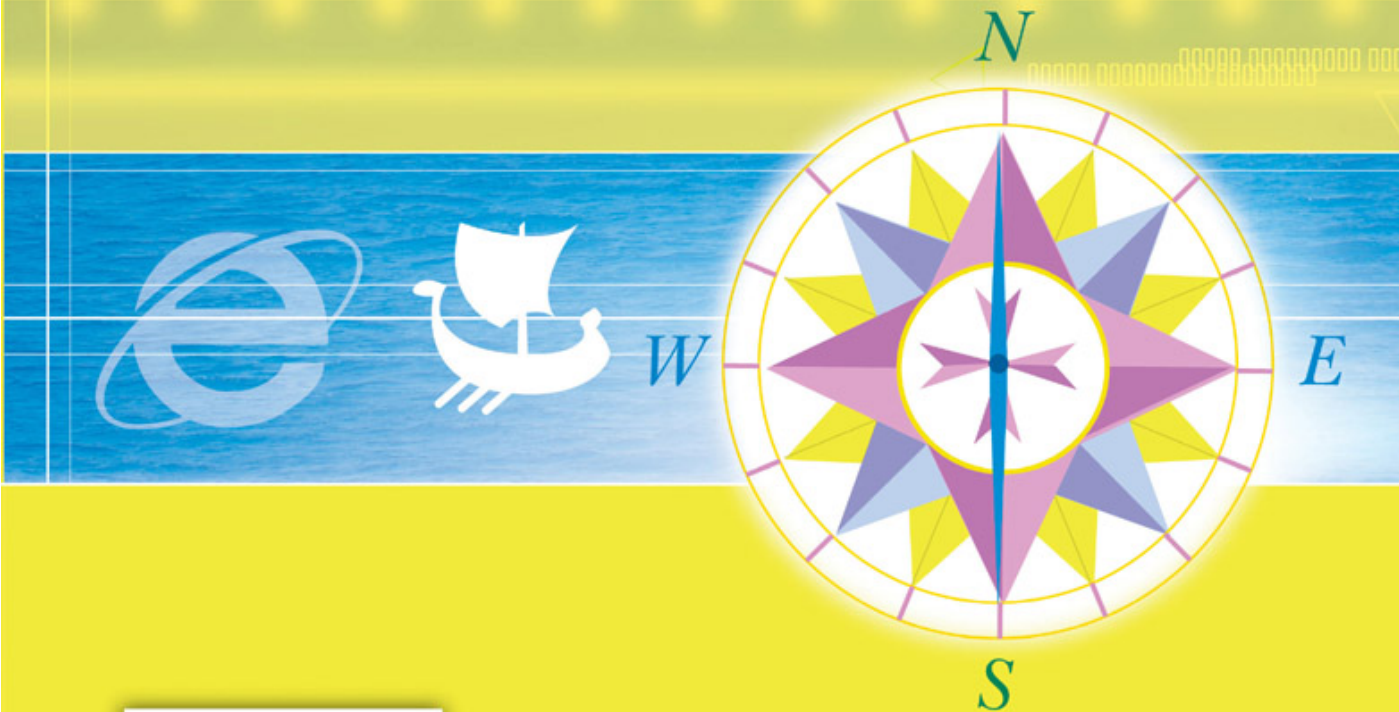


ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ  
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΚΑΤΑΝΑΛΩΤΗ

# ΟΛΑ ΟΣΑ ΠΡΕΠΕΙ ΝΑ ΓΝΩΡΙΖΟΥΜΕ ΓΙΑ ΑΣΦΑΛΗ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ



ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ  
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΚΑΤΑΝΑΛΩΤΗ  
βοιόζεται για σένα





# εν πλώ



# download

Η πλοήγηση στο διαδίκτυο (internet) αποτελεί πια μέρος της καθημερινής ζωής των περισσότερων από εμάς.

Από το διαδίκτυο αντλούμε πληροφορίες για θέματα που μας ενδιαφέρουν και μαθαίνουμε τι συμβαίνει στον κόσμο, επικοινωνούμε με φίλους και συνεργάτες μέσω του ηλεκτρονικού ταχυδρομίου (e-mail) και αγοράζουμε προϊόντα και υπηρεσίες.

