«Τα διαδικτυακά εκλήματα στα προσωπικά δεδομένα. Συμβουλές προστασίας για ασφαλή πλοήγηση»

Κωνσταντίνος Σχοινάς,

εκπαιδευτικός δευτεροβάθμιας εκπαίδευσης
Ελληνογαλλικής Σχολής Ευγένιος Ντελακρουά
kostasalgo@gmail.com

ΠΕΡΙΛΗΨΗ

Το διαδίκτυο, η μεγαλύτερη δεξαμενή πληροφοριών στον κόσμο, είναι ανοιχτό τόσο στους καλόβουλους όσο και στους κακόβουλους επισκέπτες. Ο πληθυσμός του Internet, αν και έχει δεχτεί κατά καιρούς πολλές παραβιάσεις και παρενοχλήσεις όσον αφορά την ασφάλεια των συστημάτων και την κλοπή δεδομένων, δεν έχει υιοθετήσει μια ολοκληρωμένη εκπαίδευση σε θέματα που αφορούν τη δικτυακή ασφάλεια, με αποτέλεσμα ολοένα και περισσότεροι χρήστες να βρίσκονται σε σύγχυση. Η διαδικτυακή παρενόχληση και η υποκλοπή προσωπικών δεδομένων είναι μια εξελισσόμενη "μόδα". Στην παρούσα εισήγηση αρχικά γίνεται μια σύντομη παρουσίαση όσον αφορά τα επικρατέστερα διαδικτυακά εγκλήματα και παράλληλα προτείνονται τρόποι αντιμετώπισής τους. Στο τέλος της παρουσιάζονται οδηγίες και συμβουλές για τους απλούς χρήστες και τους περισσότερο έμπειρους.

ΛΕΞΕΙΣ-ΚΛΕΙΔΙΑ: *E-mail, Phishing, Pharming, Scam Blogs, Chat rooms, File sharing.*

1. ΕΙΣΑΓΩΓΗ

Το διαδίκτυο λίγα χρόνια πριν αποτελούσε ένα περιορισμένο δίκτυο, συνήθως μεταξύ πανεπιστημιακών και στρατιωτικών μονάδων.

Με την πάροδο των ετών σημειώθηκε τεράστια ανάπτυξη και εξάπλωση του διαδικτύου σε πολλούς τομείς της καθημερινότητάς μας, με αποτέλεσμα τον εκθετικό πολλαπλασιασμό γενικής μετατροπής των δεδομένων πάσης φύσεως σε ψηφιακή ηλεκτρονική μορφή. Αντίστοιχα όμως παρατηρείται ανάπτυξη και εξάπλωση σε παγκόσμια κλίμακα όσον αφορά την υποκλοπή των προσωπικών δεδομένων.

Πρόκειται για μια μορφή απάτης που δε στοχεύει στην "τσέπη" του θύματος καταναλωτή, αλλά στην κλοπή των προσωπικών του δεδομένων και τη χρήση τους από τρίτους στο διαδίκτυο. Η απάτη αυτή εμφανίζεται κυρίως:

- Στην ηλεκτρονική αλληλογραφία (E-mail)
- Στην απόσπαση προσωπικών στοιχείων (ψάρεμα) (Phishing)
- Στην ανακατεύθυνση του browser σε πλαστογραφημένες web pages (Pharming)
- Στις ψεύτικες αγγελίες για την ανεύρεση εργασιακής απασχόλησης (Scam)

- Στις λίστες καταχωρίσεων (ιστολόγια) (Blogs)
- Στα κανάλια συζητήσεων (Chat rooms)
- Στο διαμοιρασμό αρχείων μέσα από το διαδίκτυο (File sharing)

2. ΔΙΑΔΙΚΤΥΑΚΑ ΕΓΚΛΗΜΑΤΑ

2.1. Στην ηλεκτρονική αλληλογραφία (E-mail)

Το ηλεκτρονικό ταχυδρομείο αποτελεί μια από τις πιο δημοφιλείς υπηρεσίες του διαδικτύου παρέχει το πλεονέκτημα της οικονομικής και ταχύτατης επικοινωνίας με εκατομμύρια ανθρώπους σε ολόκληρο τον κόσμο ενώ παράλληλα αποτελεί το συνηθέστερο τρόπο για τη μετάδοση ιών στα αρχεία και στα λογισμικά των υπολογιστών. Οι ιοί των υπολογιστών ξεκίνησαν αρχικά με σκοπό τη "φάρσα" μεταξύ των προγραμματιστών και τον έλεγχο της πειρατείας των προγραμμάτων. Σήμερα οι ιοί έχουν αλλάξει χρήση. Οι νέοι ιοί έχουν ως αντικείμενο την υποκλοπή, την κατασκοπεία, με σκοπό την αξιοποίηση στοιχείων και πληροφοριών για στρατιωτικούς ή και εγκληματικούς λόγους. Συνήθως υποκλέπτονται αριθμοί πιστωτικών καρτών και κωδικοί λογαριασμών (password).

