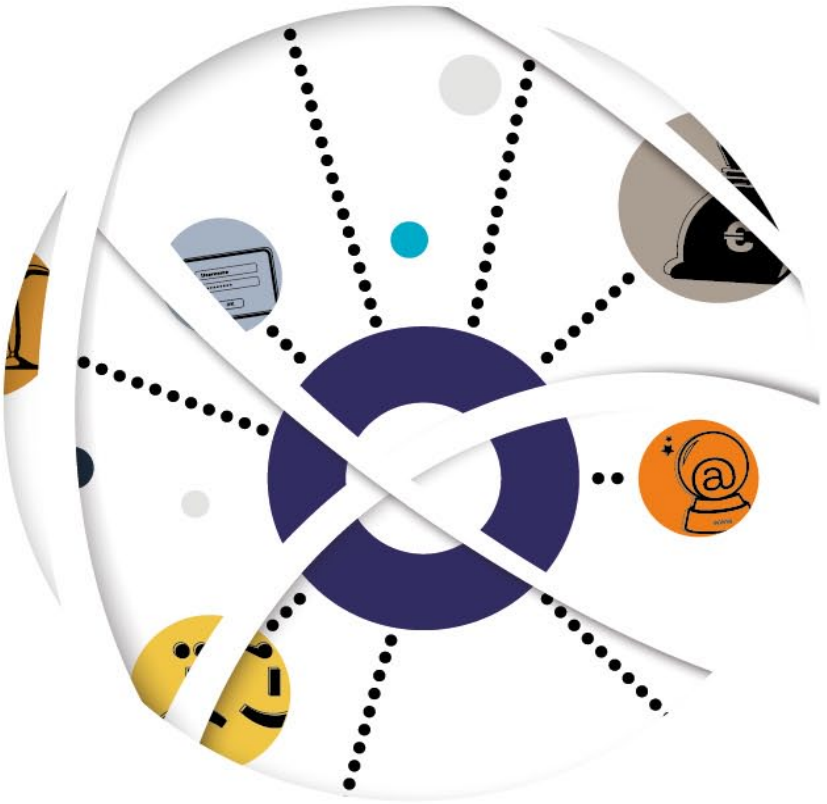
# ΑΣΦΑΛΗΣ ΠΕΡΙΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΕΝΗΜΕΡΩΘΕΙΤΕ.
ΠΡΟΣΤΑΤΕΥΤΕΙΤΕ.



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και
Διοικητικής Ανασυγκρότησης

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#το_internet_κρύβει_και_κινδύνους

#το_μέλλον_του_διαδικτύου

#νομοθεσία_στο_διαδίκτυο

#cyberbullying

#social_media_&_facebook

#παιδική_πορνογραφία_στο_διαδίκτυο

#ασφάλεια_πληροφοριών_&_βιομηχανική_κατασκοπεία

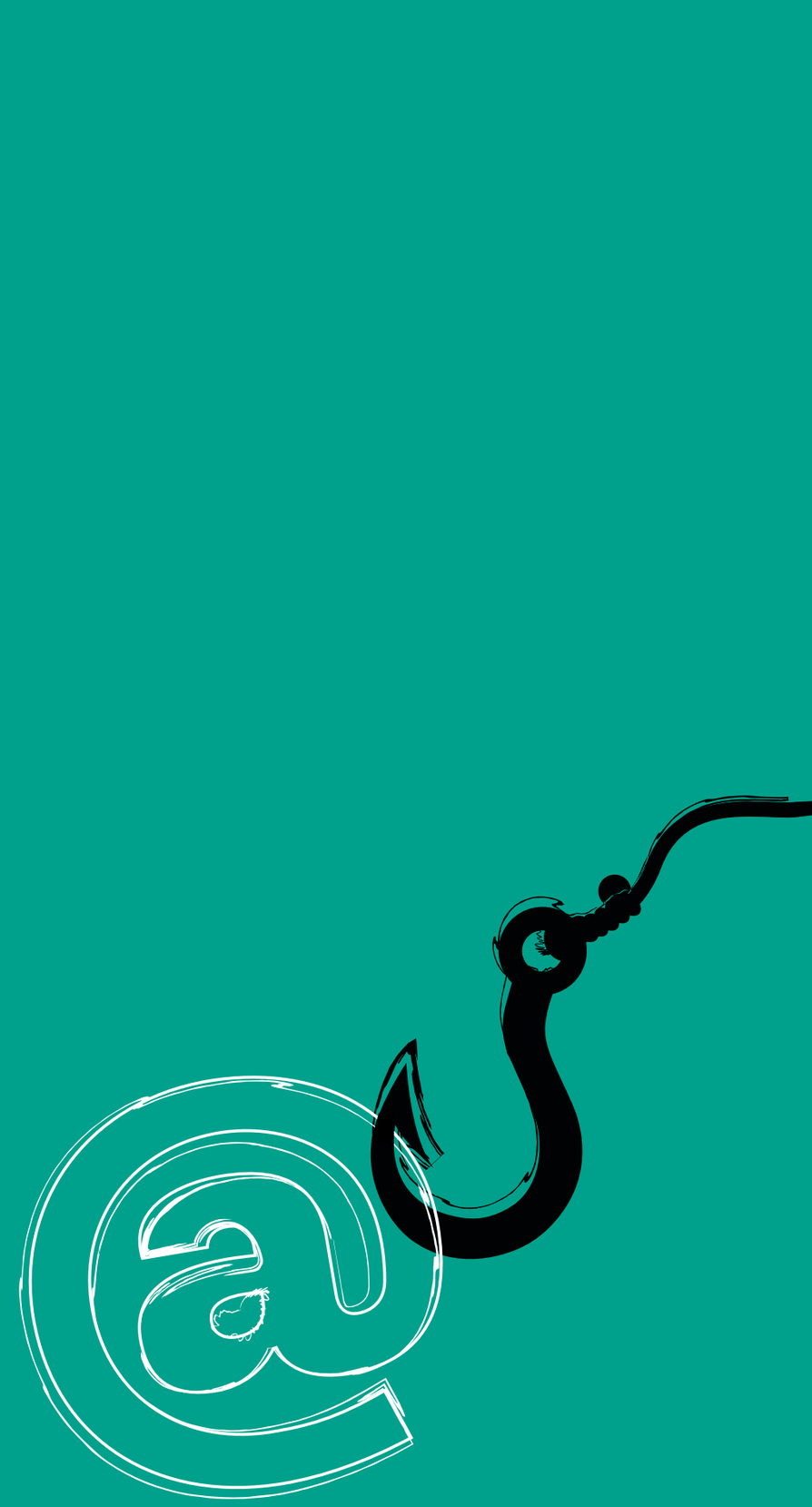
#απάτες_μέσω_διαδικτύου

#ηλεκτρονικό_ψάρεμα

ΠΕΡΙΕΧΟΜΕΝΑ

# #το_internet_κρύβει_και_κινδύνους

Μάθε πώς μπορείς να τους αναγνωρίζεις και να προστατεύεις εσένα ή τους δικούς σου από το cyberbullying, την κλοπή προσωπικών δεδομένων και άλλους κινδύνους.




# ΚΙΝΔΥΝΟΙ

*Όλο και περισσότεροι Έλληνες μπαίνουν πλέον στο Internet! Οι πιο έμπειροι είναι υποψιασμένοι για τη σκοτεινή πλευρά του Διαδικτύου, αλλά, δυστυχώς οι περισσότεροι την αγνοούν ακόμα... Κι όμως, το ηλεκτρονικό έγκλημα έχει πλέον μπει για τα καλά στη ζωή μας και αυξάνεται με ραγδαίους ρυθμούς.*

## Cyberbullying

Αποστολή κειμένων e-mail με προσβλητικό περιεχόμενο, κακόβουλη δημοσίευση φωτογραφιών σε μέσα κοινωνικής δικτύωσης-ιστολόγια, διάδοση ψευδών γεγονότων, ανώνυμες κλήσεις και μηνύματα με σκοπό την πρόκληση φόβου και ταραχής.

## Παιδική πορνογραφία

Άτομα κάθε λογής, ακόμα και υπεράνω πάσης υποψίας, φαινομενικώς φιλήσυχα και ευυπόληπτα, εκμεταλλεύονται τη θέση και τη σχέση τους με παιδιά, προκειμένου να ικανοποιήσουν το αρρωστημένο πάθος τους.

## Μέσα κοινωνικής δικτύωσης

Στην Υπηρεσία μας προσέρχονται καθημερινά άτομα, τα προσωπικά δεδομένα των οποίων έχουν δημοσιοποιηθεί παρανόμως σε ιστοσελίδες κοινωνικής δικτύωσης (Facebook, hi5 κ.λπ.), με μοναδικό σκοπό τον εξευτελισμό, την απειλή ή τον εξαναγκασμό σε κάποια πράξη ή παράλειψη.

## Αυτοκτονίες

2004-2014: 1.112 συνάνθρωποί μας προσπάθησαν να αυτοκτονήσουν με διάφορους τρόπους, εκφράζοντας την επιθυμία τους αυτή μέσω του Διαδικτύου.

## Διακίνηση-Πειρατεία λογισμικού

Η παράνομη χρήση πνευματικής εργασίας άλλων, χωρίς ρητή αναφορά στον δημιουργό της, συνιστά κλοπή πνευματικής ιδιοκτησίας και αδίκημα!