Ίσως και εσύ να έχεις ήδη πραγματοποιήσει αγορές μέσω διαδικτύου και να γνωρίζεις τις ευκολίες και τα οφέλη που προσφέρει:

- **δεν χάνεις χρόνο**
- **το κόστος των συναλλαγών είναι χαμηλό**
- **μπορείς να διαλέξεις προϊόντα και υπηρεσίες όχι μόνο από την Ελλάδα αλλά από κάθε γωνιά της γης**
- **Η ποικιλία των αγαθών και υπηρεσιών είναι τεράστια**

**Όπως, όμως, στη θαλάσσια πλοήγηση έτσι και στο διαδικτυακό "σερφάρισμα" πρέπει να γνωρίζουμε τους βασικούς κανόνες ασφαλείας για να μη βρεθούμε.... "πελαγωμένοι"!**



Ιστοσελίδες (sites) που κατά κύριο λόγο επισκεπτόμαστε προκειμένου να πραγματοποιήσουμε κάποια συναλλαγή είναι:

- Ηλεκτρονικά εμπορικά καταστήματα παντός είδους (από εισιτήρια, βιβλία και CD μέχρι προγράμματα Η/Υ, έπιπλα και ρούχα)
- Περιοδικά για συνδρομές
- Δημοπρασίες προϊόντων
- Παροχή ταξιδιωτικών υπηρεσιών

## Η ΓΝΩΣΗ ΠΡΟΦΥΛΑΣΣΕΙ

Σε γενικές γραμμές, η αγορά από το internet (διαδίκτυο) είναι ασφαλής, ιδιαίτερα όταν γίνεται από αναγνωρισμένα και μεγάλα ηλεκτρονικά καταστήματα.

Υπάρχουν όμως και κάποιες περιπτώσεις που κρύβουν κινδύνους για τους καταναλωτές.

Οι κίνδυνοι αυτοί σχετίζονται κυρίως με την αθέτηση των όρων της εμπορικής συμφωνίας (μη παράδοση των προϊόντων ή των υπηρεσιών, παράδοση ελαττωματικών αγαθών, χρέωση κρυφών εξόδων).

Στις σελίδες που ακολουθούν θα βρείς χρήσιμες πληροφορίες για την αποφυγή της ηλεκτρονικής εξαπάτησης.



<https://www.>

# ΣΑΣ



## Πώς μπορείς να αποφύγεις την παραπλάνηση;

Σε γενικές γραμμές, χρειάζεται να είσαι καχύποπτος και να προσέχεις ιδιαίτερα, διαβάζοντας τους όρους της εμπορικής συναλλαγής και ελέγχοντας τη φερεγγυότητα του ηλεκτρονικού καταστήματος με το οποίο συναλλάσσεσαι.

Υπάρχουν πολλοί τρόποι για να προστατευτεί κανείς από την εξαπάτηση κατά τη διάρκεια εμπορικών συναλλαγών στο διαδίκτυο και οποιοσδήποτε συνδυασμός τους θα σε προστατεύσει επαρκώς.

# SALE

# buy



## Ειδικότερα:

- Να διαβάζεις με προσοχή τους όρους της σύμβασης συναλλαγής
- Να διαβάζεις με προσοχή τους όρους χρήσης της ιστοσελίδας που χρησιμοποιείς
- Να βεβαιώνεσαι για τη φερεγγυότητα του ηλεκτρονικού καταστήματος με το οποίο συναλλάσσεσαι
- Να ελέγχεις τις πληροφορίες για το προϊόν, την τιμή του και το νόμισμα που θα γίνει η συναλλαγή, καθώς και για το τελικό κόστος (με τα έξοδα αποστολής)
- Να μελετάς την πολιτική επιστροφών της εταιρίας
- Να διαβάζεις προσεκτικά τους όρους ασφαλείας πληρωμών της ιστοσελίδας
- Να εξακριβώνεις το χρόνο παράδοσης του προϊόντος



