΄Ενα Ασφαλές Διαδίκτυο για ΄Ολους

Ασφάλεια και Εθισμός στο Διαδίκτυο και οι Κοινωνικές Επιπτώσεις του

Μια Μηνιαία Ηλεκτρονική ΄Εκδοση της Ελληνικής Καταναλωτικής Οργάνωσης (Ε.ΚΑΤ.Ο.) Φλώρινας

Τεύχος 29
Μάιος
2011

Περιεχόμενα

Από τη Σύνταξη

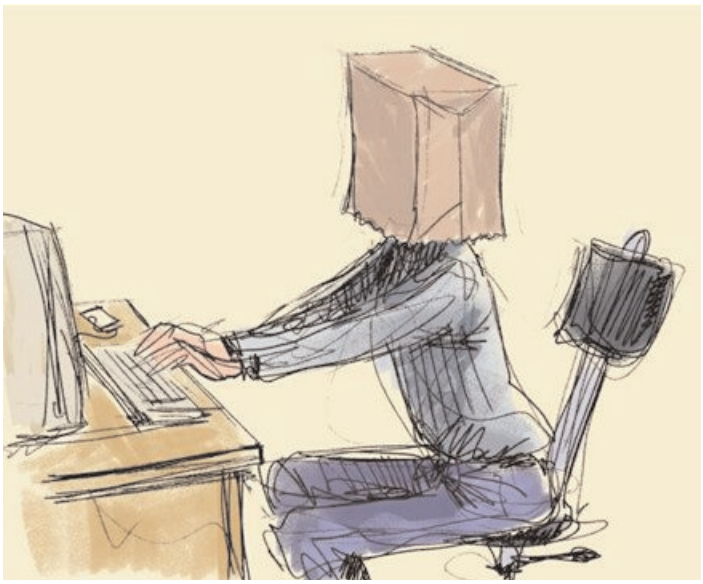
Στο τεύχος αυτό συνεχίζουμε τη δημοσίευση των εκθέσεων που έγραψαν μαθητές από Γυμνάσια της Π.Ε. Φλώρινας (4η έκθεση) για τη συμμετοχή τους στον 2ο Διαγωνισμό για το Ασφαλές Διαδίκτυο. Επίσης, συνεχίζουμε με τις ενδιαφέρουσες δημοσιεύσεις του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου (Συχνές Ερωτήσεις και Απαντήσεις για την Ασφαλή Χρήση του Διαδικτύου) και της μελέτης για την Επιρροή της Ασύρματης Ακτινοβολίας στους Ανθρώπους (3ο Μέρος). Ακόμα, φιλοξενούμε δύο άρθρα από το Πανελλήνιο Σχολικό Δίκτυο και τον Ενημερωτικό Κόμβο που διαθέτει σχετικά με την Ασφάλεια στο Internet (Κυβερνοπόλεμος και "Κατασκοπεία" στο Facebook) και την πρόσφατη ανακοίνωση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για τα μηνύματα spam.

Για το Δ.Σ. της Ε.ΚΑΤ.Ο. Φλώρινας
Ο Γενικός Γραμματέας - Στυλιάδης Κων/νος - styliadis στο sch.gr

Μέλη Δ.Σ. της Ε.ΚΑΤ.Ο. Φλώρινας
Πρόεδρος : Αλτίνης Αθανάσιος
Γεν. Γραμματέας : Στυλιάδης Κων/νος
Αντιπρόεδρος : Χρυσοχοΐδης Βασίλειος
Ταμίας : Ντίτουρα Βασιλική

Επικοινωνήστε μαζί μας :
e-mails : styliadis στο sch.gr
altinisa@yahoo.gr
algo17 στο line.gr
ntitoura στο gmail.com

Ταχυδρομική Διεύθυνση
Ελληνική Καταναλωτική Οργάνωση (Ε.ΚΑΤ.Ο.) Φλώρινας
Ι. Καραβίτη 2 - Κτίριο "ΔΙΕΘΝΕΣ"
531 00 Φλώρινα



Σεμινάριο Καταναλωτή στη Δυτική Μακεδονία - Φλώρινα, 14 Μαΐου 2011

Η Ελληνική Καταναλωτική Οργάνωση (Ε.ΚΑΤΟ.) Φλώρινας από κοινού με τον Δικηγορικό Σύλλογο Φλώρινας, την ΄Ενωση Καταναλωτών Καβάλας (ΕΝ.Κ.ΚΑ.) και το Κέντρο Προστασίας Καταναλωτών (ΚΕ.Π.ΚΑ.) Δυτικής Μακεδονίας συνδιοργανώνουν :

Σεμινάριο για Θέματα Καταναλωτή το Σάββατο 14 Μαΐου 2011 και ώρες 5.00 μμ - 9.00 μμ στο Hotel «ΠΛΕΙΑΔΕΣ» στη Φλώρινα

Ομιλητές : *Γεροστεργίου Κατερίνα*, Πρόεδρος ΕΝ.Κ.ΚΑ., *Πασχαλίδης Γιώργος*, Μέλος ΕΝ.Κ.ΚΑ., και *Θεοφύλακτος Ιωάννης*, Πρόεδρος ΚΕ.Π.ΚΑ. Δυτικής Μακεδονίας.

Ενημερωτικός Κόμβος για την Ασφάλεια στο Διαδίκτυο του Πανελλήνιου Σχολικού Δικτύου

Νέα Μορφή Ανταγωνισμού ο Κυβερνοπόλεμος : 2011-04-26

Οι βασιζόμενες στο Διαδίκτυο επιθέσεις σε κεντρικά συστήματα αποφασιστικής σημασίας όπως είναι αυτά του φυσικού αερίου, του ηλεκτρισμού και της υδροδότησης αυξήθηκαν σε όλο τον κόσμο, σύμφωνα με πρόσφατη έκθεση.

