1ο ΓΕ.Λ. Ελευθερίου Κορδελιού
Ερευνητική εργασία Α΄ Λυκείου
Β΄ Τετρ. 2011-2012
Τμήμα : PR 5

«ΑΞΙΟΠΟΙΩ ΤΟ ΔΙΑΔΙΚΤΥΟ – ΠΡΟΣΤΑΤΕΥΩ ΤΟΝ ΕΑΥΤΟ ΜΟΥ»

ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Καθηγητής: Αποστολίδης Γιάννης

Κίνδυνοι στο Διαδίκτυο

Το διαδίκτυο θεωρείται από πολλούς ένα μέσω ψυχαγωγίας, ενημέρωσης και επικοινωνίας. Πολλοί είναι όμως οι κίνδυνοι που τους επιφυλάσσει η χρήση του, καθώς αυξάνονται και ηλικιακά.

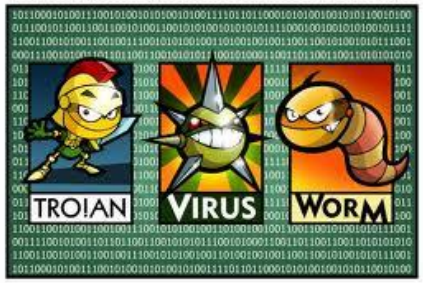
Σύμφωνα με **έρευνα** του ευρωπαϊκού Δικτύου **«EU Kids Online»:**

- Ένα 13% παιδιών ηλικίας 9-10 ετών βρέθηκε αντιμέτωπο με τουλάχιστον ένα κίνδυνο.
- Το ποσοστό ανέρχεται στο 32% στα παιδιά ηλικίας 11-12 ετών, σε 49% στα παιδιά 13-14 ετών και στο 61% για τα παιδιά 15-16 ετών.
- Τα παιδιά “μπαίνουν” στο διαδίκτυο ολοένα και σε νεότερη ηλικία. Συγκριμένα σε ηλικία 7 ετών στη Σουηδία και 8 ετών σε πολλές άλλες χώρες της Β. Ευρώπης.
- Σε όλες τις χώρες το 1/3 των παιδιών ηλικίας 9-10 ετών μπαίνει στο δίκτυο καθημερινά και το ποσοστό αυτό αυξάνεται σε 77% στα παιδιά ηλικίας 15-16.

Κατηγορίες βλαβερού λογισμικού

Με τον όρο βλαβερό λογισμικό αναφερόμαστε σε λογισμικό και σε προγράμματα που περιλαμβάνουν, μεταξύ άλλων:

- **Ιούς (viruses):** προγράμματα τα οποία είναι έτσι σχεδιασμένα ώστε να εισβάλουν στον υπολογιστή μας και να δημιουργούν ανεπιθύμητες παρενέργειες
- **Δούρειοι Ίπποι (Trojan horses)**: Προγράμματα που, ενώ φαίνεται πως δουλεύουν σωστά και με νόμιμο τρόπο, όμως στην πραγματικότητα μπορούν να προκαλέσουν αρκετές βλάβες
- **Spyware:** Προγράμματα που προσκολλούνται κρυφά σε αρχεία που κατεβάζουμε από το διαδίκτυο. Μόλις κατέβουν, αυτοεγκαθίστανται στον υπολογιστή μας και ξεκινούν την παρακολούθηση της διαδικτυακής μας δραστηριότητας.



Τι κάνουμε για να προστατευθούμε

- Αγοράστε ένα αξιόπιστο λογισμικό antivirus, εγκαταστήστε το και πραγματοποιείτε όσο το δυνατόν συχνότερα computer scans και updates.
- Απαγορεύστε την πρόσβαση σε διαδίκτυο και ηλεκτρονικό ταχυδρομείο σε όποιον δε γνωρίζει από υπολογιστές. Προσφερθείτε να τους βρείτε εσείς αυτά που θέλουν.
- Πριν ανοίξετε οποιοδήποτε εκτελέσιμο αρχείο που κατεβάσατε ή e-mail που λάβατε από άγνωστο αποστολέα, πραγματοποιήστε virus scan.
- Δώστε μεγάλη προσοχή κατά τη συμμετοχή σας σε forums και chat rooms, τόσο για τις πληροφορίες που δίνετε όσο και για αυτές που λαμβάνετε. Μην ξεχνάτε πως ποτέ δε γνωρίζετε ποιος πραγματικά είναι ο καθένας.

- Ενεργοποιείτε το firewall τουλάχιστον όποτε περιδιαβαίνετε στα «σκοτεινά σοκάκια» του Internet αλλά και όποτε δεν είστε απολύτως σίγουροι για την ασφάλεια ενός site.