# ΧΡΗΣΙΜΕΣ ΣΥΜΒΟΥΛΕΣ

## Ενημέρωση

Το Διαδίκτυο αποτελεί ένα από τα θαύματα του σύγχρονου κόσμου. Δίνει σε πραγματικό χρόνο πρόσβαση σε πληροφορία, γνώση, αλλά και ψυχαγωγία. Κάθε χρήστης του πρέπει να συνειδητοποιήσει ότι ο παγκόσμιος ιστός δεν διαφέρει σε τίποτα από μια κοινωνία. Οι πληροφορίες που παρουσιάζονται στο Διαδίκτυο δεν είναι πάντα έγκυρες. Παρ' όλα αυτά, μπορείτε να χρησιμοποιείτε το Διαδίκτυο για να αποκτήσετε ασφαλείς και έγκυρες πληροφορίες με ενημερωτικό και εκπαιδευτικό όφελος.

## Ασφάλεια

Ενημερώνετε τα προγράμματα πλοήγησης και το λειτουργικό σύστημα τακτικά. Εγκαταστήστε πρόσθετο λογισμικό ασφαλείας (antivirus, anti-spyware), καθώς και προγράμματα-«τείχη ασφαλείας» (firewall) που ελέγχουν εισερχόμενες και εξερχόμενες πληροφορίες από τον υπολογιστή σας και προλαβαίνουν τη διάδοση ιών και ανεπιθύμητων εφαρμογών, η εγκατάσταση των οποίων δεν γίνεται συνειδητά. Ενεργοποιήστε τα ενσωματωμένα χαρακτηριστικά του προγράμματος πλοήγησης που χρησιμοποιείτε, για την προστασία σας στο Διαδίκτυο. Αυτά συνήθως βρίσκονται στην ενότητα «Εργαλεία» (Tools) και την υποενότητα «Επιλογές» (Internet Options).

## Προστασία

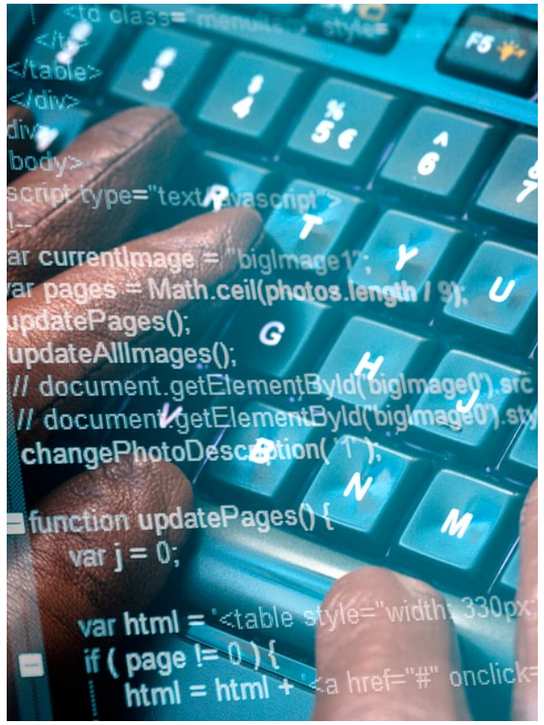
Κάτοχοι λογαριασμών e-mail λαμβάνουν συχνά διαφημιστικά ή παραπλανητικά μηνύματα από αγνώστους, που περιέχουν μολυσμένα αρχεία με ιούς, διαφημίζουν ακατάλληλο και παράνομο περιεχόμενο ή αποσκοπούν στην εξαπάτηση των χρηστών με στόχο την απόκτηση ευαίσθητων-προσωπικών πληροφοριών και την εγκατάσταση κακόβουλου λογισμικού με δυσάρεστες συνέπειες (Phishing). Βεβαιωθείτε ότι στους λογαριασμούς e-mail έχετε ενεργοποιήσει στο υψηλότερο επίπεδο το φίλτρο για τα ανεπιθύμητα μηνύματα και μην ανοίγετε ποτέ συνημμένα αρχεία που έχετε λάβει από αγνώστους. Αποφεύγετε να χρησιμοποιείτε κωδικούς που μπορεί εύκολα να τους μαντέψει κάποιος (σημαδιακές ημερομηνίες, ακολουθίες γραμμάτων ή κύρια ονόματα). Ένας ασφαλής κωδικός καλό είναι να περιλαμβάνει έξι έως οκτώ χαρακτήρες και, ιδανικά, συνδυασμό πεζών-κεφαλαίων. Διατηρείτε αντίγραφα ασφαλείας (Backup) για όσα αρχεία κρίνετε σημαντικά!

## Σωστή χρήση

Σιγουρευτείτε ότι η ανταλλαγή αρχείων δεν είναι παράνομη και το λογισμικό που χρησιμοποιείτε δεν θα λειτουργήσει ως «Δούρειος Ίππος» για να αποκτήσει ένας τρίτος πρόσβαση στον υπολογιστή. Τηρείτε τα πνευματικά δικαιώματα προκειμένου να αποφύγετε τυχόν ποινικές διώξεις! Αν αποκτάτε πρόσβαση στο Διαδίκτυο από κοινόχρηστους υπολογιστές (Internet Café), θυμηθείτε ότι δεν είστε ο μοναδικός χρήστης αυτής της συσκευής και, επομένως, δεν μπορείτε ποτέ να γνωρίζετε τι είδους πρόγραμμα εκτελείται σ' αυτόν! Καθαρίστε την προσωρινή μνήμη (cache) και το ιστορικό των ενεργειών (history) των προγραμμάτων πλοήγησης, προκειμένου να σβήσετε τα προσωπικά σας στοιχεία. Σιγουρευτείτε για τις γνωριμίες σας στο Διαδίκτυο. Στις ιστοσελίδες κοινωνικής δικτύωσης να θυμάστε ότι τα άτομα που γνωρίζετε μπορεί να μην είναι αυτά που λένε ότι είναι! Μη δίνετε ποτέ προσωπικές πληροφορίες. Αν κάποιος σας παρενοχλεί, θυμηθείτε ότι μπορείτε να βγείτε από τον ιστότοπο με ένα απλό «κλικ»!

## Όλη η οικογένεια μαζί...

**Παιδιά 5-7 ετών:** Ασχολούνται με παιχνίδια και εκπαιδευτικά sites, αλλά γρήγορα μαθαίνουν για καινούργια sites και δεν καταλαβαίνουν την έννοια του «ξένου κινδύνου» από κάποιον που έρχεται σε επαφή μαζί τους μέσω ενός φιλικού ιστότοπου ή ενός παιχνιδιού.
**Παιδιά 8-12 ετών:** Φτιάχνουν τα πρώτα τους e-mail ή instant messaging, ενώ ξεκινούν την επαφή τους με τα κοινωνικά δίκτυα που είναι δημοφιλή σε μεγαλυτέρους, εφήβους και ενήλικες.
**Έφηβοι 13-17 ετών:** Αναπτύσσουν μεγαλύτερη ανεξαρτησία, και αυτό αντανακλάται στον τρόπο με τον οποίο συμπεριφέρονται στο Διαδίκτυο. Συχνά ξεχνούν πως οτιδήποτε δημοσιεύεται στο Διαδίκτυο υπάρχει σε κοινή θέα και πιθανόν να υπάρχει για πάντα.
**Δράσεις:** Μείνετε κοντά στα παιδιά σας και εμπλακείτε σε κάθε δική τους διαδικτυακή δραστηριότητα με τον ίδιο τρόπο που κάνετε στις δραστηριότητες του σχολείου. Ενεργοποιήστε φίλτρα και ειδικό λογισμικό για γονείς, προκειμένου τα παιδιά να μη δώσουν προσωπικές πληροφορίες και να μη φτάσουν σε κάποιο site απρεπούς περιεχομένου. Μιλήστε με το παιδί σας, ούτως ώστε, αν προκύψει κάτι ξαφνικό ή ενοχλητικό, να μπορεί να κλείσει την ηλεκτρονική σελίδα. Πείτε του να μη συνομιλεί ποτέ σε απευθείας σύνδεση (chat rooms), να μη στέλνει μηνύματα και να μη μοιράζεται πληροφορίες με οποιονδήποτε!




## ΘΕΤΙΚΑ ΔΙΑΔΙΚΤΥΟΥ

Το Διαδίκτυο είναι ένα πολύ χρήσιμο εργαλείο, αρκεί να το χειριζόμαστε με ασφάλεια. Χρησιμοποιήστε το Διαδίκτυο για να βρείτε πληροφορίες, καθώς αποτελεί ανεξάντλητη πηγή γνώσης. Οι μηχανές αναζήτησης σας επιτρέπουν να πληκτρολογήσετε λέξεις κλειδιά, ονόματα ή ημερομηνίες και να λάβετε links σχετικά με το θέμα που σας ενδιαφέρει. Έχετε, επιπλέον, τη δυνατότητα να χρησιμοποιήσετε νέες μορφές εκπαίδευσης (e-learning). Τα chat rooms (εικονικά δωμάτια επικοινωνίας) και οι ιστοσελίδες κοινωνικής δικτύωσης (Facebook, Twitter, hi5) είναι οι πιο δημοφιλείς τρόποι για on-line επικοινωνία με φίλους. Μπορείτε να χρησιμοποιείτε και τα προγράμματα άμεσων μηνυμάτων (MSN, Skype). Προσοχή όμως! Πρέπει να χρησιμοποιούνται μόνο μεταξύ ατόμων που ήδη γνωρίζονται μεταξύ τους.