## Άλλοι τρόποι προστασίας:

- Να εξοπλιστείς με ειδικό λογισμικό ασφαλείας, που ανιχνεύει κακόβουλο λογισμικό στον υπολογιστή σου
- Όταν πληρώνεις, να είσαι σίγουρος για την ασφαλή και κρυπτογραφημένη σύνδεση του υπολογιστή - εμφανίζεται είτε με την αλλαγή χρώματος της περιοχής που γράφεις την ηλεκτρονική διεύθυνση, είτε με ένα σύμβολο κάτω δεξιά στο πρόγραμμα πλοήγησης, είτε με την αλλαγή της διεύθυνσης από `http://` σε `https://`
- Να μην αποθηκεύεις προσωπικούς κωδικούς πρόσβασης στον υπολογιστή
- Να μη δίνεις τους προσωπικούς κωδικούς σου σε τρίτα άτομα
- Ο κωδικός σου πρέπει, για μεγαλύτερη ασφάλεια, να περιέχει γράμματα, αριθμούς και σύμβολα
- Να μη δίνεις προσωπικές πληροφορίες μέσα από το ηλεκτρονικό ταχυδρομείο γιατί δεν είναι κρυπτογραφημένη και ασφαλής υπηρεσία
- Να προσέχεις τη διεύθυνση που γράφεις, αν είναι η πραγματική
- Προτίμησε για αγορές προπληρωμένες δικτυακές υπηρεσίες, καθώς παρέχονται από εταιρίες φερέγγυες και σοβαρές που προσφέρουν αποζημίωση σε περίπτωση εξαπάτησης
- Να χρησιμοποιείς προπληρωμένες πιστωτικές κάρτες



# Γραμμή Καταναλωτή 1520

## Κατά τη διάρκεια της συναλλαγής:

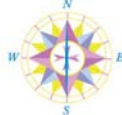
- Να αποθηκεύεις στον υπολογιστή τη συναλλαγή που πραγματοποιείς
- Να γνωρίζεις την πολιτική της εταιρίας αναφορικά με τη χρήση των προσωπικών σου δεδομένων
- Να εκτυπώνεις και να κρατάς την πολιτική επιστροφών

## Μετά την αγορά:

- Να θυμάσαι ότι έχεις τα ίδια δικαιώματα σα να είχες αγοράσει από ένα κανονικό κατάστημα
- Να κρατάς όλα τα στοιχεία επικοινωνίας - ίσως τα χρειαστείς σε περίπτωση αργοπορίας ή προβλήματος με την παράδοση του προϊόντος
- Να κρατάς αντίγραφο των όρων και των προϋποθέσεων αγοράς

## Συμβουλές για την αντιμετώπιση προβλημάτων:

- 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, πληρώνεις ο ίδιος τα έξοδα αποστολής
- Σε περίπτωση παράδοσης 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



Για οποιοδήποτε πρόβλημα, μπορείς να επικοινωνήσεις με τη Γραμμή Καταναλωτή στο 1520 και να το καταγγείλεις.



# Sign Up Here!!!



Κατά την πλοήγηση στο διαδίκτυο μπορεί κάποια στιγμή



## οι σειρήνες του διαδικτύου και η ηλεκτρονική απάτη

Χιλιάδες προϊόντα και υπηρεσίες θα προσπαθούν να τραβήξουν την προσοχή σου μέσα από καλοσχεδιασμένες ιστοσελίδες, μεγάλες προσφορές και ακόμη μεγαλύτερες υποσχέσεις.

Ο Οδυσσέας δέθηκε στο κατάρτι του καραβιού του για να μην υποκύψει στο δελεαστικό τραγούδι των σειρήνων. Εσύ μπορείς να κάνεις κάτι πιο απλό: να μάθεις πώς να αναγνωρίζεις την κρυμμένη απάτη και να αποφεύγεις τις κακοτοπιές.

πώς να  
αποφύγεις  
την απάτη

### ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΑΠΑΤΗΣ

Η ηλεκτρονική απάτη έχει πολλές μορφές και οι καταναλωτές - χρήστες του διαδικτύου θα πρέπει να είναι ιδιαίτερα προσεκτικοί και επιφυλακτικοί στις συναλλαγές τους.



