Ερευνητική Εργασία: Ασφάλεια στο Διαδίκτυο

ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ

Ερευνητική Ομάδα: Πυρουνάκης Αργύρης, Πετράκης Ματθαίος, Ρογδάκης Στέλιος, Λεμονάκης Γιώργος

ΓΕΝΙΚΟ ΛΥΚΕΙΟ ΜΟΙΡΩΝ

2011-2012

Περιεχόμενα

Ηλεκτρονική Αλληλογραφία (E-mail) 3
Α. Ιοί 5
Β. Ενοχλητική Αλληλογραφία (Spam Mail) 5
Γ. Μηνύματα Απατηλού Περιεχομένου (Hoaxes) 6
Δ. Προστασία προσωπικών δεδομένων 7
Ε. Ασφάλεια κατά την Άμεση Συνομιλία (Chat) 7
ΣΤ. Μηνύματα Οικονομικής Εξαπάτησης (Phising) 9
Προγράμματα προσβολής ενός υπολογιστή 10
Α. Ιός 10
Β. Σκουλήκια (Worms) 10
Γ. Τρόποι προστασίας 10
Δ. Τρόποι αντιμετώπισης μόλυνσης 11
Πηγές 12

Ηλεκτρονική Αλληλογραφία (E-mail)

Το Ηλεκτρονικό Ταχυδρομείο (E-mail) αποτελεί μια από τις πιο δημοφιλείς υπηρεσίες του Διαδικτύου προσφέροντας οικονομική, ταχύτατη και αξιόπιστη επικοινωνία με εκατομμύρια ανθρώπους σε ολόκληρο τον κόσμο. Διατίθεται συνήθως από τις εταιρείες παροχής σύνδεσης με το Internet ως πρόσθετη υπηρεσία και συνοδεύεται από ιδιαίτερο κωδικό. Οι χρήστες μπορούν να ανταλλάσσουν μεταξύ τους μηνύματα, στα οποία είναι δυνατόν να επισυνάπτονται αρχεία κάθε τύπου. Τα μηνύματα αυτά ξεκινούν από τον υπολογιστή του αποστολέα και, μέσω των δαιδαλωδών διαδρομών του Διαδικτύου, φτάνουν στον παραλήπτη σε διάστημα λίγων λεπτών.

Ωστόσο ο χρήστης του ηλεκτρονικού ταχυδρομείου πρέπει να είναι ιδιαίτερα προσεκτικός και να λαμβάνει αυξημένα μέτρα προστασίας, καθώς η ευρύτατη διάδοσή του και χρήση του το καθιστούν μια από τις πιο ευάλωτες υπηρεσίες του Διαδικτύου απέναντι σε κακόβουλους χρήστες. Είναι σημαντικό να διαχειριζόμαστε τη διεύθυνση της ηλεκτρονικής μας αλληλογραφίας με την ίδια προσοχή που διαχειριζόμαστε τον αριθμό του τηλεφώνου μας.

Μερικά από τα σημαντικότερα προβλήματα που μπορεί να αντιμετωπίσει ένας χρήστης ηλεκτρονικού ταχυδρομείου είναι τα παρακάτω:

α) Οι Ιοί

β) Η Ενοχλητική αλληλογραφία (spam mail) και

γ) Τα Μηνύματα απατηλού περιεχομένου (hoaxes-phishing)

δ) Προστασία προσωπικών δεδομένων

Το Internet σε ένα μεγάλο βαθμό στηρίζεται στην εμπιστοσύνη. Πρόκειται για έναν παγκόσμιο εικονικό κόσμο στον οποίο δεν βλέπετε τους ανθρώπους ή τους φορείς με τους οποίους επικοινωνείτε παίρνοντας και δίνοντας πληροφορίες. Δεν βλέπετε για παράδειγμα τον χρήστη στον οποίο στέλνετε το e-mail σας αλλά εμπιστεύεστε ότι αυτός που ισχυρίζεται ότι είναι.