Έχετε τη δυνατότητα πλέον να ενημερώνεστε και διαδικτυακά για ό,τι συμβαίνει στον κόσμο και τη χώρα σας (ηλεκτρονικές εφημερίδες/ράδιο). Το Διαδίκτυο σας επιτρέπει να ταξιδέψετε, κάνοντας on-line κρατήσεις εισιτηρίων και ξενοδοχείων, ακόμα και να κάνετε τα ψώνια σας με ένα απλό «κλικ». Τα διαδικτυακά παιχνίδια κάνουν το Διαδίκτυο διασκεδαστικό! Μπορείτε να παίξετε με τους φίλους σας και τους γονείς σας, και ιδανικά να βρείτε ένα παιχνίδι που να συνδυάζει την ψυχαγωγία με τη μάθηση. Με τη βοήθεια των γονιών σας και του Διαδικτύου μπορείτε να ανακαλύψετε καινούργια πράγματα, να διευρύνετε τους ορίζοντές σας και, γιατί όχι, να ξεδιπλώσετε τα ταλέντα σας!

**[ΝΑΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ!]**



## ΧΡΗΣΙΜΑ LINKS

Χρήσιμες συμβουλές από τη Δίωξη Ηλεκτρονικού Εγκλήματος:
**http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang=**

Οργανισμός προστασίας των δικαιωμάτων των παιδιών: **http://www.hamogelo.gr**

Ιστότοπος από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος: **www.cyberkid.gr**

Facebook της Δίωξης Ηλεκτρονικού Εγκλήματος:
**www.facebook.com/cyberkid.gr**

Μονάδα Εφηβικής Υγείας, Β' Παιδιατρική Κλινική Πανεπιστημίου Αθηνών, Νοσοκομείο Παίδων
**www.youth-health.gr**

Ελληνική Εταιρεία Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο
**www.hasiad.gr**

# #το_μέλλον_του_διαδικτύου

Εκτιμήσεις και προβλέψεις


## ΔΙΑΔΙΚΤΥΟ

Το Διαδίκτυο αποτελεί το μεγαλύτερο δίκτυο υπολογιστών στον κόσμο, το οποίο επιτρέπει την επικοινωνία και την ανταλλαγή πληροφοριών μεταξύ οποιωνδήποτε σημείων στον πλανήτη. Το Διαδίκτυο έχει χαρακτηριστεί ως η μεγαλύτερη «εφεύρεση» όλων των εποχών, κατακτώντας ολόκληρη την υφήλιο μέσα σε μόλις μερικές δεκαετίες ζωής και αποτελώντας πλέον τη μεγαλύτερη οργανωμένη κοινωνία παγκοσμίως.

Το Διαδίκτυο αποτελεί μια παράλληλη, «εικονική» παγκόσμια κοινότητα, η οποία καταλύει όλες τις κοινωνικές και πολιτιστικές διαχωριστικές γραμμές που υπάρχουν στον πραγματικό κόσμο και που τα παραδοσιακά μέσα επικοινωνίας αδυνατούν να ξεπεράσουν. Το Διαδίκτυο, σε αντίθεση με τα παραδοσιακά μέσα ενημέρωσης και επικοινωνίας, καθιστά δυνατή τη ζωντανή αμφίδρομη επικοινωνία και δίνει τη δυνατότητα της άμεσης συμμετοχής σε όλους τους χρήστες με την ελεύθερη επιλογή λήψης, παροχής και διάχυσης της πληροφορίας. Καταλύοντας τα σύνορα και εκμηδενίζοντας τις αποστάσεις, το διαδίκτυο φαίνεται να κλίνει την πλάστιγγα πλέον εμφανώς υπέρ των επικοινωνιών στην αιώνια διαμάχη μεταξύ των μεταφορών και των επικοινωνιών.



## ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Το Διαδίκτυο αριθμεί θεωρητικά μόλις λίγες δεκαετίες ζωής, στις οποίες γνώρισε εκρηκτική ανάπτυξη και αποτέλεσε το σημαντικότερο στοιχείο μετεξέλιξης της ανθρωπότητας από τη βιομηχανική εποχή στην εποχή της πληροφορίας και την ψηφιακή επανάσταση. Σημαντικοί σταθμοί στην εξέλιξη αυτή υπήρξαν οι εξής:

- **1969:** Δημιουργείται το ARPANET, ο πρόγονος του σημερινού Διαδικτύου, στο οποίο συμμετείχαν 4 μίνι υπολογιστές από αντίστοιχα ακαδημαϊκά ιδρύματα των Η.Π.Α., οι οποίοι συνδέθηκαν με ταχύτητες έως 50kbps.
- **1972:** Συστήνεται στο κοινό η ιδέα του ηλεκτρονικού ταχυδρομείου, όταν το ARPANET αριθμεί πλέον 23 διασυνδεδεμένους υπολογιστές.
- **1974:** Δημοσιεύεται από τους V. Cerf και B. Kahn, η πρώτη μελέτη για το πρωτόκολλο TCP (Transmission Control Program) το οποίο επιτρέπει την επικοινωνία μεταξύ διαφορετικών δικτύων υπολογιστών.
- **1974:** Εγκαινιάζεται το Telnet, η πρώτη εμπορική εκδοχή του ARPANET.
- **1982:** Χρησιμοποιείται για πρώτη φορά ο όρος «Internet», που ορίζει ένα συνδεδεμένο σύνολο από δίκτυα τα οποία χρησιμοποιούν το πρωτόκολλο TCP/IP.
- **1986:** Δημιουργείται το Nation Science Foundation Net (NSFNET), το οποίο διασυνδέει όλα τα πανεπιστημιακά ιδρύματα των Η.Π.Α.
- **1990:** Λειτουργεί ο πρώτος πάροχος Διαδικτύου με το όνομα «The World comes on-line» (world.std.com) που προσφέρει σύνδεση στο διαδίκτυο μέσω τηλεφώνου.
- **1990:** Η Ελλάδα συνδέεται στο Διαδίκτυο μέσω του δικτύου NSFNET.
- **1991:** Το CERN παρουσιάζει το World Wide Web, το οποίο συστήνει στο κοινό την ιδέα της χρήσης του Διαδικτύου για την παροχή πληροφορίας μέσω ιστοσελίδων υπερκειμένου (hypertext).
- **1993:** Παρουσιάζεται ο πρώτος web browser (Mosaic) από την εταιρεία National Center for Supercomputing Applications (NCSA).
- **1994:** Προσφέρονται για πρώτη φορά τραπεζικές υπηρεσίες μέσω του Διαδικτύου (Stanford Federal Credit Union).
- **1996:** Διατίθεται στην αγορά το πρώτο κινητό με πρόσβαση στο Διαδίκτυο (Nokia 9000 Communicator) και βάρος 397γρ.!
- **2008:** Η Google ανακοινώνει ότι ο κατάλογός της ξεπέρασε το 1 τρισεκατομμύριο URLs.

## Η ΕΙΚΟΝΑ ΣΗΜΕΡΑ

Από τους 4 υπολογιστές που αριθμούσε αρχικά το ARPANET, μπορεί κανείς να διαπιστώσει τη γιγαντιαία εξάπλωση του Διαδικτύου εξετάζοντας τα αντίστοιχα σημερινά νούμερα. Το 2012, οι χρήστες του Διαδικτύου ξεπέρασαν τα 2 δισεκατομμύρια παγκοσμίως, ποσοστό το οποίο αντιστοιχεί στο 30,2% του παγκόσμιου πληθυσμού. Αντίστοιχα, το ποσοστό στην Ευρώπη ανέρχεται σε 58,3% και στη Β. Αμερική σε 78,3%, με την αύξηση των χρηστών παγκοσμίως τα τελευταία 10 χρόνια να ξεπερνά το 450%.

Ο παγκόσμιος ιστός (World Wide Web) αριθμεί πλέον περίπου 50 δισεκατομμύρια ιστοσελίδες. Τα κοινωνικά δίκτυα αναπτύσσονται με ταχύτατους ρυθμούς, με το Facebook να κατέχει την πρώτη θέση, ξεπερνώντας το 1 δισεκατομμύριο χρήστες, και το YouTube να φτάνει τις 1 τρισεκατομμύριο αναπαραγωγές βίντεο.

