Πώς απειλείται η ιδιωτικότητά μας από τις νέες τεχνολογίες; - Μέτρα προστασίας

Κωνσταντίνος ΜΟΥΛΙΝΟΣ,
Εθνικός Εμπειρογνώμων, ENISA

Ημερίδα για την
Αυτοπροστασία Χρηστών και Συνδρομητών & Ασφάλεια Ηλεκτρονικών Δικτύων και Υπολογιστικών Συστημάτων

Ατζέντα

- Απειλές κατά της ιδιωτικότητας
- Μη ζητηθείσα ηλεκτρονική επικοινωνία (spam)
- Υπηρεσίες κοινωνικής δικτύωσης
  - Chat, blogs, social networks, on line games
- Παράνομο-επιβλαβές περιεχόμενο
- Συστάσεις-Συμπεράσματα

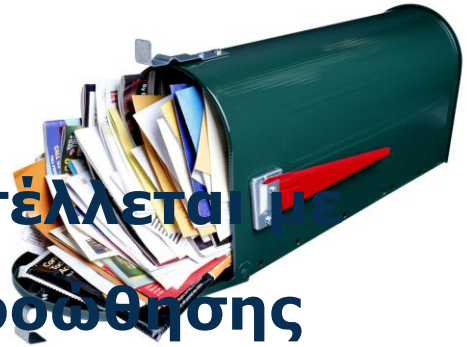
Οι νέες τεχνολογίες απειλούν την ιδιωτικότητα;

everybody
"On the Internet, ~~*nobody*~~ knows you're a dog."

Απειλές της ιδιωτικότητας

- Δημοσιοποίηση προσωπικών πληροφοριών
- Παράνομο περιεχόμενο
  - Παρακολούθηση πορνογραφικού υλικού
  - Παρακολούθηση βίαιου ή ακατάλληλου περιεχομένου
- Κλοπή ταυτότητας
- Παραβίαση όρων πολιτικής προστασίας δεδομένων
- Τεχνικές απειλές
  - Απειλές στην εφαρμογή, στα επίπεδα επικοινωνίας
  - Cookies
  - DNS
  - ....

Spam



- Ηλεκτρονική αλληλογραφία που αποστέλλεται με το σκοπό της απ’ ευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών
- Περιλαμβάνει και την επικοινωνία οργανισμών που δεν ασκούν μία από τις παραπάνω δραστηριότητες, πχ. φιλανθρωπικά ιδρύματα, σωματεία κλπ
- Εκτός από το “ κλασσικό” email, περιλαμβάνει και μηνύματα SMS και MMS

Χαρακτηριστικά του spam

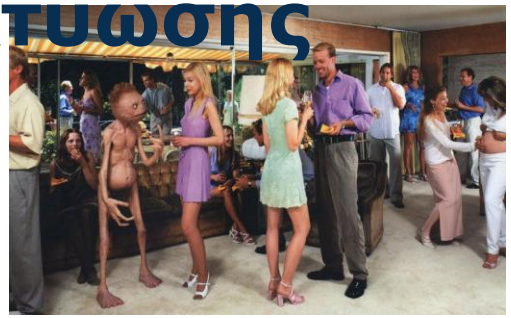
Ένα μήνυμα spam ενδέχεται να:

1. **Έχει ένα ή περισσότερα από τα παρακάτω χαρακτηριστικά:**
    1. **Μαζική αποστολή σε μεγάλο αριθμό παραληπτών (bulk email)**
    2. **Συγκάλυψη ή απόκρυψη της ταυτότητας του αποστολέα**
    3. **Έλλειψη έγκυρης διεύθυνσης τερματισμού της επικοινωνίας**
    4. **Παραπλανητικό ή ψεύτικο περιεχόμενο**
2. **Στοχεύει σε παράνομες ή εγκληματικές δραστηριότητες ("Phishing")**
3. **Περιέχει πορνογραφικό περιεχόμενο ή τυφλή βία ή προτροπή σε μίσος (φυλετικό, εθνικό, σεξουαλικό)**

