ΙΟΙ ΥΠΟΛΟΓΙΣΤΩΝ

Αγγελική Μπελεχάκη
2ο Γυμνάσιο Μελισσίων

ΤΙ ΕΊΝΑΙ ΈΝΑΣ ΊΟΣ ΥΠΟΛΟΓΙΣΤΉ;

Ένας ιός υπολογιστών είναι ένα πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να "μολύνει" τον υπολογιστή –στόχο- χωρίς τη γνώση ή την άδεια του χρήστη του.

Ο ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση.

ΧΑΡΑΚΤΗΡΙΣΤΙΚΆ ΤΩΝ ΊΩΝ ΥΠΟΛΟΓΙΣΤΏΝ

- Πολλοί προσωπικοί υπολογιστές συνδέονται πλέον με το Διαδίκτυο και σε Τοπικό δίκτυο υπολογιστών και διευκολύνουν έτσι τη διάδοση του κακόβουλου κώδικα.
- Μερικές φορές δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου του.
- Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημία, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές χιουμοριστικών. Όμως, ακόμη και αυτοί οι "καλοκάγαθοι" ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών:
  - Να καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του (system crash).
  - Μπορεί να είναι γεμάτοι προγραμματιστικά σφάλματα, τα οποία πιθανόν να οδηγήσουν στην κατάρρευση των υπολογιστικών συστημάτων και στην απώλεια δεδομένων.
  - Ένα μεγάλο ποσοστό των ιών δεν έχει σκοπό την καταστροφή των δεδομένων του χρήστη ή την παρενόχλησή του, αλλά την κλοπή προσωπικών του δεδομένων ή την εισαγωγή του υπολογιστή-στόχου σε κάποιο παράνομο δίκτυο (botnet) χωρίς τη συγκατάθεση του χρήστη.

ΕΙΔΗ ΙΩΝ

- **Malwares:** Κακόβουλο πρόγραμμα που χρησιμοποιείται για να διακόψει τη λειτουργία ενός Η/Υ. να συλλέξει "ευαίσθητες" πληροφορίες ή να αποκτήσει πρόσβαση σε υπολογιστικά συστήματα.
- **Trojan horse:** Λογισμικό που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα.
- **Adwares:** Ονομάζεται οποιοδήποτε πακέτο λογισμικού που αναδύει αυτόματα διαφημίσεις, προκειμένου να δημιουργήσει έσοδα για τον συντάκτη της
- **Spyware:** Spyware (Λογισμικό Κατασκοπίας) αναφερόμαστε σε ένα είδος κακόβουλου λογισμικό το οποίο φορτώνεται κρυφά (με ύπουλο τρόπο) σε έναν υπολογιστή χωρίς να το ξέρει ο χρήστης και εκτελείται στο παρασκήνιο κάνοντας διάφορα πράγματα πίσω από την πλάτη του χρήστη.
- **Worm:** Αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους (υπολογιστές του δικτύου) και μπορεί να το πράξει χωρίς την παρέμβαση του χρήστη.

- Εκκίνηση του Η/Υ από μολυσμένη δισκέτα, δίσκο ή cd.
- Εκτέλεση/άνοιγμα ενός μολυσμένου USB stick.
- Εκτέλεση/άνοιγμα μολυσμένων αρχείων επισυναπτόμενα σε e-mail,ή από τον Η/Υ σας.
- Άνοιγμα/ανάγνωση μολυσμένων ιστοσελίδων .
- Μέσω πρόσβασης στο internet. Συγκεκριμένα, όλα σχεδόν τα λειτουργικά συστήματα, και κυρίως τα Windows, έχουν "τρύπες" ασφαλείας τις οποίες εκμεταλλεύονται κάποιοι ιοί για να μολύνουν τον Η/Υ, ΧΩΡΙΣ να ζητήσουν σε οποιαδήποτε περίπτωση την άδεια του χρήστη για εγκατάσταση κάποιου προγράμματος.

ΤΡΌΠΟΙ ΜΕΤΆΔΟΣΗΣ ΙΏΝ

ΠΡΟΤΆΣΕΙΣ ΠΡΟΣΤΑΣΊΑΣ ΤΟΥ Η/Υ (1)

1.Antivirus
Η συσκευή του Η/Υ αποτελεί το κυριότερο μέρος της εισόδου στο διαδικτυακό χώρο. Ο πιο συνήθης τρόπος και ταυτόχρονα συχνά αποτελεσματικός φαίνεται να είναι η εγκατάσταση ενός antivirus.
Για περιβάλλοντα Microsoft windows που είναι και οι κυριότεροι αποδέκτες ιών, υπάρχει ένας μεγάλος αριθμός διαθέσιμων λογισμικών προστασίας.