Ιοί

Οι ιοί επικολλώνται συνήθως στα συνημμένα αρχεία των μηνυμάτων και μολύνουν τον υπολογιστή του χρήστη, μόλις αυτός ανοίξει το συνημμένο αρχείο του αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα αρχεία (συνήθως με κατάληξη .exe, .com, .vbs, .dll, .sh, .bat κ.ά.), ενώ πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής html) που ενεργοποιείται αυτόματα με την ανάγνωση του e-mail. Οι χρήστες θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς.

Ενοχλητική αλληλογραφία (spam mail)

Από τα πρώτα δυσάρεστα εμπόδια που κλήθηκαν (και καλούνται) να αντιμετωπίσουν οι χρήστες του Internet ήταν και είναι το spam mail. Τα τελευταία χρόνια, μάλιστα, έχει αποκτήσει και παρέα: τα διαδοχικά pop-up windows με διαφημιστικά banners, που αφαιρούν από το web τη βασική του γοητεία: την πλοήγηση.

Το λεγόμενο spam ή junk mail μπορεί να περιλαμβάνει:

- Ενοχλητικό ή και δυσάρεστο περιεχόμενο για τον παραλήπτη.
- Διαφημίσεις ιστοχώρων ή ενημερωτικά δελτία προώθησης προϊόντων ή υπηρεσιών.
- Προειδοποιητικά μηνύματα: είτε ειδοποιούν το χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες.

- Περιεχόμενο συμπαράστασης: παρουσιάζουν κάποια υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται.
- Περιεχόμενο εκφοβισμού: οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες.

Συμβουλές προστασίας από τα spam mails στην ηλεκτρονική αλληλογραφία

- Ο χρήστης θα πρέπει 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 μόνιμα, 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.
- Ο χρήστης των προγραμμάτων αλληλογραφίας πρέπει να είναι ιδιαίτερα προσεκτικός και να μην αναφέρει ποτέ σε μηνύματα e-mails προσωπικά του στοιχεία, καθώς και αριθμούς πιστωτικών καρτών ή οποιαδήποτε άλλα δεδομένα.
- Πρέπει να αλλάζει τακτικά ο κωδικός πρόσβασης στο λογαριασμό e-mail.
- Η "Απομνημόνευση του ID μου στον υπολογιστή" έτσι ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή. Εδώ φυσικά δεν ενεργοποιείται η παραπάνω επιλογή.

▪ 2.2. Στις ηλεκτρονικές συναλλαγές με τις τράπεζες (Phishing)

Το ηλεκτρονικό "ψάρεμα" είναι κάτι περισσότερο από ανεπιθύμητα και ενοχλητικά ηλεκτρονικά μηνύματα. Μπορούν να οδηγήσουν στην κλοπή των αριθμών πιστωτικών καρτών, των κωδικών πρόσβασης, των πληροφοριών λογαριασμών ή άλλων προσωπικών δεδομένων.

Ο εγκληματίας κλέβει τα προσωπικά σας στοιχεία, αναλαμβάνει την ταυτότητά σας και μπορεί να εκδώσει:

- Να κάνει αίτηση και να εκδώσει πιστωτικές κάρτες στο όνομά σας.
- Να αδειάσει τον τραπεζικό σας λογαριασμό και να χρησιμοποιήσει τις πιστωτικές σας κάρτες στο μέγιστο όριο.
- Να μεταφέρει χρήματα από το λογαριασμό όψεως στο λογαριασμό ταμιευτηρίου και να χρησιμοποιήσει αντίγραφο της κάρτας αναλήψεων για να βγάλει χρήματα από το λογαριασμό σας σε μηχανήματα ΑΤΜ σε όλο τον κόσμο.

