Εισαγωγή

Παρόλο που το διαδίκτυο προσφέρει τεράστια πλεονεκτήματα και μεγάλες ευκαιρίες, η χρήση του συνεπάγεται και διάφορους κινδύνους. Έχοντας αυτό κατά νου, οι τράπεζες λαμβάνουν εκτεταμένα μέτρα για να προστατεύσουν τις πληροφορίες που μεταβιβάζονται και διεκπεραιώνονται κατά τη διενέργεια τραπεζικών συναλλαγών στο διαδίκτυο.

Δεδομένης της δυσκολίας να «αλωθούν» τα τραπεζικά συστήματα λόγω των πολλαπλών επιπέδων ασφάλειας, οι επίδοξοι κακοποιοί αναπόφευκτα στρέφονται προς πιο ευάλωτους στόχους, όπως τείνουν να είναι οι απλοί και συχνά αδαείς χρήστες του διαδικτύου.

Εκ των πραγμάτων, οι Τράπεζες δεν είναι σε θέση να ασκήσουν έλεγχο στα συστήματα που χρησιμοποιούν οι πελάτες τους για τις τραπεζικές τους συναλλαγές στο διαδίκτυο. Επιπλέον, αυτά τα συστήματα — λόγου χάρη ένας προσωπικός υπολογιστής συνδεδεμένος στο διαδίκτυο — συνήθως χρησιμοποιούνται και για διάφορες άλλες εφαρμογές, με συνέπεια την έκθεσή τους σε πολλαπλούς κινδύνους που είναι δύσκολο να ελεγχθούν απόλυτα.

Οι σοβαρότερες και συνηθέστερες απειλές που συνδέονται με τη χρήση του διαδικτύου σήμερα είναι οι εξής:

- hacking: μη εξουσιοδοτημένη πρόσβαση στον υπολογιστή σας μέσω του διαδικτύου με αποτέλεσμα την υποκλοπή, παραποίηση ή διαγραφή των μεταβιβαζόμενων πληροφοριών.
- ιοί και worms: προγράμματα που αναπαράγονται από μόνα τους ή αποστέλλονται μέσω διαδικτύου με e-mail και μπορούν να καταστρέψουν αρχεία ή δεδομένα του υπολογιστή σας.
- Trojan (δούρειοι ίπποι) ή keyloggers, spyware: προγράμματα που, χωρίς να το γνωρίζετε, εκτελούν εργασίες οι οποίες θέτουν σε κίνδυνο την ασφάλεια του υπολογιστή σας, όπως η υποκλοπή κωδικών πρόσβασης.
- phishing: διόδευση των ανυποψίαστων χρηστών προς παραπλανητικές ιστοσελίδες–παγίδες με σκοπό την απόσπαση προσωπικών και εμπιστευτικών πληροφοριών.
- Masquerading: χρήση ψεύτικης ονομασίας, ιστοσελίδας ή διεύθυνσης για παράνομους σκοπούς.

Οι τράπεζες λαμβάνουν συνεχώς μέτρα, τα οποία παρέχουν ουσιαστική προστασία των συστημάτων τους από τυχόν απευθείας επιθέσεις εναντίον τους. Θα πρέπει όμως να λαμβάνετε κι εσείς κάποια μέτρα για την προστασία των δικών σας συστημάτων.

Ακολουθώντας τους 10 κανόνες που περιγράφονται στη συνέχεια, μπορείτε να ενισχύσετε σημαντικά την ασφάλεια του υπολογιστή που χρησιμοποιείτε για την πρόσβασή σας στο διαδίκτυο και να περιορίσετε τους κινδύνους στο ελάχιστο.

Κανόνες ασφαλείας

Κανόνας 1ος: Προστατεύστε τα απόρρητα προσωπικά δεδομένα που στέλνετε μέσω διαδικτύου .

Κάθε μη ασφαλής μεταβίβαση δεδομένων μέσω του διαδικτύου μπορεί να υποκλαπεί από μη εξουσιοδοτημένα άτομα ή να προβληθεί στα συστήματά τους. Συνεπώς, δεν θα πρέπει ποτέ να στέλνετε απόρρητα προσωπικά δεδομένα μέσω διαδικτύου, εκτός αν είναι κρυπτογραφημένα με το πρωτόκολλο κρυπτογράφησης 128-bit SSL.

