Α.Τ.Ε.Ι.Θ.
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΚΑΘΗΓΗΤΗΣ: Δρ. ΕΛΕΥΘΕΡΙΟΣ ΜΠΟΖΙΟΣ

ΕΡΓΑΣΙΑ

Δεκάλογος Ασφάλειας MS Windows

ΦΟΙΤΗΤΕΣ

ΔΙΑΜΑΝΤΗΣ ΔΗΜΗΤΡΙΟΣ

ΜΑΤΙΚΑΣ ΑΘΑΝΑΣΙΟΣ

ΔΕΚΕΜΒΡΙΟΣ 2006

ΠΕΡΙΕΧΟΜΕΝΑ

1. Εισαγωγή

1.1. Ασφάλεια Γενικά

Με τον όρο "ασφάλεια" εννοούμε την προστασία των δεδομένων,των συστημάτων, των εφαρμογών και των υπηρεσιών από φυσικές καταστροφές, ανθρώπινα σφάλματα και κακόβουλες ενέργειες, έτσι ώστε να ελαχιστοποιείται ο κίνδυνος, και ταυτόχρονα η επίδραση που θα έχει μια πιθανή διαρροή ή απώλεια δεδομένων να είναι σε αποδεκτό επίπεδο, τέτοιο ώστε να μπορεί να διορθωθεί.
Τα τελευταία χρόνια με τις όλο και φθηνότερες υπηρεσίες για την γρήγορη πρόσβαση στο διαδίκτυο και με την ταυτόχρονη πτώση των τιμών των PC, οι χρήστες τους έχουν αυξηθεί και πλέον σε μερικά χρόνια το ποσοστό αυτών που θα τα χρησιμοποιούν θα είναι μεγαλύτερο σε σχέση με αυτούς που δεν τα χρησιμοποιούν. Ταυτόχρονα με την ανάπτυξη των παραπάνω αγαθών και την αύξηση των χρηστών τους , η ασφάλεια έχει μειωθεί σε τέτοιο βαθμό που η απόλυτη ασφάλεια δεν είναι εφικτή σε καμία περίπτωση και ειδικά στην περίπτωση που ο υπολογιστής μας είναι συνδεδεμένος στο διαδίκτυο. Το ότι δεν μπορούμε να πετύχουμε την απόλυτη ασφάλεια αυτό δεν σημαίνει και ότι δεν μπορούμε να την επιτύχουμε σε κάποιο μεγάλο βαθμό.

1.2. Λανθασμένες εντυπώσεις για την ασφάλεια

Συνήθως οι χρήστες και ειδικά όσοι δεν έχουν τις κατάλληλες γνώσεις, έχουν δημιουργήσει κάποιες λανθασμένες εντυπώσεις για την ασφάλεια των Η/Υ .Οι πέντε ποιο γνωστές είναι οι εξής:

1. Δεν έχω σημαντικά πράγματα στον Η/Υ μου, άρα δεν ανησυχώ για την ασφάλεια του.

Σήμερα viruses, worms, threats (όπως Love Bug, Nimda, and Blaster) διαδίδονται μέσω του Internet σε εκατομμύρια PCs σε λίγες ώρες, δεν τους ενδιαφέρει ποιος είναι ο ιδιοκτήτης, τι έχει αποθηκευμένο και πόσο σημαντικό είναι. Ο σκοπός τους είναι να εξαπλώσουν την καταστροφή. Το σίγουρο είναι ότι κάποια στιγμή ο Η/Υ σας θα κτυπηθεί. Ακόμα και αν δεν είναι στόχος άμεσης επίθεσης / καταστροφής μπορεί να χρησιμοποιηθεί ως “zombie” για επιθέσεις “denial-of-service” ή για την αποστολή spam ή για την διάδοση πορνογραφικού υλικού (pornography) σε άλλους Η/Υ χωρίς να γίνεται αντιληπτός. Συνεπώς ως υπεύθυνοι πολίτες έχετε την υποχρέωση να προστατεύετε τον Η/Υ ώστε οι άλλοι να είναι ασφαλείς.

2. Μπορώ να προστατεύσω το Η/Υ μου αν τον αποσυνδέω από τον Internet ή αν τον σβήνω όταν δεν τον χρειάζομαι.

Λάθος. Ακόμα και αν δεν έχετε καθόλου σύνδεση στο Internet είστε στόχος! Μπορείτε να κατεβάσετε ένα ιό τη στιγμή που είστε συνδεδεμένοι αλλά να ενεργοποιηθεί μέρες αργότερα όταν θα πάτε να διαβάσετε το e-mail σας, εκτός σύνδεσης. Ακόμα και αν συνδέεστε στο Internet πολύ σπάνια μπορείτε να

"κολλήστε" ιό από κάποιο αρχείο δισκέτας, USB flash memory, CD κλπ.

3. Μπορώ να προστατευτώ από τους ιούς αν δεν ανοίγω ύποπτα e-mails / επισυναπτόμενα.

Λάθος και πάλι. Ο επόμενος ιός που θα λάβετε θα προέρχεται από τον καλύτερο σας φίλο ή τον συνάδελφο ή το προϊστάμενο σας ο οποίος είχε την διεύθυνση σας στο βιβλίο του και ο Η/Υ του χρησιμοποιήθηκε για την διάδοση του ιού. Άλλοι ιοί εισέρχονται μέσω του Web browser (όπως ο Nimda και άλλοι hybrid worms). Είναι επίσης δυνατό να ενεργοποιηθεί ο ιός απλά διαβάζοντας το e-mail σας. Συμπέρασμα, πρέπει να έχετε κάποιο λογισμικό antivirus στον Η/Υ σας.

4. Έχω Macintosh (ή Linux-based system), όχι Windows, οπότε δεν ανησυχώ.

Είναι αλήθεια ότι οι περισσότερες επιθέσεις έχουν στόχο τους Η/Υ με Microsoft Windows, αλλά υπήρξαν επιθέσεις και εναντίον Mac OS και Linux. Ορισμένοι προβλέπουν ότι οι επιθέσεις στους Mac θα ενταθούν, παρόλα τα καλά χαρακτηριστικά ασφάλειας που διαθέτουν.

5. Το σύστημα που πήρα ήρθε με προ-εγκατεστημένο πακέτο antivirus, άρα είμαι προστατευμένος.

Όχι ακριβώς. Πρώτον, αν δεν έχετε ενεργοποιήσει το πρόγραμμα για αυτόματη ανίχνευση της εισερχόμενης κίνησης δεν είστε προστατευμένοι από τις επιθέσεις e-mail και Web browser. Δεύτερον, το λογισμικό σας δεν είναι τόσο καλό όσο η πιο πρόσφατη ενημέρωση του (νέοι ιοί εμφανίζονται κάθε μέρα). Ενεργοποιήστε τη λειτουργία αυτόματης ενημέρωσης ώστε να είστε συγχρονισμένοι με τις πιο πρόσφατες εκδόσεις. Τρίτον, το λογισμικό αυτό δεν μπορεί να σας προστατεύσει από όλες τις περιπτώσεις. Συνήθως χρειάζεται ένας συνδυασμός από λύσεις, τουλάχιστον: antivirus και firewall, πλάνο συνεχούς ενημέρωσης του λειτουργικού συστήματος με τις αναβαθμίσεις - διορθώσεις (updates & patches), antispyware, antispam.

