Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

Εργασία Project Β΄ Λυκείου

Υποθέμα: ΑΠΟΚΑΤΑΣΤΑΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΥΠΟΛΟΓΙΣΤΗ

Ομάδα 5:
- **Ζωγραφάκης Σταύρος**
- **Καπελλάκης Μάριος**
- **Κουτσάκης Γιάννης**

Επιβλέπων Καθηγητής: Δετοράκης Ιωάννης

Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Στο σχολικό έτος 2012-13 η ομάδα μας ασχολήθηκε με την αποκατάσταση του ηλεκτρονικού σας υπολογιστή κατόπιν προσβολής από κάποιο ιό. Συγκεκριμένα , ασχοληθήκαμε με τους τρόπους απομάκρυνσης των ιών από τα μέσα αποθήκευσης ,την επαναφορά του υπολογιστή σας στην αρχική του κατάσταση δηλαδή πως μπορούμε να αποκαταστήσουμε τις ζημιές τόσο του λογισμικού όσο και του υλικού όπως προγράμματα και αρχεία.

Ακόμα ασχοληθήκαμε με το πως να επαναφέρετε στοιχεία από αντίγραφα ασφαλείας δηλαδή τι θα πρέπει να περιλαμβάνει ένα αντίγραφο ασφαλείας και πως το επαναφέρω στον ηλεκτρονικό υπολογιστή. Θεωρούμε λοιπόν ,επιτακτική ανάγκη να γνωρίζετε όλα αυτά τα οποία είναι αναγκαία για την ασφαλή διατήρηση του ηλεκτρονικού σας υπολογιστή ,ειδικά σε μια εποχή όπως τη δική μας όπου η έκρηξη της τεχνολογίας μας παρασύρει λ.χ. στη δημιουργία ιών αλλά παράλληλα μας επιβάλλει την προστασία μας από αυτούς.

Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

Απομάκρυνση ιών:

Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη - ορισμένοι, μάλιστα, ιοί, είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία.

Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό (antivirus). Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο.

Τα προγράμματα αυτά πρέπει να αναβαθμίζονται σε τακτική βάση, ώστε να είναι σε θέση να αντιμετωπίζουν με επιτυχία τους νεοδημιουργούμενους ιούς. Σήμερα, αρκετοί οίκοι δημιουργίας λογισμικού ασχολούνται με τη δημιουργία τέτοιων προγραμμάτων.

Τα αντιϊκά είναι σε θέση τόσο να εντοπίσουν μόλυνση τη στιγμή που αποπειράται, όσο και να "καθαρίσουν" τυχόν μολυσμένα αρχεία που εντοπίζουν. Κάθε αντιϊκό έχει το δικό του τρόπο δράσης απέναντι στους ιούς. Ωστόσο, τα περισσότερα είναι σε θέση να εργάζονται σε πραγματικό χρόνο, εντοπίζοντας τους ιούς τη στιγμή ακριβώς που αποπειρώνται να μολύνουν το σύστημα.

Ορισμένα τέτοια προγράμματα προσφέρονται δωρεάν για προσωπική χρήση (δεν καλύπτουν, ωστόσο, ούτε μικρό τοπικό δίκτυο υπολογιστών) και άλλα έναντι σχετικά χαμηλής τιμής (κανένα αντιϊκό για υπολογιστές δικτύου δεν προσφέρεται δωρεάν μέχρι σήμερα

. Θα πρέπει να σημειωθεί ότι οι δημιουργοί ιών λαμβάνουν σοβαρά υπόψη τους τις μεθόδους εντοπισμού του "προϊόντος" τους και δημιουργούν ιούς, οι οποίοι προσπαθούν να αποφύγουν τον εντοπισμό, ακόμη και με απενεργοποίηση του αντιϊκού.

Αυτό σημαίνει ότι ο χρήστης θα πρέπει να ενημερώνει τακτικότατα το λογισμικό του αλλά και να δημιουργεί τις ειδικές δισκέτες, που τα περισσότερα αντιβιοτικά προγράμματα προτείνουν τη δημιουργία τους, ώστε να είναι δυνατή η εκκαθάριση και η επαναφορά του συστήματος μετά από τυχόν μόλυνσή τους.

Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

Οι 12 Χρυσοί Κανόνες για Προστασία των υπολογιστικών συστημάτων του χώρου εργασίας σας

1ος Κανόνας

Ο σκληρός δίσκος του υπολογιστή, δεν θα πρέπει σε καμία περίπτωση να μένει ενιαίος. Αντίθετα θα πρέπει να διαχωρίζεται σε επιμέρους τομείς (partition).

Η ύπαρξη το πολύ 3-4 τομέων (ανάλογα με την χωρητικότητα του σκληρού δίσκου) δεν αποτελεί πρόβλημα, ενώ θα πρέπει όλοι να είναι διαμορφωμένοι με βάση το πρωτόκολλο NTFS. Στον πρώτο τομέα (boot_c), θα πρέπει να εκαθίστανται μόνο τα λογισμικά.

Σε ένα άλλο τομέα τα κείμενα και σε ένα τρίτο οποιοδήποτε άλλο χρήσιμο αρχείο. Ενας τομέας του σκληρού μπορεί να δεσμευτεί και εκεί να αποθηκευτεί σε μορφή ψηφιακής καταγραφής όλος ο πρώτος τομέας, μέσω ειδικού λογισμικού (GHOST).