Οι τράπεζες έχουν λάβει μέτρα, για να διασφαλίσουν πως όσα δεδομένα αποστέλλονται κατά τη διενέργεια τραπεζικών συναλλαγών στο διαδίκτυο, μεταβιβάζονται με τη χρήση ασφαλούς τεχνολογίας κρυπτογράφησης 128-bit SSL. Εισάγετε οποιονδήποτε προσωπικό σας κωδικό ή στοιχείο μόνο όταν βρίσκεστε στις ασφαλείς σελίδες της τράπεζάς σας και η σύνδεση είναι κρυπτογραφημένη . Ο απλούστερος τρόπος επαλήθευσης είναι να ελέγξετε ότι το URL της τράπεζάς σας ξεκινά με το πρόθεμα «https://» και όχι απλά "http://".

Κανόνας 2ος: Βεβαιωθείτε με ποιον έχετε να κάνετε.

Στο διαδίκτυο, δεν δηλώνουν όλοι την πραγματική τους ταυτότητα. Είναι σχετικά εύκολο για έναν ειδικό να πλαστογραφήσει μια διεύθυνση e-mail ή ακόμα και να παραχαράξει ολόκληρη ιστοσελίδα — ενδεχομένως την ιστοσελίδα κάποιας τράπεζας που θέλετε να επισκεφθείτε.

Ελέγξτε το URL στη γραμμή διευθύνσεων του προγράμματος πλοήγησης και βεβαιωθείτε ότι η διεύθυνση της τράπεζάς σας στο διαδίκτυο είναι γραμμένη σωστά. Η παραμικρή παρέκκλιση μπορεί να αποτελεί ένδειξη ότι η ιστοσελίδα είναι ψεύτικη (λ.χ. αντικατάσταση χαρακτήρων από νούμερα π.χ. Gold-g01d)

Ελέγξτε, επίσης τις πληροφορίες ασφαλείας που παρέχει το πρόγραμμα πλοήγησης (browser), και επαληθεύστε την εγγυρότητα ψηφιακού πιστοποιητικού σύμφωνα με της οδηγίες της Τράπεζάς σας

Μην γνωστοποιείτε προσωπικά δεδομένα αν δεν είστε βέβαιοι ποιος τα

λαμβάνει και ποια θα είναι η τύχη τους. Να είστε καχύποπτοι απέναντι σε κάθε παρέκκλιση από τα συνηθισμένα, όπως λόγου χάρη αιτήματα να δώσετε τους μυστικούς σας κωδικούς σε κάποια στιγμή που δεν το περιμένετε.

Ένα αγαπημένο τέχνασμα των χάκερ είναι να παριστάνουν πρόσωπα που κατέχουν θέσεις εμπιστοσύνης. Υπάρχει, λόγου χάρη, μια απάτη γνωστή ως «phishing», στο πλαίσιο της οποίας λαμβάνετε ένα e-mail που δίνει την εντύπωση ότι προέρχεται από την τράπεζά σας. Το e-mail σας ζητά να μεταβείτε στην ιστοσελίδα της τράπεζάς σας και να ανανεώσετε τους κωδικούς πρόσβασής σας. Όμως η σύνδεση (link) που εμφανίζεται στο e-mail θα σας μεταφέρει σε μια παρόμοια ιστοσελίδα, κατασκευασμένη από τον απατεώνα, ο οποίος θα είναι πλέον σε θέση να υποκλέψει τους μυστικούς κωδικούς που καλοπροαίρετα θα δώσετε. Πρέπει, λοιπόν, οπωσδήποτε να βεβαιώνεστε ότι εισάγετε τους μυστικούς κωδικούς πρόσβασής σας μόνο μέσω της αυθεντικής ιστοσελίδας της τράπεζάς σας και όχι μέσω συνδέσμων (links) σε άλλα sites, μηχανές αναζητήσεως ή e-mail.