# Η ΕΙΚΟΝΑ ΣΗΜΕΡΑ

Αντίστοιχη εικόνα παρουσιάζει η ανάπτυξη του Διαδικτύου και στην Ελλάδα. Οι χρήστες του Διαδικτύου ξεπερνούν τα 5 εκατομμύρια (>50% του πληθυσμού) παρουσιάζοντας αύξηση την τελευταία δεκαετία >250%. Αντίστοιχα, οι ευρυζωνικές συνδέσεις ξεπερνούν τις 2.500.000 και οι χρήστες του Facebook πλησιάζουν τα 4 εκατομμύρια. Ενδιαφέρον είναι ότι στις ηλικίες 13-24, το ποσοστό χρήσης αγγίζει το 90%, γεγονός που φανερώνει την περαιτέρω ραγδαία εξέλιξη του Διαδικτύου.
Τα θετικά του Διαδικτύου με τη σημερινή μορφή του είναι πολλά και ποικίλα, παρέχοντας μια πληθώρα υπηρεσιών που καλύπτει ένα μεγάλο εύρος των καθημερινών αναγκών:

- Γνώση
- Εκπαίδευση
- Πληροφορίες
- Επικοινωνία
- Ενημέρωση
- Ψυχαγωγία
- Διασκέδαση
- Αγορές
- Ταξίδια

# ΤΙ ΕΙΔΑΜΕ ΤΗΝ ΠΕΡΑΣΜΕΝΗ ΔΕΚΑΕΤΙΑ

Την περασμένη δεκαετία, μια σειρά τεχνολογικών εξελίξεων και κοινωνικών τάσεων καθιέρωσαν τη σημερινή μορφή του Διαδικτύου. Χαρακτηριστικά παραδείγματα αποτέλεσαν τα εξής:

**Social Media:** Σημαντικότερο σημείο στην εξέλιξη του Διαδικτύου την περασμένη δεκαετία αποτέλεσε αναμφίβολα η εκρηκτική ανάπτυξη των μέσων κοινωνικής δικτύωσης.
**Video sharing:** Με την ευρυζωνικότητα να είναι διαθέσιμη σε κάθε σπίτι και τις ταχύτητες να αυξάνονται σημαντικά, κατέστη πρακτικά εφικτό το video sharing, το οποίο –με πρωτοστάτη το YouTube και τις υπηρεσίες του– έγινε κομμάτι της καθημερινότητας.
**Mobile Internet – 3G – smartphones:** Πολύ σημαντική εξέλιξη αποτέλεσε τεχνολογικά και η δυνατότητα σύνδεσης στο Διαδίκτυο από τις συσκευές κινητών τηλεφώνων, που επέτρεψε στους χρήστες τού Διαδικτύου να συνδέονται από κάθε μέρος και με κάθε συσκευή.
**Online gaming**: Τεράστια ανάπτυξη γνώρισαν και τα διαδικτυακά παιχνίδια, κερδίζοντας πολύ γρήγορα μεγάλο αριθμό χρηστών. Τεράστιοι εικονικοί κόσμοι προσελκύουν καθημερινά ένα μεγάλο ποσοστό χρηστών, με κάποια από τα διαδικτυακά παιχνίδια να ξεπερνούν τους 10 εκατομμύρια χρήστες.
**Internet radio:** Το κλασικό ραδιόφωνο μεταλλάχθηκε σε μεγάλο βαθμό σε διαδικτυακό, κερδίζοντας πολλούς θαυμαστές και καταλύοντας τα σύνορα της μετάδοσης παγκοσμίως.
**Blogs:** Τα ιστολόγια αποτέλεσαν ένα από τα τελευταία trends της περασμένης δεκαετίας, δίνοντας βήμα σε όλους για έκφραση και κερδίζοντας καθημερινά εκατομμύρια θαυμαστές.



# ΤΙ ΑΝΑΜΕΝΟΥΜΕ ΝΑ ΔΟΥΜΕ ΤΗΝ ΕΠΟΜΕΝΗ ΔΕΚΑΕΤΙΑ

Με βάση τις προηγούμενες εξελίξεις, τα δείγματα τα οποία έχουν παρουσιαστεί, και την τάση για ανάπτυξη, η επόμενη δεκαετία αναμένουμε να μας παρουσιάσει νέες καινοτόμες λύσεις και υπηρεσίες. Ας ρίξουμε μια ματιά στο μέλλον, σε ορισμένα από τα θέματα που αναμένεται να μας καταπλήξουν τα επόμενα χρόνια:

**Cloud:** Το cloud έχει ήδη κάνει αισθητή την παρουσία του στην παγκόσμια αγορά ανοίγοντας νέους δρόμους στην πρόσβαση σε δεδομένα και υπηρεσίες. Η πληροφορία πλέον καθίσταται προσβάσιμη από οποιοδήποτε σημείο και από οποιαδήποτε συσκευή έχει πρόσβαση στο Διαδίκτυο, και οι υπηρεσίες δεν απαιτούν εγκατάσταση, με αποτέλεσμα οι απαιτήσεις για υπολογιστική ισχύ να μειώνονται τόσο για τους ιδιώτες όσο και για τις εταιρείες. Την επόμενη δεκαετία, περιμένουμε ολοένα και περισσότερες υπηρεσίες να μετακινηθούν στο «σύννεφο», και την παρουσίαση online λειτουργικών συστημάτων, κειμενογράφων και άλλων εργαλείων καθημερινής χρήσης, τα οποία θα διατίθενται αποκλειστικά ως cloud services.
**3D Internet:** Με τις τεχνολογίες των monitors να υποστηρίζουν ήδη 3D προβολή, αναμένεται σύντομα το Διαδίκτυο να διαθέτει 3D ιστοσελίδες και εφαρμογές, και τα 3D objects να αντικαταστήσουν τα σημερινά video και φωτογραφίες, δίνοντας ένα νέο πρόσωπο στο Διαδίκτυο.
**IPTV:** Όλες οι νέες συσκευές τηλεόρασης διαθέτουν σύνδεση στο Διαδίκτυο και οι υπηρεσίες broadcasting μέσω Διαδικτύου καλύπτουν πλέον πλήρως τις ανάγκες για μετάδοση εικόνας. Με βάση τα παραπάνω και ακολουθώντας το ραδιόφωνο, έχοντας ήδη τα πρώτα δείγματα στην αγορά, η τηλεόραση αναμένεται να μεταλλαχθεί ίσως και εξ ολοκλήρου σε Internet TV.
**E-learning – τηλεεργασία:** Δύο εφαρμογές τού Διαδικτύου που βρίσκονται πολύ καιρό σε αναμονή, αναμένεται να έλθουν στο προσκήνιο, μειώνοντας τα κόστη μετακίνησης και τα κόστη συντήρησης των εταιρειών.
**Νανοτεχνολογία:** Η νανοτεχνολογία ήδη βρίσκει εφαρμογή σε πάρα πολλούς τομείς και τα τελευταία πειράματα δείχνουν ότι συσκευές όπως οι μοριακοί υπολογιστές δεν αποτελούν πλέον άπιαστο όνειρο. Δεν αποκλείεται, λοιπόν, πολύ σύντομα οι χρήστες να διαθέτουν πανίσχυρους υπολογιστές σε ένα ρολόι χειρός ή ένα απλό ακουστικό.
**Πλήρης διασύνδεση:** Ακολουθώντας την πρόβλεψη του Bill Gates («Every device in the world will be connected») και με το IPv6 να τίθεται ήδη σε εφαρμογή σε ορισμένες χώρες της Ευρώπης, σύντομα όλες οι συσκευές θα διασυνδεθούν σε ένα υπερδίκτυο, το οποίο θα περιλαμβάνει τις οικιακές ηλεκτρικές συσκευές, τα αυτοκίνητα, τα κινητά τηλέφωνα και κάθε φορητή ή οικιακή συσκευή.
**4G, 5G και ακόμα πιο πέρα:** Ήδη από το 2009, το 4G είναι πραγματικότητα. Με τις εξελίξεις στον τομέα mobile broadband να καλπάζουν, οι επόμενες γενιές κινητών δικτύων δεν θα αργήσουν να ακολουθήσουν.

# #νομοθεσία_στο_διαδίκτυο


## ΔΙΑΔΙΚΤΥΟ

Στην ελληνική νομοθεσία δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του Διαδικτύου από άποψη Ποινικού Δικαίου.
Το μεγαλύτερο μέρος των αδικημάτων που προβλέπονται και τιμωρούνται από τον ελληνικό Ποινικό Κώδικα, πλέον διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes) αλλά και μέσω του Διαδικτύου (Internet). Σε αυτές τις περιπτώσεις εφαρμόζονται κατ' αναλογία είτε οι διατάξεις του Ποινικού Κώδικα είτε ειδικοί Ποινικοί Νόμοι.

