

10 + 1

Συμβουλές της DART για Ασφαλείς Συναλλαγές στο Διαδίκτυο

1

Πώς να βεβαιωθείτε για την φερεγγυότητα του ηλεκτρονικού καταστήματος

Μπορείτε να ενημερωθείτε για την «ταυτότητα» της ιστοσελίδας του ηλεκτρονικού καταστήματος που επισκέπτεστε, αναζητώντας την μέσα από τα μητρώα του Internet (π.χ. τη διεθνή βάση δεδομένων www.whois.net ή τη βάση ελληνικών καταχωρίσεων https://grweb.ics.forth.gr/whois_el.jsp).

Εκεί θα βρείτε σε ποιόν ακριβώς έχει καταχωρηθεί το ηλεκτρονικό κατάστημα.

Μπορείτε να αναζητήσετε την ύπαρξη ενός ειδικού

σήματος στην ιστοσελίδα που πιστοποιεί την ταυτότητά της. Ακόμα χρήσιμο θα ήταν πριν προβείτε σε αγορές να επικοινωνήσετε με τον τηλεφωνικό αριθμό του φυσικού καταστήματος (είναι υποχρεωτική η αναγραφή του στην ιστοσελίδα) για να διαπιστώσετε πως όντως πρόκειται για το κατάστημα που έχετε επιλέξει.

2

Πώς να προστατέψτε τα προσωπικά σας δεδομένα

Οι ρυθμίσεις που αφορούν στην προστασία προσωπικών δεδομένων εφαρμόζονται και στο δικτυακό περιβάλλον. Τα προσωπικά δεδομένα δεν είναι «ελεύθερο εμπόρευμα» και θα πρέπει να χρησιμοποιούνται μόνο για τον σκοπό για τον οποίο συλλέγονται και να διατηρούνται μόνο όσο είναι αναγκαίο για τους σκοπούς της συγκεκριμένης συναλλαγής. Συλλογή και επεξεργασία προσωπικών δεδομένων που δεν εντάσσονται σε συγκεκριμένη συναλλαγή μπορεί να γίνει μόνο με τη ρητή συγκατάθεση σας, αφού προηγουμένως ενημερωθείτε για τον σκοπό, τις κατηγορίες των δεδομένων κ.λπ. Η προηγούμενη συγκατάθεσή σας είναι απαραίτητη και στην περίπτωση που το ηλεκτρονικό κατάστημα ή ηλεκτρονική επιχείρηση θέλει να διαβιβάσει τα δεδομένα που σας αφορούν σε τρίτους.

3

Τί γίνεται αν υπάρξει κάποιο πρόβλημα με μια ηλεκτρονική αγορά

Σύμφωνα με τη νομοθεσία της Ευρωπαϊκής Ένωσης, μπορείς να ακυρώσεις μια υπηρεσία ή να επιστρέψεις ένα προϊόν, μέσα σε συγκεκριμένο χρονικό διάστημα - συνήθως επτά ημερών- γνωστό και ως "cooling-off period". Σε περίπτωση επιστροφής, συνήθως πληρώνεις ο ίδιος τα έξοδα αποστολής. Σε περίπτωση ελαττωματικού προϊόντος, μπορείς και πρέπει να προβείς άμεσα σε καταγγελία στις αρμόδιες υπηρεσίες. Σε περίπτωση μη εκτέλεσης μιας υπηρεσίας, δικαιούσαι την επιστροφή των χρημάτων σου.

4

Πού να απευθυνθείτε αν έχετε το οποιοδήποτε πρόβλημα με κάποιο

ηλεκτρονικό κατάστημα

- Κατ' αρχήν στο ίδιο εμπορικό κατάστημα από το οποίο αγοράσατε.
- Στον επαγγελματικό σύλλογο που εκπροσωπεί τον κλάδο του εμπόρου.
- Στο Επιμελητήριο του ηλεκτρονικού καταστήματος.
- Στην υπηρεσία προστασίας του καταναλωτή του Υπουργείου Ανάπτυξης (τηλ. 1520).
- Στις επιτροπές «φιλικού διακανονισμού», στις Νομαρχίες όλης της Ελλάδας.
- Στην υπηρεσία πελατών ή στην εκδίδουσα Διεύθυνση της Τράπεζας από την οποία πήρατε την πιστωτική σας κάρτα.
- Στις Ενώσεις Καταναλωτών: π.χ. ΕΚΠΟΙΖΩ (τηλ. 210 3304444 - Αθήνα, 2310 25 77 76 - Θεσσαλονίκη), ΙΝΚΑ (τηλ. 210 3632443 Αθήνα, 2310 535263 Μακεδονίας) ΚΕΠΚΑ (801-11-17200).
- Στο Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος στη Γενική Αστυνομική Διεύθυνση Αττικής στο τηλ. 210-6476000, καθώς και στο Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος Θεσσαλονίκης, στο τηλ. 231-0388370-5.