**TRY IT  
NOW**

**it's free!**



να θυμηθείς τον Οδυσσέα και τις περίφημες σειρήνες!

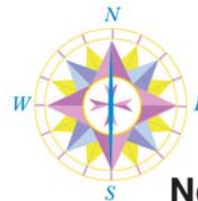
**Οι πιο συνηθισμένες μορφές απάτης είναι οι παρακάτω:**

**α) Ευκαιρίες εργασίας**

Οι απάτες που σχετίζονται με την εύρεση εργασίας, καλύπτονται συνήθως με τη μέθοδο της προσφοράς για εργασία από το σπίτι, ζητώντας ένα ποσό για αποστολή εκπαιδευτικού και βοηθητικού υλικού. Ακόμα και αν το υλικό σταλεί, κανείς δεν μπορεί να εγγυηθεί την επιτυχή πορεία της επαγγελματικής συνεργασίας. Παράλληλα, σχετίζονται και με την πλασματική παροχή υπηρεσιών.

Σε γενικές γραμμές, οι απάτες αυτές εμφανίζονται με τις παρακάτω μορφές:

- Προσφορά επαγγελματικών ευκαιριών
- Έρευνα αγοράς εργασίας
- Εργασία από το σπίτι
- Διεκπεραίωση και προώθηση πλασματικών επιταγών



**Να είσαι επιφυλακτικός και να κάνεις προσωπική έρευνα για την εταιρία (διεύθυνση επικοινωνίας, παρελθόν) πριν δεσμευτείς.**



## Γράμμα από τη Νιγηρία

### β) Υποκλοπή προσωπικών δεδομένων

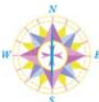
Πρόκειται για μορφή απάτης, που δε στοχεύει στην "τσέπη" του θύματος - καταναλωτή, αλλά στην κλοπή των προσωπικών του δεδομένων και τη χρήση τους από τρίτους στο διαδίκτυο.

Με τον τρόπο αυτό, οι επιτήδριοι προσπαθούν να μεταμφιεστούν χρησιμοποιώντας προσωπικά δεδομένα για να κάνουν συναλλαγές με άλλη ταυτότητα.

Η απάτη αυτή εμφανίζεται με τις παρακάτω μορφές:

- Κλοπή ταυτότητας
- "Ψάρεμα" προσωπικών πληροφοριών

Διαδεδομένη είναι η μορφή του "ψαρέματος" τραπεζικών δεδομένων μέσα από ιστοσελίδες με εμφάνιση όμοια με την επίσημη τραπεζική ιστοσελίδα.



**Η τράπεζα ποτέ δε θα σου ζητήσει επιβεβαίωση προσωπικού κωδικού, ιδιαίτερα με ηλεκτρονικό ταχυδρομείο.**

### γ) Κίνδυνοι κατά την υποσχόμενη παροχή υπηρεσιών

Σε πολλές περιπτώσεις στο διαδίκτυο, εταιρίες ή άτομα φέρονται να προσφέρουν υπηρεσίες στους χρήστες - καταναλωτές, οι οποίοι, όμως, αφού πληρώσουν για αυτές τις υπηρεσίες δεν τις λαμβάνουν ποτέ.

Κλασικές περιπτώσεις τέτοιας μορφής εξαπάτησης είναι οι παρακάτω:

- Προκαταβολή εξόδων δανείου
- Απάτες με φιλανθρωπικές προσφορές
- Επαναφορά πιστοληπτικής ικανότητας

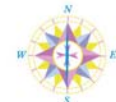
Δύο πολύ συνήθεις περιπτώσεις είναι:

#### • **Ισπανικό Λόττο**

Μας ενημερώνουν ότι κερδίσαμε ένα πολύ μεγάλο χρηματικό ποσό σε μια διεθνή λοταρία και ότι για να πάρουμε τα κέρδη, πρέπει να δώσουμε κάποια χρήματα για να καλύψουμε τα έξοδα μεταφοράς των χρημάτων.