Δημοφιλέστερα antivirus

Bitdefender Antivirus Plus

Kaspersky Anti-Virus

Norton AntiVirus

F-Secure Anti-Virus

AVG Anti-Virus

BullGuard Antivirus

G Data AntiVirus

Panda AntiVirus Pro

Avast! Pro Antivirus

Windows Defender

2.Φιλτράρισμα περιεχομένου πλοήγησης.
Το διαδίκτυο και τα περιβάλλοντα εισόδου σε αυτό (φυλλομετρητές) εκ προεπιλογής παρέχουν απρόσκοπτη είσοδο στο περιεχόμενο του ιστού. Αυτό αποτελεί και τη φιλοσοφία του διαδικτύου. Οι ιδιαιτερότητες όμως, των μαθητών χρηστών και της ενσωμάτωσης στην εκπαίδευση, η απρόσκοπτη πρόσβαση σε όλο το διαδικτυακό περιεχόμενο, αυτονόητα μπορεί να καταστεί επιζήμια.
Είναι προφανές ότι η δυνατότητα εισόδου σε ακατάλληλο ή επικίνδυνο ή παραπλανητικό περιεχόμενο πρέπει να περιορίζεται.
Αυτό μπορεί να γίνει με εφαρμογές φιλτραρίσματος της διαδικτυακής πλοήγησης.

ΠΡΟΤΆΣΕΙΣ ΠΡΟΣΤΑΣΊΑΣ ΤΟΥ Η/Υ (2)

ΠΡΟΤΆΣΕΙΣ ΠΡΟΣΤΑΣΊΑΣ ΤΟΥ Η/Υ (3)

Αντιμετώπιση μόλυνσης από ιό.
Απενεργοποίησε την Επαναφορά Συστήματος (αν υπάρχει στα windows)

Ενημέρωσε (internet update) το αντιβιοτικό/antispyware πρόγραμμα που χρησιμοποιείς και έλεγξε πάλι τον Η/Υ.

Κατέβασε κάποιο από τα Avira Free edition, Spybot, Dr.Web CureIt, Ad-Aware Free και Kaspersky Virus Removal Tool και αφού τα εγκαταστήσεις, κάνε για όσα είναι δυνατόν ανανέωση (internet update).

Κάνε επανεκκίνηση του υπολογιστή και μπες στα windows σε ασφαλή λειτουργία πατώντας πριν την εκκίνηση των Windows το πλήκτρο F8. Ψάξε με το καθένα (ένα κάθε φορά) από αυτά όλους τους δίσκους και ότι βρουν επίλεξε να καθαριστεί. Αν κάποιο από τα προγράμματα βρει κάποιον ιό, περίμενε να τελειώσει τον έλεγχο και, αφού καθαρίσει/απομονώσει/διαγράψει τον ιό, κάνε πάλι επανεκκίνηση του υπολογιστή και ψάξε πάλι με το ίδιο πρόγραμμα. Αν δεν βρει τίποτα αυτή τη φορά, συνέχισε ομοίως με έλεγχο από το 2ο πρόγραμμα.

ΑΣΦΆΛΕΙΑ ΧΡΗΣΤΩΝ

- Ασφάλεια είναι όλοι οι κανόνες που πρέπει να ακολουθούμε για τη δική μας προστασία και τι πρέπει να προσέχουμε όταν είμαστε στο διαδίκτυο και χρησιμοποιούμε οποιοδήποτε πρόγραμμα που μας δίνει τη δυνατότητα επικοινωνίας με άλλα παιδιά. Ποτέ δεν πρέπει να δίνουμε προσωπικά στοιχεία σε ανθρώπους που έχουμε γνωρίσει στο διαδίκτυο, π.χ. πού μένουμε, πώς μας λένε…
- Τις πληροφορίες σχετικά με τους κανόνες που πρέπει να ακολουθούμε για να προστατευόμαστε όταν επικοινωνούμε στο διαδίκτυο μπορούμε να τους βρούμε στις παρακάτω ιστοσελίδες:
  - **http://internet-safety.sch.gr/**
  - **http://www.pi.ac.cy/InternetSafety/**
  - **http://www.e-yliko.gr/htmls/pc_use/safety.aspx**
  - **http://www.e-yliko.gr/htmls/Safety/getsafe/index.htm**
  - **http://www.saferinternet.gr/**
  - **http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=135&Itemid=128&lang**

