

Ασφαλείς online αγορές



Γιατί να επιλέξω το διαδίκτυο

- Ποικιλία και δυνατότητα σύγκρισης προϊόντων
- Παγκοσμιοποιημένη αγορά
- Καλύτερες τιμές
- Διαθεσιμότητα όλο το 24ωρο
- Δεν απαιτεί μετακίνηση σε φυσικό κατάστημα
- Εξοικονόμηση χρόνου και χρημάτων
- Ποικιλία μεθόδων πληρωμής



Κίνδυνοι κατά τη διαδικασία online αγορών

- Υποκλοπή δεδομένων
- Παραποίηση δεδομένων
- Απατηλές συναλλαγές
- Άρνηση εξυπηρέτησης
- Μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και δίκτυα υπολογιστών (hacking-cracking)
- Κακόβουλα προγράμματα
- Ψάρεμα (phishing)





Σιγουρευτείτε ότι το site που επιλέξατε είναι αξιόπιστο

- 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** ως απόδειξη της αξιοπιστίας του e-shop. Το εικονίδιο θα πρέπει να είναι στο πλαίσιο του παραθύρου του προγράμματος περιήγησης. Είναι πράσινο στις νέες εκδόσεις των browsers.

 Στην ηλεκτρονική διεύθυνση της [Γενικής Γραμματείας Καταναλωτή](#) μπορείτε να βρείτε όλα τα ηλεκτρονικά καταστήματα που είναι εγγεγραμμένα στο Γενικό Εμπορικό Μητρώο.



Σιγουρευτείτε ότι το site που επιλέξατε είναι αξιόπιστο

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

 Στην ηλεκτρονική διεύθυνση της **Γενικής Γραμματείας Καταναλωτή** μπορείτε να βρείτε όλα τα ηλεκτρονικά καταστήματα που είναι εγγεγραμμένα στο Γενικό Εμπορικό Μητρώο.



ΠΙΣΤΕΥΤΕΙΤΕ ΤΟ ΕΝΣΤΙΚΤΟ ΣΑΣ

Κοιτάξετε 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 σας στο τηλέφωνο της εταιρείας μένουν αναπάντητες;

Πληρωμή με κάρτα. Τι πρέπει να προσέχετε



- Χρησιμοποιήστε **προπληρωμένη κάρτα**. Το μέγιστο ποσό που μπορείτε να ζημιωθείτε είναι αυτό της κάρτας.
- Χρησιμοποιήστε **πιστωτική** και όχι χρεωστική κάρτα. Έχετε καλύτερες πιθανότητες αποζημίωσης σε περίπτωση μη παραλαβής του προϊόντος.
- **Ελέγχετε το λογαριασμό** της πιστωτικής σας ανά διαστήματα για να διαπιστώσετε αν υπάρχουν «λάθος» χρεώσεις.
- **Ελέγχετε** οπωσδήποτε πριν από την πληρωμή **ότι ο ιστότοπος είναι ασφαλής**.

Πληρωμή με κάρτα. Τι πρέπει να προσέχετε

- Ποτέ **μην αποθηκεύετε τα στοιχεία** της κάρτας σας στο site που χρησιμοποιείτε.
- Ποτέ **μη δίνετε τα στοιχεία της πιστωτικής σας μέσω email ή μέσω τηλεφώνου.**
- Ποτέ **μη πληρώνετε με μεταφορά χρημάτων** σε λογαριασμό.





Πληρωμή με Paypal

- Η Paypal είναι ένας **«αξιόπιστος διαμεσολαβητής»** για online συναλλαγές. Τα χρήματα στέλνονται χρησιμοποιώντας μόνο το **paypal email** ενός χρήστη, χωρίς να γίνονται γνωστές απόρρητες πληροφορίες όπως αριθμοί πιστωτικών καρτών ή άλλες προσωπικές πληροφορίες.

Με απλά λόγια, διαχειρίζεται τις πληρωμές που κάνετε στο Internet, πληρώνοντας τα ηλεκτρονικά καταστήματα για λογαριασμό σας.