#### • **Γράμμα από τη Νιγηρία**

Αξιωματούχοι από τη Νιγηρία θέλουν τη βοήθειά μας για να βγάλουν χρήματα από τη χώρα, με αντάλλαγμα ποσοστό των χρημάτων αυτών. Ζητούν τον τραπεζικό μας λογαριασμό, που, αφού τους τον δώσουμε, τον αδειάζουν.



**Να είσαι πολύ προσεκτικός και να μην εμπιστεύεσαι εύκολα τον καθένα στο διαδίκτυο.**



## δ) Συμμετοχή σε επενδυτικά σχέδια και παραπληροφόρηση της αγοράς

Οι απάτες αυτές σχετίζονται είτε με την παραπλάνηση και την προώθηση πλασματικών επενδυτικών σχεδίων είτε με προσπάθεια χειραγώγησης της χρηματιστηριακής αγοράς και της τιμής συγκεκριμένης μετοχής - μέσω της διασποράς πλαστών ειδήσεων.

Η απάτη αυτή εμφανίζεται με τις παρακάτω μορφές:

- Πλασματικές επενδύσεις
- "Πυραμίδες"
- Διασπορά ειδήσεων για χειραγώγηση μετοχών



**Αν κάτι φαίνεται πολύ καλό για να είναι αληθινό, συνήθως μόνο αληθινό δεν είναι.**

## ε) Dialers

Μια πολύ διαδεδομένη παράνομη δραστηριότητα του διαδικτύου είναι οι dialers. Χρησιμοποιώντας προγράμματα που εγκαθίστανται στον υπολογιστή μας εν αγνοία μας, οι απατεώνες, είτε μεταφέρουν τη σύνδεσή μας σε γραμμές υψηλής χρέωσης είτε χρησιμοποιούν τη γραμμή μας για κλήσεις στο εξωτερικό.

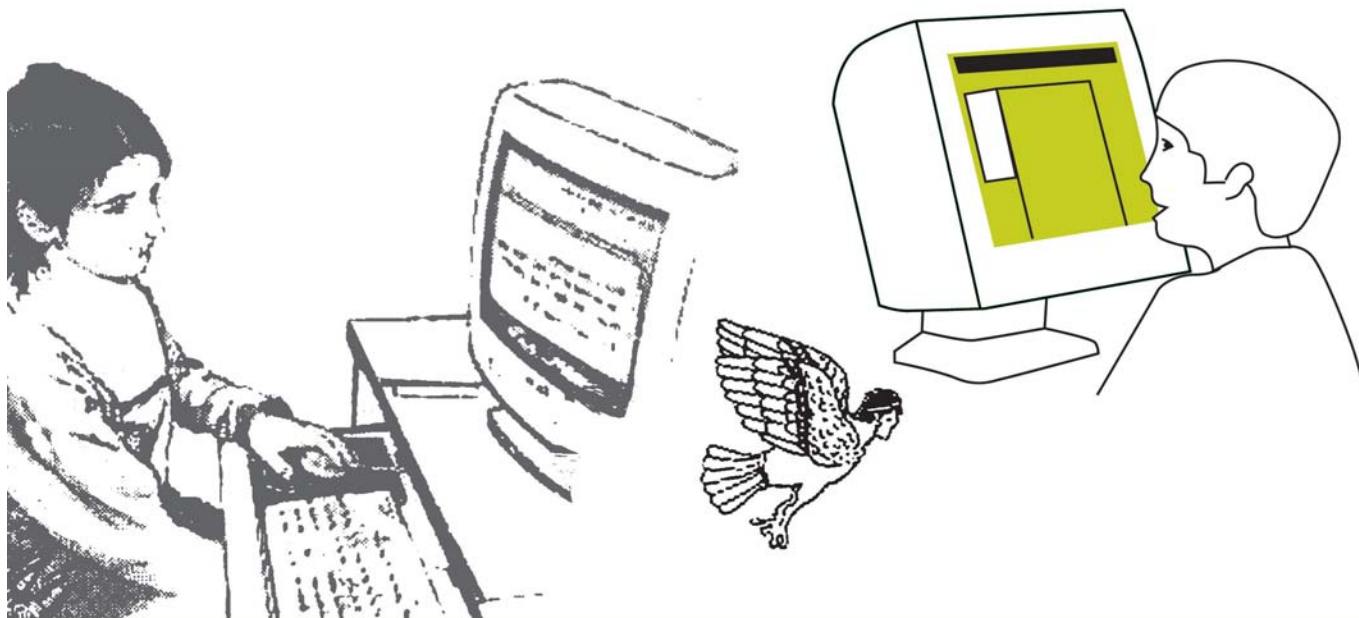
Η λειτουργία του λογισμικού αυτού, που εγκαθίσταται στον υπολογιστή συνήθως μεταμφιεσμένο σε ένα χρήσιμο πρόγραμμα, ανοίγει ουσιαστικά μια κερκόπορτα στο λειτουργικό σύστημα, την οποία χρησιμοποιούν οι απατεώνες για να κερδίζουν χρήματα. Την ίδια λειτουργία επιτελούν και κάποιες ιστοσελίδες που παρέχουν "δωρεάν" προγράμματα και υπηρεσίες, οι οποίες όμως, ειδοποιούν πρώτα το χρήστη στους όρους χρήσης της ιστοσελίδας.