Με τον τρόπο αυτό όποιος ιός και να μολύνει τον υπολογιστή, ο χρήστης δεν χάνει κάποια από τα κείμενα ή τα χρήσιμα αρχεία, ενώ παράλληλα η λειτουργία του υπολογιστή, αποκαθίσταται σε περίπου 10-15 λεπτά μιας και μέσα στην ψηφιακή καταγραφή έχουν αποθηκευτεί όλες οι ρυθμίσεις του υπολογιστή κατά την εγκατάσταση.

2ος Κανόνας

Το antivirus πρόγραμμά σας χρειάζεται τακτική ενημέρωση (update)

Δεν χρειάζεται να υπενθυμίσουμε ότι όλοι οι υπολογιστές πρέπει να έχουν εγκατεστημένο ένα πρόγραμμα προστασίας από ιούς (antivirus software scanner). Πολλοί χρήστες όμως δεν αντιλαμβάνονται ότι οι antivirus scanners μπορούν να εντοπίσουν και να καταστρέψουν ιούς που περιλαμβάνονται στην τράπεζα πληροφοριών τους (virus database). Δυστυχώς όμως καθημερινά έρχονται στο προσκήνιο καινούργιοι ιοί και για τον λόγο αυτό η συχνή ενημέρωση (μέσω του διαδικτύου πλέον σήμερα) της database των ιών, που μπορεί να εντοπίσει και απενεργοποιήσει το λογισμικό προστασίας ιών του υπολογιστή μας είναι αναγκαία όσο ποτέ άλλοτε.

Η τακτική ενημέρωση του λογισμικού antivirus, για παράδειγμα κάθε εβδομάδα ή και καθημερινά ακόμη (ανάλογα με την προστασία που θέλουμε να έχουμε), βοηθά στην αντιμετώπιση των νέων ιών που εμφανίζονται καθημερινά.

Σχεδόν όλα τα πακέτα προστασίας ιών διαθέτουν ιστοσελίδες στο διαδίκτυο (web sites) απ΄ όπου μπορεί κανείς δωρεάν να ενημερώσει το λογισμικό antivirus του υπολογιστή του. Σε μερικές περιπτώσεις οι ιστοσελίδες αυτές ανανεώνονται περισσότερες από μία φορά την ημέρα !

Ο χρήστης μπορεί να ρυθμίσει τον scheduler του antivirus λογισμικού του υπολογιστή του, ώστε να κατεβάσει από τις σχετικές ιστοσελίδες την ενημερωμένη έκδοση της database με τους νέους ιούς, 2 και 3 φορές την ημέρα (π.χ. το πρωί, το μεσημέρι και το βράδυ). Ας μην ξεχνάμε τις καταστροφές που προκάλεσαν στα αρχεια εκατομμυρίων ανυποψίαστων χρηστών σε όλο τον κόσμο οι ιοί 'I love you', 'Joke' κλπ.

Παράλληλα οι χρήστες θα πρέπει να έχουν εγκαταστήσει στον σταθμό εργασίας τους ένα λογισμικό με την ονομασία "τείχος προστασίας". Αυτό παρέχεται ήδη στην έκδοση του λογισμικού Windows XP και ενεργοποιείται μέσω των ιδιοτήτων του προσαρμογέα δικτύου. Το λογισμικό αυτό αποκρύπτει όσο είναι δυνατόν τα στοιχεία του υπολογιστή (IP ADDRESS) και δεν επιτρέπει τον εντοπισμό αυτού από

επίδοξους εισβολείς. Βέβαια πρέπει να αναφερθεί ότι κανένα αντιϊκό λογισμικό δεν μπορεί να εξασφαλίσει την προστασία του υπολογιστή κατά 100%.

Επίσης έκαστος χρήστης θα πρέπει να έχει εφοδιαστεί με το κατάλληλο λογισμικό για εντοπισμό και απομάκρυνση ιών τύπου spy_ware. Αυτοί εισέρχονται μέσα στον υπολογιστή κατά την χρονική διάρκεια όπου ο χρήστης είναι συνδεδεμένος στο διαδίκτυο και ενώ δεν προκαλούν ζημιά, μπορεί να δίνουν πρόσβαση σε άλλους χρήστες εν αγνοία των πρώτων.

3ος Κανόνας :

Μην ανοίγετε επισυναπτόμενα αρχείο (attachments) στα Emails που προέρχονται από άγνωστες πηγές.

Έχει γίνει πλέον συνήθεια οι ιοί να στέλνονται σαν attachments σε ηλεκτρονικά ταχυδρομεία, ιδιαίτερα από γνωστούς και φίλους. Οι μοντέρνες μέθοδοι που χρησιμοποιούν τα προγράμματα των ιών είναι να δημιουργούν αυτόματα πληθώρα ηλεκτρονικών ταχυδρομείων από το Email address book (λίστα με διευθύνσεις) ενός χρήστη που έχει μολυνθεί και να τα στέλνουν σε όλους τους φίλους και γνωστούς με τους οποίους αυτός επικοινωνεί...

Το κείμενο που περιέχεται στο Email με το μολυσμένο attachment, πολλές φορές είναι γνώριμο στον παραλήπτη μιας και περιέχει την υπογραφή ενός φίλου, οδηγώντας το υποψήφιο θύμα να ανοίξει το attachment χωρίς να υποψιαστεί τίποτε.