▪ **Συμβουλές προστασίας από το ηλεκτρονικό ψάρεμα (Phishing)**

Σε κάθε εισαγωγή του χρήστη στο πληροφοριακό σύστημα της τράπεζας με την οποία συναλλάσσεται, ο ενδιαφερόμενος πρέπει να βεβαιώνεται ότι έχει συνδεθεί με τον πραγματικό δικτυακό τόπο (site) της τράπεζας. Αυτό γίνεται με το ψηφιακό πιστοποιητικό ασφαλείας που έχει προμηθευτεί η τράπεζα και το οποίο πιστοποιεί ότι τα προγράμματα που μεταφέρονται στο σταθμό του χρήστη είναι τα γνήσια που έχουν εκπονηθεί από την τράπεζα, γεγονός που επιβεβαιώνεται με την ύπαρξη των παραπάνω ψηφιακών πιστοποιητικών.

Η εμφάνιση του εικονιδίου με το κίτρινο λουκέτο στο κάτω μέρος της οθόνης για όσο χρονικό διάστημα ο χρήστης χρησιμοποιεί την εφαρμογή υποδεικνύει πως η τοποθεσία web χρησιμοποιεί κρυπτογράφηση για την προστασία των ευαίσθητων προσωπικών πληροφοριών του. Όμως, το εικονίδιο με το κίτρινο λουκέτο μπορεί να είναι ψεύτικο. Για να διασφαλίσετε τη γνησιότητά του, κάντε διπλό κλικ, ώστε να διαπιστώσετε αν υπάρχει το πιστοποιητικό ασφαλείας της τοποθεσίας. Το όνομα που ακολουθεί το "Issued to" (εκδόθηκε για) θα πρέπει να αντιστοιχεί στο όνομα της τοποθεσίας. Εάν το όνομα διαφέρει, πιθανόν να βρίσκεστε σε μια ψεύτικη τοποθεσία, γνωστή και ως "spoofed" (πλαστή). Σε περίπτωση που δεν είστε σίγουροι εάν το πιστοποιητικό είναι νόμιμο, μην εισαγάγετε προσωπικά δεδομένα.

2.3. Στην παραπλάνηση σε ψεύτικες ιστοσελίδες (Pharming)

Απάτη με pharming (παραπλάνηση): ανακατεύθυνση του browser σε ψεύτικες ιστοσελίδες. Η κίνηση του διαδικτύου ανακατευθύνεται από μία τοποθεσία σε μία άλλη πανομοιότυπη, "Pharming" σημαίνει ότι εγκληματίες χάκερ ανακατευθύνουν την κίνηση του διαδικτύου από μία ιστοσελίδα σε μια άλλη, πανομοιότυπη, έτσι ώστε να σας ξεγελάσουν και να καταχωρίσετε το όνομα χρήστη και τον κωδικό χρήστη στη βάση δεδομένων της πλαστής ιστοσελίδας. Ιστοσελίδες τραπεζών ή αντίστοιχων οικονομικών οργανισμών είναι συχνά στόχοι τέτοιων επιθέσεων, κατά τις οποίες εγκληματίες προσπαθούν να αποσπάσουν προσωπικά δεδομένα, με σκοπό να αποκτήσουν πρόσβαση στον τραπεζικό σας λογαριασμό, να κλέψουν την ταυτότητά σας ή να διαπράξουν άλλου είδους απάτη στο όνομά σας. Αυτό επιτυγχάνεται με τη χρήση μιας διαδικασίας που ονομάζεται "δηλητηρίαση DNS", κατά την οποία κάποιος εισβολέας αποκτά πρόσβαση στις τεράστιες βάσεις δεδομένων που χρησιμοποιούν οι πάροχοι υπηρεσιών διαδικτύου για να δρομολογήσουν τη διαδικτυακή κίνηση.

▪ **Συμβουλές προστασίας από το Pharming**

- Με τη χρήση του λογισμικού firewall (τείχος προστασίας), που με κατάλληλες ρυθμίσεις επιτρέπει ή απορρίπτει πακέτα δεδομένων. Τα firewall τελευταίας γενιάς έχουν ενσωματωθεί στα λειτουργικά συστήματα.
- Με την αναζήτηση ψηφιακού πιστοποιητικού ασφαλείας.
- Καλύτερα να πληκτρολογούμε την ηλεκτρονική διεύθυνση στον browser παρά να οδηγούμαστε σε αυτή με χρήση βοηθητικών links.

- Ο χρήστης πρέπει αν ελέγχει το αν το κυρίως μήνυμα είναι εικόνα, με σκοπό να αποφευχθεί ο εντοπισμός τους από τα φίλτρα ανεπιθύμητης αλληλογραφίας. Αυτό μπορείτε να το καταλάβετε εύκολα αν τοποθετήσετε το δείκτη του ποντικιού στο κυρίως μήνυμα, ο δείκτης θα μετατραπεί σε χεράκι.