Για την προστασία μας απέναντι σε αυτή τη μορφή απάτης υπάρχουν πρακτικοί τρόποι προφύλαξης, όπως η φραγή κλήσεων προς το εξωτερικό και η χρήση κωδικού για την ενεργοποίηση της υπηρεσίας ή το να βγάζουμε το modem από την πρίζα όταν δε χρησιμοποιούμε το διαδίκτυο.

Το πρόβλημα αυτό δεν εμφανίζεται συνήθως σε ADSL συνδέσεις. Αυτό όμως δεν σημαίνει ότι δεν πρέπει να είμαστε προσεκτικοί.



**Σε κάθε περίπτωση πρέπει να διαβάζεις τους όρους χρήσης της ιστοσελίδας που επισκέπτεσαι και να χρησιμοποιείς συχνά λογισμικά ασφαλείας.**



## Ποιες ΚΟΙΝΩΝΙΚές ομάδες πρέπει να είναι ΠΙΟ ΠΡΟΣΕΚΤΙΚές;

### ΟΙ ΑΝΗΛΙΚΟΙ

Το διαδίκτυο, εκτός από ανεξάντλητη πηγή κάθε είδους πληροφορίας, αποτελεί μέσο ψυχαγωγίας και ένα από τα πλέον δημοφιλή μέσα επικοινωνίας μεταξύ των νέων. Τα ανήλικα άτομα αποτελούν, όμως, ιδανικό στόχο για τους επιτήδειους, οπότε θα πρέπει να δίνεται ιδιαίτερη προσοχή κατά την πλοήγηση στο διαδίκτυο.

Οι κίνδυνοι εγκυμονούν συνήθως στα εξής σημεία:

- Chat Rooms (δωμάτια επικοινωνίας) - καθώς δε γνωρίζουμε με ποιους μιλάμε
- Sites (ιστοσελίδες) με παράνομο και ανήθικο περιεχόμενο



**ΑΓΟΡΑΣΕ  
ΤΩΡΑ**

**BUY**

**ΜΟΝΑΔΙΚΗ ΕΥΚΑΙΡΙΑ!!!**



### **ΤΑ ΗΛΙΚΙΩΜΕΝΑ ΑΤΟΜΑ**

Οι συνηθέστερες μορφές απάτης που απευθύνονται κυρίως σε ηλικιωμένους είναι:

- Παραπονημένες και πλασματικές συνταγές και αγορές φαρμάκων
- Προϊόντα κατά της γήρανσης
- Προϊόντα με υποτιθέμενη διατροφική αξία
- Άλλες απάτες, σχετικές με χρηματοοικονομικές υπηρεσίες και επενδύσεις

Το διαδίκτυο παραμένει ένας τομέας υπό ελλειπή και περιορισμένο έλεγχο. Αυτό έχει ως συνέπεια να ευδοκιμεί η ανάπτυξη ύποπτων συνδιαλλαγών και παράνομων δραστηριοτήτων. Κάποιες από αυτές, που είναι πιθανό να δείς μπροστά σου κατά τη διάρκεια της πλοήγησής σου στις ιστοσελίδες, είναι και οι παρακάτω.

