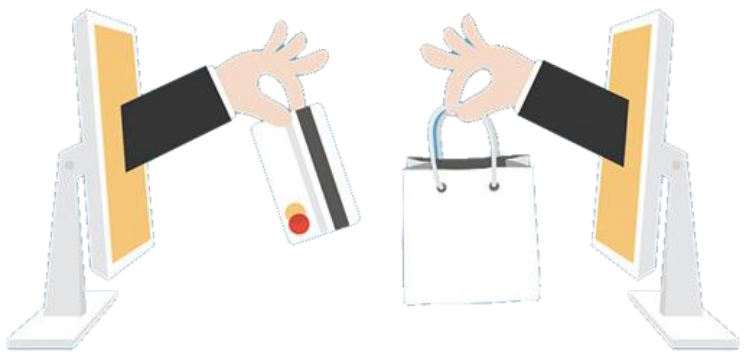
ΑΣΦΑΛΕΙΣ ONLINE ΑΓΟΡΕΣ

Κοιτάξτε το site με κριτικό μάτι. Εάν οποιαδήποτε από τις ακόλουθες ερωτήσεις, σας χτυπήσουν τον κώδωνα του κινδύνου, θα ήταν σοφό να στραφείτε σε ένα άλλο site για τις αγορές σας:

- Μήπως οι τιμές της εταιρείας, σας φαίνονται ασυνήθιστα χαμηλές;
- Μήπως μοιάζει ο εν λόγω διαδικτυακός έμπορος να είναι ερασιτέχνης;
- Υπάρχουν πολλά ορθογραφικά ή συντακτικά λάθη στο site;
- Μήπως οι κλήσεις στο τηλέφωνο της εταιρείας μένουν αναπάντητες;

Προτιμήστε ιστοσελίδες που γνωρίζετε, με συνέπεια στις υπηρεσίες τους και όσο το δυνατόν περισσότερα reviews από πελάτες.



Αναζητήστε πρωτόκολλο SSL στην ιστοσελίδα του e-shop που επιλέξατε. Όταν το πρωτόκολλο SSL είναι ενεργό, θα δείτε τα γράμματα «https» μπροστά από τη διαδικτυακή διεύθυνση. Το «s» σημαίνει ασφάλεια “secure”. Αναζητήστε το σύμβολο του κλειδωμένου λουκέτου. Το εικονίδιο θα πρέπει να είναι στο πλαίσιο του παραθύρου του προγράμματος περιήγησης. Είναι πράσινο στις νέες εκδόσεις των browsers.

Να ελέγχετε πάντα τις βασικές πληροφορίες που παρέχονται για το ηλεκτρονικό κατάστημα στην ιστοσελίδα του (π.χ. έδρα καταστήματος, ύπαρξη φυσικού καταστήματος, στοιχεία επικοινωνίας, πολιτική επιστροφών, όροι αγορών, πολιτική απορρήτου κ.α.)

Προτιμήστε τρόπους πληρωμής που σας παρέχουν μεγαλύτερη ασφάλεια και ευελιξία όπως αντικαταβολή, χρεωστική ή πιστωτική κάρτα και PayPal. Αποφύγετε την τραπεζική κατάθεση. Ο ασφαλέστερος τρόπος για να ψωνίσετε στο διαδίκτυο είναι με πιστωτική κάρτα. Σε περίπτωση που κάτι πάει στραβά, προστατεύεστε σύμφωνα με τον ομοσπονδιακό νόμο περί θεμιτής χρέωσης. Έχετε το δικαίωμα να αμφισβητήσετε χρεώσεις στην πιστωτική σας κάρτα, και μπορείτε να πάρετε πίσω τις χρεώσεις που σας υποβλήθηκαν ύστερα από έρευνα που αποδεικνύει την λανθασμένη χρέωση που σας έκανε ο πιστωτής.

Φροντίστε να διατηρείτε σε υψηλό επίπεδο την ασφάλεια του υπολογιστή σας.

- Να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις των προγραμμάτων που χρησιμοποιείτε και κυρίως τις «επιδιορθώσεις ασφαλείας». Πρόκειται για προγράμματα που εκδίδουν οι εταιρείες από τις οποίες έχετε αγοράσει το λογισμικό που χρησιμοποιείτε και καλύπτουν τυχόν κενά ασφαλείας που διαπιστώθηκαν μετά την έκδοσή του.
- Εγκαταστήστε ένα πρόγραμμα προστασίας από ιούς (antivirus) και ένα δίχτυ προστασίας (firewall), και φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις τους. Το δίχτυ προστασίας σας προφυλάσσει σε μεγάλο βαθμό από τις πιθανές «εισβολές» που θα δεχτείτε κατά τις περιηγήσεις σας στο διαδίκτυο.
- Προστατέψτε τον υπολογιστή σας με κωδικό πρόσβασης προκειμένου να αποτρέψετε την πρόσβαση σε αυτόν μη εξουσιοδοτημένων χρηστών.

Ως προς τους κωδικούς πρόσβασης που χρησιμοποιείτε στις διαδικτυακές σας συναλλαγές:

- Αλλάζετε συχνά τους κωδικούς
- Αποφεύγετε να χρησιμοποιείτε ως κωδικό πρόσβασης την ημερομηνία γέννησης, τον αριθμό τηλεφώνου ή άλλα προσωπικά σας στοιχεία.
- Αποφεύγετε να έχετε τον προσωπικό σας κωδικό πρόσβασης μέσα σε πορτοφόλια, τσάντες ή ατζέντες.
- Αποφεύγετε να χρησιμοποιείτε τους ίδιους κωδικούς πρόσβασης σε περισσότερες από μια ιστοσελίδα, κάρτα κλπ.
- Μη δίνετε τον κωδικό πρόσβασης σας σε οποιονδήποτε και κάτω από οποιεσδήποτε περιστάσεις. Εάν κάποιος, για παράδειγμα επικαλεστεί ότι τηλεφωνεί από την τράπεζα και ζητήσει τον αριθμό πρόσβασης για επαλήθευση, μην τον δώσετε. Οι Τράπεζες δεν ακολουθούν αυτή την πρακτική. Εάν έχετε αναγνώριση κλήσης, καταγράψτε τον αριθμό που αναγράφηκε στην τηλεφωνική σας συσκευή και ενημερώστε αμέσως την Αστυνομία.

SaferInternet4Kids.gr
ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