Ιδιαίτερη προσοχή χρειάζεται στο άνοιγμα αρχείων (attachments) με EXE extension που είναι εκτελούμενα προγράμματα, χωρίς αυτό να σημαίνει ότι τα υπόλοιπα αρχεία είναι λιγότερο επικίνδυνα. Αν νομίζετε ότι αρχεία με extension .PIF, .GIF, ακόμη και .TXT είναι ασφαλή έχετε λάθος. Ακόμη και τέτοια αρχεία μπορεί να μεταφέρουν ιούς. Ας μην ξεχνάμε πόσο εύκολο είναι να γίνει rename ένα αρχείο exe σε txt για παράδειγμα.

Μην ανοίγετε αρχεία αν δεν τα έχετε προηγουμένως ελέγξει με τον anti-virus scanner. Τα σύγχρονα προγράμματα anti-virus μπορεί να ρυθμιστούν για να ανιχνεύουν ιούς στα Emails που λαμβάνονται. Κατά τακτά χρονικά διαστήματα θα πρέπει ο χρήστης να δημιουργεί αντίγραφα ασφαλείας τόσο των ηλεκτρονικών μηνυμάτων όσο και των ηλεκτρονικών διευθύνσεων (επαφών) που διαθέτει στον σταθμό εργασίας του.

4ος Κανόνας :

Περιορίστε τον αριθμό των χρηστών που έχουν πρόσβαση στον υπολογιστή σας.Γνωρίζετε ότι η χρήση μαλακών δίσκων -floppy discs- και CD-ROMs από άτομα που έχουν πρόσβαση στον υπολογιστή σας, μπορεί να μεταφέρει ιούς στον υπολογιστή σας. Ένας χρήστης του υπολογιστή σας, ο οποίος δεν τηρεί τους κανόνες ασφάλειας (όπως αυτοί που αναφέρονται στο παρόν άρθρο) μπορεί να επιφέρει ανεπανόρθωτη ζημιά στον υπολογιστή σας και τα ανυπολογίστου αξίας δεδομένα που τηρείτε σε αυτόν.

Ως μια καλή λύση είναι η αποθήκευση των δεδομένων και γενικά χρήσιμων αρχείων σε διαφορετικό τμήμα του σκληρού δίσκου (partition), από αυτό των λογισμικών. Θα πρέπει να δημιουργούνται πέραν του ενός λογαριασμού "τύπου διαχειριστή¨", με χρήση κωδικού ασφαλείας.

Έτσι στην περίπτωση όπου ο λογαριασμός administrator (Windows 2000, XP), έχει πρόβλημα, να μπορεί ο χρήστης να εισέρχεται με τον δεύτερο λογαριασμό.

Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

5ος Κανόνας :

Εγκαθιστάτε τις νέες εκδόσεις λογισμικού που σκοπό έχουν την προστασία από τρύπες ασφάλειας

Υπάρχουν πολλοί ιοί σήμερα που χρησιμοποιούν 'τρύπες' και αδυναμίες των λειτουργικών συστημάτων και των εφαρμογών.

Για το λόγο αυτό να επισκέφτεστε τακτικά τις ιστοσελίδες του κατασκευαστή του λειτουργικού ή της εφαρμογής που τρέχετε στον υπολογιστή σας αναζητώντας νέες εκδόσεις (patches - μπαλώματα) τις οποίες μπορείτε να κατεβάσετε δωρεάν μέσω του διαδικτύου, ώστε να προστατεύσετε τον υπολογιστή σας από τις γνωστές (σε όλους και ιδιαίτερα στους hackers) αδυναμίες του λογισμικού που χρησιμοποιείτε.

Με χρήση της εντολής WINDOWS UPDATE, ο υπολογιστής ενημερώνεται αυτόματα με τις υπάρχουσες ασφαλιστικές δικλείδες.

6ος Κανόνας :

Ελέγχετε με το πρόγραμμα antivirus κάθε νέα δισκέττα ή CD, πριν τη χρήση στον υπολογιστή σας.

Παρόλον ότι το 85 % μολύνσεως με ιούς γίνεται μέσω Email, δεν θα πρέπει να λησμονούμε ότι το υπόλοιπο 15 % οφείλεται στην μόλυνση από δισκέττες, CDs και άλλα μαγνητικά-οπτικά μέσα αποθήκευσης δεδομένων. Δισκέττες και CDs με πειρατικό λογισμικό έχουν σε μεγάλο ποσοστό (σύμφωνα με έρευνα των εργαστηρίων Kaspersky το ποσοστό αυτό είναι περίπου 25 %) μολυνθεί με ιούς.

7ος Κανόνας :

Προσέχετε ακόμη και το λογισμικό από επίσημες πηγές ...

Ελέγχετε όπου αυτό είναι δυνατό και το λογισμικό από επίσημες πηγές (licensed CDs).

Ακόμη και αυτό το λογισμικό μπορεί να περιέχει ιούς. Όπου υπάρχει ψηφιακή υπογραφή του λογισμικού ελέγξετε την ψηφιακή υπογραφή του αντιγράφου σας, με εκείνη που δίνει ο κατασκευαστής του λογισμικού.

Το λογισμικό που κατεβάζετε από το διαδίκτυο μπορεί να περιέχει ιούς. Ακόμη και αν το λογισμικό αυτό προέρχεται από ιστοσελίδες μεγάλων & γνωστών εταιρειών.

Ας μη ξεχνάμε την επιτυχή επίθεση hackers, που έγινε στις αρχές του 2001 στην Microsoft (στις ιστοσελίδες με αντίγραφα προγραμμάτων της εταιρείας...)

8ος κανόνας:

Σε περίπτωση όπου ο υπολογιστή σας μολυνθεί από κάποιο ιό και αυτός δεν μπορεί να απομακρυνθεί, τότε είναι αναγκαία η δημιουργία αντιγράφου των δεδομένων του υπολογιστή.