Η εταιρεία λογισμικού ασφαλείας Η/Υ McAfee ερεύνησε μεταξύ 200 στελεχών των τεχνολογιών πληροφορικής (IT) που εργάζονται για εταιρείες κοινής ωφέλειας σε 14 χώρες. Οι 8 στους 10 δήλωσαν πως τα δίκτυά τους αποτέλεσαν στόχο των χάκερς πέρσι.

Ως πιθανότερη πηγή των επιθέσεων πιθανολογείται η Κίνα, ακολουθούμενη από τη Ρωσία και τις ΗΠΑ. Ο αριθμός των περιστατικών που αναφέρθηκαν ήταν υψηλότερος από αυτόν του 2009 όταν μόλις το 50% των ερωτηθέντων δήλωσαν πως είχαν πέσει θύμα επίθεσης.

Παρά το γεγονός ότι παρόμοιες επιθέσεις έχουν τη δυνατότητα να προσβάλλουν ιστοσελίδες και εταιρικά δίκτυα, οι ερευνητές δήλωσαν πως θεωρούν απίθανο η πρόθεσή τους να ήταν η διακοπή των ενεργειακών προμηθειών.

Ωστόσο, παραμένει η πιθανότητα οι επιθέσεις αυτές να κάνουν μεγαλύτερη ζημιά στο μέλλον και το 75% πιστεύει πως τη προσεχή διετία θα έχουμε σοβαρές επιθέσεις ικανές να διακόψουν την παροχή υπηρεσιών για τουλάχιστον 24 ώρες, απώλειες ζωής, προσωπικές βλάβες και επιχειρηματικές χρεοκοπίες.

Επίσης, νέος ιντερνετικός ιός απειλεί τα συστήματα του Ιράν. Μετά τον ιό-σκουλήκι *Stuxnet*, οι αρχές του Ιράν ανακοίνωσαν ότι εντόπισαν έναν νέο ιό που έχει ως στόχο να πλήξει τους υπολογιστές των υποδομών της χώρας.

Σύμφωνα με Ιρανούς αξιωματούχους, το κακόβουλο λογισμικό που ονομάστηκε *Stars* ήταν σε θέση να πλήξει τα ιρανικά συστήματα. Σε περίπτωση που οι αναφορές επιβεβαιωθούν, θα είναι η δεύτερη κυβερνοεπίθεση που καταγράφεται μέσα σε μία χρονιά στη χώρα.

Πριν από μερικούς μήνες εντοπίστηκε ο ιός Stuxnet που είχε ως στόχο να πλήξει τις εγκαταστάσεις των πυρηνικών εργοστασίων του Ιράν. Ο νέος ιός εξετάζεται προκειμένου να εντοπιστεί ο σκοπός αλλά και ο δημιουργός του.

Πηγή : *enet.gr*

Λογισμικό για Γονείς «Κατασκόπους» στο Facebook : 2011-04-29

Όλο και μικρότερα σε ηλικία παιδιά χρησιμοποιούν την υπηρεσία κοινωνικής δικτύωσης Facebook και, παράλληλα, αυξάνονται δυνητικά οι online κίνδυνοι. Για το λόγο αυτό, η αμερικανική εταιρία προϊόντων διαδικτυακής ασφάλειας ***Check Point*** κυκλοφόρησε ένα νέο πρόγραμμα λογισμικού, το οποίο επιτρέπει στους γονείς να «εποπτεύουν» (δηλαδή να παρακολουθούν κρυφά) τις δραστηριότητες των παιδιών τους στο κοινωνικό δίκτυο, χωρίς να χρειάζεται να είναι «φίλοι» με το παιδί τους.

Το πρόγραμμα, με την εύγλωττη ονομασία ***«SocialGuard»***, προειδοποιεί έγκαιρα τους γονείς, όταν ανιχνεύσει σημάδια κάποιου προβλήματος στον λογαριασμό του παιδιού τους στο Facebook, χωρίς οι ίδιοι οι γονείς να βλέπουν το περιεχόμενο, που έχει αναρτήσει και γενικά παρακολουθεί το παιδί τους (σχόλια, εικόνες, βίντεο κλπ).

Το λογισμικό ελέγχει διακριτικά, αλλά εξονυχιστικά, τα προφίλ στο Facebook και τις επικοινωνίες μεταξύ «φίλων», χρησιμοποιώντας ειδικούς αλγόριθμους, προκειμένου να εντοπίσει περιπτώσεις ενδεχόμενων απειλών (εκφοβισμών, σεξουαλικών παρενοχλήσεων, συζητήσεων περί ναρκωτικών, βίας, σκέψεων αυτοκτονίας κ.ά.).

Το SocialGuard στέλνει περιοδικά μηνύματα στους υπολογιστές των γονέων, «χτυπώντας καμπανάκι» όταν κάτι τού φαίνεται ύποπτο. Ακόμα, το πρόγραμμα εντοπίζει τη διείσδυση χάκερ, ιών και άλλων κακόβουλων προγραμμάτων στους λογαριασμούς του Facebook.

Επίσης, το λογισμικό -που διατίθεται στη διεύθυνση http://www.zonealarm.com - ελέγχει κατά πόσο οι «φίλοι», που επικοινωνούν online με το παιδί του γονέα, λένε αλήθεια για την ηλικία τους ή αν ένας ξένος επιχειρεί να καμουφλαριστεί σαν «φίλος».