- Η διεύθυνση δίωξης ηλεκτρονικού εγκλήματος απασχολείται πολύ συχνά με περιστατικά όπου ανήλικοι πέφτουν θύματα επιτήδειων στο Internet.
- Όπως επισημαίνουν οι ειδικοί είναι ανησυχητικό το γεγονός ότι ανήλικα παιδιά, παρά την ενημέρωση και τις καμπάνιες που έχουν πραγματοποιηθεί για τους κινδύνους στο διαδίκτυο, συνεχίζουν να πέφτουν θύματα επιτήδειων που τα προσεγγίζουν μέσω διαδικτύου με σκοπό τη δημιουργία πορνογραφικού υλικού.
- Η νέα γενιά αισθάνεται σίγουρη για το χειρισμό της τεχνολογίας. Τα παιδιά θεωρούν ότι ξέρουν τι κάνουν και αυτή η διαβεβαίωση φαίνεται ότι είναι αρκετή για τους γονείς. Αυτό είναι λάθος αφού εφησυχάζουν, δεν ασχολούνται είτε γιατί δεν έχουν χρόνο για να μάθουν τις λειτουργίες του διαδικτύου και τους κινδύνους του ώστε να προστατέψουν τους μικρούς χρήστες.

- Το τελευταίο διάστημα οι κακόβουλες επιθέσεις έχουν πολλαπλασιαστεί και το γεγονός ότι πολλά από τα μηνύματα που έρχονται από «φίλους» περιπλέκει τα πράγματα και δυσκολεύει την προστασία.
- Μια λύση σε αυτό το πρόβλημα θα ήταν οι χρήστες των κοινωνικών δικτύων να εξοικειωθούν με τις ρυθμίσεις ιδιωτικότητας και τις υπηρεσίες ασφαλείας που προσφέρει το κάθε μέσο κοινωνικό δίκτυο

ΥΠΆΡΧΟΥΝ ΜΕΡΙΚΟΊ ΒΑΣΙΚΟΊ ΚΑΝΌΝΕΣ ΑΣΦΑΛΕΊΑΣ ΚΑΙ ΚΑΘΗΜΕΡΙΝΈΣ ΣΥΝΉΘΕΙΕΣ ΓΙΑ ΝΑ ΠΡΟΣΑΡΜΌΣΕΤΕ ΤΑ ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ ΣΤΑ ΜΈΤΡΑ ΣΑΣ.

- Δημόσιο ή Ιδιωτικό προφίλ

Ως προεπιλογή αυτά τα δίκτυα προτείνουν στους χρήστες να δημιουργήσουν ένα δημόσιο προφίλ. Όμως έτσι όσο περισσότεροι βλέπουν το προφίλ σας και πολλαπλασιάζεται ο κίνδυνος ανεπιθύμητων επισκεπτών. Επίσης μπορείτε να δημιουργείτε post για κάποιους χρήστες.

- Το password

Δημιουργείστε ένα ισχυρό password και σε κάποια μέσα σας επιτρέπουν να χρησιμοποιείτε διπλή ταυτοποίηση (facebook, instagram) όπως έναν αριθμό ή ένα token το οποίο στέλνεται στο τηλέφωνό σας σαν μήνυμα.

- Παγίδες στις δήθεν δωρεάν προφορές

Δεν υπάρχουν δωρεάν προσφορές στα κοινωνικά δίκτυα. Αν λάβετε τέτοιο μήνυμα τότε είναι απάτη.

- Προσοχή στα links ανάμεσα στις αναρτήσεις

Τις περισσότερες φορές αυτό γίνεται για να μπουν στο λογαριασμό σας. Να χρησιμοποιείτε τα links μόνο γνωστών σας προσώπων.

- Ψάρεμα στοιχείων (Phishing)

Αν πατήσετε σε αυτό το σύνδεσμο μεταφέρεστε σε μια σελίδα που μοιάζει με τη σελίδα εισόδου του κοινωνικού δικτύου για να πληκτρολογήσετε τον κωδικό σας και αυτός να γνωστοποιηθεί στους απατεώνες.

- Τα likes κοστίζουν ακριβά

Αν θέλετε περισσότερα likes υπάρχουν εταιρείες που αναλαμβάνουν να το κάνουν φυσικά με καλή αμοιβή.