Μέτρα προστασίας - Spam

- Προς τους απλούς χρήστες – συνδρομητές
  - Προστατεύστε τη διεύθυνση ηλεκτρονικού ταχυδρομείου
  - Χρησιμοποιείστε λογισμικό φιλτραρίσματος (spyware)
  - Μη γίνετε spammer κατά λάθος
  - Προστατεύστε τον αριθμό του κινητού σας τηλεφώνου
- Προς τους παρόχους υπηρεσιών
  - Black lists/registers
  - Τεχνικές φιλτραρίσματος
  - Ανάλυση επικινδυνότητας – οργανοτεχνικά μέτρα
- Προσφυγή στις Αρχές (www.dpa.gr)
- Περισσότερα: http://www.enisa.europa.eu/pages/spam/index.htm

Υπηρεσίες κοινωνικής δικτύωσης



- **Chat**
  - **Δωμάτιο ανοιχτής επικοινωνίας**
  - **Ανταλλαγή μηνυμάτων μέσω e-mail**
- **Blogs(ιστολόγια)**
  - **Εικονικά ημερολόγια που αποθηκεύονται στο Διαδίκτυο**
  - **Weblogs, vlogs, moblogs**
- **Social networks**
  - **Δημιουργία on-line κοινοτήτων με κοινά ενδιαφέροντα**
  - http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf
- **On line games**
  - **Κυμαίνονται από stand alone παιγνίδια μέχρι MMO/VWs**
  - **Υψηλό επίπεδο διαδραστικότητας**

Μέτρα προστασίας - Chat

- Οι εικονικοί φίλοι μπορεί να είναι διαφορετικοί από αυτό που δείχνουν.
- Μη δίνετε ποτέ προσωπικές πληροφορίες.
- Ποτέ μη δίνετε πληροφορίες για την οικογένειά και τους φίλους σας.
- Αν νιώθετε ότι κάποιος σας παρενοχλεί, θυμηθείτε: μπορείτε να βγείτε με ένα απλό «κλικ».

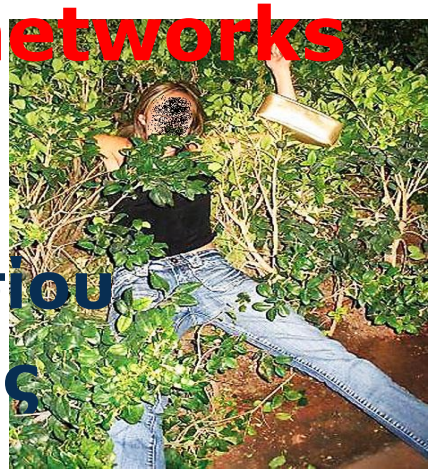
Πηγή:
www.saferinternet.gr

Μέτρα προστασίας - Blogs

- Χρησιμοποιήστε ψευδώνυμα.
- Περιορίστε την πρόσβαση στο blog σας
- Χρησιμοποιήστε τεχνολογία που προσφέρει ανωνυμία και δεν εμφανίζει το blog στα αποτελέσματα μηχανών αναζήτησης.
- Κατοχυρώστε την ηλεκτρονική σας διεύθυνση ανώνυμα.

(www.eff.org)

Μέτρα προστασίας - Social networks



- Αναθεώρηση του νομοθετικού πλαισίου
- Διαφάνεια στις πρακτικές διαχείρισης προσωπικών δεδομένων
- Ενημέρωση - εκπαίδευση
- Αποθάρρυνση της απαγόρευσης χρήσης των ιστοσελίδων κοινωνικής δικτύωσης στα σχολεία
- Εύκολη αναφορά περιστατικών
- Ευκολία χρήσης διαπεφής
- .....

Μέτρα προστασίας – Virtual Worlds

- **Προσωπικές πληροφορίες**
  - **Μόνο στον πάροχο**
  - **Μόνο σε άλλο έμπιστο είδωλο**
  - **Μην αποκαλύπτετε πληροφορίες με τις οποίες μπορεί κάποιος να σας προσεγγίσει**
- **Τεχνικά μέτρα**
  - **Anti-virus**
  - **Anti-Spyware**
  - **Συχνή αλλαγή συνθηματικού**
- **Πρόσβαση ανάλογα με την ηλικία (συγκατάθεση γονέων)**
- **Πληροφόρηση-εκπαίδευση**
  - **Αναφορές ENISA**

