικές πληροφορίες χωρίς την άδειά σας (επίθετο, όνομα ηλικία, διεύθυνση κατοικίας, αριθμό τηλεφώνου, οικογενειακό εισόδημα, ακόμα και ωράρια σχολείου ονόματα φίλων κ.λπ.) και να μην χρησιμοποιούν την κάρτα σας.

Μην επιτρέπετε ποτέ στα παιδιά σας να συναντηθούν με άτομα που γνώρισαν μέσω Διαδικτύου.

Διδάξτε τα επίσης, να αρνούνται από μόνα τους να συναντηθούν προσωπικά με άτομα που έχουν γνωρίσει στο Διαδίκτυο. Εξηγήστε τους ότι οι άγνωστοι με τους οποίους θέλουν να συναντηθούν μπορεί να είναι επικίνδυνοι.

Χρησιμοποιείστε τα λεγόμενα «φίλτρα» που είναι ειδικά προϊόντα λογισμικού με σκοπό την παρεμπόδιση της πρόσβασης σε μη επιθυμητές θέσεις «sites» (βία, πορνογραφία).

Ελέγξτε το περιεχόμενο οπτικοακουστικού υλικού, όπως CDs, δισκέτες κ.α., που αγοράζουν τα παιδιά σας ή ανταλλάσουν με τους φίλους τους.

Ενημερωθείτε σχετικά από τις αρμόδιες αρχές, όπως είναι το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος (τηλ. 210- 6476464), που θα πρέπει να επικοινωνήσετε σε περίπτωση που συναντήσετε βλαβερό ή παράνομο περιεχόμενο στο Internet.

Γονικός έλεγχος στα Windows

Ο Γονικός έλεγχος στα Windows είναι ένα χρήσιμο εργαλείο για να ελέγχετε τον χρόνο που τα παιδιά σας περνάνε μπροστά στον υπολογιστή αλλά και τα προγράμματα που χρησιμοποιούν.

Με ένα τέτοιο πρόγραμμα, μπορείτε να διαχειρίζεστε τα ακόλουθα :

* Τις ιστοσελίδες που μπορούν να προβάλλουν τα παιδιά σας
* Τις ώρες της ημέρας και το χρονικό διάστημα που μπορούν να παραμείνουν στο ίντερνετ.
* Τα παιχνίδια που μπορούν να παίξουν τα παιδιά σας
* Τα προγράμματα που μπορούν να χρησιμοποιήσουν.

Λειτουργεί σε περιβάλλον Windows 7 και Windows Vista.

Αν τώρα διαθέτετε Windows XP, κατεβάστε το “K9 Web Protection" από δω : http://www1.k9webprotection.com/getk9/download-software.php

Η βασική ιδέα είναι να δημιουργηθεί από τους γονείς λογαριασμός χρήστη για τα παιδιά ,ενώ ο γονέας είναι ο διαχειριστής του συστήματος. Στους λογαριασμούς των παιδιών μπορεί να διαχειριστεί και να ρυθμίσει όσα αναφέρθηκαν παραπάνω.

Ενεργοποίηση γονικού ελέγχου

1. Ακολουθήστε την πορεία : Έναρξη -> Πίνακας ελέγχου -> Λογαριασμοί χρηστών -> Ρύθμιση γονικού ελέγχου. Μπορεί να σας ζητηθεί ένας κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση, πληκτρολογήστε τον κωδικό ή επιβεβαιώστε.
2. Κάντε κλικ στον λογαριασμό για τον οποίο θέλετε να ρυθμίσετε το γονικό έλεγχο.
3. Κάντε κλικ στο “Ενεργός, εφαρμογή τρεχουσών ρυθμίσεων” και “OK”.

Ρυθμίσεις στη μηχανή αναζήτησης Google

Ενεργοποίηση ή απενεργοποίηση Ασφαλούς Αναζήτησης

Επισκεφτείτε τη σελίδα ρυθμίσεων αναζήτησης στη διεύθυνση www.google.gr/preferences.

Στην ενότητα "Φίλτρα Ασφαλούς Αναζήτησης" , επιλέξτε το πλαίσιο δίπλα από το στοιχείο "Φιλτράρισμα ακατάλληλων αποτελεσμάτων" για να φιλτράρονται βίντεο και εικόνες με ακατάλληλο σεξουαλικό περιεχόμενο από τις σελίδες αποτελεσμάτων Αναζήτησης Google, καθώς και αποτελέσματα που ενδέχεται να περιλαμβάνουν συνδέσμους προς ακατάλληλο περιεχόμενο. Αν δεν επιλέξετε αυτό το πλαίσιο, θα παρέχονται τα πιο σχετικά αποτελέσματα για το ερώτημά σας και ενδέχεται να εμφανίζεται ακατάλληλο περιεχόμενο όταν πραγματοποιείτε αναζήτηση για αυτό.

Ρυθμίστε σε ποιο βαθμό θα πρέπει να φιλτράρει η Ασφαλής Αναζήτηση το σκληρό σεξουαλικό περιεχόμενο (ιστοσελίδες, εικόνες και βίντεο) από τα αποτελέσματά σας.