Πηγή :*Έθνος online*

http://internet-safety.sch.gr

Εκθέσεις Μαθητών Γυμνασίων Π.Ε. Φλώρινας
2ος Μαθητικός Διαγωνισμός στην Π.Ε. Φλώρινας :
"Ποιους Κανόνες Πρέπει να Ακολουθώ για Ασφαλή Πλοήγηση;"

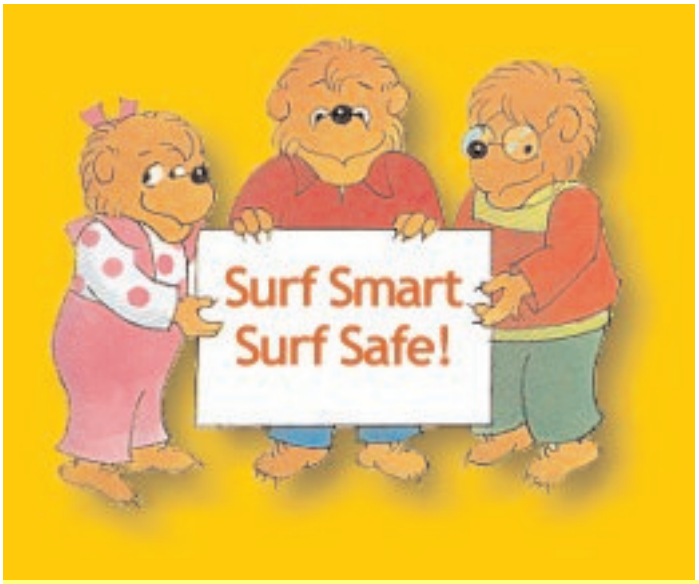
4η Έκθεση

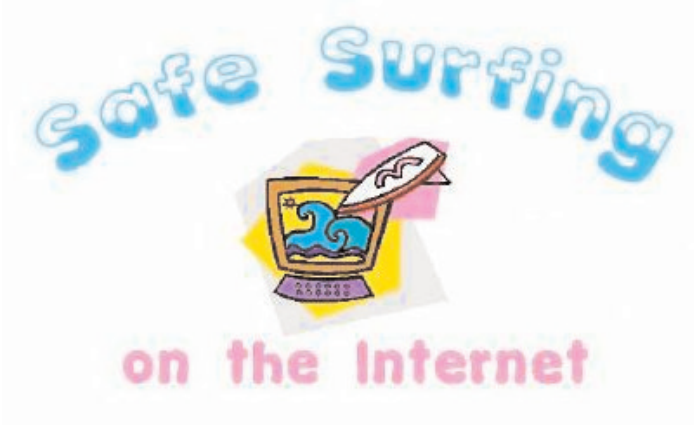
Το Internet είναι ένα θαυμάσιο εργαλείο και μέσο αλλά έχει επίσης και την δυνατότητα να είναι πολύ επικίνδυνο γιατί είναι γεμάτο με ιούς και "αρπακτικά" που επιθυμούν να λυμαίνονται τους αθώους και τους εύπιστους. Γι' αυτό το λόγο υπάρχουν κανόνες που μπορεί ο χρήστης να ακολουθήσει προκειμένου να προστατευτεί κατά την πλοήγηση στο Διαδίκτυο.
Αρχικά θα πρέπει να φροντίσουμε για την εγκατάσταση στον υπολογιστή μας ενός αντιϊκού προγράμματος (antivirus program) το οποίο θα μας προστατεύει από τους περισσότερους ιούς. Αξίζει να αναφερθούμε στο ότι όταν είμαστε συνδεδεμένοι στο Διαδίκτυο θα πρέπει να ενεργοποιούμε ένα πρόγραμμα "τείχους προστασίας" (firewall) ώστε να αποτρέπουμε την ανεπιθύμητη πρόσβαση στον υπολογιστή μας από τρίτους.
Επίσης είναι σημαντικό να τονιστεί η απαραίτητη προσοχή που απαιτείται να δίνουμε στα διάφορα προγράμματα που "τρέχουμε" στον υπολογιστή μας. Συγκεκριμένο παράδειγμα είναι ότι τα προγράμματα των οποίων δεν γνωρίζουμε τον κατασκευαστή ή δεν τα έχουμε προμηθευτεί από το εμπόριο έχουν αυξημένες πιθανότητες να έχουν κάποιο ιό.
Χαρακτηριστική περίπτωση αποτελεί το ότι σε ευαίσθητα και ταυτόχρονα "καυτά" θέματα όπως είναι η ασφάλεια των δεδομένων, η προστασία της ανωνυμίας και φυσικά η προάσπιση του ιδιωτικού απορρήτου, οι όποιες κινήσεις μας απαιτούν προσεκτικό συνδυασμό και μεθοδικότητα.
Ακόμα, δεν ανοίγουμε e-mail από αγνώστους αποστολείς γιατί έχουν συνημμένους ιούς. Επιπρόσθετα είμαστε πολύ προσεκτικοί με τα άτομα τα οποία συνομιλούμε.
Τέλος, ένας από τους σημαντικότερους κανόνες είναι να αποφεύγουμε να δίνουμε προσωπικά δεδομένα σε διάφορες ιστοσελίδες ή σε τρίτους (αριθμός τηλεφώνου/ταυτότητας/πιστωτικής κάρτας, ΑΦΜ, ονοματεπώνυμο κ.ά.).
Τελειώνοντας, καταλήγουμε στο συμπέρασμα ότι ο μόνος τρόπος για να είμαστε πραγματικά σίγουροι για την ασφάλεια και του υπολογιστή μας, η λύση δεν είναι η απόλυτη αποχή αλλά η προσοχή και η εγρήγορση των χρηστών ώστε να μην είναι θύματα κάποιων επιτήδειων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Internet στη σελίδα http://www.e-yliko.gr
2. Internet στη σελίδα http://www.safekids.com

Ρ.Α-Ε, Γυμνάσιο Λεχόβου





Συχνές Ερωτήσεις και Απαντήσεις για την Ασφαλή Χρήση του Διαδικτύου

(Μέρος 3ο)

Ανταλλαγή Αρχείων

6 Η Ανταλλαγή Αρχείων Ταυτίζεται με τα Δίκτυα peer-to-peer;

Ένα δίκτυο peer-to-peer (P2P) είναι μια τεχνολογία που επιτρέπει σε όσους είναι συνδεδεμένοι σε αυτό να ανταλλάσσουν αρχεία. Είναι ένας από τους πολλούς τρόπους με τους οποίους γίνεται ανταλλαγή αρχείων στο Διαδίκτυο. Όμως, χάρη στην ανωνυμία που προσφέρουν, αυτά τα δίκτυα έχουν συχνά συσχετισθεί με την παράνομη ανταλλαγή αρχείων.