Παράνομο-επιβλαβές περιεχόμενο

- Παιδική πορνογραφία
- Ρατσιστικό-ξενοφοβικό περιεχόμενο
- Βία-σατανισμός-ναρκωτικά
- Ευρωπαϊκό πρόγραμμα για ασφαλέστερο Internet
  - Κατάταξη του παιχνιδιού σε ηλικιακές ομάδες
  - Χαρακτηρισμός περιεχομένου
  - Επιβεβαίωση ταυτότητας
- Στόχος κυρίως τα παιδιά
- Αναφορά περιστατικών, http://www.safeline.gr

Γονείς και έλεγχος

- Κατανόηση του διαδικτύου και των εφαρμογών
- Ενημέρωση σχετικά με κινδύνους (π.χ www.saferinternet.gr)
- Έλεγχος του τρόπου χρήσης του Internet από τα παιδιά
  - http://www.sip-bench.eu/sipbench.php?page=results2007&lang=en
- Επαφή με Αρχές σε περιπτώσεις προβλημάτων

Πρακτικές συμβουλές – γενικά (1)

- ★ Αποφεύγετε να δίνετε προσωπικά δεδομένα
- ★ Διαβάζετε την πολιτική προστασίας δεδομένων στους διαδικτυακούς τόπους που επισκέπτεστε
- ★ Χρησιμοποιείτε προσωπικά firewalls και anti-virus για συνδέσεις από το σπίτι
- ★ Αποφεύγετε τα cookies (ρυθμίσεις web browser)
- ★ Κλείνετε τα 'ύποπτα' αναδυόμενα παράθυρα
- ★ Μην απαντάτε σε αυτόκλητα μηνύματα
- ★ Διατηρείστε μια «ιδιωτική» διεύθυνση ηλεκτρονικού ταχυδρομείου

Πρακτικές συμβουλές – γενικά (2)

- Μην δίνετε ευαίσθητες προσωπικές πληροφορίες σε μη προστατευμένες (π.χ SSL) συνδέσεις
- Εισάγετε μόνο τις εντελώς απαραίτητες προσωπικές πληροφορίες στις απ' ευθείας φόρμες
- Μην συμπληρώνετε τα optional πεδία των φορμών
- Προσοχή στα προεπιλεγμένα πεδία των φορμών
- Αναζητείστε επιλογές opt-out ή opt-in όταν καταχωρείσθε σε mailing lists

Πρακτικές συμβουλές – γενικά (3)

- Όποτε μπορείτε χρησιμοποιείστε Τεχνολογίες φιλικές προς την ιδιωτικότητα (Privacy Enhancing Technologies)
- Χρησιμοποιείτε δωρεάν υπηρεσίες ηλεκτρονικού ταχυδρομείου αντί ISP
- Χρησιμοποιείτε προπληρωμένες κάρτες για τους ISP
- Ζητείστε τα μέτρα προστασίας που λαμβάνει ο ISP
- Αναζητείστε διαδικτυακούς τόπους με ψηφιακές σφραγίδες

Συστάσεις

- **Τοπικές Αρχές:**
  - Η ενημέρωση πρέπει να ξεκινά από τα σχολεία
  - Ενσωμάτωση του μαθήματος Ασφάλειας στο σχολικό πρόγραμμα
  - Εκπαίδευση των εκπαιδευτικών σχετικά με την ασφαλή χρήση του διαδικτύου
  - Δημιουργία κανονιστικού πλαισίου για χρήση κινητών τηλεφώνων στα σχολεία
- **Βιομηχανία. Ανάγκη για ευκολότερη:**
  - Πρόσβαση στην πληροφορία την σχετική με προστασία
  - Δημιουργία προσωπικού προφίλ
  - Τοποθέτηση περιορισμών στην πρόσβαση του προφίλ
  - Αναγνώριση περιστατικών
- **Όλοι οι εμπλεκόμενοι φορείς**
  - Μεγαλύτερη προβολή του θέματος
  - Αναφορά περιστατικών - χρήση κινητών
  - Βελτίωση μηχανισμών ελέγχου από γονείς

Στοιχεία επικοινωνίας

Κωνσταντίνος ΜΟΥΛΙΝΟΣ, ENISA

Mail: Konstantinos.Moulinos@enisa.europa.eu

Tel: +30 2810 391363

Fax: +30 2810 391895