Κανόνας 3ος: Προσοχή με απόρρητα προσωπικά δεδομένα και μέσα πρόσβασης

Προστατέψτε τους κωδικούς και τα μέσα πρόσβασής σας (PIN, συσκευές παραγωγής κωδικών μιας χρήσης ή «έξυπνες» κάρτες) από κάθε μη εξουσιοδοτημένη χρήση. Ποτέ μην αποθηκεύετε απόρρητα προσωπικά δεδομένα (κωδικούς πρόσβασης, PIN, αριθμούς πιστωτικών καρτών) στον σκληρό δίσκο του υπολογιστή σας. Αν ο Η/Υ δεν χρησιμοποιείται μόνο από εσάς (λόγου χάρη, ο υπολογιστής στης δουλειά σας), θα είναι δυνατό τρίτοι να δουν τα στοιχεία. Επιπλέον, μπορεί κάποια ειδικά προγράμματα που έχουν κατορθώσει να παρεισφρήσουν στον υπολογιστή σας, να είναι σε θέση να υποκλέψουν τα δεδομένα σας και να τα μεταβιβάσουν, λόγου χάρη, μέσω e-mail. Αν χρησιμοποιείτε εξοπλισμό ασφαλείας, όπως συσκευή ανάγνωσης «έξυπνων» καρτών με πληκτρολόγιο εισαγωγής PIN, βεβαιωθείτε ότι εισάγετε τους μυστικούς κωδικούς μόνο όταν σας το ζητά η συσκευή.

Το πιο σημαντικό είναι να μην αποθηκεύετε τον κωδικό σύνδεσής σας με το Διαδίκτυο. Έτσι θα είναι πιο εύκολο να προστατευθείτε από ανεπιθύμητες συνδέσεις.

Κανόνας 4ος: Επιλέξτε ασφαλή κωδικό πρόσβασης

Αν θέλετε να χρησιμοποιήσετε τον υπολογιστή σας για να ξεκινήσετε μια εφαρμογή όπως το online banking, συνήθως αρχίζετε με την εισαγωγή ενός κωδικού πρόσβασης. Πρόκειται για ένα προσωπικό εμπιστευτικό στοιχείο, το οποίο σας βοηθά να αποδείξετε την ταυτότητά σας και δείχνει ότι είστε εξουσιοδοτημένοι να χρησιμοποιήσετε σε έναν συγκεκριμένο υπολογιστή ή σε μια συγκεκριμένη εφαρμογή. Συνεπώς, είναι ζήτημα ζωτικής σημασίας να μην αποκαλύπτετε σε κανέναν το συγκεκριμένο στοιχείο. Επίσης, δεν πρέπει να γράφετε πουθενά τον κωδικό πρόσβασης, ο οποίος θα

πρέπει να είναι μοναδικός και να μαντεύεται δύσκολα.

Καλό είναι ο κωδικός πρόσβασης να περιλαμβάνει από έξι έως οκτώ χαρακτήρες και έναν συνδυασμό πεζών και κεφαλαίων γραμμάτων, αριθμών και ειδικών συμβόλων. Επίσης, να αποφεύγεται η χρήση κύριων ονομάτων, γνωστοί όροι της καθομιλουμένης, επαναλήψεις ενός χαρακτήρα (π.χ. ΑΑΑ-ΑΑΑ) ή ακολουθίες γραμμάτων του πληκτρολογίου (π.χ. qwerty). Υπάρχουν διάφορες μέθοδοι επιλογής κωδικών πρόσβασης που δύσκολα μαντεύονται: μια απλή μέθοδος είναι να φτιάξετε έναν κωδικό από τα πρώτα γράμματα ενός γνωμικού ή ποιήματος. Η προσθήκη ειδικών συμβόλων ή αριθμών μπορεί να περιπλέξει ακόμα περισσότερο τα πράγματα. Λόγου χάρη, το «2gmsksa» μπορεί να σημαίνει «δυο γάιδαροι μαλώνανε σε ξένο αχυρώνα». Αλλάζετε προληπτικά τον κωδικό πρόσβασής σας σε τακτά χρονικά διαστήματα και οπωσδήποτε εάν έχετε λόγους να υποψιάζεστε ότι έχει υποκλαπεί.