1.3. Επικίνδυνες ενέργειες χρηστών

Οι περισσότεροι χρήστες δεν έχουν την παραμικρή ιδέα πόσο επικίνδυνη είναι η συμπεριφορά τους όταν είναι online. Έτσι κάνουν επικίνδυνες ενέργειες που μπορούν να βλάψουν την ασφάλεια τους. Οι δέκα ποιο επικίνδυνες ενέργειες είναι οι εξής:

- 01. Άνοιγμα συνημμένων e-mail αγνώστου αποστολέα.
- 02. Εγκατάσταση μη εξουσιοδοτημένων εφαρμογών.
- 03. Απενεργοποίηση ή αδρανοποίηση αυτοματοποιημένων εργαλείων ασφάλειας.
- 04. Άνοιγμα email (HTML ή απλού κειμένου) αγνώστου αποστολέα.
- 05. Τυχερά παιχνίδια, πορνογραφία και άλλα sites αμφιβόλου νομιμότητας.
- 06. Διανομή κωδικών, στοιχείων αναγνώρισης, και smart cards.
- 07. Άσκοπη περιήγηση σε άγνωστα, επισφαλή και αναξιόπιστα WWW sites.
- 08. Σύνδεση σε άγνωστα, επισφαλή και αναξιόπιστα δίκτυα WiFi.
- 09. Εισαγωγή πληροφοριών σε WWW scripts, forms, και σελίδες εγγραφής.
- 10. Συμμετοχή σε chat rooms, και social networking sites.

Πολλές από τις παραπάνω ενέργειες είναι αναπόφευκτες γι'αυτό θα πρέπει να προσέχετε όταν τις πραγματοποιήτε .

2. Δεκάλογος Ασφάλειας

Καμιά εφαρμογή ούτε τεχνική μπορεί να σας προστατεύσει 100%, αλλά μπορείτε να φτάσετε αρκετά κοντά σε αυτό το ποσοστό. Ο παρακάτω δεκάλογος αφορά τους χρήστες των MS Windows και δείχνει τα βήματα που πρέπει να ακολουθήσουν για να πετύχουνε ένα αρκετά μεγάλο ποσοστό ασφάλειας.

2.1. Firewalls - Antivirus Εφαρμογές

2.1.1. Firewalls

Ο υπολογιστής σας έχει περίπου 65.000 πύλες με τις οποίες μπορούν να μοιραστούν πληροφορίες στο Διαδίκτυο ή με έναν άλλο υπολογιστή. Ένα καλό διπλής κατεύθυνσης Firewall ελέγχει όλη την εξερχόμενη και εισερχόμενη κυκλοφορία. Μπορεί να σας προειδοποιήσει σε οτιδήποτε ασυνήθιστο, σύμφωνα με τους κανόνες ή τις διαδικασίες που αποφασίζετε. Στην ανάγκη μπορεί ακόμη και να κλείσει όλες τις πύλες σας. Ειδικά για την πρόσβαση στο Διαδίκτυο μπορείτε να το βάλετε στο πιο υψηλό επίπεδο ασφάλειας και να το θέσετε για όλα τα προγράμματα να σας προειδοποιεί για την πρόσβασή τους σ' αυτό. Μπορείτε επίσης να επιλέξετε τα προγράμματα που εμπιστεύεστε να μπαίνουν χωρίς να σας προειδοποιεί. Εάν δεν είστε βέβαιοι για ένα πρόγραμμα που θέλει πρόσβαση στον υπολογιστή σας, ή από τον υπολογιστή σας στο διαδίκτυο, μπορείτε να την αρνηθείτε. Τα Firewall είναι απαραίτητα γιατί αποτρέπουν τις επιθέσεις trojan και hacking. Η έκδοση XP με SP2(service pack 2) των Windows διαθέτουν Firewall το οποίο όμως δεν είναι τόσο ικανό να σας προστατέψει σε σχέση με άλλες εφαρμογές Firewall που κυκλοφορούν, γι'αυτο θα πρέπει να εγκαταστήσετε κάποιο άλλο το οποίο θα πρέπει να είναι επώνυμο και θα έχει πάρει καλές κριτικές από γνωστούς και αξιόπιστους δικτυακούς τόπους, οργανισμούς και περιοδικά πληροφορικής που κάνουνε τεστ σε τέτοιες εφαρμογές. Πολλά από αυτά είναι και freeware(π.χ. Zone alarm home,comodo,outpost).Αφού εγκαταστήσετε ένα Firewall θα πρέπει να το ρυθμίσετε έτσι ώστε να βρίσκεται σε συνεχή λειτουργία και να προσέχετε ποιες εφαρμογές θα επιτρέπει να έχουν πρόσβαση στο διαδίκτυο και ποιες πύλες θα είναι ανοιχτές. Επίσης θα πρέπει να βλέπετε συχνά τα logs του για να έχετε υπόψιν την κίνηση του δικτύου. Σημαντικό είναι επίσης να το κάνετε συχνά update.

2.1.2. Εφαρμογές Antivirus - Anti-Trojan

Η εγκατάσταση ενός Antivirus ή/και ενός Anti-Trojan προγράμματος στο σύστημά σας είναι το επόμενο πιο ουσιαστικό μέτρο ασφάλειας που χρειάζεστε. Όταν ένας ιός ανιχνεύεται, το πρόγραμμα θα μετακινήσει το μολυσμένο αρχείο προς μια περιοχή καραντίνας για την απολύμανση ή την αφαίρεση του. Αυτό αποτρέπει το αρχείο malware από την επαφή του με οποιοδήποτε άλλο πρόγραμμα. Για την καλύτερη προστασία σας καλό θα ήταν να χρησιμοποιήσετε δυο εφαρμογές Antivirus και η μια από τις δυο θα πρέπει να έχει ρυθμιστεί να κάνει real-time-scan. Για να αποκτήσετε κάποιο θα πρέπει να κάνετε ότι σας συμβουλεύουμε και ποιο πάνω για τα Firewall. Πάρα πολύ σημαντικό είναι να ενημερώνετε συνεχώς το antivirus και την βάση του.

2.2. Τι να κάνετε και τι όχι

Να είστε πολύ προσεκτικοί εάν αισθάνεστε ότι πρέπει να χρησιμοποιήσετε οποιαδήποτε P2P (peer-to-peer) υπηρεσία για τη διανομή/ανταλλαγή των αρχείων σε ολόκληρο το Διαδίκτυο. Στην πραγματικότητα, θα προτείναμε να μη χρησιμοποιείτε P2P όπως KaZaA, Morpheus, BearShare, Grokster και Audiogalaxy καθόλου, γιατί αυτά είναι γεμάτα με malware. Επίσης να προτιμάτε εφαρμογές που τρέχουν ως server και όχι client. Μην καθορίζετε ως κοινόχρηστο οποιοδήποτε άλλο φάκελο εκτός από αυτούς που επιλέγουν αυτές οι υπηρεσίες. Προστατέψετε τα ευαίσθητα αρχεία σας σε οποιοδήποτε υπολογιστή που χρησιμοποιείτε για να συνδέσετε με το Διαδίκτυο. Μην βάζετε τα ιδιωτικά αρχεία στους κοινόχρηστους φακέλλους. Κρατήστε το Antivirus σας πάντα σε λειτουργία. Ακόμα καλύτερα, χρησιμοποιήστε μια εφαρμογή προστασίας πρόσβασης αρχείων/φακέλλων για να κλειδωθεί η πρόσβαση σε όλους τους άλλους τομείς του σκληρού δίσκου σας.