Για την αποφυγή προβλημάτων που μπορούν να προκύψουν από την επίσκεψη και τη συνδιαλλαγή με τέτοιες ιστοσελίδες, καλό θα είναι να γνωρίζεις τι θεωρείται παράνομη δραστηριότητα.



## Ποιες είναι οι παράνομες δραστηριότητες στο διαδίκτυο;



**CHAT ROOMS**

**Γενικά, οι παράνομες δραστηριότητες στο διαδίκτυο σχετίζονται με τα παρακάτω:**

- Παιδική πορνογραφία
- Ρατσισμός
- Σατανισμός
- Προώθηση Ναρκωτικών Ουσιών - ιδίως μέσα από chat rooms (δωμάτια επικοινωνίας)
- Τυχερά παιχνίδια - παράνομο στοίχημα (ακόμα και από νόμιμες στο εξωτερικό εταιρίες ή καζίνο)
- Προσβολές και εκμετάλλευση γενετήσιας αξιοπρέπειας
  - Εμπορία ανθρώπινων οργάνων
  - Διακίνηση videos προσωπικών σχέσεων

**Σε περίπτωση που συναντήσεις κάποια τέτοια δραστηριότητα, επικοινωνήσε αμέσως με τη Δίωξη Ηλεκτρονικού Εγκλήματος της Γενικής Ασφάλειας (τηλ.: 210 6476464)**

**Start Chatting**



**HOT VIDEOS**



Εκτός από τις απάτες, που στόχο έχουν την εξαπάτηση των καταναλωτών - χρηστών, ιδιαίτερα διαδεδομένες είναι και οι απειλές για την ασφάλεια των υπολογιστών.

Τα προγράμματα αυτά έχουν τη δυνατότητα να πλήξουν το σύστημα αρχείων του υπολογιστή αλλά ακόμα και να δημιουργήσουν έσοδα για τους επιτήδειους χρεώνοντας υπέρογκα τους τηλεφωνικούς μας λογαριασμούς.

### Το κακόβουλο λογισμικό εμφανίζεται στις παρακάτω μορφές:



**Υπάρχουν άλλοι Κίνδυνοι  
για την ασφάλεια στην πλοήγηση;**



## Adware - Spyware

Πρόκειται για προγράμματα που έχουν επιπλέον κρυμμένες λειτουργίες σε σχέση με αυτό που διαφημίζουν ότι κάνουν. Οι κρυμμένες αυτές λειτουργίες, έχουν ως στόχο είτε την παρακολούθηση των συνηθειών του χρήστη κατά την πλοήγησή του στο διαδίκτυο και τη χρήση των πληροφοριών αυτών για διαφημιστικούς σκοπούς, είτε την εγκατάσταση προγραμμάτων για τη χρήση του υπολογιστή από τρίτους, χωρίς την έγκριση του χρήστη.

Συνηθέστερα, τέτοιας μορφής αρχεία είτε εγκαθίστανται στον υπολογιστή μας χωρίς να το γνωρίζουμε, κατά τη διάρκεια της πλοήγησής μας στο διαδίκτυο, είτε τα εγκαθιστούμε άθελά μας εμείς, νομίζοντας ότι επιτελούν μια άλλη λειτουργία.

**Για την αντιμετώπιση αυτών των προβλημάτων, ο καλύτερος τρόπος είναι η εγκατάσταση του απαραίτητου ειδικού λογισμικού και ο ανά τακτά διαστήματα έλεγχος του υπολογιστή.**

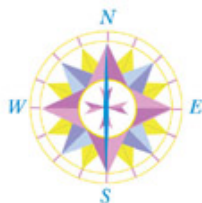


## Trojan Horses

Πρόκειται για κακόβουλο λογισμικό, που λειτουργεί ως Δούρειος Ίππος. Εμφανίζεται με μια μορφή φιλική προς το χρήστη, περιέχει, όμως, κρυμμένο λογισμικό που επιτελεί μια λειτουργία βλαβερή για την ασφάλεια του υπολογιστή και της πλοήγησής μας στο διαδίκτυο.