2.4. Στις αγγελίες για την ανεύρεση εργασίας (Scam)

Αυτές οι ψεύτικες αγγελίες για την εύρεση εργασίας γίνονται όλο και πιο κομψές και συχνά χρησιμοποιούν συνηθισμένη εικόνα ή πειστικά εταιρικά λογότυπα και φρασεολογία. Πολλές φορές διαθέτουν και συνδέσμους προς πλαστές ιστοσελίδες, που εμφανίζονται ως τοποθεσίες πραγματικών εταιρειών. Επιπλέον κάποιες φορές ακόμα χρεώνουν για υπηρεσίες που δε θα παράσχουν ποτέ. Έπειτα από μερικές μέρες, οι κλέφτες κλείνουν το scam και εξαφανίζονται.

- **Συμβουλές προστασίας από το Scam**

Ποτέ μη δίνετε κανένα προσωπικό στοιχείο που δε σχετίζεται με τη δουλειά (όπως στοιχεία ταυτότητας, τον αριθμό φορολογικού μητρώου, τον αριθμό της πιστωτικής σας κάρτας, την ημερομηνία γέννησης και την οικογενειακή σας κατάσταση)στο διαδίκτυο, μέσω e-mail.

- Να δημοσιεύσετε το βιογραφικό σας μόνο σε ιστοσελίδα εύρεσης εργασίας που εφαρμόζει πολιτική προστασίας προσωπικών δεδομένων και επιτρέπει την πρόσβαση από τον εξωτερικό κόσμο στα βιογραφικά αποκλειστικά σε πιστοποιημένα γραφεία εύρεσης εργασίας.
- Να διασταυρώνετε τα στοιχεία κάθε ενδεχόμενου εργοδότη, επαγγελματία ή γραφείου εύρεσης εργασίας. Ο καλύτερος τρόπος για να εξακριβώσετε τα στοιχεία ενός ενδεχόμενου εργοδότη είναι να επισκεφθείτε τα γραφεία της αντίστοιχης εταιρείας, σε ώρες εργασίας.
- Να μην εμπιστεύεστε όσους σας ζητούν χρήματα εκ των προτέρων για να σας βρουν δουλειά.
- Ποτέ μη δεχθείτε να πληρώσετε για "αποκλειστικές" πληροφορίες σχετικά με θέσεις εργασίας ή για να πάρετε κάποια συγκεκριμένη θέση. Στην περίπτωση όμως που πληρώσετε για υπηρεσίες εύρεσης εργασίας, μη δώσετε τα στοιχεία της πιστωτικής σας κάρτας ή του τραπεζικού σας λογαριασμού.
- Να αξιολογείτε προσεκτικά τα στοιχεία επαφής που δίνονται σε αγγελίες εργασίας ή σε σχετικά e-mail και να προσέχετε εάν υπάρχουν ανορθογραφίες, κάποια διεύθυνση e-mail που δεν αναφέρει το όνομα της εταιρείας ή εάν η περιοχή ή ο ταχυδρομικός κώδικας δεν είναι παντού τα ίδια.
- Να πληκτρολογείτε τις διευθύνσεις των ιστοσελίδων (URL) στο browser αντί να χρησιμοποιείτε links.
- Να δημιουργήσετε διεύθυνση ηλεκτρονικού ταχυδρομείου και έναν ξεχωριστό λογαριασμό για όλες τις μη προσωπικές επικοινωνίες.
- Εάν κάποια ευκαιρία υπόσχεται υπερβολικά πολλά ή κάτι άλλο δε φαίνεται σωστό, μάλλον πρόκειται για παραπλανητικό μήνυμα.

2.5. Στα ηλεκτρονικά ημερολόγια (Blogs)

Η πρακτική του blogging, η τήρηση προσωπικού ημερολογίου στο Διαδίκτυο, μεγαλώνει δραματικά, ειδικά ανάμεσα στους εφήβους, οι οποίοι ορισμένες φορές διατηρούν ημερολόγια blog χωρίς να το γνωρίζουν οι γονείς ή οι κηδεμόνες τους.