Ασφαλίστε τα Instant Messages (IMs). Μια καλή ιδέα είναι να χρησιμοποιηθεί ένα εργαλείο κρυπτογράφησης IM για να προστατέψει το MSN, το Yahoo, τα μηνύματα AIM, ή ICQ σας.

Θυμηθείτε επίσης ότι ακόμα κι αν μόνο ένας υπολογιστής είναι συνδεδεμένος με το Διαδίκτυο, οποιοσδήποτε άλλος υπολογιστής που μοιράζεται αυτή την σύνδεση, ή που μοιράζεται τα αρχεία σε ένα δίκτυο, χρειάζεται την ίδια προστασία. Για κάθε υπολογιστή που συνδέεται με το τοπικό σας δίκτυο (LAN) απαιτείται ένα όνομα χρήστη και ένας κωδικός πρόσβασης. Για σκληρούς δίσκους που καθορίζονται ως κοινόχρηστοι, στα Windows 98 απαιτείται user name και password, στα Windows XP πρέπει να ρυθμιστεί να μην επιτρέπετε η "ανώνυμη σύνδεση" ή οποιαδήποτε πρόσβαση από τις ομάδες ή τους χρήστες έξω από το τοπικό LAN σας.

Μην αφήσετε ποτέ μια εφαρμογή ή ένα εκτελέσιμο που κατεβάσατε από το διαδίκτυο να εκτελεστεί από μόνο του. Να είστε προσεκτικοί με τα αρχεία που τελειώνουν σε exe, bat, vbs, ή com. Να τα ελέγχετε με εφαρμογές antivirus, anti-spyware και anti-trojan, πριν τα κάνετε «unzip» και τα εκτελέσετε. Οι περισσότερες εφαρμογές antivirus επιτρέπουν τον έλεγχο μεμονωμένων αρχείων. Μην περιμένετε ο έλεγχος πραγματικού χρόνου να τα «πιάσει» όλα.

Μην δεχτείτε να τρέξει ένα ActiveX Control ή μια Java Class εκτός αν προέρχεται από μια έμπιστη περιοχή. Είναι καλύτερο ο browser να ζητά την άδεια σας. Εάν χρησιμοποιείτε τον Internet Explorer, αυτές οι επιλογές βρίσκονται στο Control

Panel > Internet Options > Security > Internet - Custom Level. Οι χρήστες του Mozilla, Netscape, και Opera προτρέπονται εξορισμού.

Εάν χρησιμοποιείτε τον Internet Explorer θέστε εκτός λειτουργίας το "Install on Demand" έτσι ο browser σας, θα αναγκαστεί να σας ρωτήσει εάν απαιτούνται πρόσθετο λογισμικό προκειμένου να εμφανιστεί σωστά το περιεχόμενο. Αυτή η ρύθμιση βρίσκεται στο Control Panel > Internet Options > Advanced.

Μην ενεργοποιείται JavaScript για το ηλεκτρονικό ταχυδρομείο ή τα συνημμένα ηλεκτρονικού ταχυδρομείου. Το JavaScript μπορεί να βοηθάει στο browsing στο Διαδίκτυο, αλλά είναι επικίνδυνο όταν επιτρέπεται για το ηλεκτρονικό ταχυδρομείο.

Απενεργοποιήστε το HTML ή χρησιμοποιήστε απλό κείμενο για το ηλεκτρονικό ταχυδρομείο. Χρησιμοποιήστε ένα φίλτρο για τα web bugs. Τα worms ηλεκτρονικού ταχυδρομείου μπορούν να εκτελέσουν απλά και μόνο βλέποντας το HTML περιεχόμενό.

Τα συνημμένα αρχεία πάντα να τα βλέπετε χωριστά και μόνο αφού έχουν ανιχνευθεί για malwares.

Μην χρησιμοποιήσετε ποτέ το ηλεκτρονικό ταχυδρομείο για να στείλετε προσωπικές σας οικονομικές πληροφορίες όπως οι αριθμοί πιστωτικών καρτών, οι αριθμοί τραπεζικού λογαριασμού, ή SSN/SIN. Ακόμα κι αν χρησιμοποιείτε κρυπτογράφηση και το ηλεκτρονικό ταχυδρομείο είναι για νόμιμη επιχείρηση, δεν μπορείτε να είστε σίγουροι ότι ο παραλήπτης θα προστατεύσει αυτές τις πληροφορίες μόλις παραδοθεί και αποκρυπτογραφηθεί.

Βεβαιωθείτε ότι ο browser σας είναι SSL-capable (Secure Socket Layer) και η δύναμη κρυπτογράφησης, είναι περισσότερο από 128-bit. Οι περισσότεροι ασφαλείς websites δεν θα δεχτούν τους browser με λιγότερα.

Κρατήστε πάντα το λειτουργικό σύστημά (OS) και τον browser σας ενημερωμένο, όπως και οποιαδήποτε υπηρεσία ή εφαρμογή έχει πρόσβαση στο Διαδίκτυο. Εφαρμόστε τα «updates» και τα «patches» από τη Microsoft, όποτε είναι διαθέσιμα. Για να ενημερωθείτε ποια «updates» έχετε λάβει, πηγαίνετε στο ημερολόγιο των «updates».

2.3. Ασφάλεια σε οποιαδήποτε ταχύτητα online

2.3.1. Browsers

Διαμορφώστε τον browser σας για τη μέγιστη μυστικότητα. Αναγκάστε τον να σας προτρέψει για την άδεια για οτιδήποτε πιθανό. Για περισσότερες λεπτομέρειες στο πώς να το κάνει αυτό ανατρέξτε στο τμήμα βοηθείας του.

Να καθαρίζετε την «cache» του browser σας, που είναι γνωστή και ως «Temporary Internet Files» ή TIF, και το «history» του browser συχνά. Πάντα καθαρίστε τα μετά από την επίσκεψη σας σε οποιοδήποτε site που δώσατε προσωπικά δεδομένα όπως σε «online banking» ή αγορά από το διαδίκτυο. Υπάρχει λογισμικό που μπορεί να κάνει αυτή την εργασία. Κάποιοι browsers, όπως ο Opera ή firefox, μπορούν να ρυθμιστούν να καθαρίζουν την «cache» και την «history» ακριβώς μετά το κλείσιμο

του προγράμματος. Για τους χρήστες του Internet Explorer: Πάρτε ένα φίλτρο content/browser Ιστού για να αποτρέψετε τη μακρινή επαφή περιοχών μέσω των ad banners και των ενσωματωμένων web bugs. Ο internet Explorer μπορεί να είναι ένας ασφαλής και ικανός browser εάν τον διαμορφώνετε και προστατεύετε κατάλληλα. Μερικοί από τους λόγους ως προς γιατί ο IE είχε τα προβλήματα ασφάλειας δεν οφείλονται στη Microsoft, αλλά κατά ένα μεγάλο μέρος στους ανάρμοστους και ανενημέρωτους χρήστες. Παρόλα αυτά θα ήταν καλύτερο να προτιμήσετε κάποιον άλλο browser όπως ο firefox που θεωρείτε ασφαλέστερος, με περισσότερες επιλογές και ευκολίες σε σχέση με τον IE.