Πλεονεκτήματα Paypal

- Τα διάφορα ηλεκτρονικά καταστήματα δεν μαθαίνουν ποτέ τα στοιχεία της πιστωτικής σας κάρτας, άρα δεν χρειάζεται να ανησυχείτε τόσο πολύ για την αξιοπιστία τους.
- Το ότι το paypal έχει δεχθεί να συνεργαστεί με το συγκεκριμένο e-shop είναι μία ακόμα ένδειξη αξιοπιστίας.
- Το Paypal μπορεί να παρέμβει σε περιπτώσεις που το ηλεκτρονικό κατάστημα κάνει κάτι που δεν θα έπρεπε.



Κίνδυνοι κατά τη διαδικασία online αγορών



Η διακίνηση προϊόντων και οι μεταφορές χρηματικών ποσών στο διαδίκτυο προσελκύουν σχεδόν πάντα το ενδιαφέρον **hackers** και «**διαδικτυακών απατεώνων**», οι οποίοι προσπαθούν να αποκομίσουν παράνομα οφέλη με πολλούς και συχνά **ευρηματικούς τρόπους**.

Προσοχή στα Μηνύματα "Phishing"

Χάκερ στέλνουν μαζικά μηνύματα ηλεκτρονικού ταχυδρομείου σε χρήστες του Διαδικτύου και τους ζητούν να ενημερώσουν τις πληροφορίες του τραπεζικού λογαριασμού τους, πιστωτικές κάρτες, ή άλλες δημοφιλείς περιοχές αγορών.

Το **e-mail** μπορεί να αναφέρει ότι τα στοιχεία του λογαριασμού σας έχουν λήξει, έχουν παραβιαστεί ή χαθεί και ότι θα πρέπει να τα στείλετε ξανά αμέσως στην εταιρεία.

Μην απαντάτε σε κάθε αίτημα για οικονομική πληροφόρηση που λαμβάνετε με μήνυμα ηλεκτρονικού ταχυδρομείου.



Phishing filters

- Οι καινούριες εκδόσεις των προγραμμάτων περιήγησης έχουν **ενσωματωμένα phishing filters** τα οποία λειτουργούν προστατευτικά προειδοποιώντας τον χρήστη ότι υπάρχει κίνδυνος.
- Σε περίπτωση που δεν είναι ενσωματωμένα **υπάρχει δυνατότητα δωρεάν εγκατάστασης.**



Προσοχή στα προσωπικά σας δεδομένα

- **Μη δίνετε περισσότερες πληροφορίες απ' ό,τι χρειάζεται.** Εάν π.χ. μια ιστοσελίδα που πουλάει ρούχα σας ζητήσει τον αριθμό κοινωνικής ασφάλισης, κλείστε τη συναλλαγή, σαρώστε τη συσκευή σας και αποφύγετε τις συναλλαγές σε αυτή τη σελίδα στο μέλλον.
- Αναζητήστε στην ιστοσελίδα πληροφορίες που δηλώνουν ότι **τα προσωπικά σας στοιχεία θα επεξεργαστούν μόνο για την ολοκλήρωση της αγοράς σας.** Επίσης, πρέπει να υπάρχει αναφορά στην πολιτική του καταστήματος για τα προσωπικά δεδομένα, και συγκεκριμένα, ποιες πληροφορίες αποθηκεύονται κατά την ηλεκτρονική συναλλαγή και πώς χρησιμοποιούνται.



Μην εμπιστεύεσαι



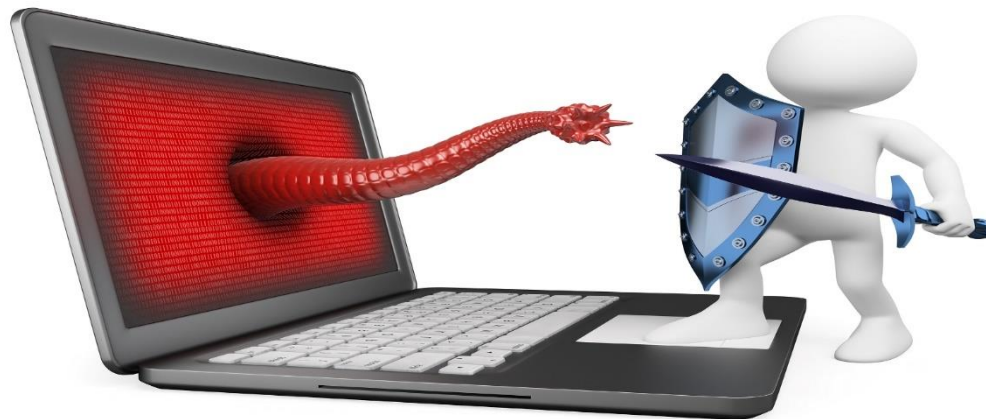
- Μην είστε εύπιστοι σε **έρευνες που σας υπόσχονται χρήματα**. Συνήθως είναι απάτες και εμφανίζονται αρκετά συχνά σε μέσα κοινωνικής δικτύωσης ως προσφορές με τη μορφή pop-ups.