Σύμφωνα με κάποιες πρόσφατες μελέτες, τα μισά από τα ημερολόγια blog σήμερα δημιουργούνται από εφήβους από τους οποίους δύο στους τρεις δημοσιοποιούν την ηλικία τους, τρεις στους πέντε αποκαλύπτουν την τοποθεσία όπου κατοικούν και έναν στους πέντε να αποκαλύπτει το πλήρες όνομά του. Αυτό συμβαίνει χωρίς να λέγεται ότι υπάρχουν πιθανοί κίνδυνοι από τη δημοσιοποίηση αυτού του τύπου προσωπικών λεπτομερειών. Και καθώς πολλά νεαρά άτομα δημιουργούν όλο και περισσότερα ημερολόγια blog, οδηγούνται σε έναν αυξανόμενο ανταγωνισμό μεταξύ τους για να τραβήξουν την προσοχή. Μερικές φορές αυτό μπορεί να τα οδηγήσει να δημοσιεύσουν ακατάλληλο υλικό, όπως προκλητικές εικόνες των εαυτών τους ή των φίλων τους.

- **Συμβουλές προστασίας για τα Blogs**
- Καθιερώστε κανόνες για τη χρήση του διαδικτύου, αν η χρήση γίνεται κυρίως από νεαρά άτομα.
- Σχολαστικός έλεγχος και επιμέλεια για το περιεχόμενο πριν το δημοσιεύσουμε. Πληροφορίες που πιθανόν φαίνονται ακίνδυνες, όπως το σήμα ή το όνομα του σχολείου ή οι φωτογραφίες της πόλης, μπορούν, με κατάλληλους συνδυασμούς, να φανούν χρήσιμες σε επιτήδειους.
- Δοκιμάστε την υπηρεσία δημιουργίας ημερολόγιων blog και βρείτε εάν προσφέρει ιδιωτικά ημερολόγια με προστασία κωδικού πρόσβασης.
- Επισκεφθείτε το ημερολόγιο του παιδιού σας συχνά και επιθεωρήστε το. Επισκεφθείτε άλλα ημερολόγια για να βρείτε καλά παραδείγματα ώστε να τα υιοθετήσουν τα παιδιά σας.
- Μην παρέχετε ποτέ προσωπικές πληροφορίες, όπως επώνυμο, πληροφορίες επικοινωνίας, διεύθυνση κατοικίας, αριθμούς τηλεφώνων, όνομα σχολείου, ηλεκτρονική διεύθυνση, επώνυμο φίλων ή συγγενών, όνομα άμεσης επικοινωνίας, ηλικία ή ημερομηνία γέννησης.
- Μη δημοσιεύετε ποτέ προκλητικές φωτογραφίες του εαυτού σας ή κάποιων άλλων και βεβαιωθείτε πως όποια φωτογραφία δημοσιεύεται δεν αποκαλύπτει κάποιες προσωπικές πληροφορίες.
- Θεωρήστε πως ό,τι δημοσιεύεται στο διαδίκτυο είναι μόνιμο. Οποιοσδήποτε μπορεί να εκτυπώσει ένα ημερολόγιο ή να το αποθηκεύσει στον υπολογιστή του.
- Χρησιμοποιήστε τοποθεσίες παροχής ημερολογίων blog με ξεκάθαρους όρους χρήσης και βεβαιωθείτε πως μπορείτε να προστατέψετε με κωδικό πρόσβασης και τα ενεργά ημερολόγια blog και όχι μόνο τους λογαριασμούς. (Εάν όχι, είναι καλύτερο να θεωρήσετε πως οποιοσδήποτε μπορεί να το δει.)

- Αποφεύγετε να υπερβάλλετε ή να ανταγωνίζεστε με άλλους δημιουργούς ημερολογίων (bloggers).
- Διατηρήστε τα ημερολόγια blog θετικά και μην τα χρησιμοποιείτε για να δυσφημήσετε ή να επιτεθείτε σε άλλους.

2.6. Στην άμεση συνομιλία των chat

Το chat στο διαδίκτυο είναι ένας τρόπος άμεσης επικοινωνίας ενός συνόλου ανθρώπων, οι οποίοι βρίσκονται συγκεντρωμένοι σε έναν συγκεκριμένο δικτυακό χώρο που ονομάζεται "δωμάτιο επικοινωνίας" (chat room) και πληκτρολογούν ο ένας στον άλλο μηνύματα κειμένου ή χρησιμοποιούν μικρόφωνο και κάμερα για ζωντανή συνομιλία. Η χρήση των ψευδωνύμων επιτρέπει στους χρήστες να διατηρούν την ανωνυμία τους. Αυτή ακριβώς η δυνατότητα, μαζί με την ψευδαίσθηση του παιδιού-χρήστη ότι είναι ασφαλές επειδή βρίσκεται στον φυσικό χώρο του σπιτιού του, του σχολείου του ή ενός internet cafe, μπορεί να μετατρέψει αυτό τον τρόπο της επικοινωνίας σε μια από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του διαδικτύου. Υπάρχουν συχνά καταγγελίες παιδιών ότι, κατά τη διάρκεια τέτοιου είδους συνομιλιών, έχουν υποστεί λεκτική ή σεξουαλική παρενόχληση, ενώ έχουν δεχτεί από αγνώστους προτροπές για συνάντηση σε πραγματικό χώρο. Σε χώρες του εξωτερικού έχουν επισημανθεί έως τώρα δεκάδες περιπτώσεις παιδιών που εξαφανίστηκαν, έπεσαν θύματα παιδόφιλων ή κυκλωμάτων παιδικής πορνογραφίας ή παρασύρθηκαν από αγνώστους τους οποίους «συνάντησαν» σε δωμάτια επικοινωνίας.