2.3.2. Προσοχή στις πληροφορίες σας

Να είστε προσεκτικοί για ποιες πληροφορίες μοιράζεστε στα websites. Μην συμπληρώνετε σε φόρμες οποιαδήποτε προσωπικά στοιχεία, εκτός αν είστε απολύτως βέβαιοι ότι δεν θα χρησιμοποιηθούν με άσχημο τρόπο. Διαβάστε την «Privacy Policy» τους. Ακριβώς επειδή έχουν μια δεν σημαίνει ότι δεν θα χρησιμοποιήσουν τις πληροφορίες σας. Διαβάστε το προσεκτικά. Εάν είναι αόριστο, μη σαφής, ή απών, μην μοιραστείτε τίποτα μαζί τους.

Παραμείνετε μακριά από όλα αυτά που έχουν να κάνουν με τους καταλόγους και τα αιτήματα διευθύνσεων που χρησιμοποιούν τις προσωπικές πληροφορίες σας. Αποφύγετε τις περιοχές που προσφέρουν κάποιο είδος βραβείου ή δωρεάν δώρου σε αντάλλαγμα με τις λεπτομερείς επαφές σας. Είναι βέβαιο ότι αυτά είναι κάποια μορφή κλοπής ταυτότητας scam, ή spam.

Μην χρησιμοποιήστε το "click here to unsubscribe" σε spam e-mail. Αυτό που κάνει πραγματικά είναι να ελέγχει ότι το spam παραδόθηκε σε μια έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου και να επιβεβαιώνει ότι το είδατε. Ο αποστολέας δεν έχει καμία πρόθεση να τιμήσει το αίτημα σας. Από την ανταπόκριση θα πάρετε περισσότερο spam από τον ίδιο αποστολέα, καθώς επίσης και από εκείνων που πωλήθηκε η επιβεβαιωμένη διεύθυνσή σας. Διαγράψτε το spam χωρίς να ανταποκριθήτε σε τίποτα.

Μην δώστε την προσωπική (ISP, Internet Service Provider) διεύθυνση ηλεκτρονικού ταχυδρομείου σας σε έναν εμπορικό ιστοχώρο , είτε για αγορά κάτι on-line είτε για την απάντηση μιας έρευνας. Χρησιμοποιήστε έναν διαθέσιμο, ελεύθερο webmail λογαριασμό άντι αυτού. Αυτοί λαμβάνονται εύκολα από Hotmail, Yahoo, Google κ.λπ....

Μην χρησιμοποιήστε την προσωπική διεύθυνση ηλεκτρονικού ταχυδρομείου σας κατά την ταχυδρόμηση στους πίνακες μηνυμάτων, ή στις ομάδες πληροφόρησης. Πάντα χρησιμοποιήστε μια διεύθυνση webmail. Οι αράχνες και οι αντιολισθητικές αλυσίδες ελέγχουν συνεχώς αυτές τις θέσεις για τις έγκυρες διευθύνσεις που χρησιμοποιούν για το spam. Πολλοί ιστοχώροι παρέχουν μια επιλογή στο σχεδιάγραμμά σας είτε για να κρύψουν είτε να αποκαλύψουν τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας.

Επίσης αποφύγετε να δώσετε την προσωπική διεύθυνση ηλεκτρονικού ταχυδρομείου σας στους φίλους που δεν μπορούν να προστατευθούν τόσο καλά και

να ενημερωθούν όπως εσείς. Χρησιμοποιείστε webmail.

Τα Anonymizers ή τα proxies μπορούν να βοηθήσουν όπου η μυστικότητα και η ασφάλεια διατρέχουν κίνδυνο κατά το browsing. στους νέους ιστοχώρους και την ταχυδρόμηση σε ορισμένες ομάδες πληροφόρησης.

Δοκιμάστε μια ή περισσότερες από τις ελεύθερες υπηρεσίες για να εξετάσουν την ασφάλεια της σύνδεσης των υπολογιστών σας στο Διαδίκτυο. Εξετάστε τα αποτελέσματα προσαρμόστε τα στο Firewall σας και στο δίκτυο σας και εφαρμόστε τα patches λογισμικού όπως απαιτείται για την καλύτερη υπεράσπιση σας.

2.3.3. Πάντα να κρατάτε Back UP

Είναι πολύ σημαντικό να φυλάσσεται τα προσωπικά σας αρχεία και όλο το σύστημα σε άλλα μέσα αποθήκευσης εκτός του κυρίου δίσκου σας για να μπορείτε να τα αποκαταστήσετε σε περίπτωση καταστροφής του δίσκου ή καταστροφή του λειτουργικού ή των αρχείων σας από άλλες αιτίες όπως ιοί. Στα windows XP μπορείτε να ενεργοποιήσετε την επαναφορά συστήματος που διαθέτουν για να γυρίσετε σε προηγούμενη κατάσταση το σύστημα σας, στην οποία δεν είχε δημιουργηθεί ακόμα κάποιο σφάλμα ή κάποια απώλεια.

2.4. Ασφάλιση του Δικτύου σας

Θέστε εκτός λειτουργίας το NetBIOS σε περίπτωση που ο υπολογιστής σας δεν είναι σε κάποιο LAN. Το NetBIOS είναι ένα σύνολο διεπαφών λογισμικού που μπορεί να επιτρέψει τη διανομή των αρχείων ή των φακέλλων σε ένα δίκτυο με άλλους hosts μέσω των Windows network shares. Το κοινό σύστημα αρχείων Διαδικτύου είναι το εργαλείο NetBIOS. Αυτό επιτρέπει σε έναν host να χρησιμοποιήσει τα μακρινά αρχεία από ένα άλλο PC σαν να ήταν στον υπολογιστή του. Αυτό κάνει το NetBIOS, μια απειλή στη μεμονωμένη μυστικότητα και ασφάλεια στο διαδίκτυο. Αφήνει επίσης το PC σας ανοικτό και τρωτό στα ανώνυμα logons, τις μακρινές προσβάσεις ληξιαρχείων και τις μακρινές κλήσεις διαδικασίας από ξένους.

Εάν δεν ενδιαφέρεστε για την αρχείο-διανομή και επιθυμείτε να έχετε μια ασφαλέστερη εμπειρία Διαδικτύου, πρέπει να θέσετε εκτός λειτουργίας τις συνδέσεις σε όλα τα πρωτόκολλα, τις υπηρεσίες και τους προσαρμογείς εκτός από το TCP/ IP που δεσμεύεται είτε στον Dial-up Adapter, είτε στον DSL Adapter, είτε στο Cable Interface, είτε στο LAN Interface. Πρέπει να είστε ο administrator του PC σας για να αλλάξετε αυτές τις ρυθμίσεις.

2.5. Σερφάρισμα και Cookies

Τα cookies είναι αρχεία κειμένου που περιέχουν πληροφορίες επισκεπτών ενός website. Αυτές οι πληροφορίες παραχωρούνται από τον χρήστη κατά την πρώτη επίσκεψη του στο website (μέσω του server). Ο server καταγράφει αυτές τις

πληροφορίες σε ένα αρχείο και το αποθηκεύει στον υπολογιστή σας. Όταν ξαναμπείτε σε αυτό το website ο server βρίσκει τις πληροφορίες που χρειάζεται και συνεχίζει κερδίζοντας κάποιον χρόνο.