- Το συχνό backup σώζει νεύρα (και ζωές)! Ανά τακτά χρονικά διαστήματα σώστε τα αρχεία που έχουν σημασία για εσάς σε εξωτερικό σκληρό δίσκο, CD/DVD ή usb drive ώστε σε περίπτωση που χαθούν ή σβηστούν να έχετε αντίγραφο ασφαλείας. Να θυμάστε πάντα πως οποιοδήποτε σημαντικό αρχείο καλό είναι να το έχετε πάντα και εκτός υπολογιστή.

- Προσέχετε τα browser games που παίζετε να είναι από αξιόπιστες ιστοσελίδες και όσα ζητούν εγγραφή με λογαριασμό να μη ζητούν προσωπικές ή/και απόρρητες πληροφορίες.

Μην πανικοβάλλεστε. Στις περισσότερες περιπτώσεις μεγάλης ζημιάς μετά από μόλυνση με ιούς, η καταστροφή δεδομένων έγινε από τον πανικοβλημένο χρήστη του υπολογιστή, ο οποίος κατέστρεψε οριστικά τα δεδομένα του με λάθος ενέργειες. **Θα ήταν προτιμότερο να αφήσετε τη διαδικασία αποκατάστασης σε ειδικούς, αν δεν αισθάνεστε σίγουροι για τις ενέργειές σας.**

Κωδικοί πρόσβασης – Τι να αποφεύγω

Πολλοί χρήστες είναι πολύ αφελείς σε αυτό το θέμα και χρησιμοποιούν εύκολους κωδικούς πρόσβασης, κάνοντας εύκολη υπόθεση για τους δράστες την πρόσβαση στα προσωπικά δεδομένα των θυμάτων τους.

- Δεν χρησιμοποιούμε κωδικούς πρόσβασης που βασίζονται σε προσωπικά στοιχεία για να τους θυμόμαστε πιο εύκολα. Αυτό το γνωρίζουν και οι εισβολείς. Συχνά οι σύντομοι αριθμητικοί κωδικοί πρόσβασης αποκαλύπτονται βάσει του έτους και την ημερομηνία γέννησης του θύματος. Αλλά βοηθήματα, όπως τα ονόματα κατοικίδιων η αγαπημένων προσώπων, εντοπίζονται επίσης από την έρευνα των εισβολέων.

- Ορισμένες εφαρμογές επιτρέπουν για λόγους ασφαλείας την αποθήκευση του κωδικού πρόσβασης, ωστόσο καλό θα ήταν να αποφύγετε την πρακτική αυτή, διότι δεν είναι πάντα βέβαιο ότι ο κωδικός πρόσβασης αποθηκεύετε σε ασφαλή, κωδικοποιημένη μορφή. Ορισμένα προγράμματα αποθηκεύουν τους κωδικούς πρόσβασης μη κωδικοποιημένους, σε απλό κείμενο στο σύστημα, γεγονός που επιτρέπει την ανάγνωση τους από τυχόν εισβολείς.

Κωδικοί πρόσβασης-Πώς τους επιλέγω

- Χρησιμοποιήστε έναν κωδικό πρόσβασης που αποτελείται από ένα συνδυασμό γραμμάτων, αριθμών και συμβόλων και είναι δύσκολο να τον μαντέψει κάποιος.

π.χ. μπορείτε να χρησιμοποιήσετε τα πρώτα γράμματα από την πρόταση "Σήμερα, στις 10 Ιουλίου, δημιουργώ έναν ασφαλή κωδικό πρόσβασης με τουλάχιστον 25 χαρακτήρες"

Σ,σ10Ι,δεακπμτ25χ

Με την αρχική πρόταση ως βοήθεια δεν θα έχετε κανένα πρόβλημα να θυμάστε τον κωδικό πρόσβασης σας.

- Μην χρησιμοποιείτε μόνο έναν μοναδικό κωδικό πρόσβασης για όλους τους σημαντικούς λογαριασμούς σας.
- Ο επιλεγμένος κωδικός πρόσβασης θα πρέπει να είναι γνωστός μόνο σε εσάς, μην τον κοινοποιείτε ούτε σε γνωστούς ούτε σε συγγενείς, και μην τον σημειώνετε.

Μαθήτριες:

ΜΠΕΡΑΤΖΕ ΚΩΝΣΤΑΝΤΙΝΑ
ΜΠΛΙΑΤΖΕ ΤΙΝΑ
ΜΠΡΕΓΚΑΪ ΤΖΕΝΗ
ΧΡΗΣΤΟ ΧΡΙΣΤΙΝΑ
ΠΑΠΑΔΑΚΗ ΠΑΣΧΑΛΙΝΑ

Ευχαριστούμε!!