Ο βασικός τρόπος εξάπλωσης των ιών παραμένει ακόμα και σήμερα το ηλεκτρονικό ταχυδρομείο e-mail, μόνο που σήμερα σε σχέση με παλαιότερα, λόγω της μεγάλης πληθώρας προγραμμάτων που κυκλοφορούν παράνομα στο διαδίκτυο είναι αυξημένες οι πιθανότητες να προβληθεί ένας υπολογιστής με ιό.

Ενώ, όμως, οι ιοί εξαπλώνονται πλέον μέσω του ηλεκτρονικού ταχυδρομείου, ο βασικός τρόπος άμυνας έχει παραμείνει ο ίδιος.

Τα προγράμματα *antivirus* εξακολουθούν να αποτελούν τη μόνη αποτελεσματική μορφή άμυνας από την πλευρά των χρηστών. Μειονέκτημα σε αυτή την περίπτωση είναι ότι <u>ο ιός πρέπει να κυκλοφορήσει πρώτος</u> και μετά οι εταιρίες προστασίας να προσαρμόσουν τα προγράμματά τους ώστε να τον αναγνωρίζουν και να τον μπλοκάρουν.

Αυτό που μπορούν -και πρέπει- να κάνουν οι χρήστες είναι να είναι υποψιασμένοι.

- Μην ανοίγετε όλα τα μηνύματα που σας έρχονται και σας υπόσχονται αγάπες και λουλούδια, χρήματα ή οτιδήποτε άλλο, ακόμα κι αν έρχονται από κάποιο γνωστό σας.
- Προτιμήστε να επιβεβαιώσετε την αποστολή κάποιου ύποπτου μηνύματος με κάποιο τηλέφωνο ή με e-mail πριν το ανοίξετε, προκειμένου να είστε βέβαιοι ότι δεν στάλθηκε εν αγνοία του αποστολέα από κάποιον ιό που μόλυνε τον υπολογιστή του.

Βέβαια υπάρχει και η πιθανότητα της αυτόματης μόλυνσης αφού οι ιοί που εξαπλώνονται μέσω e-mails έχουν τη δυνατότητα να μολύνουν τον υπολογιστή σας απλά και μόνο διαβάζοντας το e-mail. Αυτό είναι δυνατό να γίνει λόγω μιας αδυναμίας του Outlook και της χρήσης του Windows scripting Host. Αν χρησιμοποιείτε κάποιο άλλο πρόγραμμα πιθανόν να μην έχετε πρόβλημα.

Αν έχετε εγκατεστημένη κάποια παλαιότερη έκδοση του Outlook αναβαθμίστε την. Η νέα έκδοση (6) του Outlook Express δεν έχει πλέον κενό στην ασφάλεια και δε χρειάζεται οι χρήστες να απενεργοποιήσουν το Windows Scripting Host. Επιπλέον με τις τελευταίες ενημερώσεις των Windows προστέθηκε μια πολύ χρήσιμη υπηρεσία ελέγχου των επισυναπτόμενων αρχείων (Attachment Execution Service).

Τα e-mails αυτά που έρχονται σε μορφή HTML μπορεί να περιέχουν ένα script σε κάποια γλώσσα σεναρίου (Java, Visual Basic), που όταν εκτελεστεί να κάνει τη ζημιά στους χρήστες. Τα μηνύματα που έρχονται σε μορφή HTML είναι δυνατόν να περιέχουν scripts, αντίθετα με τα μηνύματα καθαρού κειμένου (plain text) που δεν περιέχουν ούτε scripts, αλλά ούτε και κάποιου άλλου είδους μορφοποίηση.