Κανόνας 5ος: Χρησιμοποιείτε προγράμματα μόνο από αξιόπιστες πηγές

Μην κατεβάζετε στον σκληρό σας δίσκο προγράμματα από το διαδίκτυο, εκτός αν μπορείτε να είστε βέβαιοι ότι η πηγή είναι αξιόπιστη. Εξακριβώστε την ταυτότητα του προμηθευτή. Με τη φόρτωση προγραμμάτων ή το άνοιγμα συνημμένων αρχείων e-mail, μπορούν να παρεισφρήσουν στον υπολογιστή σας ιοί ή δούρειοι ίπποι (Trojan Horses, keyloggers). Μην ανοίγετε συνημμένα αρχεία αν δεν γνωρίζετε τον αποστολέα τους ή το περιεχόμενό τους. Πρώτα αποθηκεύστε το περιεχόμενο και στη συνέχεια, προτού το ανοίξετε, ελέγξτε το με κάποιο πρόγραμμα ασφαλείας Πριν εγκαταστήσετε προσθήκες (plugins) ήχου ή τρισδιάστατης εικόνας στο πρόγραμμα πλοήγησής σας διαβάζετε πάντα πολύ προσεκτικά τους όρους της άδειας χρήσης των προγραμμάτων και απαντάτε με προσοχή στις ερωτήσεις του τύπου 'Yes or No' κατά τη διάρκεια της εγκατάστασής τους στον υπολογιστή σας. Υπάρχει το ενδεχόμενο να δώσετε εσείς οι ίδιοι εν αγνοία σας την άδεια στους κατασκευαστές των προγραμμάτων αυτών να εγκαταστήσουν στον υπολογιστή σας κακόβουλο λογισμικό (spyware, ιοί) με απρόβλεπτες συνέπειες.

Κανόνας 6ος: Χρησιμοποιείτε ενημερωμένες εκδόσεις προγραμμάτων

Να χρησιμοποιείτε μόνο την ενημερωμένη έκδοση του προγράμματος πλοήγησης στο διαδίκτυο και του λειτουργικού συστήματος που προτιμάτε. Μόνο οι πιο πρόσφατες εκδόσεις κατοχυρωμένου διαδικτυακού λογισμικού εγγυώνται στο μέγιστο βαθμό την εξάλειψη κάθε γνωστού ρήγματος ασφαλείας.

Οι κατασκευαστές λογισμικού αναπτύσσουν, επίσης, μικρά προγράμματα γνωστά ως διορθώσεις σφαλμάτων (bug fixes) ή διορθωτικές εκδόσεις (patches), για την επίλυση προβλημάτων ασφαλείας που έχουν ανακαλύψει. Μείνετε συντονισμένοι με τις πιο πρόσφατες εξελίξεις: οι περισσότεροι κατασκευαστές διατηρούν για

τον σκοπό αυτό υπηρεσίες ενημέρωσης. Η Microsoft, λόγου χάρη, παρέχει στη διεύθυνση http://update.microsoft.com, μια υπηρεσία η οποία θα ελέγξει πόσο ενημερωμένος είναι ο Internet explorer και το λειτουργικό σύστημα Windows, και θα σας εφοδιάσει με τις τυχόν απαραίτητες διορθωτικές εκδόσεις.

Κανόνας 7ος: Εκτελέστε έλεγχο ασφαλείας στον υπολογιστή σας

Πριν χρησιμοποιήσετε τον υπολογιστή σας για τραπεζικές συναλλαγές στο διαδίκτυο, αφιερώστε μερικά λεπτά για να εκτελέσετε έναν έλεγχο ασφαλείας. Ενεργοποιήστε τα χαρακτηριστικά ασφαλείας που προστατεύουν τον υπολογιστή σας από μη εξουσιοδοτημένη πρόσβαση. Σε αυτά περιλαμβάνονται, λόγου χάρη, ο κωδικός που σας ζητά το λειτουργικό σύστημα ή το πρόγραμμα προφύλαξης οθόνης (screen saver) να εισάγετε, κατά την εκκίνηση του υπολογιστή.

Να έχετε κατά νου ότι αν δεν είστε ο μοναδικός χρήστης ενός υπολογιστή — όπως, λόγου χάρη, συμβαίνει στα Internet café — δεν μπορείτε ποτέ να γνωρίζετε ακριβώς τι είδους προγράμματα εκτελούνται. Είναι δυνατόν ακόμα και να έχει γίνει παρέμβαση στο πληκτρολόγιο. Σε ένα τέτοιο περιβάλλον είναι αδύνατον να περιμένετε ότι η ασφάλεια θα είναι απόλυτη. Αν χρησιμοποιήσετε κάποιο Internet cafe για τη διενέργεια online τραπεζικών συναλλαγών, να καθαρίζετε πάντα στη συνέχεια την προσωρινή μνήμη (cache) και το ιστορικό ενεργειών (history) του προγράμματος πλοήγησης, έτσι ώστε να σβήνονται τα ίχνη σας και μαζί τα προσωπικά σας στοιχεία.