## ΠΟΙΝΙΚΟΣ ΚΩΔΙΚΑΣ

Άρθρο **292Α** «Εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών»
Άρθρο **348Α** «Πορνογραφία Ανηλίκων»
Άρθρο **348Β** «Προσέλκυση παιδιών για γενετησίους λόγους»
Άρθρο **348Γ** «Πορνογραφικές παραστάσεις ανηλίκων»
Άρθρο **361** «Εξύβριση»
Άρθρο **362** «Δυσφήμιση»
Άρθρο **363** «Συκοφαντική δυσφήμιση»
Άρθρο **370** «Παραβίαση του απορρήτου των επιστολών»
Άρθρο **370Α** «Παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας»
Άρθρο **370Β** «Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα»
Άρθρο **370Γ** «Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών»
Άρθρο **385** «Εκβίαση»
Άρθρο **386Α** «Απάτη με υπολογιστή»



## ΝΟΜΟΙ ΚΑΙ ΠΡΟΕΔΡΙΚΑ ΔΙΑΤΑΓΜΑΤΑ

### Ηλεκτρονικές Επικοινωνίες - Τηλεπικοινωνίες

**Νόμος 2867/2000** «Οργάνωση και λειτουργία του τομέα των τηλεπικοινωνιών»
**Νόμος 3431/2006** «Περί ηλεκτρονικών επικοινωνιών και άλλες διατάξεις»
**Νόμος 3783/2009** «Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις»

### Πνευματική Ιδιοκτησία

**Νόμος 2121/1993** «Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα»

### Προσωπικά Δεδομένα

**Νόμος 2472/1997** «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»
**Νόμος 3471/2006** «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Ν. 2472/97»

### Παίγνια

**Νόμος 2433/1996** «Ρύθμιση θεμάτων ΟΠΑΠ και άλλες διατάξεις»
**Νόμος 4002/2011** «Ρύθμιση της αγοράς παιγνίων»

### Απόρρητο των επικοινωνιών

**Νόμος 2225/1994** «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας» όπως έχει τροποποιηθεί έως σήμερα
**Π.Δ. 47/2005** «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του»
**Νόμος 3674/2008** «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις»

### Διατήρηση Δεδομένων

**Νόμος 3917/2011** «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις»

Σύμφωνα με τον ανωτέρω νόμο οι εταιρείες παροχής υπηρεσιών Διαδικτύου **δεν** διατηρούν στοιχεία συνδρομητών και δεδομένα που αντιστοιχούν και σε ηλεκτρονικά ίχνη, πέραν του διαστήματος των δώδεκα (12) μηνών από την ημερομηνία της επικοινωνίας.

### Ηλεκτρονικό Εμπόριο

**Π.Δ. 150/2001** «Ηλεκτρονικές υπογραφές»
**Π.Δ. 131/2003** «Ηλεκτρονικό εμπόριο κ.λπ.»

### Καταπολέμηση ορισμένων μορφών και εκδηλώσεων ρατσισμού και ξενοφοβίας μέσω του ποινικού δικαίου και μέσω Διαδικτύου

**Νόμος 4285/2014** «Τροποποίηση του Ν. 927/1979 (Α΄ 139) και προσαρμογή του στην απόφαση-πλαίσιο 2008/913/ΔΕΥ της 28ης Νοεμβρίου 2008, για την καταπολέμηση ορισμένων μορφών και εκδηλώσεων ρατσισμού και ξενοφοβίας μέσω του ποινικού δικαίου»

# ΓΝΩΜΟΔΟΤΗΣΕΙΣ

-**Υπ' αριθμ. 9 από 29-06-2009 Γνωμοδότηση του Εισαγγελέα Α.Π. κ. Γ. Σανιδά**, όπου διασαφηνίστηκε ότι: **1)** Το απόρρητο των επικοινωνιών **δεν καλύπτει** α) **την επικοινωνία μέσω του Διαδικτύου (Internet)** και β) **τα εξωτερικά στοιχεία της επικοινωνίας (ονοματεπώνυμα και λοιπά στοιχεία συνδρομητών, αριθμοί τηλεφώνων, χρόνος και τόπος κλήσεως, διάρκεια συνδιάλεξης κ.λπ.). 2)** Οι εισαγγελικές, ανακριτικές και προανακριτικές αρχές, πολύ δε περισσότερο τα Δικαστικά Συμβούλια και τα Δικαστήρια, **δικαιούνται να ζητούν από τους παρόχους των υπηρεσιών επικοινωνίας μέσω του Διαδικτύου (Internet) τα ηλεκτρονικά ίχνη μιας εγκληματικής πράξεως, την ημεροχρονολογία και τα στοιχεία του προσώπου στο οποίο αντιστοιχεί το ηλεκτρονικό ίχνος**, από τους λοιπούς δε παρόχους των υπηρεσιών επικοινωνίας τα **«εξωτερικά στοιχεία» της επικοινωνίας, και ο πάροχος υποχρεούται να τα παραδίδει χωρίς να είναι αναγκαίο να προηγηθεί άδεια κάποιας Αρχής και ιδία της ΑΔΑΕ. 3)** Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών αλλά και οποιαδήποτε άλλη Ανεξάρτητη Αρχή ούτε νομιμοποιείται ούτε δικαιούται να ελέγξει με οποιονδήποτε τρόπο, αμέσως ή εμμέσως, το εάν η περί άρσεως ή μη του απορρήτου απόφαση των οργάνων της Δικαιοσύνης είναι σύννομη ή όχι.

-**Υπ' αριθμ. 12/2009 Γνωμοδότηση του Εισαγγελέα Α.Π. κ. Ι. Τέντε**, με την οποία **παγιώθηκε** η θέση της Εισαγγελίας του Αρείου Πάγου στο συγκεκριμένο ζήτημα. Ειδικότερα στην εν λόγω τελευταία επί του θέματος Γνωμοδότηση αναφέρονται τα εξής ενδιαφέροντα: **α)** «...Οι περιπτώσεις που ενδιαφέρουν στο προκείμενο, ήτοι οι περιπτώσεις στις οποίες οι ανακριτικές αρχές για την εντόπιση του δράστη εξυβριστικών, συκοφαντικών, απειλητικών, εκβιαστικών τηλεφωνικών κλήσεων ή μηνυμάτων, κατά τη διενέργεια προκαταρκτικής εξετάσεως, προανακρίσεως ή κυρίας ανακρίσεως, κατόπιν εγκλήσεως κατά κανόνα του παθόντος, δέκτη των εν λόγω κλήσεων κ.λπ., ζητούν την ανακοίνωση εκ μέρους των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών στοιχείων σχετικών με την ταυτότητα ή τη θέση της συνδέσεως ή του χρήστη, εκφεύγουν του προστατευτικού πεδίου της διατάξεως του άρθρου 19 §1 του Συντάγματος. Στις προαναφερόμενες περιπτώσεις δεν πρόκειται για επικοινωνία ή ανταπόκριση κατά την έννοια της συνταγματικής διατάξεως. Οι επαφές αυτές ως εκ του σκοπού και του περιεχομένου τους, το οποίο είναι ευθέως εγκληματικό (Καρράς, Ποινικό Δικονομικό Δίκαιο αριθ. 705), αφενός δεν συνιστούν "ανταλλαγή απόψεων, διανοημάτων κ.λπ." και αφετέρου δεν γίνονται στο πλαίσιο σχέσεως οικειότητας και εμπιστευτικότητας (Χρυσογόνος, ανωτ. σελ. 260, Τσακυράκης, ανωτ. σελ. 997, 998). Επομένως, δεν συντρέχει ο δικαιολογητικός λόγος προστασίας του απορρήτου, δηλαδή η διαφύλαξη του προσώπου από τον κίνδυνο παραβιάσεως της εν ευρεία έννοια προσωπικής ελευθερίας του και της παγιδεύσεώς του με την έκθεσή του σε κάθε είδους συνέπειες από τυχόν υπερβολικές και αστόχαστες εκφράσεις κατά την ιδιωτική και εμπιστευτική επικοινωνία του, και, κατ' ακολουθίαν, η επικοινωνία αυτού του είδους δεν προστατεύεται ως τοιαύτη από το Σύνταγμα και, συνακολούθως, από τη διάταξη του άρθρου 4 §1 του Ν. 3471/2006. **β)** Συνεπώς προς τα ανωτέρω, οι ανακριτικές αρχές, ανταποκρινόμενες στο προστατευτικό καθήκον του Κράτους, εκδηλούμενο ως θετική υποχρέωση αυτού προς διασφάλιση της ανεμπόδιστης και αποτελεσματικής ασκήσεως των δικαιωμάτων του ατόμου, κατ' άρθρο 25 §1 του Συντάγματος, και ενεργούσες σύμφωνα με τη συνταγματική επιταγή για παροχή έννομης προστασίας (άρθρο 20 του Συντάγματος) και τιμωρήσεως των εγκλημάτων (άρθρα 96 §1 και 87 §1 του Συντάγματος) μπορούν, στα πλαίσια του δικαιώματός τους να συγκεντρώνουν τα αναγκαία αποδεικτικά στοιχεία για τη βεβαίωση του εγκλήματος (άρθρα 251, 239 §§1-2 και 248 ΚΠΔ), **να ζητούν τα προαναφερόμενα στοιχεία, χωρίς την προηγούμενη τήρηση της διαδικασίας άρσεως του απορρήτου** του εκτελεστικού της διατάξεως του άρθρ. 19 §1 εδ. Β' του Συντάγματος Ν. 2225/1994, αφού, όπως ελέχθη, δεν πρόκειται για απόρρητο. **γ)** Είναι αυτονόητο ότι πρέπει να διενεργείται κυρία ανάκριση ή προκαταρκτική εξέταση ή προανάκριση μετά από παραγγελία εισαγγελέα καθώς και ότι ο τακτικός ανακριτής ή ο παραγγέλλων εισαγγελέας, σύμφωνα με βασική αρχή ισχύουσα επί των ανακρίσεων, θα ζητήσει τα στοιχεία για τα οποία γίνεται λόγος, αφού, μετά τήρηση των αρχών της αναλογικότητας, κρίνει ότι, βάσει των στοιχείων που μέχρι τη στιγμή εκείνη διαθέτει, είναι δυνατόν να υποτεθεί ευλόγως ότι μόνο με αυτό το μέσο θα γίνει δυνατή η βεβαίωση του εγκλήματος και η ανακάλυψη του δράστη (Καρράς, ανωτ., αριθ. 44)...».