Μην ξεχνάτε ότι κάθε γράμμα ,πριν φτάσει στον προορισμό του περνά από τουλάχιστον ένα διακομιστή του Ιντερνετικού μας φορέα (ISP) ή από κάποιον άλλο, εγκατεστημένο στη εταιρεία ή τον οργανισμό που εργαζόμαστε. Ποιος μπορεί να εγγυηθεί ότι ένας περίεργος διαχειριστής συστήματος δεν θα μπει στον πειρασμό να ρίξει ένα αδιάκριτο βλέμμα στην αλληλογραφία σας;

Το web-based e-mail είναι οι λογαριασμοί που λειτουργούν μέσω Διαδικτύου και μπορείς να τον προσπελάσεις με τον Φυλλομετρητή (όπως Yahoo, Hotmail, GMail κ.λπ.) οι οποίοι αν και θεωρούνται πιο ασφαλείς ισχύει ότι για τους παραπάνω. Στην ουσία κανένας λογαριασμός e-mail δεν παρέχει απόλυτη ασφάλεια αν και γενικά σχεδόν όλες οι εταιρείες παροχής τέτοιων υπηρεσιών έχουν αναβαθμίσει πάρα πολύ τις παρεχόμενες υπηρεσίες τους διαχωρίζοντας τα ενοχλητικά και βλαβερά e-mail (spam).

Ο μόνος τρόπος ασφάλειας στη διακίνηση της ηλεκτρονικής αλληλογραφίας σας είναι, είτε χρησιμοποιούμε κανονικό είτε web-based e-mail, η κρυπτογράφηση των μηνυμάτων μας πριν την αποστολή.

Α. Ιοί

Η μετάδοση ιών μέσω ηλεκτρονικού ταχυδρομείου είναι ο συνηθέστερος τρόπος διάδοσής τους. Οι ιοί επικολλώνται συνήθως στα συνημμένα αρχεία των μηνυμάτων και μολύνουν τον υπολογιστή του χρήστη, μόλις αυτός ανοίξει το συνημμένο αρχείο.

Δε θα πρέπει λοιπόν οι χρήστες να ανοίγουν ποτέ μηνύματα τα οποία προέρχονται από άγνωστο αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα εκτελέσιμα αρχεία (συνήθως με κατάληξη .exe, .com, .vbs, .dll, .sh, .bat κ.ά.), ενώ πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής .html) που ενεργοποιείται αυτόματα με την ανάγνωση του email.

Θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Για αυτό το λόγο είναι καλό να απενεργοποιείται η προεπισκόπηση στα εισερχόμενα μηνύματα, ώστε αυτά να μην ανοίγουν αυτόματα.

Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (Εισερχόμενης και Εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς.

Β. Ενοχλητική Αλληλογραφία (Spam Mail)

Το λεγόμενο Spam ή Junk mail είναι μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Στο spam mail συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς επίσης και διάφοροι άλλοι τύποι e-mail (π.χ. ανεπιθύμητα newsletters).Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Internet και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Internet και κινδυνεύει η ασφάλεια των δικτύων.

Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα να μην απαντάει σε μηνύματα τέτοιου είδους, ούτε και σε αυτά με την ένδειξη «*remove me from the mailing list*», τα οποία αντί να αποσύρουν την ηλεκτρονική του διεύθυνση, όπως υπόσχονται, επιβεβαιώνουν ότι είναι ενεργή και συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα.

Ο χρήστης μπορεί να χρησιμοποιήσει τα φίλτρα που του προσφέρουν τα περισσότερα Web-Mail για να διαγράφει τα μηνύματα αυτά, ή να ρυθμίσει κατάλληλα το πρόγραμμα διαχείρισης αλληλογραφίας του υπολογιστή του, μέσω των επιλογών που δίνονται από τις καρτέλες στο μενού του προγράμματος.

Επίσης, στο Διαδίκτυο υπάρχουν προγράμματα καταπολέμησης των Spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη.

Γ. Μηνύματα Απατηλού Περιεχομένου (Hoaxes)

Πρόκειται για ενοχλητικού τύπου μηνύματα ηλεκτρονικού ταχυδρομείου

1. **Προειδοποιητικά** : είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες, είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή για το σύστημα

2. **Συμπαράστασης** : παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται

3. **Εκφοβισμού** : οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες.