Κανόνας 8ος: Ενεργοποιείστε τις ρυθμίσεις ασφαλείας του προγράμματος πλοήγησης

Ενεργοποιείστε τις ρυθμίσεις ασφαλείας του προγράμματος πλοήγησής σας στο διαδίκτυο. Μπορείτε να ενισχύσετε σημαντικά την ασφάλειά σας στο διαδίκτυο, με την έξυπνη χρήση των επιλογών ασφαλείας του προγράμματος πλοήγησής σας και μόνο. Πρέπει οπωσδήποτε να μπλοκάρετε τα ActiveX Controls και να επιτρέπετε την εκτέλεση προγραμμάτων Java Applet μόνο κατόπιν επιβεβαίωσης.

Πρόκειται για μικρά, ανεξάρτητα προγράμματα ενεργού περιεχομένου (active content programs), τα οποία εκτελούνται στον υπολογιστή σας και μπορούν, σε συγκεκριμένες περιπτώσεις, να ενεργοποιήσουν ανεπιθύμητες λειτουργίες (όπως την αποστολή του κωδικού πρόσβασής σας σε κάποιον τρίτο, μέσω e-mail). Αποφεύγετε τη λειτουργία αυτόματης καταχώρισης του προγράμματος πλοήγησης, η οποία αποθηκεύει τα ονόματα χρήστη και τους κωδικούς πρόσβασης που εισάγετε και προτείνει αντιστοιχίσεις.

Τα Cookies αποθηκεύουν πληροφορίες σε ένα ειδικό αρχείο του σκληρού σας δίσκου, αλλά δεν διαβάζουν άλλου είδους δεδομένα. Αν έχετε αμφιβολίες, μην επιτρέπετε σε κάποια ιστοσελίδα να καταγράφει πληροφορίες στον σκληρό σας δίσκο, επειδή αργότερα μπορεί να χρησιμοποιηθούν για τη δημιουργία ενός προφίλ χρήστη. Η

απόρριψη, όμως, των cookies σε μόνιμη βάση δεν αποτελεί πάντα την πλέον ενδεδειγμένη στρατηγική. Αν απορρίψετε ένα cookie, ενδέχεται να μην μπορείτε να χρησιμοποιήσετε κάποιες ιστοσελίδες. Αν το αποδεχθείτε, ο διακομιστής θα σας αναγνωρίζει κάθε φορά που επιστρέφετε στην ιστοσελίδα. Έτσι ο διακομιστής έχει τη δυνατότητα να δημιουργήσει «αρχείο» και να καταρτίσει ένα προφίλ χρήστη. Καταγράφει στοιχεία όπως οι όροι αναζήτησης που χρησιμοποιείτε και οι σελίδες που επισκέπτεστε. Μόλις γίνουν γνωστές οι προτιμήσεις και τα ενδιαφέροντά σας μπορούν να τοποθετηθούν στοχευμένα διαφημιστικά πλαίσια. Με τις κατάλληλες ρυθμίσεις του προγράμματος πλοήγησης έχετε τη δυνατότητα να απολαμβάνετε τα καλά των cookies, εμποδίζοντας ταυτόχρονα τους μη εξουσιοδοτημένους τρίτους να καταγράφουν τη συμπεριφορά σας για ανεπιθύμητους λόγους.

Κανόνας 9ος: Εγκαταστήστε προγράμματα ανίχνευσης ιών και πρόσθετο λογισμικό ασφαλείας

Εγκαταστήστε πρόσθετο λογισμικό ασφαλείας. Υπάρχουν προβλήματα ασφαλείας που δεν μπορούν να λυθούν μόνο με τα τυπικά εργαλεία του λειτουργικού σας συστήματος. Ένα σημαντικό πρόσθετο εργαλείο είναι ένα πρόγραμμα ανίχνευσης ιών (antivirus, antispyware), το οποίο ενημερώνεται συνεχώς, άρα είναι σε θέση να εντοπίζει νέους ιούς. Σχεδόν κάθε μέρα ανακαλύπτονται νέοι ιοί και είναι πάρα πολύ πιθανό να προσβληθείτε ενώ «σερφάρετε» στο διαδίκτυο.