-**Υπ' αριθμ. 9/2011 Γνωμοδότηση του Εισαγγελέα Α.Π. κ. Α. Κατσιρώδη** (επιβεβαιώνει τα προαναφερόμενα)

-**Υπ' αριθμ. 5058 από 14-12-2012 Γνωμοδότηση-παραγγελία του Εισαγγελέα Α.Π. κ. Ι. Τέντε.**

**Αποφάσεις**

Νέος **Κανονισμός Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr**

Απόφαση **750/2** (19-02-2015) της **Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)** που τέθηκε σε ισχύ στις 24 Μαρτίου 2015.

# ΣΥΝΘΗΚΕΣ

Οι αξιόποινες πράξεις που λαμβάνουν χώρα στο Διαδίκτυο δημιουργούν πλήθος νομικών προβλημάτων λόγω της περίπλοκης λειτουργίας των **υπολογιστών** καθώς και λόγω των ιδιαιτεροτήτων του **Διαδικτύου**. Ακριβώς τα προβλήματα αυτά επιχειρεί να επιλύσει και η **Σύμβαση για το Κυβερνοέγκλημα**.

Με τη Συνθήκη του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-Crime), η οποία υπογράφηκε στις 23 Νοεμβρίου 2001 στη Βουδαπέστη και η οποία σημειωτέον δεν έχει κυρωθεί ακόμη από την Ελλάδα, επιχειρείται η **χάραξη κοινής αντεγκληματικής πολιτικής** και η υιοθέτηση από τα **συμβαλλόμενα κράτη νομοθετικών μέτρων προκειμένου να αντιμετωπιστούν από κοινού τα εγκλήματα που τελούνται στον Κυβερνοχώρο.**

# #cyberbullying

Όταν η ψυχολογική βία στο
Διαδίκτυο απειλεί κάθε παιδί


## ΤΙ ΕΙΝΑΙ ΤΟ CYBERBULLYING

Ίσως έχει τύχει σε εσένα ή σε κάποιο φίλο σου να δείτε μια παραλλαγμένη φωτογραφία σας στο Διαδίκτυο ή να έχετε δεχθεί ένα προσβλητικό μήνυμα. Τα παραπάνω είναι **περιστατικά ψηφιακής παρενόχλησης** και, όσο αστεία κι αν είναι γι' αυτόν που τα έκανε ή για τα άτομα που τα είδαν, δεν φαίνονται καθόλου αστεία σε αυτούς που προσβάλλονται.

Η ψηφιακή παρενόχληση (cyberbullying) **είναι οποιαδήποτε επαναλαμβανόμενη πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς, που πραγματοποιείται μέσω της χρήσης ψηφιακών συσκευών (Η/Υ, κινητών τηλεφώνων)**. Η ψηφιακή παρενόχληση είναι εσφαλμένη και απαράδεκτη συμπεριφορά. Δεν πρέπει σε καμία περίπτωση να παραβλέπεται ή να αγνοείται.

Το φαινόμενο γνωρίζει έξαρση τον τελευταίο καιρό παγκοσμίως και δεν είναι λίγα τα περιστατικά και στη χώρα μας.
Το φαινόμενο του **cyberbullying** είναι περίπλοκο, καθώς μπορεί το bullying να έχει «αντικαταστήσει» κατά μία έννοια την παλιά «καζούρα» στα σχολεία, όμως έχει εντελώς διαφορετικά στοιχεία. Ο ψηφιακός εκφοβισμός μοιάζει πολύ με τον απλό εκφοβισμό, αφού υπάρχει θύτης, θύμα και παρατηρητές. Έχει, όμως, και μερικές διαφορές όπως:

- Μπορεί να φτάσει σε πολύ λίγο χρόνο σε πολλούς παραλήπτες.
- Τα ηλεκτρονικά μηνύματα είναι σχεδόν αδύνατον να ελεγχθούν.
- Ο θύτης νιώθει ότι μπορεί να παραμείνει ανώνυμος.
- Η έλλειψη προσωπικής επαφής με το θύμα κάνει το δράστη σκληρότερο.
- Το θύμα πλήττεται στο σπίτι και στον προσωπικό του χώρο.



## ΤΙ ΕΙΝΑΙ ΤΟ CYBERBULLYING

**Τα μέσα που χρησιμοποιούνται για την παρενόχληση μέσω Διαδικτύου είναι:**

- το ηλεκτρονικό ταχυδρομείο (e-mail)
- τα γραπτά μηνύματα
- μέσα κοινωνικής δικτύωσης (social media)
- δωμάτια επικοινωνίας (chat rooms)
- ιστολόγια (blogs)
- διαδικτυακά παιχνίδια (Internet gaming)

### Πώς εκδηλώνεται το cyberbullying

Αυτοί που ασκούν εκφοβισμό χρησιμοποιούν τις νέες τεχνολογίες για να παρενοχλήσουν, να απειλήσουν, να εκφοβίσουν, να δυσφημήσουν και, σε μερικές περιπτώσεις, να υποδυθούν τρίτους ή να υποκλέψουν την ταυτότητά τους. Μερικές από τις πιο κοινές μεθόδους είναι οι εξής:

- Αποστολή κειμένων, e-mail ή άμεσων μηνυμάτων με προσβλητικό περιεχόμενο (σε instant messengers ή chat rooms).
- Κακόβουλη δημοσίευση φωτογραφιών σε μέσα κοινωνικής δικτύωσης (social networks), ιστολόγια (blogs) ή άλλες ιστοσελίδες με μοναδικό σκοπό την παρενόχληση.
- Διάδοση φημών και ψευδών γεγονότων με σκοπό τη δυσφήμηση σε τρίτους σε μέσα κοινωνικής δικτύωσης, ιστολόγια, ιστοσελίδες κ.λπ.
- Ανώνυμες κλήσεις και μηνύματα με σκοπό την πρόκληση φόβου και ταραχής.
- Χρήση του ονόματος ξένου χρήστη με σκοπό τη διάδοση φημών και ψεμάτων για κάποιον τρίτο (κλοπή ταυτότητας).
- Δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας άλλους να δημοσιεύσουν μηνύματα μίσους.
- Αποστολή ειδικών προγραμμάτων trojan horses (δούρειοι ίπποι) με σκοπό να δημιουργήσουν πρόβλημα μέσω της υποκλοπής κωδικών.
- Εκφοβισμός στη διάρκεια ενός διαδραστικού παιχνιδιού.

## ΠΡΟΦΙΛ ΘΥΤΗ-ΘΥΜΑΤΟΣ

Ο καθένας μας μπορεί να πέσει θύμα ψηφιακής παρενόχλησης. Μπορεί να γίνει και θύτης ή ακόμη πιο συχνά να γίνει παρατηρητής.
Η ψηφιακή παρενόχληση ίσως ελκύει παιδιά που δεν έχουν παρενοχλήσει ποτέ στην πραγματική ζωή, επειδή πιστεύουν ότι είναι ανώνυμα όταν χρησιμοποιούν το Διαδίκτυο ή το κινητό τους. Θα μπορούσαν να κάνουν πράγματα που δεν θα διανοούνταν να τα διαπράξουν πρόσωπο με πρόσωπο, και να χρησιμοποιήσουν τις νέες τεχνολογίες για να αναστατώσουν εσκεμμένα ένα φίλο, έναν άγνωστο, ακόμα κι ένα δάσκαλο. Πολλές φορές μπορεί ακόμα και να ενδώσουν στην πίεση συνομηλίκων τους και να προωθήσουν ένα e-mail με εκφοβιστικό περιεχόμενο δίχως να αναλογιστούν τις συνέπειες.

### Για ποιους λόγους μπορεί κάποιος να εκφοβίζει μέσω του Διαδικτύου;

- Ανάγκη για επιβολή
- Θυμός
- Ζήλια
- Διασκέδαση
- Ψυχολογική καταπίεση
- Αντεκδίκηση
- Ανάγκη για προσοχή

### Πώς αισθάνονται τα θύματα;

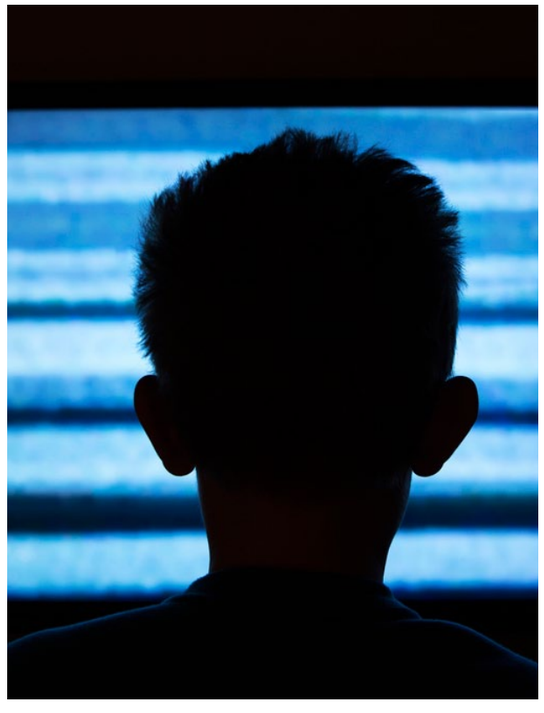
- Θυμό
- Αγανάκτηση
- Θλίψη
- Ντροπή
- Φόβο

### Συνέπειες

Το cyberbullying φαντάζει ίσως αθώο αστείο, μπορεί να έχει, όμως, πολύ σοβαρές συνέπειες όπως:

- Αποχή από τα μαθήματα
- Απότομη πτώση στις σχολικές επιδόσεις
- Εκτέλεση πράξεων αντίθετων με το χαρακτήρα του παιδιού ή παράνομες πράξεις λόγω εκβιασμού
- Κατάθλιψη
- Αυτοκτονία

Χαρακτηριστική είναι η περίπτωση της 13χρονης Megan από τις Η.Π.Α., που έπασχε από κατάθλιψη και η οποία αυτοκτόνησε όταν ο διαδικτυακός της φίλος Josh την «παράτησε». Αποδείχτηκε ότι ο φίλος ήταν στην πραγματικότητα η μητέρα μιας φίλης με την οποία η Megan είχε τσακωθεί...