Πολλές web σελίδες τα χρησιμοποιούν για να παρακολουθήσουν τις κινήσεις σας μέσα σε αυτή, ποιες σελίδες επισκέπτεσαι, πόσο χρόνο παραμένεις σε κάθε σελίδα, με ποια σειρά τις βλέπεις κτλ. Το cookie είναι ένας μοναδικός προσωπικός αριθμός και χρησιμοποιείται για να εξάγουν τις πληροφορίες σας από τις βάσεις δεδομένων τους. Συνήθως είναι μια σειρά γραμμάτων αρκετά μακριά ώστε να είναι μοναδική. Φυλάσσονται σε ένα αρχείο που λέγεται, ανάλογα με το browser που χρησιμοποιείτε: cookies ή cookies.txt ή MagicCookie . Ακόμα και αν αλλάξετε ISP ή αναβαθμίσετε τον browser τα cookies παραμένουν αποθηκευμένα στο δίσκο σας. Αν ανοίξετε και διαβάσεετε τα αποθηκευμένα cookies θα δείτε ονόματα από web σελίδες που ούτε έχετε ακούσει ούτε έχετε επισκεφτεί ποτέ!

Και που είναι το πρόβλημα λοιπόν με τα cookies?Πολλές φορές, όταν πατάτε ένα link για να μεταφερθείτε σε μια web σελίδα, ο browser σας συνδέεται όχι μόνο με τον server όπου είναι εγκατεστημένη η web σελίδα που ζητήσατε αλλά και με άλλους servers. Αυτό γίνεται τόσο γρήγορα που δεν το αντιλαμβάνεστε! Κατά τη διάρκεια αυτών των συνδέσεων οι διάφορες εταιρίες που πουλάνε χονδρικά διαφημιστικό χώρο τοποθετούν τα cookies, που σας φαίνονται άγνωστα, στο δίσκο σας. Οι εταιρίες αυτές διατηρούν βάσεις δεδομένων, τεραστίων διαστάσεων, και καταγράφουν το ποιος κοιτάει ποιες web σελίδες. Οι μεγαλύτερες από αυτές έχουν τοποθετήσει cookies σε εκατομμύρια υπολογιστές παρακολουθώντας έτσι δισεκατομμύρια κινήσεων καθημερινά.

Παράλληλα, αν χρησιμοποιείτε μερικές από τις γνωστές μηχανές αναζήτησης πρέπει να ξέρετε ότι όλες οι αναζητήσεις που κάνετε καταγράφονται και αναλύονται. Όποια web σελίδα χρησιμοποιεί cookies μπορεί να ανταλλάξει στοιχεία με τις εταιρίες που αγοράζουν και πουλάνε χονδρικά διαφημιστικό χώρο. Αυτό σημαίνει ότι αν μια εταιρία καταφέρει να βάλει στο χέρι τα στοιχεία σας όλες οι άλλες, πελάτες της, ενδέχεται να μάθουν ποιος είστε κάθε φορά που επισκέπτεστε την web σελίδα τους.

Αντιμετώπιση:Που αποθηκεύονται τα cookies; Στον Internet Explorer συνήθως βρίσκονται στο C:\Windows\Cookies\ ή στο C:\Documents and Settings\Administrator\Cookies. Στους υπόλοιπους browsers βρίσκονται συνήθως στο φάκελο που είναι εγκατεστημένος ο browser. Το απλούστερο πράγμα που μπορείτε να κάνετε είναι αλλάξετε τα attributes του cookies.* σε read-only. Ακόμα, μπορείτε να ρυθμίσετε τον browser που χρησιμοποιείτε να μη δέχεται cookies η να δέχεται μόνο από τους servers που κρίνετε απαραίτητο, όπως για παράδειγμα οι web σελίδες που προσφέρουν προσωπικό περιεχόμενο, ή δωρεάν e-mail. Αυτές δεν επιτρέπουν την πρόσβαση αν ο browser σας δεν δέχεται cookies. Ρυθμίστε λοιπόν τον browser σας να σας προειδοποιεί για κάθε απόπειρα τοποθέτησης ενός cookie στο σκληρό σας δίσκο και να αποφασίζετε αν το θέλετε ή όχι στη στιγμή. Όμως έχετε υπόψη σας ότι μπορεί να γίνει ιδιαίτερα ενοχλητικό μιας και υπάρχουν web σελίδες που σας βάζουν μέχρι και 20-30 cookies σε κάθε κλικ που κάνετε. Ακόμα καλό είναι να βάλετε τον browser σας να τα σβήνει κάθε φορά που κλείνετε το πρόγραμμα.

2.6. Αόρατο Σερφάρισμα

Κάθε υπολογιστής στο διαδίκτυο έχει μία μοναδική διεύθυνση IP. Οι χρήστες cable έχουν πιθανώς μια ή δύο στατικές διευθύνσεις που αλλάζουν σπάνια. Οι χρήστες DSL και Dialup, μπορούν να έχουν δυναμικές που αλλάζουν με κάθε σύνδεση. Οι δυναμικές IP μπορούν να επισημανθούν χρησιμοποιώντας Reverse-DNS εάν το δίκτυο ή ο ISP το επιτρέπουν. Κάθε διεύθυνση Reverse-DNS είναι μοναδική. Ακόμα κι αν η δυναμική διεύθυνση IP σας αλλάζει, η διεύθυνση Reverse DNS θα παραμείνει η ίδια.

Η διεύθυνση IP επιτρέπει στον ISP σας και άλλους υπολογιστές να επικοινωνήσουν με το PC σας. Αν δεν υπήρχε η IP στους Η/Υ, θα ήταν σαν να είχαμε ένα τηλέφωνο χωρίς dialtone. Δεν θα υπήρχε καμία επικοινωνία με άλλους Η/Υ. Παρόλα αυτά, υπάρχουν τρόποι να κρύψουμε ή να κρυπτογραφήσουμε τη διεύθυνση IP.

Τα proxies είναι απλά servers που συνδέουν τους χρήστες με ένα δίκτυο. Συνήθως συνδέει ένα τοπικό δίκτυο όπως μια επιχείρηση με ένα άλλο δίκτυο (παραδείγματος χάριν, το Διαδίκτυο) ή ακόμα και με τον ISP (Internet Service Provider). Επιτρέπει σε πολλούς Η/Υ να έχουν πρόσβαση σε ένα δίκτυο με μια ή περισσότερες διευθύνσεις. Αυτοί οι servers μπορούν να είναι πολύ χρήσιμοι, συμβάλλοντας στην ασφάλεια, τη ταχύτητα και τη μυστικότητα σε εκείνους που επιθυμούν να απολαύσουν αληθινά το Διαδίκτυο χωρίς να αποκαλύπτονται οι ταυτότητές τους.

Πληροφορία ειδικά για τους χρήστες dialup: Μεγάλα downloads μπορεί να είναι απελπιστικά αργά με dialup. Με τη σύνδεση σε έναν web proxy server μπορείτε να επιταχύνετε το download αφού ο proxy παίρνει πρώτος τα αρχεία και σας τα δίνει έπειτα με μεγάλη ταχύτητα.

Με τη χρησιμοποίηση ενός ανώνυμου (http) proxy server , χρησιμοποιείτε την IP τους αντί της δικής σας για να έχετε πρόσβαση στο Διαδίκτυο. Ένα ανώνυμο proxy αφαιρεί, καλύπτει ή κρυπτογραφεί την IP σας με οποιαδήποτε αιτήματα υποβάλλεται. Για αυτό για να είναι αποτελεσματικά τα proxies, είναι επίσης σημαντικό να είναι απενεργοποιημένη η Java, τα Javascript και τα cookies στον browser σας. Αυτό μειώνει την αισθητική του site αλλά είναι πιο ασφαλές.

Οι περισσότεροι σύγχρονοι browsers μπορούν να διαμορφωθούν για τη χρήση Proxy Server. Παρακάτω είναι τα γενικά παραδείγματα για το πώς γίνονται οι ρυθμίσεις σε ποικίλους browsers.