Ο ουσιαστικός κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοσή τους και, κατά συνέπεια, η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. Εκτός αυτού, δημοσιοποιούνται ευρέως και πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου, καθιστώντας τους ιδιοκτήτες τους ευκολότερα θύματα κάθε τέτοιου είδους ενοχλήσεως.

Τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από την τυποποιημένη φράση «*στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε*» ("*send this to everyone you know*"). Στην περίπτωση των «προειδοποιητικών» μηνυμάτων εμφανίζονται ως αποστολείς μεγάλες και γνωστές εταιρείες, με σκοπό να ξεγελάσουν το χρήστη και να τον κάνουν να εμπιστευτεί το περιεχόμενο του μηνύματος.

Ο χρήστης πρέπει να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του και προκαλεί άνευ λόγου πανικό. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες που ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

Δ. Προστασία προσωπικών δεδομένων

Ο χρήστης των προγραμμάτων αλληλογραφίας πρέπει να είναι ιδιαίτερα προσεκτικός και να μην αναφέρει ποτέ σε μηνύματα, τα προσωπικά του στοιχεία, καθώς και αριθμούς πιστωτικών καρτών ή οποιαδήποτε άλλα ευαίσθητα δεδομένα. Τα emails είναι από τους συνηθέστερους στόχους των κάθε είδους hackers, οι οποίοι μπορούν να υποκλέψουν αυτά τα στοιχεία. Γενικά είναι καλό να αλλάζει τακτικά ο κωδικός πρόσβασης του λογαριασμού email .

Ιδιαίτερη προσοχή χρειάζεται η διαχείριση λογαριασμών Web-Mail , οι οποίοι είναι πολύ πρακτικοί και διαθέσιμοι από παντού, αλλά και με χαμηλό δείκτη προστασίας προσωπικών δεδομένων. Σε αυτούς τους λογαριασμούς συχνά παρέχεται επιλογή για απομνημόνευση του ονόματος χρήστη και του κωδικού στον υπολογιστή, ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή («*Απομνημόνευση του ID μου σε αυτό τον υπολογιστή*»). Είναι προτιμότερο, φυσικά, να μην ενεργοποιείται η παραπάνω επιλογή.

Ε. Ασφάλεια κατά την Άμεση Συνομιλία (Chat)

Το Chat στο Διαδίκτυο είναι ένας τρόπος άμεσης επικοινωνίας ενός συνόλου ανθρώπων, οι οποίοι βρίσκονται συγκεντρωμένοι σε έναν συγκεκριμένο δικτυακό χώρο που ονομάζεται «Δωμάτιο Επικοινωνίας» (Chat Room) και πληκτρολογούν ο ένας στον άλλο μηνύματα κειμένου ή χρησιμοποιούν μικρόφωνο και κάμερα για ζωντανή συνομιλία. Το Chat αποτελεί μια κοινωνική δραστηριότητα ιδιαίτερα δημοφιλή ανάμεσα στους νέους, διότι τους προσφέρει έναν εύκολο και ανέξοδο τρόπο επικοινωνίας και γνωριμίας με ανθρώπους από όλο τον κόσμο.

Η συζήτηση αυτή μπορεί να πραγματοποιηθεί είτε σε ιστοχώρους του Διαδικτύου χωρίς να χρειαστεί η εγκατάσταση κάποιου προγράμματος, είτε εγκαθιστώντας το κατάλληλο λογισμικό (όπως στην περίπτωση εφαρμογών-πελάτη για το δημοφιλές IRC, ή των διαφόρων τύπων Messengers). Στα περισσότερα δωμάτια επικοινωνίας η πρόσβαση είναι ελεύθερη και μπορεί ο καθένας, χρησιμοποιώντας απλά ένα ψευδώνυμο, να παρακολουθεί ή να συμμετέχει σε συζητήσεις.

Υπάρχει ωστόσο και η δυνατότητα «Ιδιωτικής Συνομιλίας», όταν κάποιοι από τα μέλη της ομάδας αποφασίζουν να απομονωθούν από τους άλλους σε ένα ιδιαίτερο «Δωμάτιο» και να επικοινωνούν μόνο μεταξύ τους.