- **Συμβουλές προστασίας στα chat**

Προέχει σωστή ενημέρωση για αυτό τον τρόπο επικοινωνίας. Ένα από τα σημαντικότερα προβλήματα είναι η έλλειψη γνώσεων σχετικά τόσο από τους γονείς όσο και από τους εκπαιδευτικούς.

2.7. Στο διαμοιρασμό αρχείων.

Είναι η δυνατότητα που προσφέρει το διαδίκτυο στους χρήστες του να διαμοιράζονται αρχεία κάθε είδους. Πραγματοποιείται με προγράμματα (ελεύθερα ή με πληρωμή) όπως τα εξής: Προγράμματα για Windows: KaZaa, Limewire, Morpheus, SwapNut,WinMX.

Καθένα από τα ανωτέρω προγράμματα λειτουργεί έτσι ώστε να κάνει κοινόχρηστο ένα μέρος του σκληρού δίσκου του τοπικού υπολογιστή σε όλους χρήστες, οι οποίοι είναι συνδεδεμένοι στο διαδίκτυο και χρησιμοποιούν το ίδιο πρόγραμμα. Επομένως κάθε μέλος της ιδιότυπης αυτής κοινότητας μπορεί να αναζητεί αρχεία στους υπολογιστές των μελών της και να δημιουργεί ένα αντίγραφο οποιουδήποτε από αυτά τα αρχεία στον δικό του υπολογιστή. Κατά την αντιγραφή των αρχείων υπάρχει απευθείας σύγχρονη επικοινωνία μεταξύ υπολογιστών, γι' αυτό τα προγράμματα αυτά ονομάζονται και ομότιμης σύνδεσης (peer-to-peer).

Η ευρύτατη χρήση της δυνατότητας αυτής του διαδικτύου οφείλεται στην μεγάλη ευκολία εύρεσης και τοπικής αποθήκευσης κάθε είδους αρχείου

(μουσικής, εικόνων, προγραμμάτων), με μηδαμινό κόστος για το χρήστη. Η συγκέντρωση των ταυτόχρονα διασυνδεδεμένων χρηστών σε κάθε τέτοιο πρόγραμμα διαμοιρασμού αρχείων ανέρχεται σε μερικά εκατομμύρια. Δημιουργούνται έτσι μερικές από τις μεγαλύτερες διαδικτυακά πληθυσμιακές κοινότητες, μέσα στις οποίες διακινείται σχεδόν ανεξέλεγκτα κάθε είδους υλικό.