Η διαδικασία αυτή θα πρέπει να γίνεται με χρήση επανεγράψιμων CDs / DVDs. Ο λόγος είναι ότι στην περίπτωση που εντοπιστεί κάποιο μολυσμένο αρχείο στο επανεγράψιμο, αυτό μπορεί να διαγραφεί, ενώ σε δίσκους μιας χρήσης αυτό δεν είναι εφικτό.

Αποφύγετε να συνδέσετε τον υπολογιστή στο δίκτυο καθώς και με άλλο υπολογιστή μέσω ethernet cable, usb cable και γενικά δικτύου. Ο καλύτερος τρόπος είναι να απομακρύνεται τον σκληρό δίσκο απο τον μολυσμένο υπολογιστή και να τον τοποθετήσετε σε ένα άλλο υγιή ως slave.

Με τον τρόπο αυτό δεν χρησιμοποιείται το λογισμικό του μολυσμένου σκληρού και ο ιός εντοπίζεται άμεσα.

Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

9ος Κανόνας :

Συνδιάστε διάφορες τεχνικές anti-virus

Μην καθησυχάζετε με την αυτόματη έναρξη ενός προγράμματος antivirus σε τακτικά διαστήματα στον υπολογιστή σας.

Υπάρχουν και άλλες τεχνικές οι οποίες όταν συνδυαστούν με το πρόγραμμα antivirus που τρέχει τακτικά στον υπολογιστή σας, μπορεί να δώσουν καλύτερη ασφάλεια. Για το σκοπό αυτό μπορείτε να εγκαταστήσετε:

- Ένα antivirus monitor. Αυτό είναι ένα πρόγραμμα που είναι μόνιμα φορτωμένο στην μνήμη (memory resident) και το οποίο ελέγχει όλα τα αρχεία πριν ανοίξουν στον υπολογιστή σας.
- Ένα integrity checker που ελέγχει την ακεραιότητα των δεδομένων. Ο integrity checker ελέγχει αρχεία, υποκαταλόγους και disc sectors για οποιαδήποτε μεταβολή που μπορεί να αποτελεί ένδειξη μόλυνσης από ιό και ενημερώνει τον χρήστη του υπολογιστή ανάλογα.
- Ένα 'φρουρό συμπεριφοράς' (behavioural guard). Αυτός ελέγχει για ιούς όχι μόνο από την μοναδιαία 'υπογραφή' του λογισμικού αλλά και από τον τρόπο συμπεριφοράς και τη σειρά ενεργειών που εκτελεί το ύποπτο πρόγραμμα.

Ο συνδυασμός των παραπάνω μπορεί να δώσει μεγαλύτερη ασφάλεια.

10ος Κανόνας :

Δημιουργήστε ένα δίσκο εκκίνησης (start-up disk) ελεύθερο από ιούς και φυλάξτε τον σε ασφαλές μέρος (για ώρα ανάγκης)

Σε πολλές περιπτώσεις ένας μολυσμένος υπολογιστής δεν μπορεί να ξεκινήσει, παρόλον ότι ο ιός μπορεί να μην έχει σβήσει χρήσιμα δεδομένα από τον υπολογιστή σας.

Στις περιπτώσεις αυτές χρησιμοποιείται τη δισκέτα ή το CD το οποίο έχετε φτιάξει για το σκοπό αυτό προηγουμένως με τη βοήθεια του antivirus προγράμματος του υπολογιστή σας.

Η δισκέτα ή το CD θα σας βγάλει ασπροπρόσωπους σε δύσκολες καταστάσεις, αφού μπορεί να ξεκινήσει τον υπολογιστή σας και να σας βοηθήσει να σβήσετε τους ιούς που έχουν μολύνει τον υπολογιστή σας (Μόνο για Windows 95,98,Me).

11ος Κανόνας :

Παίρνετε τακτικά αντίγραφα (back-up) των αρχείων σας

Σε περίπτωση που χρήσιμα δεδομένα του υπολογιστή σας καταστραφούν από διάφορες αιτίες (που περιλαμβάνουν μόλυνση με ιούς) η χρήση αντιγράφων ασφαλείας (back-up) μπορεί να σας βοηθήσει στην επανάκτηση των αρχείων σας.

Σε αντίθετη περίπτωση μπορεί να χάσετε αρχεία που αντιστοιχούν σε μήνες ή χρόνια δουλειάς (με καταστρεπτικές συνέπειες για την εργασία σας).

Τα αντίγραφα θα πρέπει να τηρούνται και σε χώρο μακριά από το χώρο δουλειάς σας, έτσι ώστε σε περίπτωση πυρκαγιάς να μην υποστείτε ανεπανόρθωτη ζημιά.

12ος Κανόνας :

Μην πανικοβάλεστε

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.

Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

Η επικινδυνότητα υψηλών χρεώσεων στο διαδίκτυο (Internet) - ΟΙ ΡΟΖ ΠΑΓΙΔΕΣ

Οι ιστοσελίδες αυτές που διαφημίζονται και από κανάλια τηλεόρασης, προκαλούν το κοινό να δει ΄καυτά videos΄, εντελώς δωρεάν, με πρόσβαση στο αντίστοιχο web site. Αν πειστεί ο χρήστης να "κατεβάσει" στον υπολογιστή του το λογισμικό, με το οποίο θα δει τα υποτιθέμενα δωρεάν videos... ... Τι γίνεται στη συνέχεια; Φορτώνεται στον υπολογιστή τους το λογισμικό που λίγο πριν έχουν απ&omicron

8 Εύκολα βήματα για να καταργήσετε Ιό

Έχουμε διαπιστώσει ότι οι επισκέπτες μας έχουν αφαιρέσει πολλούς ιούς ακολουθώντας τα οχτώ εύκολα βήματα παρακάτω. Αν ακολουθήσετε αυτά τα βήματα όπως ακριβώς αναφέρονται δεν θα πρέπει να έχετε οποιαδήποτε προβλήματα αφαιρώντας λοιμώξεις από τον υπολογιστή σας.

Βήμα 1

Επανεκκινήστε τον υπολογιστή σας

Για να ξεκινήσετε προχωρήστε και επανακκινήστε τον υπολογιστή που έχει προσβληθεί. Αν ο μολυσμένος υπολογιστή είναι απενεργοποιημένος, ενεργοποιήστε τον.

Βήμα 2

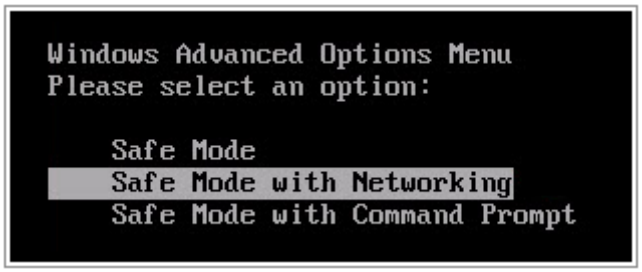
Πιέστε το πλήκτρο F8 κατά την επανεκκίνηση του υπολογιστή

Αμέσως, ο υπολογιστής αρχίζει να κάνει εκκινήση, πατήστε το πλήκτρο F8 πολλές φορές. Πατώντας το πλήκτρο F8 μπορείτε να αποκτήσετε πρόσβαση στο μενού επιλογών για προχωρημένους.

Βήμα 3

Επιλέξτε Safe Mode with Networking

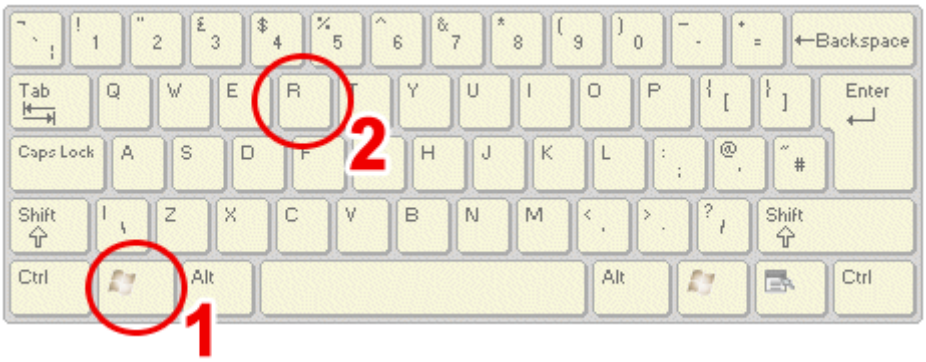
Μόλις είστε στο μενού επιλογών για προχωρημένους, χρησιμοποιήστε τα βέλη σας και επιλέξτε το Safe Mode with Networking επιλογή. Πατήστε enter όταν έχετε επιλέξει αυτή τη δυνατότητα. Τα Windows θα είναι πλέον εκκίνηση σε Safe Mode with Networking.



Βήμα 4

Ανοίξτε παράθυρο Run

Τώρα που ο ιός δεν είναι σε εγρήγορση είναι καιρός να αρχίσετε την αφαίρεση. Στο πληκτρολόγιό σας, κάντε κλικ και κρατήστε το πλήκτρο των Windows, στη συνέχεια πιέστε το πλήκτρο R. Δείτε παρακάτω διάγραμμα πληκτρολόγιο.



Βήμα 5

Εισάγετε το URL «απομάκρυνση» και πατήστε «enter»

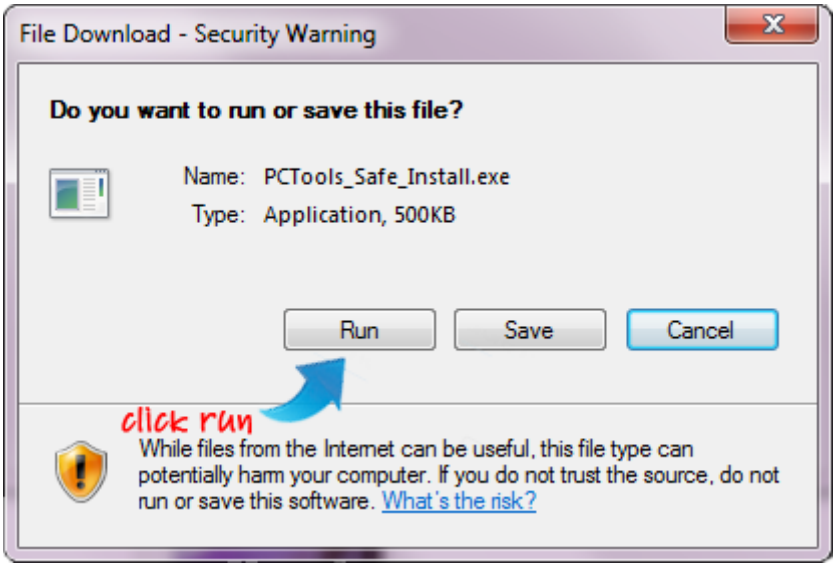
Αφού πατήσετε το Windows και το πλήκτρο R, πλαίσιο Εκτέλεση των Windows θα ανοίξει. Πληκτρολογήστε ακριβώς αυτά που βρίσκονται μέσα στο πλαίσιο στο εξής παράθυρο εκτέλεσης

««Iexplore http://www.spywarehelpcenter.com/»»remove και μετά κάντε κλικ στο OK: Αφού κάνετε κλικ στο OK, ο υπολογιστής σας θα συνδεθεί με την ιστοσελίδα μας και μετά να κατεβάσετε το πρόγραμμα το οποίο ονομάζεται ιός Spyware Doctor με PC Tools.