5

Πώς να «εμπιστευθείτε» τα στοιχεία της πιστωτικής σας κάρτας στο

Διαδίκτυο

Πολλές φορές διστάζουμε να δώσουμε τον αριθμό της πιστωτικής μας κάρτας. Ο δισταγμός αυτός είναι κυρίως ψυχολογικός, αφού υπάρχουν θέματα που πρέπει να προσέξει κανείς, όμως η φιλολογία που έχει αναπτυχθεί περί τεραστίου προβλήματος ασφάλειας δεν ανταποκρίνεται στην πραγματικότητα. Όπως προκύπτει από τη διεθνή εμπειρία, μικρό ποσοστό των κρουσμάτων απάτης που αφορούν σε κάρτες, έχουν σχέση με τις διαδικτυακές συναλλαγές. Με τη σύγχρονη κρυπτογράφηση των δεδομένων μειώνονται σημαντικά οι περιπτώσεις ηλεκτρονικής απάτης. Ακόμη και στην περίπτωση που παρατηρήσετε περιέργες χρεώσεις έχετε δικαίωμα (μέσα σ' ένα εύλογο χρονικό διάστημα) να ακυρώσετε τη συναλλαγή και να ζητήσετε να σας επιστραφούν τα χρήματα. Αν παρ' όλα αυτά συνεχίζετε να είστε επιφυλακτικοί, χρησιμοποιείστε εναλλακτικούς τρόπους, όπως είναι η αντικαταβολή, ή μετάδοση του αριθμού της κάρτας σας με fax, ή οι προπληρωμένες κάρτες.

6

Χρησιμοποιήστε ασφαλή μέσα για τις συναλλαγές σας

Για τις συναλλαγές σας αξιοποιείτε ώριμες και δοκιμασμένες τεχνολογίες ασφάλειας. Ειδικότερα μη μεταδώσετε ποτέ ευαίσθητες πληροφορίες όπως π.χ. αριθμούς πιστωτικών καρτών στο Διαδίκτυο, εάν αυτές δεν είναι κρυπτογραφημένες με κάποιο γνωστό και αξιόπιστο αλγόριθμο. Ελέγξτε ότι το πρόγραμμα πλοήγησης που χρησιμοποιείτε έχει την ένδειξη https αντί για http στο πεδίο διεύθυνσης όταν πραγματοποιείτε συναλλαγές.

7

Προστατέψτε τα προσωπικά σας δεδομένα

Είναι γνωστό ότι ποτέ καμία σοβαρή επιχείρηση δεν πρόκειται να σας ενοχλήσει για να σας ζητήσει προσωπικά δεδομένα, όπως ημερομηνίες γέννησης, αριθμούς πιστωτικών καρτών κ.λπ. μέσω τηλεφώνου ή e-mail. Ειδικότερα στο θέμα τηλεφώνου μπορεί να σας ζητήσουν να επιβεβαιώσετε τη ταυτότητά σας μόνο αν τους έχετε καλέσει εσείς και σε καμία περίπτωση το αντίστροφο. Το phishing είναι μια τεχνική που χρησιμοποιούν απατεώνες για να σας υφαρπάξουν τα προσωπικά σας στοιχεία. Η απάτη αυτή λειτουργεί ως εξής: η τράπεζά σας υποτίθεται ότι αποστέλλει e-mail στα οποία σας ζητά να επιβεβαιώσετε τα στοιχεία σας σε κάποιο ιστότοπο. Ο δικτυακός τόπος στον οποίο παραπέμπεστε αποτελεί ακριβές αντίγραφο του κανονικού δικτυακού τόπου της επιχείρησης με την οποία συνεργάζεστε, ωστόσο διαχειρίζεται από επιτήδειους με σκοπό να σας πείσουν να τους δώσετε τα προσωπικά σας στοιχεία, για να πραγματοποιήσουν συναλλαγές από το λογαριασμό σας εν αγνοία σας. Σε περίπτωση που λάβατε κάποιο τέτοιο mail επικοινωνήστε με την επιχείρηση που συνεργάζεστε και αναφέρετέ τους το περιστατικό. Αναζητήστε την επιχείρησή σας στο Google και σε καμία περίπτωση μην ακολουθήσετε τους συνδέσμους που σας προτείνουν. Επίσης τα περισσότερα προγράμματα πλοήγησης διαθέτουν μηχανισμούς anti-phishing τους οποίους καλό είναι να ενεργοποιήσετε.