Οι υπηρεσίες και η τεχνολογία peer-to-peer χρησιμοποιούνται όλο και περισσότερο από τη βιομηχανία του θεάματος για την παροχή νόμιμων υπηρεσιών περιεχομένου μέσω του Διαδικτύου.

7 Πού Μπορώ να Μάθω Περισσότερα για την Ανταλλαγή Αρχείων και για τα Πνευματικά Δικαιώματα;

Πολλοί οργανισμοί παρέχουν εκτενή πληροφόρηση για τα πνευματικά δικαιώματα και την ανταλλαγή αρχείων. Σας παραθέτουμε μια ενδεικτική λίστα με οργανισμούς και ιστοσελίδες που παρέχουν χρήσιμες πληροφορίες :

" Ελληνική Εταιρεία Προστασίας της Πνευματικής Ιδιοκτησίας ΑΕΠΙ : http://www.aepi.gr

" Ένωση Ελλήνων Παραγωγών Ηχογραφημάτων IFPI : http://www.ifpi.gr

" Ευρωπαϊκή Επιτροπή : http://europa.eu.int/comm/internal_market/

" World Intellectual Property Organisation WIPO : http://www.wipo.int/enforcement/en/

" Motion Picture Association of America MPAA : http://www.mpaa.org/piracy_AndLaw.asp

Blogging

1 Τι Είναι τα weblogs ή blogs;

Η λέξη "weblog" προέρχεται από το συνδυασμό δύο λέξεων : "*Web*" που σημαίνει Διαδίκτυο και "*log*" που σημαίνει καταχώρηση. Συνήθως χρησιμοποιείται η σύντμηση "*blog*". ***Blogging*** ονομάζεται η διαδικασία δημιουργίας και φόρτωσης πληροφοριών σε ένα blog, ενώ ο δημιουργός λέγεται ***blogger***.

Τα *blogs* ή *ιστολόγια*, όπως λέγονται στα Ελληνικά, είναι εικονικά ημερολόγια που αποθηκεύονται στο Διαδίκτυο και μπορούν να δημιουργηθούν πολύ εύκολα από οποιονδήποτε καθώς δεν χρειάζονται ειδικές τεχνικές γνώσεις για τη δημιουργία τους. Τα blogs αποτελούνται γενικά από κείμενο και εικόνες και μπορεί να έχουν μορφή ημερολογίου.

Vlog είναι το blog στο οποίο οι χρήστες δημοσιεύουν και βίντεο εκτός από γραπτά σχόλια. Τα ***Moblog*** ή *Mobile Logs* χρησιμοποιούν δυνατότητες δημοσίευσης υλικού στο Διαδίκτυο μέσω του κινητού τηλεφώνου.

2 Διατρέχω Κάποιον Κίνδυνο αν Δημιουργήσω το Δικό μου blog;

Ένας από τους μεγαλύτερους κινδύνους στα blogs είναι το να μπει κανείς στον πειρασμό να αποκαλύψει προσωπικές πληροφορίες που μπορεί να διαδοθούν σε όλο τον κόσμο και να χρησιμοποιηθούν εις βάρος του (π.χ. κλοπή ταυτότητας). Μπορείτε να χρησιμοποιήσετε κάποιο ψευδώνυμο για να προστατεύσετε την ταυτότητά σας. Να θυμάστε ότι όλοι έχουν δικαίωμα να προστατεύσουν την ιδιωτική τους ζωή. Αν σκοπεύετε να δημοσιεύσετε πληροφορίες και εικόνες για τρίτους, πρέπει πρώτα να πάρετε την άδειά τους.

Ένας ακόμη κίνδυνος είναι η καταπάτηση των πνευματικών δικαιωμάτων. Δεν πρέπει να χρησιμοποιείτε υλικό (π.χ. κείμενο, εικόνα, ήχο, βίντεο) ή σχέδιο blog από ιστοσελίδες άλλων ατόμων χωρίς την άδειά τους. Επίσης, ποτέ μη δημοσιεύετε προσβλητικό (π.χ. ρατσιστικό) ή παράνομο (τζόγος, πορνογραφία κ.ά.) υλικό.

Αναδημοσίευση από το Έντυπο :

"FAQ - Συχνές ερωτήσεις και απαντήσεις για την ασφαλή χρήση του Διαδικτύου", 2η έκδοση – Νοέμβριος 2010

ISBN 978-960-99061-0-4

(συνεχίζεται)

Η Ασύρματη Ακτινοβολία και η Επιρροή της στους Ανθρώπους

Πόση Ακτινοβολία Δεχόμαστε από τις Συσκευές μας και πώς θα Προστατευτούμε

(Μέρος 3ο)

Των ΑΝΤΖΗΣ ΣΑΛΤΑΜΠΑΣΗ, ΚΩΣΤΑ ΔΕΛΗΓΙΑΝΝΗ
Εικονογράφηση : ΝΙΚΟΣ ΚΟΥΡΤΗΣ

Εφημερίδα Καθημερινή (14.11.2009)
http://www.kathimerini.gr/4dcgi/_w_articles_kath-common_100073_14/11/2009_1290367

07.15 - Κινητό Τηλέφωνο
365 Φορές Πάνω Από το Όριο!