Βήμα *6*

Εκτελέστε την «PC» Tools αρχείο εγκατάστασης

Όταν δείτε το PC Tools Download κουτί, Κάντε κλικ στο κουμπί «Run». . Αφού κάνετε κλικ στο “Εκτέλεση” κουμπί, PC Tools θα ξεκινήσει. Αν ο υπολογιστής σας ρωτά εάν είστε σίγουροι ότι θέλετε να εκτελέσετε PC Tools, κάντε κλικ στο OK. Ο PC Tools εγκατάστασης θα ξεκινήσει. Μετά την πλήρη εγκατάσταση PC Tools η σάρωση του ιού θα αρχίσει αυτόματα να.



Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

Βήμα 7

Η PC Tools θα σαρώσει τον υπολογιστή σας

Μετά αφού PC Tools έχει σαρώσει τον υπολογιστή σας και έχει βρει τον ιό είναι καιρός να το αφαιρέσετε. Απλά κάντε κλικ στο "Fix είναι ελεγμένο" για να αφαιρέσετε τον ιό.

*Παρακαλείστε να σημειώσετε: Δεν θα δείτε το πραγματικό όνομα του ιού στη λίστα των λοιμώξεων που βρέθηκαν. Το όνομα του ιού στο PC Tools βάση δεδομένων είναι διαφορετικό από το όνομα του ιού που βλέπετε στον υπολογιστή σας. Αν δείτε διάφορες λοιμώξεις στα αποτελέσματα σάρωσης τότε αυτό σημαίνει ότι PC Tools βρήκε τον ιό.

Βήμα 8

Στερεώστε ,ελέγξτεκαι καταχωρήσετε την PC Tools

Αφού κάνετε κλικ στο κουμπί "Fix είναι ελεγμένο" θα έχετε την ευκαιρία να χρειαστεί να εγγραφείτε PC Tools για να αφαιρέσετε τον ιό. Παρακαλούμε εγγραφείτε στο PC Tools και ο ιός θα αφαιρεθεί.

Εγγραφή στο PC Tools προσφέρει υψηλού επιπέδου παροχές, συμπεριλαμβανομένων σε πραγματικό χρόνο ,συνεχή προστασία έναντι πιθανών απειλών.

Θα εντοπίζει και θα απομακρύνει τυχόν μελλοντικές απειλές που μπορεί να προκύψουν, συμπεριλαμβανομένων των ιών, λογισμικό υποκλοπής spyware, trojans, μητρώου λοιμώξεις και περισσότερα.

Είναι μια μεγάλη όλα-σε-ένα λύση για τις ανάγκες της ασφάλειας του υπολογιστή σας και γι 'αυτό το συνιστούμε.

Μετά την εγγραφή στο PC Tools, ο ιός θα αφαιρεθεί, και μετά θα μπορείτε με ασφάλεια να κάνετε επανεκκίνηση σε κανονική κατάσταση λειτουργίας. Ο ιός θα έχει καταργηθεί μετά την επανεκκίνηση του ηλεκτρονικού υπολογιστή.

Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

Επαναφορά ηλεκτρονικού υπολογιστή στην αρχική του κατάσταση

Από ποια μέρει αποτελείται ένα υπολογιστικό σύστημα τα οποία κινδυνεύουν από τον ιό και ποιοι είναι οι τρόποι επαναφοράς του στην αρχική του κατάσταση;

Το υλικό (hardware)

Αναφέρεται σε όλες τις συσκευές και τα εξαρτήματα από τα οποία αποτελείται ένας Η/Υ. Περιλαμβάνει ότι μπορούμε να δούμε και να αγγίξουμε σε ένα Η/Υ.

Μέρη Κεντρικής Μονάδας

Το μόνο εξάρτημα το οποίο μπορεί να προσβληθεί από κάποιο ιό και είναι μέρος της κεντρικής μονάδας είναι η μητρική κάρτα(Motherboard M/B)ή Κύρια Κάρτα (Mainboard).Η μητρική κάρτα ή αλλιώς Κύρια κάρτα είναι ένα μεγάλο τυπωμένο κύκλωμα στο οποίο συνδέονται και μέσω του οποίου επικοινωνούν όλες οι μονάδες του ηλεκτρονικού υπολογιστή. Η μητρική κάρτα περιλαμβάνει τα εξής

- Υποδοχή τοποθέτησης του επεξεργαστή
- Δίνει τη δυνατότητα αλλαγής του επεξεργαστή με άλλο μεγαλύτερης
- ταχύτητας (αναβάθμιση επεξεργαστή)
- Υποδοχή σύνδεσης μνήμης
- Υποδοχή βύσματος τροφοδοσίας
- Ελεγκτή με δύο υποδοχές για σύνδεση σκληρών δίσκων και μονάδων CD-ROM τύπου IDE
- Ελεγκτή με υποδοχή για σύνδεση μονάδων δισκέτας
- Ελεγκτής με βύσμα (θύρα) για