3. ΣΥΜΒΟΥΛΕΣ ΠΡΟΣ ΧΡΗΣΤΕΣ

- Να θυμάστε ότι το διαδίκτυο δεν είναι ασφαλές. Ωστόσο υπάρχουν και διαρκώς
  αναπτύσσονται διάφορα μέσα τα οποία σας επιτρέπουν να βελτιώσετε την προστασία των δεδομένων σας. Συνεπώς να χρησιμοποιείτε όλα τα διαθέσιμα μέσα για την προστασία των δεδομένων και των επικοινωνιών σας, όπως τη νόμιμη κρυπτογράφηση για τα εμπιστευτικού χαρακτήρα ηλεκτρονικά μηνύματά σας καθώς και κωδικούς πρόσβασης για τον προσωπικό τους υπολογιστή.
- Εγκαταστήστε ένα antivirus & antispyware πρόγραμμα ή όλα-σε-ένα πρόγραμμα ασφάλειας στο διαδίκτυο.
- Εγκαταστήστε τα προγράμματα ασφαλείας που παρέχουν ενεργή προστασία σε πραγματικό χρόνο. Μερικά δωρεάν προγράμματα προστασίας από ιούς μπορεί να ανιχνεύσουν μόνο τους ιούς που έχουν ήδη μολύνει τον υπολογιστή σας. Ωστόσο, εάν ο υπολογιστής σας δεν έχει ήδη μολυνθεί, ενδέχεται να μην είναι σε θέση να επιτύχουν τη δωρεάν ανίχνευση ιών σε όλες τις περιοχές.
- Να θυμάστε ότι κάθε συναλλαγή σας, κάθε επίσκεψή σας στο διαδίκτυο, αφήνει ίχνη. Αυτά τα "ηλεκτρονικά ίχνη" (cookies) μπορούν να χρησιμοποιηθούν, εν αγνοία σας, για να διαμορφωθεί ένα προφίλ για το άτομό σας και τα ενδιαφέροντά σας. Αν δεν επιθυμείτε να συμβεί αυτό, σας παροτρύνουμε να τα σβήνετε χρησιμοποιώντας τα τελευταία τεχνικά μέσα.
- Η ανώνυμη πρόσβαση και χρήση υπηρεσιών, καθώς και τα ανώνυμα μέσα εξόφλησης λογαριασμών, αποτελούν την καλύτερη προστασία της ιδιωτικότητάς σας. Αναζητήστε τα τεχνικά μέσα που διασφαλίζουν την ανωνυμία σας όπου χρειάζεται.
- Να είστε σε επαγρύπνηση και να κάνετε επιλογή σχετικά με το τι κατεβάζετε στον υπολογιστή σας. Μην κάνετε λήψη δωρεάν παιχνιδιών και δωρεάν λογισμικού. Να θυμάστε ότι η ηλεκτρονική σας διεύθυνση αποτελεί προσωπικό σας δεδομένο και ότι άλλα πρόσωπα μπορεί να επιθυμούν να το χρησιμοποιήσουν για διαφορετικούς σκοπούς, όπως είναι η εισαγωγή της σε καταλόγους ή σε λίστες χρηστών. Μη διστάζετε να ρωτάτε για το σκοπό του καταλόγου ή άλλης χρήσης. Μπορείτε να ζητήσετε την παράλειψη των στοιχείων σας, εφόσον δεν επιθυμείτε να εγγραφείτε σε μια τέτοια λίστα.
- Να είστε επιφυλακτικοί με τόπους διαδικτύου όπου ζητούνται περισσότερα στοιχεία από όσα είναι απαραίτητα για την πρόσβαση ή την ολοκλήρωση μιας συναλλαγής, ή όταν δεν σας εξηγούν το λόγο για τον οποίο σας ζητούν τόσες πληροφορίες.

- Να θυμάστε ότι φέρετε πλήρη ευθύνη έναντι του νόμου για την επεξεργασία των δεδομένων (για παράδειγμα, αν φορτώνετε παράνομα στοιχεία από το διαδίκτυο στον υπολογιστή σας ή αντίστροφα) και ότι τα ίχνη σας μπορούν να βρεθούν ακόμα και στην περίπτωση που χρησιμοποιείτε ψευδώνυμο.
- Μην αποστέλλετε κακόβουλη αλληλογραφία. Μπορεί να στραφεί εναντίον σας και επιπλέον να υποστείτε τις συνέπειες του νόμου.
- Ο Παροχέας Υπηρεσιών Διαδικτύου που χρησιμοποιείτε είναι υπεύθυνος για την ορθή χρήση των δεδομένων που του παρέχετε. Ρωτήστε τον/την τι είδους δεδομένα συλλέγει, επεξεργάζεται και αποθηκεύει, με ποιον τρόπο και για ποιο σκοπό. Να επαναλαμβάνετε την ερώτηση αυτή κατά διαστήματα. Να επιμένετε για την αλλαγή τους αν είναι λανθασμένα ή για τη διαγραφή τους αν είναι υπερβολικά, ξεπερασμένα ή περιττά. Να ζητάτε από τον παροχέα σας να ενημερώνει τρίτους, στους οποίους έχει διαβιβάσει ή κοινοποιήσει τα δεδομένα σας, για τυχόν τροποποιήσεις.
- Να ενημερώνεστε για τους κινδύνους που σχετίζονται με την ασφάλεια και την ιδιωτικότητα στο διαδίκτυο, καθώς και για τις διαθέσιμες μεθόδους και τεχνικές για τη μείωση αυτών των κινδύνων.
- Αν σκοπεύετε να στείλετε δεδομένα σε άλλη χώρα, πρέπει να γνωρίζετε ότι ενδέχεται να παρέχεται μικρότερη προστασία εκεί. Αν τα εν λόγω δεδομένα αφορούν εσάς, είστε σαφώς ελεύθερος να τα διαβιβάσετε/κοινοποιήσετε. Ωστόσο, οφείλετε να συμβουλευτείτε, για παράδειγμα, την αρμόδια αρχή στη χώρα σας, προκειμένου να βεβαιωθείτε ότι επιτρέπεται η διαβίβαση δεδομένων, πριν αποστείλετε δεδομένα άλλων προσώπων στο εξωτερικό. Ίσως χρειαστεί να ζητήσετε από τον αποδέκτη να παράσχει τις απαραίτητες εγγυήσεις για την προστασία των δεδομένων.
- Να θυμάστε ότι η καλύτερη ασπίδα τους εαυτού σας από τους κακόβουλους τους διαδικτύου είναι η πολυπλοκότητα των κωδικών σας (passwords). Απλώς, πρέπει να επιλέγετε κωδικούς πρόσβασης που μπορούν να βρεθούν με μεγαλύτερη δυσκολία και κάνουν τη διαδικασία πιο χρονοβόρα και ασύμφορη. Το πόσο δύσκολο είναι να βρεθεί ένας κωδικός εξαρτάται από το μήκος του, που δεν πρέπει να είναι λιγότερο από οκτώ σύμβολα. Η πολυπλοκότητα εξαρτάται, βέβαια, και από το ποια σύμβολα θα χρησιμοποιήσετε. Αν επιλέξετε μόνον αριθμούς, περιορίζεστε αμέσως σε δέκα σύμβολα. Αν τα συνδυάσετε με πεζά και κεφαλαία γράμματα, ο αριθμός αυξάνεται πολύ περισσότερο (62 με το λατινικό αλφάβητο). Αν, πάλι, χρησιμοποιήσετε και όλα τα υπόλοιπα σύμβολα του πληκτρολογίου, ο αριθμός αγγίζει το 95.