<u>Proxy Settings in Internet Explorer 6.x</u>

1. Κάντε click στο "Service" ή "Internet Options"
2. Κάντε click στο "Connections"

a. Αν χρησιμοποιείται Dial-Up σύνδεση, επιλέξτε την σύνδεση σας και κάντε click στο "Settings".

b Αν χρησιμοποιείται LAN σύνδεση, κάντε click στο "LAN Settings" στο πλαίσιο "Local Area Network (LAN) Settings"

3. Ενεργοποιήστε το "use a proxy server"

4. Στα πεδία "Address" και "port", πληκτρολογείστε το όνομα του proxy και την πόρτα.
5. Αν χρειάζεται, ενεργοποιήστε το "bypass proxy server for local addresses"
6. Κάντε click στο "OK"
7. Κάντε click στο "OK" για να κλείσει το παράθυρο επιλογών του Internet Explorer.

Mozilla
1. Κάντε click στο "Edit" ή "Preferences"
2. Κάντε click στο "Category" ή "Advanced" ή "Proxies"
3. Επιλέξτε "Manual proxy configuration"
4. Κάντε click στο "View" στο "Manual proxy configuration"
5. Ρύθμιση Proxy για τα ακόλουθα πρωτόκολλα: HTTP, FTP, etc.

Opera 7.x
1. Κάντε click στο "Tools"
2. Κάντε click στο "Preferences"
3. Κάντε click στο "Network"
4. Κάντε click στο "Proxy Servers"
5. Set proxies

Φυσικά, το να ρυθμίσετε τον browser σας για να χειρίζεται proxies δεν είναι αρκετό. Πρέπει να βρείτε, να διαλέξετε, και ελέγχετε τους ανώνυμους proxy servers για την ασφάλεια, την αυθεντικότητα, τη διαθεσιμότητα και το εύρος ζώνης.

2.7. HOSTS File

Για να αφαιρέσετε και να εμποδίσετε τα website ads , το offensive περιεχόμενο και τα malwares, μπορείτε να αγοράσετε κάποιο λογισμικό ή μπορείτε να χρησιμοποιήσετε τα ελεύθερα λογισμικά για οποιοδήποτε browser. Το αρχείο των Hosts που βρίσκεται μέσα στα Windows μπορεί να χρησιμοποιηθεί για να εμποδίσει ads, banners, cookies, web bugs και τους πιο πολλούς hijackers , φράζοντας τους Servers και τα sites που τα εισάγουν, στον υπολογιστή σας.
Παράδειγμα - το ακόλουθο λήμμα 127.0.0.1 ads.badsoftware.com εμποδίζει όλα τα αρχεία που παρέχονται από τον κεντρικό υπολογιστή badsoftware στις σελίδες που σερφαρετε σταματώντας την παρακολούθηση των κινήσεων σας. Το αρχείο των Hosts είναι η πρώτη θέση που ένας browser ψάχνει μια διεύθυνση IP (εκτός αν χρησιμοποιείτε έναν proxy server) όταν δακτυλογραφείτε μια URL όπως www.happycampers.com. Εάν δεν βρίσκει το domain name στο αρχείο των Hosts, μόνο τότε κάνει τον browser να ρωτά τον DNS server. Για αυτόν το λόγο το αρχείο των Hosts μας βοηθάει εξερετικα στο μπλοκάρισμα των website ads. Το hosts είναι ένα αρχείο κειμένου που μπορείτε να ανοίξετε στο σημειωματάριο. Στην κορυφή βρίσκετε μια εξήγηση απλής σύνταξης. Κάθε γραμμή είναι μια διεύθυνση IP, ένα domain name, και ένα προαιρετικό σχόλιο που τοποθετείτε μετά από το σύμβολο α #.Για παράδειγμα μοιάζει με αυτό: *127.0.0.1 localhost # this is the universal IP*

address of all local computers .

Η 127.0.0.1 είναι μια διεύθυνση IP αποκαλούμενη "loopback" επειδή αναφέρεται στον τοπικό υπολογιστή μόνο. Η διεύθυνση loopback μας δίνει έναν τρόπο να εξετάσουμε το λογισμικό Ιστού χωρίς φυσικά να συνδεθούμε με ένα δίκτυο. Για να χρησιμοποιήσετε το αρχείο των hosts και να εμποδίσετε τα web ads, προσθέτετε έναν κατάλογο hosts που εξυπηρετούν το δυσάρεστο ή κακόβουλο περιεχόμενο με αυτές τις περιοχές που συνδέονται, στη διεύθυνση “loopback”. Όταν θα πάτε να επισκεφθείτε μια από αυτές τις διευθύνσεις, ο browser σας κοιτάζει στον υπολογιστή σας για τις σελίδες αυτές και δεν επισκέπτεται ποτέ τον κεντρικό υπολογιστή αυτών των σελίδων. Οι σελίδες αυτές δεν επιδεικνύονται ποτέ και ο server τους δεν έχει καμία ευκαιρία να φορτώσει banner, cookie, ή malicious Javascript αρχεία στον υπολογιστή σας. Πολλά ad-blocking hosts files , για διάφορους σκοπούς, είναι διαθέσιμα για download στο διαδίκτυο. Ένα άλλο χαρακτηριστικό του hosts file είναι ότι δεν επιτρέπει σε κάποιο malware που μπήκε στον υπολογιστή σας να συνδεθεί με το “σπίτι” του. Γι' αυτό είναι πολύ σημαντικό να κρατάτε το hosts file ενημερωμένο.

Στις περισσότερες περιπτώσεις ένα μεγάλο αρχείο hosts τείνει να επιβραδύνει τη μηχανή. Εντούτοις, αυτό συμβαίνει μόνο στα Windows 2000 και XP. Τα Windows 98/se και Me δεν επηρεάζονται. Για να επιλύσετε αυτό το ζήτημα κάντε τα εξής:
ανοίξτε τον “Services Editor"
Start > Run (type) "services.msc" (no quotes)
πάτε στο "DNS Client", δεξί-κλικ και επιλέξτε: Properties
Κάντε κλικ στο drop-down arrow για "Startup type"
Επιλέξτε: Manual, κλικ Apply/Ok και επανεκκινήστε .

Εάν βλέπετε ένα ad ενώ χρησιμοποιείται ένα ad-blocking hosts file , αυτό σημαίνει ένα από δύο πράγματα, είτε το ad βρίσκετε στον server σας , ή είναι νέο. Για να ανακαλύψετε από που προέρχεται το ad, κάντε δεξί κλικ πάνω του και επιλέξτε "Copy Shortcut". Εάν το ad βρίσκεται στο site, δεν μπορείτε να το εμποδίσετε με το hosts file δεδομένου ότι τα hosts file εμποδίζουν μόνο ολόκληρα sites. Για έναν νέο server που περιέχει ads, κολλήστε το domain portion αυτού του URL στο αρχείο των hosts σας με επαναπροσανατολισμό στο 127.0.0.1.