α. είσοδο πληκτρολογίου τύπου PS2
β. είσοδο ποντικιού τύπου PS2
γ. παράλληλη επικοινωνία (parallel port)
δ. σειριακή επικοινωνία (serial port)
ε. σύνδεση τύπου USB (Universal Serial Bus)

7. Υποδοχές επέκτασης τύπου ISA, PCI, AGP
8. Διάδρομοι επικοινωνίας με ελεγκτές διαδρόμων επικοινωνίας
9. Ολοκληρωμένο ρολόι ‘’συστήματος’’
10. Ολοκληρωμένο κύκλωμα Βασικού Συστήματος Εισόδου – Εξόδου (Basic Input-Output System, BIOS)

Τρόποι αποκατάστασης μητρικής κάρτας

Όλα τα παραπάνω συνδέονται με την μητρική κάρτα ή αλλιώς με την κύρια κάρτα άρα αυτό σημαίνει ότι αν καταστραφεί η μητρική κάρτα από την εισβολή ιού τότε ο ηλεκτρονικός υπολογιστής είναι άχρηστος αφού πάνω σ’αυτόν συνδέονται όλες οι επιμέρους κάρτες γραφικών. Η λύση είναι είτε να αγοράσει μία καινούρια κάρτα μνήμης όπου μπορεί να μην το συμφέρει είτε να αγοράσει ένα καινούριο ηλ3εκτρονικό υπολογιστή.

Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

Το λογισμικό(software)

Ένας Η/Υ δεν μπορεί να λειτουργήσει αν δεν του εισάγουμε μια σειρά εντολών για να τις εκτελέσει. Το λογισμικό είναι αυτό που δίνει ΄΄πνοή΄΄ στο υλικό.

Το λογισμικό χωρίζεται σε δύο υποδιέστερες κατηγορίες:

1. Λογισμικό Συστήματος.

Περιλαμβάνει το Λειτουργικό Σύστημα (Operating System, OS)

Το λειτουργικό Σύστημα είναι ένα σύνολο προγραμμάτων το οποίο μας επιτρέπει να λειτουργήσουμε τον υπολογιστή αλλά και να ΄΄τρέξουμε΄΄ την πληθώρα των προγραμμάτων. Μας προσφέρει ένα περιβάλλον επικοινωνίας ανάμεσα στον Η/Υ και στο χρήστη. Είναι ο σύνδεσμος (ενδιάμεσος) ανάμεσα στο χρήστη και το υλικό μέρος

Τρόποι αποκατάστασης λογισμικού συστήματος: Οι τρόποι αποκατάστασης του λογισμικού (software) χωρίζεται σε δύο κατηγορίες: Η πρώτη είναι η ολική επαναφορά του συστήματος από μία πλήρης εικόνα που έχουμε είδη φροντίσει να κρατήσουμε (με το πρόγραμμα ghost,acronis) και μετά επιμέρους back ups για σημαντικά έγγραφα. Ενώ η δεύτερη είναι να επαναφέρουμε αρχεία μόνο του χρήστη.

2. Προγράμματα – Εφαρμογές.

Πρόγραμμα ονομάζουμε μια σειρά εντολών που έχουμε γράψει. Τις εντολές αυτές εκτελεί ο Η/Υ με σκοπό να επεξεργαστεί κατάλληλα τα δεδομένα που του δίνουμε ώστε να ολοκληρωθεί μία συγκεκριμένη εργασία.

Τρόποι αποκατάστασης προγραμμάτων-εφαρμογών:

Οι τρόποι αποκατάστασης των προγραμμάτων είναι εύκολος αφού μπορείς να δημιουργήσεις ένα back up έτσι ώστε να διασωθούν όλα τα προγράμματα ή αλλιώς αν δεν δημιουργήσεις ένα back up μπορείς να τα ξαναστήσεις από την αρχή.
Στις εφαρμογές δεν μπορείς να δημιουργήσεις back up παραμόνο να της ξανακατεβάσεις και να τις εγκαταστήσεις στον ηλεκτρονικό σου υπολογιστή ξανά.

Επαναφορά στοιχείων από αντίγραφο ασφαλείας

Τα αντίγραφα ασφαλείας είναι ίσως η πιο σημαντική εργασία που πρέπει να κάνουμε σε τακτά χρονικά διαστήματα για την αποφυγή απώλειας δεδομένων.

Αυτή η διαδικασία θα μας σώσει από μια μελλοντική καταστροφή που θα μπορούσε να προκληθεί από καταστροφή κάποιου σκληρού δίσκου, τη δράση ενός κακόβουλου λογισμικού έναν λάθος χειρισμό κτλ.

Τα αρχεία στο σκληρό δίσκο του υπολογιστή μας ποτέ δεν μπορούμε να θεωρήσουμε ότι είναι ασφαλή με οποιονδήποτε τρόπο και να τα προστατεύσουμε τον υπολογιστή.

Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

ΧΡΗΣΙΜΟΤΗΤΑ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ

Η δημιουργία αντιγράφων ασφαλείας των αρχείων σας προστατεύει από τη μόνιμη απώλεια ή αλλαγή τους σε περίπτωση ακούσιας διαγραφής τους, επίθεσης από ιό τύπου worm ή από ιό ή σε περίπτωση αστοχίας του λογισμικού ή του υλικού. Εάν συμβεί κάτι από τα παραπάνω και έχετε δημιουργήσει αντίγραφα ασφαλείας των αρχείων σας, τότε μπορείτε εύκολα να κάνετε επαναφορά αυτών των αρχείων.