Κάντε κλικ στην επιλογή **Αποθήκευση** στο κάτω μέρος της σελίδας.

Αν είστε συνδεδεμένοι στο Λογαριασμό σας Google, μπορείτε επίσης να κλειδώσετε το φίλτρο Ασφαλούς Αναζήτησης για να μην μπορεί να αλλάξει από άλλους χρήστες. Κάντε κλικ στην επιλογή **Κλείδωμα Ασφαλούς Αναζήτησης**.

Ασφαλής λειτουργία στο youtube

Η ασφαλής λειτουργία είναι μια προαιρετική ρύθμιση που σας βοηθά να αποκλείσετε πιθανώς προσβλητικό περιεχόμενο το οποίο μπορεί να μην θέλετε να βλέπετε εσείς ή κάποιο άλλο μέλος της οικογένειάς σας, όταν απολαμβάνετε το YouTube.

Τρόπος ενεργοποίησης της ασφαλούς λειτουργίας:

Μεταβείτε στο κάτω μέρος μιας σελίδας του YouTube και κάντε κλικ στο αναπτυσσόμενο μενού της ενότητας "Ασφάλεια".

Επιλέξτε "Ενεργοποιημένο" ή "Απενεργοποιημένο" για ενεργοποίηση ή απενεργοποίηση της λειτουργίας.

Τρόπος κλειδώματος της ασφαλούς λειτουργίας:

Αν θέλετε να είναι ενεργοποιημένη η ασφαλής λειτουργία κάθε φορά που επισκέπτεστε το YouTube, πρέπει να την κλειδώσετε.

Συνδεθείτε στο λογαριασμό σας στο YouTube.

Μεταβείτε στο κάτω μέρος μιας σελίδας του YouTube και κάντε κλικ στο αναπτυσσόμενο μενού της ενότητας "Ασφάλεια".

Αν ενεργοποιήσετε τη λειτουργία, θα εμφανιστεί μια πρόσθετη επιλογή κλειδώματος της ασφαλούς λειτουργίας στο συγκεκριμένο πρόγραμμα περιήγησης.

Για τους εκπαιδευτικούς και τους γονείς

s@ferinternet.gr

Διαδίκτυο και υπερβολική ενασχόληση

- Η πρόληψη από την «εξάρτηση» στο Διαδίκτυο είναι εύκολη, αρκεί να λάβετε εγκαίρως υπόψη σας τα σημάδια που δείχνει ένα παιδί και να **ζητήσετε άμεσα βοήθεια από τους ειδικούς.**

- Ως εκπαιδευτικός μπορείτε να βοηθήσετε στον εντοπισμό των παιδιών που οδεύουν προς την εξάρτηση από το Διαδίκτυο, καθώς γνωρίζετε τις καθημερινές τους συνήθειες και μπορείτε άμεσα να δείτε αλλαγές στον τρόπο συμπεριφοράς. Έτσι λοιπόν, **αν παρατηρήσετε τα παρακάτω συμπτώματα:**

  - » Εκνευρισμός όταν το παιδί είναι εκτός Διαδικτύου
  - » Χρήση του Διαδικτύου πολύ περισσότερο από το προτιθέμενο
  - » Ξαφνική σχολική αποτυχία
  - » Διαταραχές ύπνου και αλλαγή των συνηθειών ύπνου/κούραση και υπνηλία μέσα στην τάξη
  - » Μειωμένη φυσική δραστηριότητα
  - » Διαταραχή στις διαπροσωπικές σχέσεις
  - » Αλλαγή των συνηθειών του παιδιού, όπως π.χ. παραμέληση φίλων, αγαπημένων χόμπι
  - » Παραμέληση της προσωπικής υγιεινής

επικοινωνήστε άμεσα με τη **Γραμμή Βοηθείας ΥποΣΤΗΡΙΖΩ 800 11 800 15 / help@saferinternet.gr** του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου.

Ακρωνύμια και emoticons

Σε αίθουσες ανοιχτής επικοινωνίας (τα λεγόμενα «chat rooms») ή στα ηλεκτρονικά μηνύματα γίνεται πολύ συχνά χρήση συντομεύσεων. Οι συντομεύσεις αυτές είναι κατά κύριο λόγο στην αγγλική γλώσσα. Ο παρακάτω πίνακας περιλαμβάνει μερικά από τα πιο συνηθισμένα **ακρωνύμια**, με στόχο να μπορείτε από εδώ και στο εξής να τα αναγνωρίζετε στις διαδικτυακές επικοινωνίες των παιδιών σας και όχι μόνο:

^5	High 5 (κόλλα το)
24/7	24 ώρες την μέρα, 7 μέρες τη βδομάδα
3RS	Xeris (ξέρεις)
8LS	Thelis (θέλεις)
ANW	Any way (τέλος πάντων)
ASAP	As soon as possible (το συντομότερο δυνατόν)
ASL ή A/S/L	Age, Sex, Location (ηλικία, φύλο, τοποθεσία)
AFK	Away from keyboard (δεν είμαι κοντά σε πληκτρολόγιο)
B/c	Because (επειδή)
B4N	Bye for now (χαιρετώ για την ώρα)
BBL	Be back later (θα γυρίσω αργότερα)
BRB	Be right back (γυρίζω αμέσως)
BTW	By the way (παρεμπιπτόντως)
C	See? (βλέπεις;)
Comp	Computer (υπολογιστής)
CU	See you (τα λέμε)
CUL	See you later (τα λέμε αργότερα)
F2F	Face to Face (πρόσωπο με πρόσωπο)
FAQ	Frequently asked questions (συχνές ερωτήσεις)
JJ	Just joking (αστειεύομαι)
GL	Good luck (καλή τύχη)
GM	Good morning (καλημέρα)
GNT	Ginete (γίνεται)
GT	Giati (γιατί)

G2G / GTG	Got to go (πρέπει να φύγω)
IC	Ise (είσαι)
IDK	I don't know (δεν ξέρω)
L8R	Later (αργότερα)
LMIRL	Let's meet in real life (ας συναντηθούμε)
LOL	Laugh out loud (γελάω δυνατά)
LY4E	Love you forever (σ' αγαπώ για πάντα)
MLM	Milame (μιλάμε)
MR	Moro (μωρό)
MT	Meta (μετά)
MZ	Mazi (μαζί)
NA GN	Na gini (να γίνει)
NMZ	Nomizo (νομίζω)
NP	No problem (κανένα πρόβλημα)
PAL	Parents are listening (ακούνε οι γονείς μου)
PAW	Parents are watching (με παρακολουθούν (γονείς)
PLS	Please (παρακαλώ)
POS	Parent Over Shouler (γονέας από πίσω μου)
S^, S'UP	What's up? (τι γίνεται;)
SRY	Sorry (συγγνώμη)
THLS	Thelis (θέλεις)
THNX	Thanks (ευχαριστώ)
TLK	Telika (τελικά)
TPT	Τίποτα (τίποτα)
TR	Tora (τώρα)
TTYL	Talk to you later (τα λέμε αργότερα)
W8	Wait (περίμενε)
WB	Welcome back (καλώς ήλθες πίσω)
WTGP	Want to go private? (θέλεις να μιλήσουμε σε ιδιωτικό χώρο;)
WYCM	Will you call me? (Θα μου τηλεφωνήσεις)

Τα **emoticons** είναι εικονίδια που έχουν ως στόχο να συμβολίσουν κάποιο ιδιαίτερο συναίσθημα. Τα σύμβολα emoticons αποτελούνται από χαρακτήρες οι οποίοι, όταν πληκτρολογούνται σε συνέχεια και διαβάζονται με το κεφάλι γυρισμένο 90 μοίρες προς τα αριστερά, θυμίζουν συγκεκριμένες γκριμάτσες της γνωστής φιγούρας «Smiley». Έτσι π.χ. το emoticon :-) σημαίνει χαρά.

Μερικά από τα emoticons που χρησιμοποιούνται ευρέως σε ηλεκτρονικά μηνύματα, σε chat rooms, κ.λπ. είναι τα παρακάτω:

:-)	χαμόγελο
:-(	λύπη
;-)	κλείνω το μάτι
:-O	έκπληξη
:-p	βγάζω τη γλώσσα
0 :-)	άγγελος
:-*	φιλάκι
:-#	κρατάω μυστικό
%-I	μπερδεμένος
>:-(	κακία / νεύρα
8-)	φοράω γυαλιά
QQ	δάκρυα

Χρήσιμες ιστοσελίδες για την ασφάλεια στο Διαδίκτυο

http://www.saferinternet.gr
Δράσης Ενημέρωσης και Επαγρύπνησης
του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου

http://www.safeline.gr
Ανοιχτή Γραμμή Καταγγελιών παράνομου περιεχομένου
στο Διαδίκτυο – Ελληνικό Κέντρο Ασφαλούς Διαδικτύου

http://www.saferinternet.gr/helpline
Γραμμή Βοηθείας ΥποΣΤΗΡΙΖΩ 800 11 800 15
Ελληνικού Κέντρου Ασφαλούς Διαδικτύου

http://internet-safety.sch.gr
Ασφάλεια στο Διαδίκτυο - Ενημερωτικός Κόμβος Π.Σ.Δ.

http://www.kidsatsafety.gr
Kids@Safety Internet, Κινητό & Παιδί

http://www.google.gr/familysafety/
Κέντρο οικογενειακής ασφάλειας

http://www.pegi.info/gr/
Πανευρωπαϊκό σύστημα κατάταξης
για τα ηλεκτρονικά παιχνίδια

Βιβλιογραφία-πηγές

- http://www.saferinternet.gr
- Ιστοσελίδα Ελληνικής Αστυνομίας
- Διάφορα αρχεία από το Διαδίκτυο
- Εκπαιδευτικά εγχειρίδια