Η χρήση των ψευδωνύμων επιτρέπει στους χρήστες να διατηρούν την ανωνυμία τους. Αυτή ακριβώς η δυνατότητα, μαζί με την ψευδαίσθηση του παιδιού-χρήστη ότι είναι ασφαλές, επειδή βρίσκεται στο φυσικό χώρο του σπιτιού του, του σχολείου του ή ενός ιντερνετ-καφέ, μπορεί να μετατρέψει τον τρόπο αυτό της επικοινωνίας σε μια από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του Διαδικτύου. Υπάρχουν συχνά καταγγελίες παιδιών ότι, κατά τη διάρκεια τέτοιου είδους συνομιλιών, έχουν υποστεί λεκτική ή σεξουαλική παρενόχληση, ενώ έχουν δεχτεί από αγνώστους προτροπές για συνάντηση σε πραγματικό χώρο. Σε χώρες του εξωτερικού έχουν παρουσιασθεί έως τώρα δεκάδες περιπτώσεις παιδιών που εξαφανίσθηκαν, έπεσαν θύματα παιδοφίλων ή κυκλωμάτων παιδικής πορνογραφίας, ή παρασύρθηκαν από αγνώστους τους οποίους «συνάντησαν» σε δωμάτια επικοινωνίας. Ένα από τα σημαντικότερα προβλήματα είναι και η έλλειψη γνώσεων σχετικά με αυτόν τον τρόπο επικοινωνίας, τόσο από τους γονείς, όσο και από τους εκπαιδευτικούς.

Και μόνο η συμμετοχή σε τέτοιου είδους χώρους αποτελεί από μόνη της μια επικίνδυνη πρακτική. Σε περίπτωση όμως που δε μπορούν οι γονείς να αποτρέψουν ή να ελέγξουν τα παιδιά τους, οφείλουν τουλάχιστον να τους επιστήσουν την προσοχή, γιατί αυτά συχνά ξεγελιούνται και αποκαλύπτουν πολλά προσωπικά τους στοιχεία σε αγνώστους, οι οποίοι καταφέρνουν να κερδίσουν την εμπιστοσύνη τους.

Οι συμμετέχοντες σε τέτοιου είδους συνομιλίες δε θα πρέπει με κανέναν τρόπο να αποκαλύπτουν την ταυτότητά τους, ούτε τα προσωπικά τους στοιχεία (διεύθυνση, αριθμό τηλεφώνου, e-mail, όνομα σχολείου, πόλη), να μη δέχονται ποτέ να στείλουν τη φωτογραφία τους σε αγνώστους, ούτε να τους συναντούν σε πραγματικό χώρο. Επίσης, οφείλουν να γνωρίζουν πως σε καμιά περίπτωση δεν είναι ασφαλείς λόγω της ανωνυμίας τους. Ένας ικανός χρήστης του Διαδικτύου είναι σε θέση να εντοπίσει την IP διεύθυνση του υπολογιστή τους, να αποκτήσει πρόσβαση σε προσωπικά τους αρχεία, να μολύνει τον υπολογιστή τους με ιούς ή σκουλήκια, τα οποία συχνότατα κυκλοφορούν σε τέτοιου είδους χώρους.

Τα παιδιά θα πρέπει να ενθαρρύνονται να συζητούν με τους γονείς τους για τις συνομιλίες τις οποίες παρακολουθούν μέσα σε chat-rooms, να μιλάνε για τους νέους φίλους τους, όπως θα έκαναν και για τους φίλους που γνωρίζουν στην πραγματική τους ζωή, να αναφέρουν κάθε περίπτωση κατά την οποία έχουν υποστεί παρενόχληση, οποιουδήποτε είδους. Οι γονείς, με τη σειρά τους, θα πρέπει να προτρέπουν τα παιδιά τους να χρησιμοποιούν αυτή τη δυνατότητα του Διαδικτύου για να επικοινωνήσουν με φίλους τους που βρίσκονται μακριά και τους οποίους τα παιδιά ήδη γνωρίζουν, και όχι ως μέσο νέων γνωριμιών.