ΣΕ ΠΟΙΑ ΑΡΧΕΙΑ ΠΡΕΠΕΙ ΝΑ ΕΧΩ ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ

Πρέπει να δημιουργηθούν αντίγραφα ασφαλείας για οποιοδήποτε αρχείο είναι δύσκολη ή αδύνατη η αντικατάστασή του, ενώ θα πρέπει να δημιουργείτε αντίγραφα ασφαλείας για τα αρχεία που αλλάζετε συχνά. Εικόνες, βίντεο, μουσική, έργα και οικονομικά στοιχεία είναι μερικά παραδείγματα αρχείων για τα οποία πρέπει να δημιουργείτε αντίγραφα ασφαλείας .Δεν χρειάζεται να δημιουργείτε αντίγραφα ασφαλείας για προγράμματα διότι μπορείτε να χρησιμοποιήσετε τους δίσκους των αρχικών προϊόντων για να κάνετε επανεγκατάσταση τους, ενώ παράλληλα τα προγράμματα καταλαμβάνουν πολύ χώρο στο δίσκο.

Τρόπος δημιουργίας αντιγράφων ασφαλείας

Οι τρόποι που μπορούμε να κρατάμε αντίγραφα ποικίλουν :

Α) ως προς το τρόπο λήψης τους

- Χειροκίνητη διαδικασία (Τις αντιγραφές τις κάνουμε μόνοι μας).
- Χρήση Ειδικού Προγράμματος (Αυτόματα, ή όχι)

Β) ως προς τα αποθηκευτικά μέσα

- Ειδικές συσκευές αντιγράφων ασφαλείας
- Εσωτερικός ή εξωτερικός σκληρός δίσκος
- Αφαιρούμενα αποθηκευτικά μέσα όπως DVD-R, CD-R , Tapes κτλ.

Γ) ως προς το είδος δημιουργίας

- Αντίγραφα δεδομένων μόνο των Αρχείων μας.
- Αντίγραφα δεδομένων μόνο του Λειτουργικού Συστήματος.
- Αντίγραφα δεδομένων ολόκληρου του σκληρού δίσκου. (Λειτουργικό + Αρχεία).

Παρακάτω θα αναλύσουμε τα μέσα δημιουργίας Αντιγράφων Ασφαλείας.Κατ' αρχήν θα πρέπει να αποφασίσουμε τι μέσο θα χρησιμοποιήσουμε για να αποθηκεύσουμε τα Αντίγραφα Ασφαλείας.

- DVD ή CD (χρησιμοποιούμε την λύση αυτή όταν το μέγεθος των αρχείων μας μπορεί να χωρέσει σε ένα ή δύο από αυτά. Όταν χρειάζεται μεγάλη ποσότητα DVDs ή CDs προτιμούμε άλλη λύση).
- Δεύτερος Εσωτερικός Σκληρός Δίσκος στον ΗΥ μας (Καλή λύση προτείνεται αρκεί ο δεύτερος σκληρός δίσκος να είναι διαφορετικό μηχάνημα και να μην είναι απλά ο ίδιος δίσκος χωρισμένος σε δύο κομμάτια).
- Εξωτερικός Σκληρός Δίσκος (πολύ καλή λύση προτείνεται).
- Σε άλλον ΗΥ που βρίσκεται στο δίκτυό μας (καλή λύση προτείνεται, ίσως αργεί η μεταφορά).
- Σε USB Flash Disk ή σε Δισκέτα (να αποφεύγουμε αυτόν τον τρόπο δεν είναι ασφαλής).

Οι Ιοί των Ηλεκτρονικών Υπολογιστών
Αποκατάσταση Ηλεκτρονικού Υπολογιστή

Το επόμενο που θα πρέπει να ξέρουμε είναι το ποιά είναι εκείνα τα αρχεία που μας είναι πραγματικά χρήσιμα, που βρίσκονται, τί μέγεθος έχουν για να τα συμπεριλάβουμε στα Αντίγραφα Ασφαλείας.

Πόσο συχνά πρέπει να δημιουργούνται αντίγραφα ασφαλείας.

Εξαρτάται από τον αριθμό των αρχείων που δημιουργείτε και τη συχνότητα δημιουργίας τους. Εάν δημιουργείτε νέα αρχεία κάθε μέρα, τότε ίσως πρέπει να δημιουργείτε αντίγραφα ασφαλείας κάθε εβδομάδα ή και κάθε μέρα. Εάν δημιουργείτε πολλά αρχεία περιστασιακά, για παράδειγμα, όταν αποθηκεύετε πολλές ψηφιακές φωτογραφίες από ένα πάρτι γενεθλίων ή μια αποφοίτηση, τότε δημιουργήστε τα αντίγραφα ασφαλείας αμέσως. Καλύτερα είναι να προγραμματίσετε τακτική, αυτόματη δημιουργία αντιγράφων ασφαλείας έτσι ώστε να μην χρειάζεται καν να το σκεφτείτε. Μπορείτε να επιλέξετε την καθημερινή, εβδομαδιαία ή μηνιαία δημιουργία αντιγράφων ασφαλείας. Μπορείτε επίσης να δημιουργείτε αντίγραφα ασφαλείας με μη αυτόματο τρόπο, μεταξύ των αυτόματων αντιγράφων ασφαλείας.