Συνήθως η ημέρα μας αρχίζει μ' ένα τηλεφώνημα. Σύμφωνα με τα διεθνή όρια ασφαλείας, η ακτινοβολία δεν πρέπει να ξεπερνά τα 5 με 6 μιλιβάτ/ανά τετραγωνικό μέτρο. Ο οικιακός μετρητής έδειξε 1.827 (!) μιλιβάτ -365 φορές πάνω από το όριο- τη στιγμή που το τηλέφωνο καλούσε, όπως και κατά τη διάρκεια της συνομιλίας ! Να σημειώσουμε ότι στη δική μας μέτρηση η απόσταση μετρητή - κινητού ήταν περίπου 10 εκατοστά, ενώ όταν συνομιλούμε χωρίς hands free, το κινητό εφάπτεται στο κεφάλι και η απόσταση... μηδενίζεται.

Όταν το κινητό φορτίζει, η μέτρηση κυμαίνεται σε φυσιολογικά όρια, ωστόσο οι ειδικοί συμβουλεύουν να μη φορτίζουμε το κινητό δίπλα στο κεφάλι μας. Σε κλειστούς, μικρούς χώρους, όπως το ασανσέρ, το αυτοκίνητο ή τα τούνελ των αυτοκινητοδρόμων, η ακτινοβολία αυξάνεται, καθώς το κινητό προσπαθεί πιο έντονα να "πιάσει" σήμα.

09.30 - Ασύρματο Δίκτυο Internet (Router)
Μην Ξεχνάτε να το Κλείνετε

Η ελευθερία που μας προσφέρει η ασύρματη τεχνολογία είναι πολύ σημαντική, ενώ το γεγονός ότι αποφεύγουμε τα ενοχλητικά καλώδια την κάνει ακόμη πιο δημοφιλή. Το απαραίτητο router τοποθετείται τις περισσότερες φορές στο γραφείο ή σε οποιοδήποτε άλλο σημείο υπάρχει υποδοχή τηλεφώνου, συχνά δίπλα στον καναπέ, όπου περνάμε τη μισή ημέρα, ή ακόμα χειρότερα στην κρεβατοκάμαρα. Στο σπίτι, όπου έγινε η μέτρηση, το router είναι τοποθετημένο σ' ένα ντουλάπι δίπλα στο κρεβάτι. Η μέτρηση έδειξε 15,20 μιλιβάτ, τριπλάσια από το όριο, σε απόσταση 10 εκατοστών, ενώ δίπλα στην κεραία η ακτινοβολία άγγιξε τα 578 μιλιβάτ (100 φορές μεγαλύτερη του ορίου)! Υπολογίστε ότι αυτό το ποσό εκπέμπεται συνεχώς, όσο το router παραμένει αναμμένο - ακόμη κι όταν δεν χρησιμοποιείτε το Internet. Άρα, μπορεί η ακτινοβολία να είναι μικρότερη του κινητού π.χ., όμως τη λαμβάνετε συνεχώς.

14.00 - Ασύρματος Back Server
Μακριά του Όσο Λειτουργεί

Πρόκειται για ένα σκληρό δίσκο, ο οποίος συνδέεται ασύρματα με τον υπολογιστή μας και κάνει back-up στα πολύτιμα αρχεία μας. Η θέση του συνήθως είναι πάνω στο γραφείο μας, αλλά στο σπίτι όπου έγινε η μέτρηση οι οικοδεσπότες τον είχαν τοποθετήσει κάτω από το κρεβάτι τους.

Και οι δύο αυτές θέσεις είναι ακατάλληλες, αφού η μέτρηση έδειξε 15,20 μιλιβάτ, τρεις φορές πάνω από το όριο. Η συσκευή εκπέμπει ακτινοβολία φυσικά την ώρα που λειτουργεί, λαμβάνοντας ασύρματα και αποθηκεύοντας τα αρχεία σας. Την ώρα που αυτό συμβαίνει, καλό είναι να είστε μακριά από τη συσκευή. Όταν την έχετε κλειστή, μπορείτε να την τοποθετείτε οπουδήποτε θέλετε.

16.00 - Φούρνος Μικροκυμάτων
Από Μακριά κι Αγαπημένοι

Μεσημέρι έφτασε, ώρα για φαγητό. Από τις πλέον δημοφιλείς οικιακές συσκευές στις σύγχρονες κουζίνες είναι ο φούρνος μικροκυμάτων, που προσφέρει ευκολία και χρόνο. Συχνά μάλιστα δεν τον χρησιμοποιούμε μόνο για να ζεστάνουμε για λίγο το φαγητό μας, αλλά για πολύ περισσότερη ώρα, προκειμένου να ξεπαγώσουμε τρόφιμα, να ψήσουμε ή να ζεστάνουμε νερό. Ειδικά δε τα τελευταία χρόνια, στις καινούργιες κουζίνες, η θέση του βρίσκεται περίπου στο ύψος του κεφαλιού και συνήθως όση ώρα λειτουργεί στεκόμαστε μπροστά του σε μικρή απόσταση. Η μέτρησή μας έδειξε 11,53 μιλιβάτ, διπλάσια του ορίου, σε μια απόσταση 20 - 30 εκατοστών. Εν ολίγοις : αφήστε τον να δουλεύει μόνος του, όση ώρα λειτουργεί καλό είναι να απομακρύνεστε, και εσείς και κυρίως τα μικρά παιδιά. Αυξημένη σε σχέση με τα επιτρεπτά όρια είναι η ακτινοβολία που εκπέμπει και ο συμβατικός φούρνος όταν λειτουργεί, οπότε καλό είναι και σε αυτή την περίπτωση να κάνετε το ίδιο.