ΣΤ. Μηνύματα Οικονομικής Εξαπάτησης (Phising)

Το **Phishing** (*αγγλικός νεολογισμός βασιζόμενος στη λέξη fishing=ψάρεμα*) είναι ένας τρόπος οικονομικής εξαπάτησης ανυποψίαστων πελατών, οι οποίοι λαμβάνουν μηνύματα από «αξιόπιστες» πηγές (τράπεζες, εταιρείες κ.λπ.) που τους ζητούν προσωπικά τους στοιχεία (συνήθως αριθμούς πιστωτικών καρτών, αριθμούς λογαριασμών τραπέζης, κωδικούς πρόσβασης κ.α.), προκειμένου να διεκπεραιώσουν μία συναλλαγή.

Η πλειοψηφία των Phishing μηνυμάτων επικαλείται κάποιο επείγον πρόβλημα ή κάποια «μοναδική ευκαιρία» και ζητά από τον ανυποψίαστο παραλήπτη να απαντήσει άμεσα, είτε για να αποκατασταθεί το πρόβλημα είτε για να επωφεληθεί της ευκαιρίας.

Οι τεχνικές εξαπάτησης που χρησιμοποιούνται είναι ποικίλες. Είτε υπάρχει μια παραποιημένη διεύθυνση ιστού (URL) μέσα στο περιεχόμενο του μηνύματος, η οποία, εκ πρώτης όψεως, φαίνεται σωστή, όταν όμως επιλεγεί από τον χρήστη οδηγεί σε σελίδες ακατάλληλου περιεχομένου. Είτε χρησιμοποιούνται εντολές Javascript ώστε να μπερδευτεί η γραμμή διευθύνσεων και να οδηγήσει σε διαφορετικό ιστοχώρο, είτε χρησιμοποιούνται τα ίδια τα Scripts των τραπεζών ή των εταιρειών και σε αυτήν την περίπτωση οι χρήστες λαμβάνουν ένα μήνυμα που φαίνεται γνήσιο και τους ζητά να επιβεβαιώσουν το λογαριασμό τους ακολουθώντας ένα σύνδεσμο που δείχνει να αντιστοιχεί σε αυθεντικό δικτυακό τόπο.

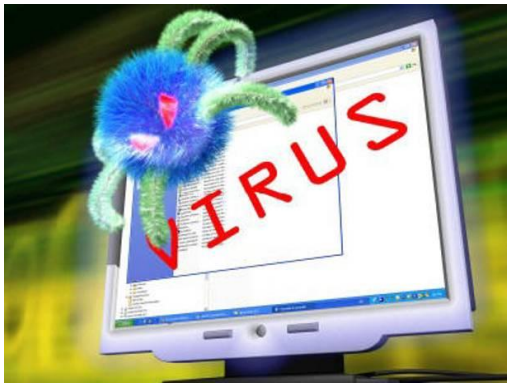
Παρόλο που οι περισσότεροι φυλλομετρητές έχουν ήδη ενσωματώσει τεχνολογία Anti-Phishing προκειμένου να ανιχνεύουν τις σελίδες που ανοίγει ο χρήστης και να τον ειδοποιούν για το αν βρίσκεται σε σελίδα phishing, τα θύματα από τέτοιες επιθέσεις αυξάνονται ανησυχητικά σε όλον τον κόσμο. Ο χρήστης πρέπει να είναι ιδιαίτερα καχύποπτος απέναντι σε τέτοια μηνύματα και να επαληθεύει το περιεχόμενό τους επικοινωνώντας με την εταιρεία ή την τράπεζα που το έστειλε, όχι μέσω του μηνύματος, αλλά με τον τρόπο που χρησιμοποιούσε ως τώρα.