8

Ακολουθήστε τους κανόνες Συναλλαγών

Σε δικτυακούς τόπους όπου πραγματοποιούνται δημοπρασίες ή αγοραπωλησίες αγαθών μεταξύ των χρηστών είναι απαραίτητο να ακολουθείτε τους κανόνες που διέπουν τη λειτουργία των συγκεκριμένων δικτυακών τόπων. Μην επιχειρήσετε κατευθείαν συναλλαγές με χρήστες εάν αυτό δε προβλέπεται από τους κανόνες λειτουργίας της συγκεκριμένης υπηρεσίας. Επίσης, σε πολλές περιπτώσεις, μπορείτε να αναζητήσετε το ιστορικό των ανθρώπων με τους οποίους σκέφτεστε να προχωρήσετε σε συναλλαγή, για να δείτε αν υπήρξαν συνεπείς σε παλιότερες συναλλαγές τους, καθώς και πόσο ευχαριστημένοι είναι άλλοι χρήστες από τους οποίους αγόρασαν ή πούλησαν αγαθά.

9

Σιγουρευτείτε για την ασφάλεια πρόσβασης από υπολογιστές σε κοινή

χρήση

Αν αποκτάτε πρόσβαση στο Διαδίκτυο από υπολογιστές σε τοπικά δίκτυα ή σε Internet Cafe, ή αν χρησιμοποιείτε το φορητό υπολογιστή της εταιρείας όπου εργάζεστε να έχετε πάντοτε κατά νου ότι δεν είστε ο μοναδικός άνθρωπος που έχει πρόσβαση στη συσκευή αυτή, και επομένως, δεν μπορείτε ποτέ να γνωρίζετε ακριβώς τι είδους πρόγραμμα εκτελείται στον υπολογιστή – έστω και αν δε φαίνεται.

Σε ένα τέτοιο περιβάλλον, είναι καλό να καθαρίζετε πάντοτε την προσωρινή μνήμη (cache) και το ιστορικό των ενεργειών (history) των προγραμμάτων πλοήγησης, ενέργεια που σβήνει τα ίχνη και τα προσωπικά σας στοιχεία και που μπορεί να εκτελεστεί πολύ εύκολα συνήθως από την κατηγορία «Εργαλεία» (Tools) και μετά «Επιλογές» Internet Options, αν χρησιμοποιείτε internet Explorer.

10

Εγκαταστήστε προγράμματα ανίχνευσης ιών και πρόσθετο

Λογισμικό ασφαλείας

Προβλήματα ασφαλείας που δεν μπορούν να λυθούν μόνο με τα τυπικά εργαλεία του λειτουργικού συστήματος, είναι δυνατόν να αντιμετωπιστούν με την εγκατάσταση πρόσθετου λογισμικού ασφαλείας. Τέτοια εργαλεία είναι προγράμματα ανίχνευσης ιών (antivirus, antispyware) που ενημερώνονται συνεχώς και είναι σε θέση να αντιμετωπίσουν νέες απειλές.

Επίσης, υπάρχουν προγράμματα – «τείχη ασφαλείας» (firewall) που ελέγχουν κάθε εισερχόμενη και εξερχόμενη πληροφορία από τον υπολογιστή σας και μπορούν να προλάβουν τη διάδοση ιών και ανεπιθύμητων εφαρμογών των οποίων η εγκατάσταση δεν έχει γίνει συνειδητά. Μπορείτε να βρείτε τέτοια προγράμματα ασφαλείας σε καταστήματα πώλησης λογισμικού ή μπορείτε να κατεβάσετε κάποια από αυτά από το Διαδίκτυο.

ΑΣΦΑΛΩΣ...10 + 1

Τα οφέλη παραγωγικότητας από την εφαρμογή των διαδικτυακών τεχνολογιών στην επιχείρηση - λόγω αυξημένης αποδοτικότητας, μείωσης του κόστους συναλλαγών και διευκόλυνσης της πρόσβασης στην παγκόσμια αγορά - δεν είναι αποκλειστικό προνόμιο των πολυεθνικών οργανισμών και των επιχειρήσεων της βαριάς βιομηχανίας. Είναι νέα απαίτηση και μπορούν να αξιοποιηθούν κατάλληλα και από τις μικρές επιχειρήσεις ενσωματώνοντας συστήματα που εξασφαλίζουν την ασφάλεια της επιχείρησής σας, παρέχοντας νέες δυνατότητες ανταγωνισμού που προσφέρουν τα νέα μέσα. Τα οφέλη είναι αμφίδρομα και για εσάς τους καταναλωτές, όπως μείωση χρόνου και κόστους, μεγάλη επιλογή προϊόντων χωρίς καμία μετακίνηση κ.α. Τα δυο συναλλασσόμενα μέρη όμως πρέπει να τηρείτε τους κανόνες ασφάλειας και να ενημερώνεστε, ώστε να απολαμβάνετε τις δυνατότητες της νέας «αγοράς»

ΑΣΦΑΛΩΣ...