(συνεχίζεται)

Φραγμός στα Spam e-mails με Οδηγία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Φραγμούς στα διαφημιστικά email, sms και mms, αλλά και τις διαφημιστικές τηλεφωνικές κλήσεις και τα fax, τα λεγόμενα spam, θέτει με οδηγία της η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Σκοπός της οδηγίας αυτής, είναι η ταυτοποίηση του χρήστη ο οποίος επιθυμεί να λαμβάνει spam για την προώθηση προϊόντων ή υπηρεσιών. Ειδικότερα, με την εν λόγω οδηγία επιδιώκεται η εφαρμογή ενός συστήματος ("opt-out") το οποίο για την αποστολή spam απαιτεί την προηγούμενη ρητή συγκατάθεση του αποδέκτη του διαφημιστικού email, sms, κ.λπ.

Αντίθετα, κατ' εξαίρεση, επιτρέπεται η αποστολή spam χωρίς τη συγκατάθεση του αποδέκτη, υπό την προϋπόθεση ότι ο αποστολέας απέκτησε τα στοιχεία της ηλεκτρονικής διεύθυνσης του αποδέκτη νομίμως, στο πλαίσιο προηγούμενης παρόμοιας συναλλαγής και υπό την πρόσθετη προϋπόθεση ότι παρέχει στον αποδέκτη τη δυνατότητα να ασκήσει το δικαίωμα αντίρρησης, με τρόπο εύκολο και σαφή (σύστημα "opt-out").

Ακόμη, ο χρήστης που ενδιαφέρεται να λαμβάνει διαφημιστικά email, κ.λπ. πρέπει να το δηλώνει γραπτά ή με ηλεκτρονικό τρόπο και η δήλωσή του μπορεί να ανακαλείται οποτεδήποτε.

Επίσης, όταν ο συνδρομητής ή χρήστης δηλώνει τη συγκατάθεσή του για την αποστολή διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου σε συγκεκριμένη ηλεκτρονική διεύθυνση, ο υπεύθυνος επεξεργασίας οφείλει κατ' αρχάς να επιβεβαιώνει ότι ο συνδρομητής ή χρήστης έχει πρόσβαση στη διεύθυνση αυτή.

Η δήλωση συγκατάθεσης στην περίπτωση αυτή γίνεται, είτε με την αποστολή μηνύματος ηλεκτρονικού ταχυδρομείου από την ηλεκτρονική διεύθυνση του συνδρομητή ή χρήστη σε ηλεκτρονική διεύθυνση του υπεύθυνου επεξεργασίας, είτε με άλλο τρόπο, όπως π.χ. μέσω της ιστοσελίδας του υπεύθυνου επεξεργασίας.

Η ίδια επιβεβαίωση, για τη συγκατάθεση αποστολής μηνυμάτων, ακολουθείται και για την αποστολή sms και mms στα κινητά τηλέφωνα, όπως και για τα μηνύματα μέσω fax σε σταθερά τηλέφωνα.

Τέλος, η οδηγία, στην οποία περιλαμβάνονται τεχνικά μέτρα για την αποφυγή μαζικής αποστολής μηνυμάτων, συνοδεύεται από παράρτημα με παραδείγματα εφαρμογής των ορθών πρακτικών αποστολής spam.

http://www.nooz.gr 2 Μαι 2011

Πηγή : ΑΠΕ- ΜΠΕ, Π. Τσιμπούκης

Δικτυωμένοι από Κούνια οι Ευρωπαίοι Έφηβοι http://www.techit.gr 27 Απρ 2011

Όταν ακούει κανείς μαμάδες να ρωτάνε πώς να γραφτούν στο Facebook για να καταλάβουν τι κάνουν τα παιδιά τους τόσες ώρες συνδεδεμένα στο Internet, δεν χρειάζεται καμία επίσημη έρευνα για να δείξει την εξάπλωση του Facebook. Μόλις ήρθε όμως και η τελευταία επιβεβαίωση από το ***eukidsonline.net***, το ερευνητικό πρόγραμμα που μελετά τις διαδικτυακές συνήθειες των παιδιών στην Ευρώπη.

Σύμφωνα με τη στατιστική έρευνα για το πόσο χρησιμοποιούν οι έφηβοι τα μέσα κοινωνικής δικτύωσης, οι Έλληνες έφηβοι είναι από τους πιο κολλημένους με το Facebook. Δεν απέχουν βέβαια πολύ από τους συνομηλίκους τους στις άλλες 24 χώρες που συμπεριλαμβάνονται στην έρευνα.

Ο ηλικιακός περιορισμός που θέτουν τα περισσότερα δίκτυα για την εγγραφή, δεν φαίνεται να αποτρέπει επαρκώς τα παιδιά, που σύμφωνα με το δημοσίευμα της Κυριακάτικης Ελευθεροτυπίας, συχνά δηλώνουν ψεύτικη ηλικία για να δικτυωθούν "*όπως οι μεγάλοι*".

Σε ποσοστό 77% στις ηλικίες 13-16 και 38% στα 9-12 είναι γραμμένα τουλάχιστον σε ένα δίκτυο. Σε 15 από τις 25 χώρες τα μικρότερα παιδιά είναι πιθανότερο να αφήσουν δημόσιο το προφίλ τους όπου αναρτούν προσωπικές πληροφορίες. Σε όσες χώρες οι γονείς εμφανίζονται αυστηρότεροι, θέτοντας απαγορεύσεις, τα μικρότερα παιδιά φαίνεται πως υπακούουν. Μετά τα 13 όμως, περίπου οι μισοί έφηβοι διατηρούν λογαριασμούς παρακούοντας τους γονείς.