Εγκαταστήστε ένα τείχος ασφάλειας (firewall) στον υπολογιστή σας. Το firewall είναι ένα πρόγραμμα, το οποίο ελέγχει κάθε εισερχόμενη και εξερχόμενη κυκλοφορία ανάμεσα στον υπολογιστή σας και στο Διαδίκτυο και επιτρέπει μόνο τις εξουσιοδοτημένες συνδέσεις. Έτσι ελαχιστοποιείτε την πιθανότητα διάνοιξης μιας 'κερκόπορτας' (back door) στον υπολογιστή σας από hackers οι οποίοι θα την χρησιμοποιούν κάθε φορά που βρίσκεστε στο διαδίκτυο, για να στέλνουν, λόγου χάρη, εν αγνοία σας ανεπιθύμητα e-mail (spam). Η ύπαρξη τείχους ασφαλείας (firewall) μπορεί να σας προστατεύσει από τέτοιου είδους επιθέσεις.

Ενημερωθείτε για τα προγράμματα firewalls που διατίθενται στην αγορά είτε μέσω των εταιρειών εξειδικευμένου λογισμικού είτε από τα καταστήματα ηλεκτρονικών υπολογιστών τα οποία επίσης προσφέρουν μεγάλη ποικιλία προγραμμάτων που συμβάλουν στην ενίσχυση της ασφάλειας του Η/Υ σας, όπως συσκευές προστασίας πρόσβασης και κρυπτογράφησης.

Κανόνας 10ος: Να δημιουργείτε τακτικά αντίγραφα ασφαλείας

Η διατήρηση αντιγράφων ασφαλείας των αρχείων σας (backups) είναι ένας από τους χρυσούς κανόνες για κάθε χρήστη υπολογιστή — είτε διενεργεί τραπεζικές συναλλαγές στο διαδίκτυο είτε όχι. Συνήθως είναι εξαιρετικά περίπλοκο, αν όχι αδύνατο, να διασώσετε δεδομένα μετά τη διαγραφή ή την καταστροφή τους. Ένας βολικός τρόπος δημιουργίας αντιγράφων ασφαλείας είναι η χρήση κινητών μονάδων σκληρού δίσκου, συσκευών εγγραφής CD ή DVD, ή μονάδων μαγνητοταινίας.

Όποια μέθοδο και αν επιλέξετε, μην ξεχνάτε να δημιουργείτε σε τακτική βάση αντίγραφα ασφαλείας των νέων ή τροποποιημένων αρχείων. Επίσης, φυλάξτε τα αντίγραφα ασφαλείας σε ασφαλές μέρος, δηλαδή ξεχωριστά από τον υπολογιστή σας και προστατευμένα από κάθε μη εξουσιοδοτημένη πρόσβαση.

Γλωσσάριο

Active X Control	Μικρό πρόγραμμα των Windows το οποίο μπορεί, λόγου χάρη, να εκτελεστεί με τη βοήθεια ενός προγράμματος πλοήγησης. Τα Active X Control μπορεί ήδη να βρίσκονται στον υπολογιστή σας ή μπορεί να φορτωθούν αυτόματα όταν επισκέπτεστε κάποια ιστοσελίδα.
Cookie	Μικρό αρχείο κειμένου που αποθηκεύεται στον υπολογιστή σας από το πρόγραμμα πλοήγησης κατόπιν εντολής ενός διακομιστή και περιλαμβάνει στοιχεία, όπως οι δικτυακές προτιμήσεις σας. Τα cookies μπορεί να ενεργούν ως ηλεκτρονικά «σημειωματάρια» του διακομιστή, καταγράφοντας συνήθειες του χρήστη του συστήματος πλοήγησης, όπως ποιες ιστοσελίδες επισκέπτεται, πόσο συχνά και για πόση ώρα, ή αν μια ιστοσελίδα θα πρέπει να αποσταλεί στον χρήστη σε εξατομικευμένη μορφή.
Java Applet	Η Java είναι μια γλώσσα προγραμματισμού που αναπτύχθηκε στις αρχές της δεκαετίας του 1990. Το Java Applet είναι ένα μικρό πρόγραμμα που ερμηνεύεται και εκτελείται στο πρόγραμμα πλοήγησης αφού φορτωθεί από το διαδίκτυο. Οι εντολές java ενσωματώνονται στις σελίδες HTML και εκτελούνται κατά τη φόρτωσή τους.
Keylogger	Πρόγραμμα καταγραφής πληκτρολόγησης που εγκαθίσταται στον υπολογιστή εν αγνοία του χρήστη του.
Masquerading	Χρήση ψεύτικου ονόματος, ιστοσελίδας ή διεύθυνσης για παράνομους σκοπούς.
Phishing	Είναι η διόδευση ανυποψίαστων επισκεπτών 'νόμιμων' ιστοσελίδων προς άλλες ιστοσελίδες-παγίδες με σκοπό την απόσπαση προσωπικών και εμπιστευτικών πληροφοριών (passwords, e-mails κλπ) για παράνομη χρήση. Συνήθως διαπράττεται μέσω e.mail το οποίο εμφανίζεται προερχόμενο από αξιόπιστη πηγή και οδηγεί μέσω link