Η συνηθέστερη κρυμμένη λειτουργία είναι η δυνατότητα που δίνεται σε τρίτους να ανοίξουν μια πόρτα επικοινωνίας με τον υπολογιστή και να χρησιμοποιούν την τηλεφωνική σύνδεση του χρήστη, υπερχρεώνοντας το λογαριασμό του. Μια άλλη λειτουργία είναι η καταστροφή αρχείων του χρήστη. Τέτοια προγράμματα δεν εμφανίζονται μόνο με τη μορφή λογισμικού αλλά κυκλοφορούν και μέσω ηλεκτρονικού ταχυδρομείου.

Σε γενικές γραμμές, τα Trojan Horses κυκλοφορούν είτε ως προγράμματα είτε ως ηλεκτρονικά μηνύματα και αποτελούν ένα πολύ μεγάλο κίνδυνο για τον υπολογιστή. Για να αντιμετωπίσεις το πρόβλημα θα πρέπει να είσαι ιδιαίτερα προσεκτικός στο τι "κατεβάζεις" από το διαδίκτυο και στο τι ηλεκτρονικά μηνύματα ανοίγεις και διαβάζεις.



**Η εγκατάσταση ειδικού λογισμικού, αποτελεί μια καλή ασπίδα προστασίας ενάντια στην εξάπλωση αυτής της απειλής.**



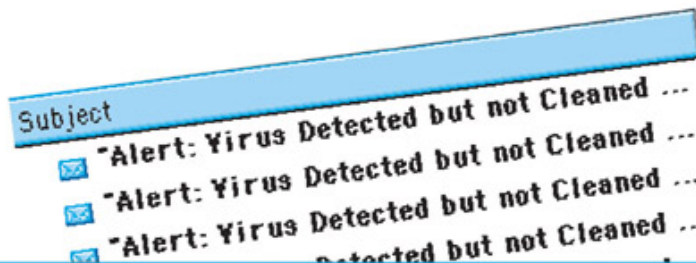
# Trojan Horses

## Internet Virus

Η πιο γνωστή απειλή για την ασφάλεια του υπολογιστή προέρχεται από τους ιούς.

Οι ιοί αυτοί λειτουργούν όπως και οι κανονικοί ιοί για τους ανθρώπους (ο υπολογιστής μπορεί να αρρωστήσει μόνο με την επαφή με μια μολυσμένη ιστοσελίδα ή αρχείο) και εκμεταλλεύονται κάποια ρωγμή στο σύστημα ασφάλειας του υπολογιστή για να το μολύνουν.

Έχουν τη δυνατότητα αναπαραγωγής και αντιμετωπίζονται με την εγκατάσταση ειδικού αμυντικού λογισμικού.



# Internet Virus

## ΑΠΟΡΙΕΣ, ΠΑΡΑΠΟΝΑ, ΚΑΤΑΓΓΕΛΙΕΣ

Όλοι μας μπορούμε να απευθυνόμαστε για ενημέρωση, παράπονα και καταγγελίες στην τηλεφωνική γραμμή του Καταναλωτή **1520**, η οποία λειτουργεί καθημερινά Δευτέρα έως Παρασκευή από τις 8:00 έως τις 22:00 και Σάββατο 8:30 έως 15:00.

Επίσης έχουμε τη δυνατότητα να επισκεφθούμε τη Γενική Γραμματεία

Καταναλωτή ή να επικοινωνήσουμε με [e-mail:info@efpolis.gr](mailto:info@efpolis.gr)



Τηλεφωνική Γραμμή Καταναλωτή: 1520  
Τηλεφωνικό Κέντρο: 210 3816241, 210 3893000  
website: [www.efpolis.gr](http://www.efpolis.gr)  
e-mail: [info@efpolis.gr](mailto:info@efpolis.gr)  
Πλατεία Κάνιγγος 1, 101 81 Αθήνα  
Κτίριο Υπουργείου Εμπορίου, 1ος όροφος