Πολλές φορές δεν εξυπηρετεί κανέναν σκοπό το να εμποδίζετε το ad banner από την επίδειξη, όπως στα περισσότερα άλλα αρχεία των hosts, ενώ μολύνεστε από ένα παράσιτο μεσώ script ή κατεβάζοντας το από τον ιστοχώρο. Το αντικείμενο είναι να κάνετε σερφ γρηγορότερα συντηρώντας την ασφάλεια, την προστασία και τη μυστικότητά σας. Καλό θα ήταν να κατεβάσετε το Hosts.zip από τους MVPs(Most Valuable Professionals) της microsoft και να το κάνετε Unzip σε έναν "temp" φάκελλο και να τοποθετήσετε στην κατάλληλη εγκατεστημένη θέση. Αυτή είναι: Windows 95/98/Me: c:windowshosts, Windows NT/2000/XP pro: c:winntsystem32driversetchosts, Windows XP home: c:windowssystem32driversetchosts.

Σε αυτούς που χρησιμοποιούν proxy τα παραπάνω δεν θα δουλέψουν. Θα πρέπει να προσέξουν ότι είναι τσεκαρισμένη η επιλογή "bypass proxy server for local addresses" στον browser τους.

2.8. Instant messaging

Το στιγμιαίο μήνυμα επιτρέπει σε σας να ξέρετε πότε οι φίλοι σας είναι σε ανοικτή γραμμή και να τους στέλνετε μηνύματα σε πραγματικό χρόνο. Είναι ένας σημαντικός τρόπος να διατηρήστε σε επαφή με τους φίλους, την οικογένεια και τους επιχειρησιακούς συνεταίρους σας. Είναι είναι ένα από τα ταχύτερα αναπτυσσόμενα και μεγαλύτερα τμήματα στο διαδίκτυο. Το στιγμιαίο μήνυμα, ή ακριβώς IM, καθιστά εύκολο και διασκεδαστικό τρόπο να διατηρείτε επαφές με άλλα άτομα. Όπως με οποιαδήποτε άλλη δραστηριότητα στο διαδίκτυο, οι παγίδες και οι κίνδυνοι αναμένουν τον απρόσεκτο.

Οι IM servers παρέχουν τη δυνατότητα να μεταφερθεί κείμενο, φωνή, βίντεο μηνύματα και αρχεία. Κατά συνέπεια, οι instant messengers μπορούν να μεταφέρουν σκουλήκια, ιούς, trojans και spywares. Οι "Cyber-criminals" μπορούν να χρησιμοποιήσουν τα IMs για να κερδίσουν την έμμεση πρόσβαση στους υπολογιστές χωρίς το άνοιγμα μιας listening port, παρακάμπτοντας αποτελεσματικά το firewall.

Η απόλυτη ασφάλεια στα IM μπορεί να επιτευχθεί μόνο αν δεν δώσετε στο αντίστοιχο πρόγραμμα πρόσβαση στο διαδίκτυο. Αν θέλετε όμως να τα χρησιμοποιείτε με την μεγαλύτερη δυνατή ασφάλεια θα πρέπει να προσέξετε τα εξής:

Προσέχετε όταν δημιουργείτε το ψευδώνυμό σας ("nickname"). Τα προγράμματα άμεσων μηνυμάτων σάς ζητούν να δημιουργήσετε ένα nickname, που είναι αντίστοιχο με μια διεύθυνση e-mail. Το nickname δεν θα πρέπει να αποκαλύπτει ή να παραπέμπει σε προσωπικά στοιχεία. Για παράδειγμα, προτιμήστε το ψευδώνυμο Ποδοσφαιρόφιλος αντί για το Γιάννης Πειραιάς.

Δημιουργήστε φραγμούς στα ανεπιθύμητα άμεσα μηνύματα. Μην προσθέτετε το όνομα οθόνης ή τη διεύθυνση e-mail σας σε δημόσιους χώρους (π.χ. σε μεγάλους καταλόγους του Διαδικτύου ή σε προφίλ διαδικτυακών κοινοτήτων) και μην δίνετε τέτοιες πληροφορίες σε ξένους. Κάποιες υπηρεσίες άμεσων μηνυμάτων συνδέουν το όνομα οθόνης με τη διεύθυνση e-mail σας όταν εγγράφεστε. Το γεγονός ότι η διεύθυνση e-mail σας είναι εύκολα διαθέσιμη σημαίνει ότι πιθανόν να διατρέχετε αυξημένο κίνδυνο επιθέσεων spam και phishing.

Ποτέ μην αποκαλύπτετε ευαίσθητα προσωπικά στοιχεία, όπως αριθμοί πιστωτικής κάρτας ή κωδικοί πρόσβασης, κατά τις συζητήσεις μέσω άμεσων μηνυμάτων.

Να επικοινωνείτε μόνο με άτομα που περιλαμβάνονται στη λίστα επαφών ή φίλων σας. Ποτέ μην ανοίγετε εικόνες, μην κατεβάζετε αρχεία και μην κάνετε κλικ σε συνδέσμους που λάβατε από άτομα που δεν γνωρίζετε. Εάν λάβετε κάτι τέτοιο από έναν γνωστό σας, επικοινωνήστε μαζί του για να βεβαιωθείτε ότι το μήνυμα (και τα συνημμένα του) είναι αξιόπιστα. Εάν δεν είναι, κλείστε το άμεσο μήνυμα.

2.9. Clean-up των Windows

2.9.1. Προσθέστε/αφαιρέστε τα προγράμματα

Μπορούμε να αρχίσουμε με την αφαίρεση εγκατεστημένων εφαρμογών που δεν

χρησιμοποιείτε αυτήν την περίοδο ούτε θα χρησιμοποιήσετε καθόλου στο μέλλον. Αυτό μπορεί να γίνει επιλέγοντας κατάργηση σε κάθε εφαρμογή από το παράθυρο προσθαφαίρεση προγραμμάτων του πινάκα ελέγχου ή επιλέγοντας τον unistaller τις συγκεκριμένης εφαρμογής. Αν δεν υπάρχει καμία από τις δυο επιλογές μπορείτε απλά να διαγράψετε τον φάκελο που περιέχεται η εφαρμογή.

2.9.2 System File Checker

Ο System File Checker (sfc.exe) είναι μια λειτουργία γραμμής εντολών που ανιχνεύει και ελέγχει τις εκδόσεις όλων των προστατευμένων system files. Εάν ο System File Checker ανακαλύψει ότι ένα προστατευμένο αρχείο έχει επικαλυφθεί, ανακτά τη σωστή έκδοση του αρχείου από το φάκελλο %systemroot%system32dllcache, και αντικαθιστά έπειτα το ανακριβές αρχείο.

Πατήστε την έναρξη > run και δώστε "sfc /$l*scannow" ,έπειτα πατήστε OK.
Σύνταξη και παράμετροι:
scannow -Scans all protected system files αμέσως.
/scanonce -Scans all protected system files μια φορά.
/scanboot -Scans all protected system files κάθε φορά που ξεκινάει ο υπολογιστής.
/cancel -Ακυρωση όλων των scans από protected system files.
/quiet -Αντικατεστησε όλα τα λανθασμένα file versions χωρίς να ενημερώνεις τον χρήστη.
/enable -Επεστρεψε στις εργοστασιακες ρυθμισεις,που σημαινει ενημερωσε τον χρηστη για να γινει διωρθωση αν βρεθει καποιο λαθος.
/purgecache -Purges the Windows File Protection file cache και scan all protected system files αμεσως .
/cachesize=x -Δώσε το μέγεθος, σε MB, από το Windows File Protection file cache.

