

ΑΣΦΑΛΕΙΣ ONLINE ΑΓΟΡΕΣ



ΓΙΑΤΙ ΝΑ ΕΠΙΛΕΞΩ ΤΟ ΔΙΑΔΙΚΤΥΟ



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

ΚΙΝΔΥΝΟΙ ΚΑΤΑ ΤΗ ΔΙΑΔΙΚΑΣΙΑ ONLINE ΑΓΟΡΩΝ

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

ΕΜΠΙΣΤΕΥΤΕΙΤΕ ΤΟ ΕΝΣΤΙΚΤΟ ΣΑΣ

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;

ΤΙ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΕΧΟΥΜΕ



- ➡ 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.)

ΤΙ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΕΧΟΥΜΕ



- ➡ 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.

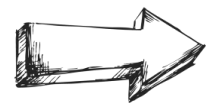
Στην ηλεκτρονική διεύθυνση της Γενικής Γραμματείας
Καταναλωτή μπορείτε να βρείτε όλα τα ηλεκτρονικά
καταστήματα που είναι εγγεγραμμένα στο Γενικό
Εμπορικό Μητρώο.

ΠΛΗΡΩΜΗ ΜΕ ΚΑΡΤΑ: ΤΙ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΕΧΟΥΜΕ



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.

ΠΛΗΡΩΜΗ ΜΕ ΚΑΡΤΑ: ΤΙ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΕΧΟΥΜΕ



Ελέγχετε το λογαριασμό της πιστωτικής σας ανά διαστήματα για να διαπιστώσετε αν υπάρχουν «λάθος» χρεώσεις.



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.

**ΠΛΗΡΩΜΗ ΜΕ
ΔΙΑΜΕΣΟΛΑΒΗΤΕΣ:
ΤΙ ΠΡΕΠΕΙ ΝΑ
ΓΝΩΡΙΖΟΥΜΕ**



Υπάρχουν τραπεζικές υπηρεσίες που λειτουργούν ως «αξιόπιστοι διαμεσολαβητές» για online συναλλαγές. Μια από αυτές είναι και η γνωστή PayPal. Τα χρήματα στέλνονται χρησιμοποιώντας μόνο το email ενός χρήστη, χωρίς να γίνονται γνωστές απόρρητες πληροφορίες όπως αριθμοί πιστωτικών καρτών ή άλλες προσωπικές πληροφορίες.

ΠΛΗΡΩΜΗ ΜΕ PAYPAL: ΤΙ ΠΡΕΠΕΙ ΝΑ ΓΝΩΡΙΖΟΥΜΕ



Τα διάφορα ηλεκτρονικά καταστήματα δεν μαθαίνουν ποτέ τα στοιχεία της πιστωτικής σας κάρτας, άρα δεν χρειάζεται να ανησυχείτε τόσο πολύ για την αξιοπιστία τους.



Όταν ένας αξιόπιστος τραπεζικός διαμεσολαβητής, όπως η PayPal, δεχθεί να συνεργαστεί με συγκεκριμένο e-shop είναι μία ακόμα ένδειξη αξιοπιστίας για το e-shop.



Το PayPal μπορεί να παρέμβει σε περιπτώσεις που ένα ηλεκτρονικό κατάστημα λειτουργήσει παράνομα, και να σας επιστρέψει τα χρήματα.

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.

ΠΡΟΣΟΧΗ ΣΤΑ ΜΗΝΥΜΑΤΑ "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!

ΠΡΟΣΟΧΗ ΣΤΑ ΠΡΟΣΩΠΙΚΑ ΣΑΣ ΔΕΔΟΜΕΝΑ



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 και αποφύγετε τις συναλλαγές σε αυτή τη σελίδα στο μέλλον.



Αναζητήστε 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.

ΕΛΕΓΞΤΕ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΟΥ ΥΠΟΛΟΓΙΣΤΗ ΣΑΣ

- ➡ Φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις των προγραμμάτων που χρησιμοποιείτε και κυρίως τις «επιδιορθώσεις ασφαλείας».
- ➡ Εγκαταστήστε ένα πρόγραμμα προστασίας από ιούς (antivirus) και ένα δίκτυο προστασίας (firewall), και φροντίστε να λαμβάνετε τακτικά τις ενημερωμένες εκδόσεις τους.
- ➡ Προστατέψτε τον υπολογιστή σας με κωδικό πρόσβασης προκειμένου να αποτρέψετε την πρόσβαση σε αυτόν μη εξουσιοδοτημένων χρηστών.

Αποφεύγετε να πραγματοποιείτε οικονομικές συναλλαγές μέσω διαδικτύου από Internet café, δημόσιες βιβλιοθήκες και άλλους χώρους στους οποίους πολλοί χρήστες έχουν πρόσβαση στους ίδιους υπολογιστές . Προτιμήστε τον προσωπικό σας υπολογιστή ή κάποιον για τον οποίο είστε βέβαιοι για το επίπεδο ασφάλειας.

ΑΣΦΑΛΗ 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.

**ΝΑ
ΔΙΑΒΑΖΕΤΕ
ΠΑΝΤΑ ΤΟΥΣ
ΟΡΟΥΣ
ΚΑΙ ΤΙΣ
ΠΡΟΫΠΟΘΕ-
ΣΕΙΣ**



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.

«ΝΑΙ» ΣΤΙΣ ΕΥΚΑΙΡΙΕΣ ΑΛΛΑ ΜΕ ΠΡΟΣΟΧΗ!



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.

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

www

ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ



www.saferinternet4kids.gr



www.help-line.gr

Γραμμή βοήθειας



www.safeline.gr

Γραμμή παράνομου περιεχομένου



www.inhope.org
www.betterinternetforkids.eu



ITE

ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ



www.forth.gr



Συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση
Διευκόλυνση «Συνδέοντας την Ευρώπη»