Θέματα Ασφάλειας στο Internet

Έρευνα από Δημοσιεύματα του Ελληνικού Τύπου

Οι Παιδόφιλοι στον Ιστό της "Αράχνης"

Το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής παρέλαβε τον Οκτώβριο του 2010 ένα ειδικό λογισμικό από το FBI με την κωδική ονομασία "***Αράχνη***". Το ειδικό αυτό πρόγραμμα αποτελεί τη μεγαλύτερη διαδικτυακή επιχείρηση εντοπισμού πορνογραφικού υλικού σε παγκόσμιο επίπεδο και οι αμερικανικές διωκτικές αρχές τού έχουν δώσει την ονομασία "***Operation FairPlay***", ενώ στην επιχείρηση αυτή ήδη συμμετέχουν οι περισσότερες ευρωπαϊκές αστυνομίες.

Ο τζίρος από την παιδική πορνογραφία στο Internet εκτιμάται ότι μόνο για το 2009 έχει ξεπεράσει τα 500 δισεκατομμύρια ευρώ παγκοσμίως και θεωρείται ως ένας από τους πιο κερδοφόρους εγκληματικούς τομείς. Το ιδιαίτερο με το λογισμικό "Αράχνη" είναι ότι οι Αμερικανοί πράκτορες του FBI έχουν καταχωρίσει σ' αυτό όλες τις φωτογραφίες, τα βίντεο και άλλα αρχεία που έχουν κατορθώσει να εντοπίσουν απ' όλο τον κόσμο και τα οποία περιέχουν παιδοφιλικό υλικό. Το κάθε ηλεκτρονικό αρχείο από τα προηγούμενα διαθέτει τον δικό του μοναδικό αριθμό αναγνώρισης.

Όταν κάποιος χρήστης του Internet στείλει ή παραλάβει ένα από τα παραπάνω σημαδεμένα αρχεία με παιδοφιλικό υλικό, αμέσως το πρόγραμμα"Αράχνη" ειδοποιεί την Αστυνομία τόσο για το ποιος είναι ο αποστολέας όσο και για το ποιος είναι ο παραλήπτης. Το σύνολο των αρχείων με παιδοφιλικό υλικό που είναι καταχωρημένα στο υπόψιν λογισμικό ξεπερνά τα 30 εκατομμύρια, κυρίως φωτογραφίες και βίντεο. Το λογισμικό ενημερώνεται σε καθημερινή βάση και σε απευθείας σύνδεση διοχετεύει τις νέες πληροφορίες στις αστυνομίες που είναι χρήστες του συστήματος.

Η "Αράχνη" μπορεί να καταγράψει την IP διεύθυνση του αποστολέα και του παραλήπτη και στη συνέχεια με εισαγγελική εντολή ο Πάροχος Υπηρεσιών Διαδικτύου (ISP) παραδίδει τα στοιχεία αυτά στην αρμόδια Αστυνομία. Είναι μάλιστα χαρακτηριστικό ότι δεν είναι λίγες οι περιπτώσεις που οι παιδόφιλοι χρησιμοποιούν ξεκλείδωτα ασύρματα οικιακά δίκτυα (WiFi) για να διακινήσουν το υλικό τους, με αποτέλεσμα να εμφανίζεται ως διακινητής ο ιδιοκτήτης του ασύρματου δικτύου, που προφανώς δεν έχει καμία εμπλοκή στην όλη υπόθεση.

Είναι γνωστό ότι στη χώρα μας τιμωρείται ακόμα και η κατοχή παιδοφιλικού υλικού, με ανώτερη προβλεπόμενη ποινή τα 7 χρόνια, αλλά εξαιτίας των πολύ αργών ρυθμών απονομής της Δικαιοσύνης, οι δράστες δεν τιμωρούνται στην πλειονότητα των περιπτώσεων και ελάχιστες έως καμία υποθέσεις έχουν τελεσιδικήσει από τις 558 δικογραφίες που έχουν ολοκληρωθεί.

Για να αντιμετωπιστεί αυτή η καθυστέρηση στην απονομή της Δικαιοσύνης, μία πρόταση των ειδικών είναι να δημοσιοποιούνται τα ονόματα των παιδόφιλων αμέσως μετά την καταδίκη τους και μία άλλη είναι η εφαρμογή του βρετανικού μοντέλου, όπου ενημερώνονται οι κάτοικοι της περιοχής στην οποία κατοικεί ένα παιδόφιλος για τις πράξεις του γείτονά τους.

"ΤΑ ΝΕΑ" 15 Οκτ 2010

Οι Γερμανοί Είπαν "Nein" στο Street View του Google

Η Γερμανία είναι ίσως η πρώτη ευρωπαϊκή χώρα που οι κάτοικοί της είπαν σε μεγάλο ποσοστό ΟΧΙ στην εμφάνιση των σπιτιών τους στο δημοφιλές αλλά και αμφιλεγόμενο πρόγραμμα Street View του Google. Πιο συγκεκριμένα, περισσότεροι από 244.000 Γερμανοί ζήτησαν να μην φαίνονται οι οικείες τους στο Street View και τα αιτήματα αυτά ανέρχονται στο 3% του συνολικού αριθμού των νοικοκυριών στις 20 μεγαλύτερες πόλεις της Γερμανίας καθώς θεωρούν ότι η δημοσιοποίηση στο Internet εικόνων από ιδιωτικές κατοικίες παραβιάζει την ιδιωτική ζωή.