Πρέπει να συνδεθείτε ως administrator ή ως μέλος της ομάδας των administrators για να τρέξετε τον System File Checker. Εάν ο φάκελλος %systemroot%system32dllcache είναι αλλοιωμένος ή ακατάλληλος προς χρήση, χρησιμοποιείστε sfc /scannow, sfc/$l*scanonce, ή sfc/$l*scanboot για να επισκευάσει το περιεχόμενο του καταλόγου Dllcache. (Σημειώστε ότι %systemroot% διευκρινίζει τη θέση του φακέλλου Windows System32 στην ιδιαίτερη πλατφόρμα των Windows σας. Παράδειγμα: SYSTEMROOT=C:Windows).

Είναι ορθή πρακτική, να τρέχει ο ελεγκτής αρχείων συστημάτων όποτε προσθέτετε ή αφαιρείτε τις εφαρμογές από το PC σας για να εξασφαλίσετε την ακεραιότητα των αρχείων του συστήματος. Για τους χρήστες Window XP αυτό είναι αυτόματο.

2.9.3. Windows Update

Αν θέλετε το λειτουργικό σας να είναι πιο σταθερό με λιγότερα σφάλματα και λιγότερες τρύπες ασφάλειας θα πρέπει να να εγκαταστήσετε όλα τα service packs που έχουν βγει για την έκδοση των Windows που έχετε και να έχετε την επιλογή για αυτόματο update ενεργή.

2.9.4. Temporary Files

Αν και δεν είναι πραγματικά επιβλαβή αρχεία, τα προσωρινά αρχεία μπορούν να γεμίσουν πολύ μεγάλο χώρο στον δίσκο σας. Πολλά malwares κρύβονται συχνά στους temp φακέλλους και τους προσωρινούς φακέλλους αρχείων Διαδικτύου έτσι είναι μια καλή ιδέα να καθαριστούν κατά διαστήματα.

Ο καθαρισμός δίσκων, που διαθέτουν τα Windows μπορεί να βρεθεί στο φάκελλο προγράμματα > βοηθήματα > εργαλείων συστήματος στο μενού έναρξη.

2.9.5. Υπόλοιπα καθαρισμού από τη Registry

Κατά τη διάρκεια της ζωής των λειτουργικών συστημάτων, ειδικά εάν είναι μακροχρόνιος, η registry μπορεί να γεμίσει με άκυρες και άχρηστες καταχωρήσεις. Εάν η registry γίνει πάρα πολύ μεγάλη, οι λειτουργίες γίνονται λίγο πιο αργά και ο υπολογιστής αργεί να εκκινήσει. Σιγουρευτείτε ότι έχετε καθαρίσει τελειως όλα, στο temp σας αρχεία, έχετε απεγκαταστήσει και έχετε διαγράψει όλα τα ανεπιθύμητα αρχεία συμπεριλαμβανομένων και εκείνων στον κάδο ανακύκλωσης. Για τον καθαρισμό της registry μπορείτε να χρησιμοποιήσετε κάποιο πρόγραμμα που κάνει αυτήν την δουλειά.

2.9.6. Ανασυγκρότηση σκληρών δίσκων

Ένα από τα σημαντικότερα πράγματα που πρέπει να κάνετε σχεδόν κάθε βδομάδα το πολύ δυο αν θέλετε να γίνετε γρήγορα είναι η ανασυγκρότηση δίσκου. Αν δεν την κάνετε σε τόσο τακτά διαστήματα θα σας παίρνει ώρες για να ολοκληρωθεί και μερικά κατακερματισμένα αρχεία δεν θα επανέρχονται. Με την ανασυγκρότηση εκτός του ότι προστατεύετε τα αρχεία σας από ανεπανόρθωτη βλάβη, ο υπολογιστής σας λειτουργεί πιο γρήγορα. Για να κάνετε ανασυγκρότηση μπορείτε να χρησιμοποιείτε τον ανασυγκροτητή των Windows που βρίσκετε στα εργαλεία συστήματος στο μενού έναρξη. ΠΡΟΣΟΧΗ! Μην χρησιμοποιείτε τον υπολογιστή ενώ γίνετε ανασυγκρότηση.

2.9.7. Επαναφορά συστήματος

Αφού εκτελέσετε τις παραπάνω λειτουργίες πηγαίνετε και επιλέξτε την επαναφορά συστήματος από τα εργαλεία συστήματος στο μενού έναρξη και δημιουργήστε ένα σημείο επαναφοράς. Σε περίπτωση που κάτι δεν πάει καλά μπορείτε να πάτε και να επαναφέρετε τον υπολογιστή σας σε εκείνο το σημείο γι' αυτό να δημιουργείτε συχνά σημεία επαναφοράς ώστε να μην έχετε πολλές απώλειες μετά την επαναφορά από ρυθμίσεις και λειτουργίες που είχατε κάνει.

2.10 Antivirus - Anti-trojan - Anti Spyware Εφαρμογές

Πέρα από τους ιούς, τα σκουλήκια και τα trojans υπάρχει ένας ολόκληρος τομέας εισβολής προγραμμάτων που χρησιμοποιούνται για την κατασκόπευση, τη διαφήμιση, και την πειρατεία. Μπορείτε να γεμίσετε από αυτά τα παράσιτα τον υπολογιστή σας λόγω της άγνοιά σας, της έλλειψης προσοχής κατά το σερφ και το κατέβασμα στοιχείων από τους ιστοχώρους.

Τουλάχιστον μία φορά την εβδομάδα, ή συχνότερα ανάλογα με πόσο χρόνο ξοδεύετε on-line, να κάνετε τους πλήρεις ελέγχους του PC σας με αντι-tojan ,αντι-virus και αντί spyware προγράμματα, είτε πριν είτε μετά από τις οδηγίες στο μέρος 2.9. Αυτό θα εξασφαλίσει ότι το σύστημά σας είναι καθαρό και τρέχει καλά. Είναι σημαντικό να κρατηθούν όλες αυτές οι εφαρμογές ενημερωμένες για τους ίδιους λόγους. Δυο πάρα πολύ καλές και freeware εφαρμογές που μπορείτε να χρησιμοποιήσετε είναι το Spybot Search & Destroy και το Lavasoft's Ad-Aware SE Personal Edition.

3. Επίλογος

Η ασφάλεια πραγματικά, ...δεν είναι τόσο δύσκολη. Το πιο δύσκολο είναι να αναπτύξετε ένστικτο σχετικά με τα ηλεκτρονικά μηνύματα και τους ιστοχώρους. Αυτό όμως θέλει πολύ εξάσκηση.

Συχνά ακούμε την ερώτηση, τι μπορούν να κάνουν οι μέσοι χρήστες του Διαδικτύου για να διασφαλίσουν την ασφάλειά τους. Αυτό που θα απαντούσαμε εμείς είναι «Τίποτα...είσαι χαμένος από χέρι.» !

Αυτό, όμως, δεν είναι αλήθεια και στην πραγματικότητα είναι λίγο πιο περίπλοκα τα πράγματα. Είστε χαμένοι από χέρι αν δεν κάνετε κάτι για να προστατέψετε τον εαυτό σας, αλλά υπάρχουν πολλά πράγματα που μπορείτε να κάνετε για να αυξήσετε την ασφάλειά σας στο Διαδίκτυο. Με την εφαρμογή όσων σας συμβουλεύουμε να κάνετε στον παραπάνω δεκάλογο θα πετύχετε ένα αρκετά ικανοποιητικό βαθμό ασφάλειας , ειδικά αν είστε χρήστες των λειτουργικών MS Windows.

4. Βιβλιογραφία-Πηγές

www.microsoft.com

www.go-online.gr

PC Magazine

www.adslgr.com

www.virus.gr

www.castlecop.com

www.asxetos.gr