	τον παραλήπτη σε παράνομη ιστοσελίδα όπου προτρέπεται να εισάγει προσωπικά στοιχεία τα οποία και υποκλέπτονται.
Trojan (Δούρειος ίππος)	Πρόκειται για προγράμματα που, εκτελούν διαφορετική λειτουργία από αυτή που παρουσιάζουν στον χρήστη και η οποία θέτει σε κίνδυνο την ασφάλεια του υπολογιστή. Στόχος των περισσότερων Trojan είναι να υποκλέψουν ευαίσθητα δεδομένα, όπως κωδικούς πρόσβασης, PIN κλπ και να τα αποστείλουν με e-mail ή μέσω του διαδικτύου στον «ιδιοκτήτη» τους. Τα αποκαλούμενα «back door» Trojan παρέχουν στους χάκερ απομακρυσμένη πρόσβαση σε υπολογιστές, τους οποίους μπορούν πλέον να ελέγχουν.
Spyware	Συνώνυμο του Trojan
URL (Uniform Resource Locator)	Τυποποιημένη ηλεκτρονική διεύθυνση που καθορίζει σε ποιο σημείο του Διαδικτύου είναι τοποθετημένες σελίδες, αρχεία ή εικόνες. π.χ. http://www.hba.gr
Worms	Προγράμματα που αυτοαναπαράγονται και εξαπλώνονται από υπολογιστή σε υπολογιστή μέσω δικτύων. Στόχος τους είναι να προσβάλλουν όσο το δυνατόν περισσότερους Η/Υ ενός δικτύου και να προκαλέσουν ζημιές.
Διορθωτική έκδοση (patch)	Μικρό πρόγραμμα που έχει αναπτυχθεί για την επίλυση, το συντομότερο δυνατό, προβλημάτων που έχουν εντοπιστεί στην υπάρχουσα έκδοση κάποιου προγράμματος.
Ιοί	Προγράμματα που αυτοαναπαράγονται και εξαπλώνονται στο διαδίκτυο, παραδείγματος χάρη, με επισυναπτόμενα αρχεία σε e-mail. Οι ιοί μπορούν μερικές φορές να προκαλέσουν μεγάλες ζημιές στους προσβεβλημένους υπολογιστές.
Κυβερνοχώρος (cyberspace)	Όρος που αναφέρεται μεταφορικά στον χώρο που δημιουργείται ανάμεσα στα δίκτυα ηλεκτρονικών υπολογιστών, για παράδειγμα οι ιστοσελίδες βρίσκονται στον

κυβερνοχώρο.

Προσωρινή μνήμη (cache) Προσωρινός χώρος αποθήκευσης στον σκληρό δίσκο του υπολογιστή σας ή ενός εξωτερικού υπολογιστή.

Τείχος προστασίας (firewall) Πρόκειται για συστήματα που ελέγχουν την κυκλοφορία δεδομένων ανάμεσα σε ένα τοπικό δίκτυο ή έναν υπολογιστή και άλλα δίκτυα, όπως το διαδίκτυο. Αποστολή του τείχους προστασίας είναι να προστατεύει το τοπικό δίκτυο ή τον υπολογιστή από μη εξουσιοδοτημένες προσβάσεις. Το προσωπικό firewall είναι ένα πρόγραμμα που εκπληρώνει την αποστολή του τείχους προστασίας στον υπολογιστή σας, δηλαδή σας προστατεύει από κάθε ανεπιθύμητη πρόσβαση, χωρίς να χρειάζεται πρόσθετο σύστημα.