ΕΠΙΛΟΓΟΣ

Κλείνοντας θα ήθελα να τονίσω ότι, ανεξάρτητα απ' τις προσωπικές προσδοκίες ή αναστολές, καλούμαστε να ζήσουμε σε ένα τεχνολογικό περιβάλλον. Η δαιμονοποίηση του διαδικτύου θα μας θέσει στο περιθώριο των εξελίξεων που συντελούνται στη σύγχρονη παγκοσμιοποιημένη κοινωνία. Με δεδομένο τον πολύπλοκο αμφιλεγόμενο ρόλο του λοιπόν, οφείλουμε να αξιολογήσουμε τις αντιφάσεις του και να αναδείξουμε δυναμικά τον

λειτουργικό του ρόλο, αντιμετωπίζοντας τους κινδύνους που συνοδεύουν την ανεξέλεγκτη χρήση του. Γιατί είναι γεγονός ότι το διαδίκτυο μπορεί να αποδειχθεί φιλικό αλλά και εχθρικό, χρήσιμο και επικίνδυνο συλλογικό αλλά και ατομικιστικό, φορέας ελεύθερης έκφρασης και επιστημονικής γνώσης αλλά και όργανο ελέγχου και εμπορικής προπαγάνδας. Συνεπώς η προστασία από τους ποικίλους κινδύνους δεν πρέπει να επαφίεται στους αρμόδιους φορείς και ειδικούς αλλά να αποτελεί βασική προτεραιότητα όλων των χρηστών του διαδικτύου. Ελπίζω ότι η συγκεκριμένη εισήγηση κινήθηκε, προς αυτή την κατεύθυνση με απλές αλλά ταυτόχρονα σαφείς διευκρινίσεις.

ΒΙΒΛΙΟΓΡΑΦΙΑ (WEB)

- http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-LawAndInternet.html
- http://download.pgp.com/pdfs/Intro_to_Crypto_040600_F.pdf
- http-www.ebusinnes-lab.gr
- http://office.microsoft.com/el-gr/outlook/HA011400021032.aspx
- http://www.microsoft.com/hellas/protect/default.mspx
- http--www.ebusiness-lab.gr-Portals-12-Ptyxiakes-Presentations-daramouskas_prostasia_proswpikwn_dedomenw
- http://portal.kathimerini.gr/4dcgi/_w_articles_kathworld_16_24/12/2009_315831
- http://dide.flo.sch.gr/Plinet/Tutorials/Tutorials-LawAndInternet.html
- www.cnc.uom.gr/services/WEB_DECEPTION.pdf
- ttp://blogthea.gr/NextStep/internet/17357-ceaeon
- http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTALiieeao-adhaoao.html