Εάν έχετε αμφιβολίες κλείστε αμέσως το παράθυρο και σαρώστε τη συσκευή σας για κακόβουλο λογισμικό.

Προστασία από κακόβουλα λογισμικά

➤ Ελέγξτε τη συσκευή σας

Βεβαιωθείτε ότι ο browser σας είναι ενημερωμένος, κάντε τα απαραίτητα updates στο λειτουργικό σας σύστημα και βεβαιωθείτε ότι έχετε επαρκή προστασία από κακόβουλο λογισμικό.



Online αγορές από ασφαλή σημεία πρόσβασης στο διαδίκτυο

Προτιμήστε να κάνετε τις αγορές σας από **ασφαλή δίκτυα, π.χ. οικιακά και όχι δημόσια**. Σε κάθε περίπτωση πρέπει να αλλάζετε ανά τακτά χρονικά διαστήματα τους κωδικούς πρόσβασης στο router σας.



Χρησιμοποιήστε ασφαλή password

- Να αποφεύγετε να χρησιμοποιείτε τους **ίδιους κωδικούς** σε πολλές διαφορετικές ιστοσελίδες. Ακόμα περισσότερο πρέπει να αποφεύγετε να χρησιμοποιείτε τον ίδιο κωδικό με το mail ή τον τραπεζικό λογαριασμό σας.
- Χρησιμοποιήστε **ισχυρούς κωδικούς** πρόσβασης που να περιέχουν αριθμούς, γράμματα και σύμβολα
- **Μην αποθηκεύεται τους κωδικούς** σας στον browser που χρησιμοποιείτε



«Ναι» στις ευκαιρίες αλλά με προσοχή!

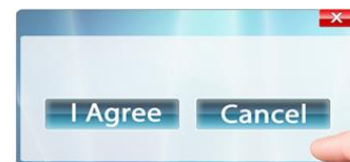


Αν κάτι σας φαίνεται πολύ καλό για να είναι αληθινό, τότε πολύ πιθανό να μην είναι. Δώστε βάση στις λεπτομέρειες, όπως π.χ. στην ορθογραφία ή τη σύνταξη των διαφημίσεων για τις προσφορές. Πολύ συχνά οι απάτες γίνονται με ανακριβείς μεταφράσεις, οπότε προσφορές με λάθη που «βγάζουν μάτι» είναι αρκετά πιθανό να κρύβουν απάτη.



Να διαβάσετε πάντα τους Όρους και τις Προϋποθέσεις

Πριν προβείτε στην παραγγελία σας, είναι απαραίτητο να υπολογίσετε το συνολικό κόστος και να ενημερωθείτε για τους τρόπους πληρωμής, την πολιτική επιστροφών, την πολιτική ακύρωσης ή τι γίνεται σε περίπτωση που η παραγγελία σας χαθεί. Όλες αυτές οι πληροφορίες, θα πρέπει να **αναγράφονται ξεκάθαρα** στην ιστοσελίδα του e-shop.



Για περισσότερες πληροφορίες επισκεφθείτε την πλατφόρμα [“Feelsafe”](#) που δημιουργήθηκε από τη **Δίωξη Ηλεκτρονικού Εγκλήματος** σε συνεργασία με την **Εθνική Συνομοσπονδία Ελληνικού Εμπορίου**.



ΕΛΛΗΝΙΚΟ ΚΕΝΤΡΟ ΑΣΦΑΛΟΥΣ ΔΙΑΔΙΚΤΥΟΥ-ΕΝΗΜΕΡΩΣΗ



SaferInternet4Kids.gr

ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ

 www.saferinternet4kids.gr



Γραμμή βοήθειας



 www.safeline.gr

Γραμμή παράνομου περιεχομένου



 www.inhope.org
www.betterinternetforkids.eu



www.forth.gr



Συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση
Διευκόλυνση «Συνδέοντας την Ευρώπη»