Γενικά, οι αξιόπιστες εταιρείες και τράπεζες δεν καταφεύγουν σε γενικόλογα μηνύματα προκειμένου να εξυπηρετήσουν τους πελάτες τους, ούτε τους ζητούν να αποκαλύψουν τους κωδικούς τους.

Σήμερα κυκλοφορούν αρκετά προγράμματα anti-phishing, τα οποία είτε ελέγχουν το περιεχόμενο των ιστοσελίδων που διατρέχει ο χρήστης, είτε το περιεχόμενο των e-mails που λαμβάνει, προκειμένου να διαπιστώσουν αν πρόκειται για phishing, ενώ αποκαλύπτουν και το πραγματικό όνομα του ιστοχώρου που επισκέπτεται ο χρήστης. Τέλος, τα γνωστά προγράμματα anti-spam μπορούν να μειώσουν τον αριθμό των απατηλών μηνυμάτων που λαμβάνει ο χρήστης.

Προγράμματα προσβολής ενός υπολογιστή

Α. Ιός



Ο ιός του υπολογιστή είναι ένα τμήμα προγράμματος, το οποίο δημιουργεί αντίγραφα του εαυτού του και επισυνάπτεται σε ένα νομότυπο πρόγραμμα με σκοπό να «μολύνει» άλλα προγράμματα. Όταν το μολυσμένο πρόγραμμα εκτελεστεί (το λεγόμενο «άνοιγμα μολυσμένου αρχείου»), κάτω από ορισμένες συνθήκες, προσπαθεί να μολύνει και άλλα προγράμματα, να διαγράψει, να αλλάξει ή να κρυπτογραφήσει αρχεία. Η ύπαρξη ιών είναι ένα από τα σημαντικότερα προβλήματα του Διαδικτύου. Υπάρχουν σήμερα χιλιάδες διαφορετικοί ιοί, οι οποίοι προσβάλλουν εκατομμύρια υπολογιστών σε όλον τον κόσμο. Πολλοί έχουν τη δυνατότητα να μεταλλάσσονται και να διαφέρουν σε μεγάλο βαθμό από τον αρχικό ιό. Σε περίπτωση που μιλάμε για υπολογιστές δικτύων, η καταστροφή έχει ακόμα μεγαλύτερες διαστάσεις, καθώς μολύνονται και καταστρέφονται αρχεία εταιρειών, πανεπιστημίων, υπουργείων, ακόμα και κυβερνήσεων.

Β. Σκουλήκια (Worms)

Πρόκειται για προγράμματα υπολογιστών τα οποία αντιγράφουν τον εαυτό τους σε δίκτυα Η/Υ. Χρησιμοποιούν το Internet ως μέσο διάδοσής τους (Emails, Irc Chat κ.λπ.). Αναπαράγονται από υπολογιστή σε υπολογιστή, εκμεταλλευόμενα τα κενά των Λειτουργικών Συστημάτων των υπολογιστών. Οι μολυσμένοι υπολογιστές μετά από κάποιο διάστημα κατακλύζονται από αντίγραφα του «σκουληκιού» και δε μπορούν να λειτουργήσουν.

Γ. Τρόποι προστασίας

1) Επιλογή ενός καλού αντιβιοτικού προγράμματος (Antivirus).

2) Τακτική ανίχνευση όλου του δίσκου με το αντιβιοτικό σας πρόγραμμα.

3) Συνεχής ανανέωση (Update) του αντιβιοτικού προγράμματος.

4) Έλεγχος κάθε αποθηκευτικού μέσου με το αντιβιοτικό σας πρόγραμμα πριν το ανοίξετε.

5) Τήρηση αντιγράφων ασφαλείας (Back Up) όλων των αρχείων σας.

6) Συχνές επισκέψεις στην τοποθεσία των κρίσιμων ενημερώσεων των Windows (το πλέον διαδεδομένο αλλά και ευάλωτο Λειτουργικό Σύστημα) όπου προσφέρονται δωρεάν αρχεία (Patches) διόρθωσης/κάλυψης των πιθανών κενών-ελλείψεων του λειτουργικού σας. Προτείνεται μάλιστα να ενεργοποιήσετε στον υπολογιστή σας την αυτόματη ενημέρωση των Windows.