Περιοδικό "Ταχυδρόμος" 6 Νοε 2010

Παγιδευμένα στο Διαδίκτυο τα Ελληνόπουλα

Σημαντικά είναι τα συμπεράσματα μιας πανευρωπαϊκής μελέτης του Οργανισμού ***EU Kids Online***, σύμφωνα με τα οποία ένα στα τρία Ελληνόπουλα διαθέτει ηλεκτρονικό προφίλ στις ιστοσελίδες κοινωνικής δικτύωσης που είναι ορατό από όλους τους άλλους χρήστες (ανοιχτό προφίλ). Είναι επίσης χαρακτηριστικό ότι πολλά παιδιά αναγράφουν ψευδή η-

Θέματα Ασφάλειας στο Internet

Έρευνα από Δημοσιεύματα του Ελληνικού Τύπου

λικία στο προφίλ τους καθώς η διατήρηση προφίλ σε πολλές από τις ιστοσελίδες αυτές επιτρέπεται μόνο από την ηλικία των 13 ετών και άνω.
Σύμφωνα πάντα με τα συμπεράσματα της παραπάνω μελέτης, προφίλ σε ιστοσελίδες κοινωνικής δικτύωσης στη χώρα μας διαθέτει το 70% των παιδιών ηλικίας 13 έως 16 ετών αλλά και το 33% των παιδιών 9 έως 12 ετών. Επίσης, ένα ποσοστό παιδιών από 10% έως 14%, ανάλογα με την ηλικία, αναγράφουν πλήρη στοιχεία στο προφίλ τους, όπως είναι η διεύθυνση του σπιτιού τους, το τηλέφωνο ή το σχολείο στο οποίο φοιτούν. Πολλά είναι τα παιδιά που διαθέτουν περισσότερους από 100 εικονικούς "φίλους" στις ιστοσελίδες αυτές, με τους περισσότερους από τους οποίους δεν έχουν συναντηθεί ποτέ στην πραγματική ζωή.
"ΤΑ ΝΕΑ" 20 Απρ 2011

Ζωντανές Εκπομπές από το YouTube

Η πολύ δημοφιλής ιστοσελίδα παρακολούθησης βίντεο YouTube θα προσφέρει σύντομα και σε απλούς χρήστες τη δυνατότητα να αναμεταδίδουν δωρεάν αθλητικές αναμετρήσεις, συναυλίες αλλά και συνέδρια και γενικότερα ζωντανές τηλεοπτικές εκπομπές. Αν και υπάρχουν ήδη ιστοσελίδες που παρέχουν υπηρεσίες *live streaming*, η δημοτικότητα και η υποδομή που διαθέτει το YouTube υπόσχονται ήχο και εικόνα πολύ υψηλού επιπέδου.
"Η Καθημερινή" 17 Απρ 2011

Απόλυση Λόγω Εθισμού στο Facebook

Με την υπ' αριθμ. 34/2011 απόφασή του, το Πρωτοδικείο Αθηνών έκρινε ότι οι επισκέψεις εργαζομένων στο Facebook αλλά και σ' άλλες σχετικές ιστοσελίδες κατά την ώρα εργασίας αποτελούν νόμιμο λόγο καταγγελίας της σύμβασης εργασίας και μάλιστα χωρίς αποζημίωση. Με την παραπάνω απόφασή του, το Πρωτοδικείο Αθηνών δικαίωσε αεροπορική εταιρεία που είχε απολύσει κάποια υπάλληλό της επειδή αυτή επισκεπτόταν καθημερινά και επί πολλές ώρες διάφορες ιστοσελίδες.
Το Πρωτοδικείο έκρινε επίσης ότι η απόλυση της εργαζομένης έγινε νόμιμα και στα πλαίσια του καλώς νοούμενου συμφέροντος της εργοδότριας επιχείρησης καθώς πραγματικό κίνητρο της καταγγελίας της σύμβασης ήταν η πλημμελής και μη προσήκουσα άσκηση των συμβατικών υποχρεώσεων της εργαζομένης, η οποία δημιούργησε προβλήματα στην ομαλή και αποδοτική άσκηση της εργασίας της.
"ΤΑ ΝΕΑ" 19 Απρ 2011
"ΠΟΛΙΤΗΣ" (Φλώρινα) 21 Απρ 2011

Η Νέα Νιγηριανή Απάτη

Αν τυχόν λάβετε ένα e-mail από έναν πολύ στενό σας φίλο με περιεχόμενο όπως το παρακάτω *"Βρίσκομαι στην Αγγλία για κάτι πολύ επείγον αλλά μου έκλεψαν το πορτοφόλι και όλα τα προσωπικά μου έγγραφα. Η τηλεφωνική επικοινωνία είναι αδύνατη. Καταθέστε στον παρακάτω λογαριασμό όσα χρήματα μπορείτε και θα σας τα επιστρέψω μόλις γυρίσω πίσω..."*, είναι πολύ πιθανό ο φίλος σας να έχει πέσει θύμα μιας νέας νιγηριανής απάτης, που μετράει ήδη αρκετές εκατοντάδες θύματα και στη χώρα μας. Εσείς, φυσικά, δεν θα πρέπει να βιαστείτε να καταθέσετε χρήματα στον υποτιθέμενο λογαριασμό, γιατί είναι σίγουρο ότι δεν θα τα πάρετε πίσω.
Το θέμα είναι βέβαια πώς μπόρεσαν οι διαδικτυακοί απατεώνες να αποκτήσουν τον έλεγχο (στην ουσία τον κωδικό πρόσβασης) του ηλεκτρονικού ταχυδρομείου του φίλου σας. Μια περίπτωση είναι να σταλεί στον κάτοχο ενός e-mail ένα προειδοποιητικό μήνυμα όπου δήθεν ο πάροχός του (ISP) τού ζητάει να κάνει επιβεβαίωση του κωδικού πρόσβασης (password) για να γίνει αναβάθμιση του λογαριασμού του. Αν κάνει το λάθος και δώσει τον μυστικό κωδικό, τότε ανοίγει την κερκόπορτα στους ψηφιακούς απατεώνες. Το πρόβλημα με τις ψηφιακές απάτες είναι ότι αυτές συνεχώς εξελίσσονται και τα κείμενά τους γίνονται όλο και πιο πειστικά και αληθοφανή.
"ΤΑ ΝΕΑ" 15 Οκτ 2010