7) Ανίχνευση μέσω του αντιβιοτικού κάθε νέου αρχείου που «κατεβάζετε» από το Internet.

8) Αν χρησιμοποιείτε Irc Chat, απενεργοποιείστε την επιλογή αυτόματης αποδοχής αρχείων και αυτόματης εκτέλεσης των αρχείων που σας στέλνουν.

9) Επιλέξτε την πλήρη εμφάνιση των καταλήξεων των αρχείων στον υπολογιστή σας. Ίσως κάποιος να σας στείλει μια «φωτογραφία» ως photo.jpg.vbs. Αν δεν έχετε την παραπάνω επιλογή ενεργοποιημένη, θα εκτελέσετε το αρχείο το οποίο θα περιέχει κάθε άλλο παρά φωτογραφία.

10) Διατηρείτε και ανανεώνετε συχνά μια δισκέτα για αποκατάσταση ζημιών από ιούς, την οποία προσφέρουν συνήθως τα ίδια τα αντιβιοτικά προγράμματα.

Δ. Τρόποι αντιμετώπισης μόλυνσης

1) Αν έχετε μολυνθεί από ιό και έχετε εγκατεστημένο αντιβιοτικό πρόγραμμα, βάλτε το να κάνει πλήρη έλεγχο όλου του σκληρού σας δίσκου (Full System Scan). Αν βρει τον ιό, θα προβεί αυτόματα στις κατάλληλες ενέργειες, είτε διαγράφοντάς τον, είτε απομονώνοντάς τον από το υπόλοιπο σύστημα.

2) Σε περίπτωση που το αντιβιοτικό σας αδυνατεί να αποκαταστήσει τη ζημιά, μη διαγράψετε κανένα μολυσμένο αρχείο. Επανελέγξτε τα μολυσμένα αρχεία με κάποιο άλλο πρόγραμμα, ίσως αυτό να έχει δυνατότητα αποκατάστασης που δεν έχει το πρώτο πρόγραμμα.

3) Αν ο ιός έχει γίνει «διάσημος» λόγω μεγάλης διάδοσης του, τότε προσπαθήστε να βρείτε από το Διαδίκτυο το πρόγραμμα απομάκρυνσης του ιού (Virus Removal Tool) επισκεπτόμενοι τις κατάλληλες διευθύνσεις (εδώ πρέπει να γνωρίζετε την ακριβή ονομασία του ιού, προκειμένου να βρείτε το κατάλληλο για αυτόν πρόγραμμα) και, αφού το κατεβάσετε σε μια «καθαρή» δισκέτα, τρέξτε το στον υπολογιστή σας πάνω από μία φορά.

4) Σε περίπτωση που ούτε το αντιβιοτικό σας, ούτε το ειδικό πρόγραμμα απομάκρυνσης μπορεί να «καθαρίσει» τον υπολογιστή σας, τότε υπάρχει μεγάλη πιθανότητα να απαιτηθεί να κάνετε Μορφοποίηση (Format) και εγκατάσταση εκ νέου του Λειτουργικού Συστήματος και των προγραμμάτων σας. Σε αυτήν την περίπτωση είναι καλό να έχετε κρατήσει αντίγραφα όλων των προγραμμάτων που υπάρχουν στον υπολογιστή σας, για να μπορέσετε μετά το format να τα ξαναπεράσετε. Φυσικά, θα πρέπει να έχετε Αντίγραφα Ασφαλείας (Back Up) των προσωπικών σας αρχείων.

5) Γνωστές εταιρείες προσφέρουν τη δυνατότητα ελέγχου και απομάκρυνσης των ιών του υπολογιστή σας on-line.

Πηγές

- http://www2.e-yliko.gr/htmls/safety/smail.aspx
- Εικόνες: http://images.google.gr