# ΠΡΟΦΙΛ ΘΥΤΗ-ΘΥΜΑΤΟΣ

### Τρόποι δράσης

Σε περίπτωση που έχεις πέσει θύμα εκφοβισμού μέσω Διαδικτύου, τότε πρέπει να προβείς σε μια σειρά ενεργειών:

- Απόφυγε να απαντήσεις στις απειλές του δράστη. Απαντώντας επιθετικά φέρνουμε νέες απειλές και την ικανοποίηση στο δράστη ότι η παρενόχληση λειτουργεί.
- Άλλαξε λογαριασμό e-mail ή «κατέβασε» τη σελίδα δικτύωσης και, αν είναι εφικτό, δημιούργησε νέους λογαριασμούς.
- Διατήρησε αποδεικτικά της δράσης συμπεριλαμβάνοντας όσα περισσότερα στοιχεία μπορείς όπως ημερομηνίες και ώρες, λογαριασμούς ηλεκτρονικού ταχυδρομείου και λοιπά. Καλό θα είναι τα στοιχεία αυτά να υπάρχουν και σε εκτυπωμένη μορφή.
- Αφαίρεσε από τις λίστες των «φίλων» αυτόν που σε παρενόχλησε, και ρύθμισε το προφίλ κοινωνικής δικτύωσης ώστε να είναι «απόρρητο», αν δεν είναι ήδη.
- Εάν ο θύτης είναι γνωστό σου πρόσωπο, ζήτησέ του να σβήσει τα μηνύματα και να αποκαταστήσει την αλήθεια σε περίπτωση διάδοσης φημών. Είναι σημαντικό να ενημερωθούν οι γονείς του παιδιού για τη συμπεριφορά του, με βασικό σκοπό να περιοριστεί ο θύτης.
- Σε περίπτωση που η παρενόχληση πραγματοποιηθεί σε κάποια ιστοσελίδα κοινωνικής δικτύωσης (π.χ. Facebook, Hi5), κάνε αναφορά για το περιστατικό στους διαχειριστές της ιστοσελίδας.
- Μην κρατάς τους εκφοβισμούς για τον εαυτό σου. Δεν είσαι μόνος! Πρέπει οπωσδήποτε να αναφέρεις το περιστατικό σε έναν ενήλικα, είτε πρόκειται για γονείς είτε για κάποιον εκπαιδευτικό ή άλλο κοντινό και έμπιστο άτομο, και φυσικά να το καταγγείλεις, ακόμα και μόνος σου, καλώντας τη Δίωξη Ηλεκτρονικού Εγκλήματος στο 11188.

### Σε περίπτωση που ο εκφοβισμός πραγματοποιηθεί μέσω κάποιας ιστοσελίδας κοινωνικής δικτύωσης ή chat room:

- **Facebook:** Εάν κάποιος χρήστης σάς ενοχλεί στο Facebook, αναφέρετέ τον πατώντας την επιλογή «Αναφορά/Μπλοκάρισμα» (Report/Block) που βρίσκεται στο προφίλ του. Στο μενού ενεργειών τής αναφοράς μπορείτε να δηλώσετε την αιτία της αναφοράς, π.χ. παριστάνει εσάς (κλοπή ταυτότητας), σας προσβάλλει. Μπορείτε, επίσης, να επιλέξετε να μπλοκάρετε κάποιο χρήστη που σας ενοχλεί, ώστε να μη λαμβάνετε μηνύματά του. Ένας καλός οδηγός ασφαλείας για παιδιά και γονείς βρίσκεται στο www.facebook.com/safety. Οι χρήστες κάτω των 13 ετών απαγορεύονται και μπορείτε να αναφέρετε την ύπαρξή τους στο **https://www.facebook.com/help/157793540954833**.
  Επίσης, στο **www.facebook.com/help/215543298568604/** μπορείτε να βρείτε τη διαδικασία επαναφοράς «κλεμμένου» λογαριασμού Facebook.
- MySpace: Οδηγός ασφαλείας βρίσκεται στο www.myspace.com/safety.
- Youtube: Εάν υπάρχει «ανεβασμένο» κάποιο κακόβουλο βίντεο, μπορείτε να το αναφέρετε πατώντας την επιλογή «Report» που βρίσκεται κάτω από το βίντεο.
- Instant messaging: MSN-Yahoo: Επιλέγοντας το «Help tab» θα ανοίξετε πολλαπλές επιλογές, μία εκ των οποίων είναι το «Report Abuse».
- Chat rooms: Στη συντριπτική πλειοψηφία τους υπάρχουν ρυθμιστές (moderators) που είναι συνήθως πολύ αυστηροί με περιπτώσεις κακόβουλης επίθεσης. Καλό θα ήταν να επικοινωνήσετε μαζί τους μέσω e-mail αναφέροντας το συγκεκριμένο πρόβλημα.

# ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

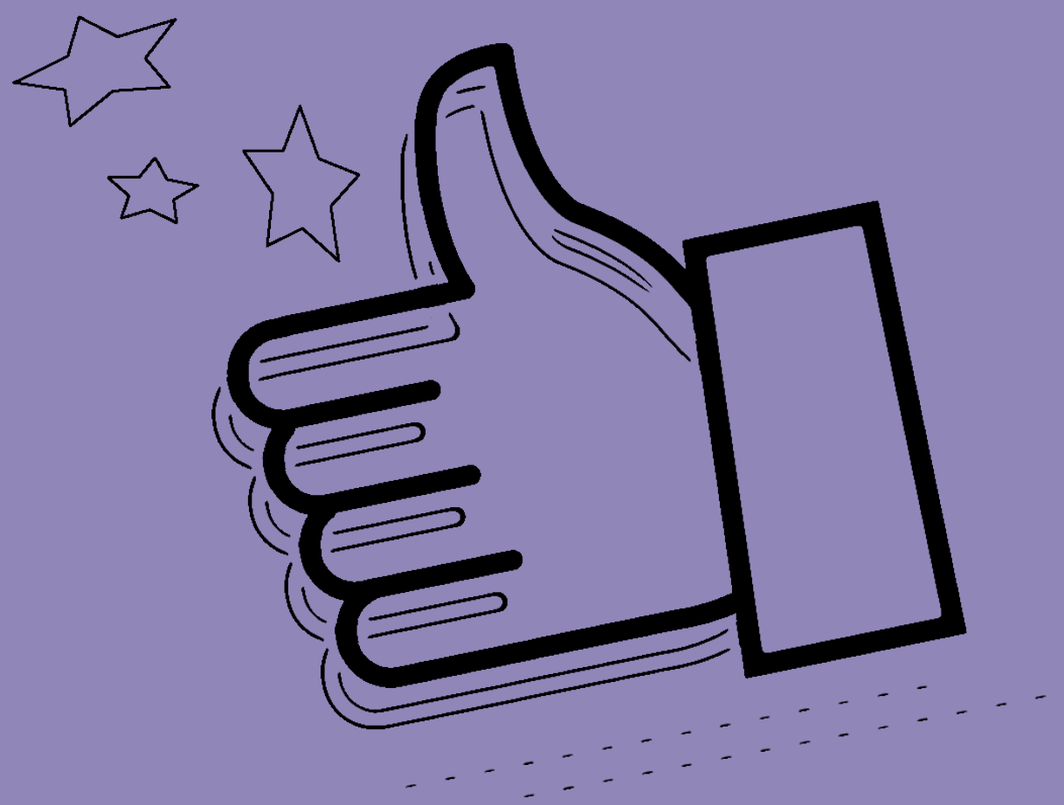
- Προστασία προσωπικών δεδομένων από ιστοσελίδες κοινωνικής δικτύωσης. Περιορίζοντας τις διαθέσιμες πληροφορίες για τον εαυτό μας ή την οικογένειά μας μειώνουμε τις πιθανότητες να πέσουμε θύματα άγνωστων δραστών.
- Δεν είναι σωστό να κάνουμε φίλους τους πάντες σε ιστοσελίδες κοινωνικής δικτύωσης.
- Να συμπεριφέρεστε στους άλλους online, όπως θα κάνατε στην πραγματική ζωή. Αν κάποιος σας αντιμετωπίζει με αγένεια ή είναι απότομος, μην απαντάτε. Θα δει ότι δεν έχει αποτελέσματα και θα σταματήσει τα προσβλητικά μηνύματα. Αν όχι και τα καταχρηστικά μηνύματα συνεχίζονται, ζητήστε βοήθεια από έναν έμπιστο ενήλικα.
- Ποτέ μην ανοίγετε ένα μήνυμα από κάποιον που δεν γνωρίζετε.
- Διαγράψτε περίεργα μηνύματα ηλεκτρονικού ταχυδρομείου ή γραπτά μηνύματα από ανθρώπους που δεν γνωρίζετε. Σε περίπτωση αμφιβολίας, ζητήστε συμβουλές από έναν έμπιστο ενήλικα.
- «Google yourself!». Χρησιμοποιήστε μια μηχανή αναζήτησης ανά τακτά διαστήματα και πραγματοποιήστε αναζήτηση με το όνομά σας ή το ψευδώνυμο που χρησιμοποιείτε στο Διαδίκτυο. Έτσι θα μπορείτε να εποπτεύετε την εικονική σας παρουσία.
- Δεν χρειάζεται να είστε «πάντα συνδεδεμένοι» - αποσυνδεθείτε και κλείστε τον υπολογιστή. Δώστε στον εαυτό σας ένα διάλειμμα. Μη μένετε online για πάρα πολύ χρόνο.
- Βάλτε τη φαντασία σας να δουλέψει όταν δημιουργείτε κωδικούς πρόσβασης. Μη χρησιμοποιείτε κωδικούς που εύκολα μπορεί κανείς να φανταστεί (ημερομηνία γέννησης κ.ά.).
- Αν δείτε κάτι στο Διαδίκτυο ή λάβετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή γραπτό μήνυμα που σας κάνει να αισθανθείτε άβολα, κλείστε τον υπολογιστή ή το τηλέφωνο και ζητήστε συμβουλές από έναν αξιόπιστο ενήλικα.

**Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος δεν ποινικοποιεί το χαμόγελο των παιδιών. Οι παιδικές παρεξηγήσεις δεν είναι cyberbullying. Στο cyberbullying το θύμα αισθάνεται τρόμο, ταραχή, απελπισία, βρίσκεται σε μια οριακή κατάσταση. Οι διαπιστώσεις της Υπηρεσίας είναι ότι τα παιδιά δεν είναι τρομοκρατημένα, αλλά παιδιά με ζωντάνια και αυτοπεποίθηση, που ξέρουν τι θέλουν. Το κλειδί είναι η ενημέρωση και η διαπαιδαγώγηση μέσα από τα σχολεία, ώστε να καταλάβουν τα παιδιά ότι το Internet δεν είναι ανώνυμο. Ο καθένας έχει την ταυτότητά του μέσα στο Διαδίκτυο, η οποία μπορεί να βρεθεί.**



# #social_media_&_facebook

Κίνδυνοι και συμβουλές σχετικά με τα δημοφιλή κοινωνικά δίκτυα στο Internet



## ΤΙ ΕΙΝΑΙ ΟΙ ΙΣΤΟΣΕΛΙΔΕΣ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ;

Πρόκειται για ιστοσελίδες που προσφέρουν στους χρήστες τους τη δυνατότητα να δημιουργήσουν το προσωπικό τους **προφίλ**, να παρουσιάσουν τον εαυτό τους και να επικοινωνήσουν με άλλους χρήστες στο Διαδίκτυο. Οι χρήστες αυτοί μπορεί να είναι γνωστοί από την καθημερινή ζωή τους ή εντελώς άγνωστοι. Μέσα από αυτή την επικοινωνία δημιουργούνται **online κοινότητες**, όπου άνθρωποι με κοινά ενδιαφέροντα μπορούν να μοιράζονται πληροφορίες και να εκφράζουν τις απόψεις τους. Δε χρειάζονται ιδιαίτερες τεχνικές γνώσεις για να δημιουργήσει κανείς το προφίλ του και να ανεβάσει περιεχόμενο (σχόλια, φωτογραφίες, βίντεο), το οποίο θα μοιραστεί αργότερα με άλλους χρήστες.

Οι ιστοσελίδες κοινωνικής δικτύωσης είναι ιδιαίτερα δημοφιλείς στην Ελλάδα, με πιο γνωστές τις: Facebook, Twitter, MySpace, YouTube. Όπως ισχύει γενικά για το Διαδίκτυο, λέμε **ΝΑΙ στη χρήση των Μέσων Κοινωνικής Δικτύωσης**, αλλά ακολουθώντας βασικούς κανόνες.
Η γνώση των κανόνων ασφαλείας, η ανάπτυξη κριτικής και αντιληπτικής ικανότητας και η ικανότητα αναγνώρισης των κινδύνων είναι βασικά εφόδια για την ασφαλή πλοήγησή μας στα Μέσα Κοινωνικής Δικτύωσης.



## ΚΙΝΔΥΝΟΙ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

**Χρήση της πληροφορίας για άλλο σκοπό.**
Στα κοινωνικά δίκτυα ο χρήστης έχει τη λανθασμένη αίσθηση ότι οι πληροφορίες που ανεβάζει είναι διαθέσιμες μόνο στους φίλους του. Στην πραγματικότητα, έχουν πρόσβαση σε αυτές και άλλοι χρήστες της ιστοσελίδας, οι οποίοι μπορούν να τις χρησιμοποιήσουν με σκοπό την καθημερινότητά σας εντός και εκτός του Διαδικτύου. Για παράδειγμα, ένα σχόλιο που απευθύνεται σε φίλους, θα μπορούσε να διαβαστεί από τον εργοδότη σας και να δημιουργήσει λανθασμένες εντυπώσεις για την επαγγελματική σας ζωή.

**Η πληροφορία μένει για πάντα στο Διαδίκτυο.**
Μια φωτογραφία ή ένα σχόλιο που ανεβαίνει σε μια σελίδα κοινωνικής δικτύωσης δημοσιεύεται σε έναν αριθμό χρηστών. Ακόμη κι αν επιλέξετε να αποσύρετε αυτή την πληροφορία, αυτή παραμένει αποθηκευμένη στα αρχεία της εταιρείας όπου ανήκει η σελίδα, απλώς δεν εμφανίζεται στο Διαδίκτυο. Επίσης, οποιοσδήποτε από τους χρήστες τη βλέπει, μπορεί να την αντιγράψει και να τη χρησιμοποιήσει στο μέλλον.

**Αποποίηση των πνευματικών δικαιωμάτων.**
Σε αρκετές από τις ιστοσελίδες κοινωνικής δικτύωσης, όπως το Facebook, τίθεται ως όρος για την εγγραφή του χρήστη η αποποίηση των πνευματικών δικαιωμάτων για το περιεχόμενο που ανεβάζει. Ως αποτέλεσμα, οι φωτογραφίες που δημοσιοποιείτε περνούν στην ιδιοκτησία της εταιρείας που κατέχει την ιστοσελίδα, και μπορούν να χρησιμοποιηθούν από οποιονδήποτε.

**Παρενόχληση - Stalking - Cyberbullying.** Δημοσιοποιώντας πληροφορίες όπως το ονοματεπώνυμο, η διεύθυνση, ο αριθμός τηλεφώνου σας ή ακόμη το όνομα του σχολείου σας ή της επιχείρησης όπου εργάζεστε, κάνετε γνωστή σε κάθε χρήστη την πραγματική σας ταυτότητα. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν από κακόβουλους χρήστες για να σας παρακολουθήσουν ή ακόμη και να σας απειλήσουν. Ιδιαίτερη προσοχή χρειάζεται και κατά τη δημοσιοποίηση φωτογραφιών, οι οποίες μπορούν να παραποιηθούν με ψηφιακό τρόπο και να διανεμηθούν με σκοπό να σας δυσφημίσουν ή να σας απειλήσουν.

**Εντοπισμός θέσης.**
Πολλοί χρήστες επιλέγουν να δημοσιεύσουν στις ιστοσελίδες κοινωνικής δικτύωσης πού βρίσκονται κάθε στιγμή. Είτε γίνεται συνειδητά, με την επιλογή της δημοσίευσης της θέσης μέσα από την ιστοσελίδα, είτε αυτόματα, με τη χρήση εφαρμογών στο κινητό σας, πρέπει να θυμάστε ότι η δημοσίευση της θέσης σας μπορεί να χρησιμοποιηθεί από κακόβουλους χρήστες, από απαγωγείς για να σας εντοπίσουν, ή από επίδοξους διαρρήκτες για να γνωρίζουν πότε λείπετε από το σπίτι.

**Κλοπή Ταυτότητας.**
Πρόκειται για την περίπτωση όπου κάποιος χρήστης του Διαδικτύου παριστάνει εσάς και παραπλανά ή παρενοχλεί άλλους χρήστες. Μπορεί να εκδηλωθεί με δύο τρόπους: α) με την κλοπή του πραγματικού σας προφίλ, β) με τη δημιουργία ενός νέου προφίλ που θα περιλαμβάνει τα δικά σας στοιχεία, όπως ονοματεπώνυμο ή φωτογραφίες.

**Δημοσιοποίηση προσωπικών δεδομένων από τρίτους χρήστες.**
Όσο προσεκτικός κι να είναι ένας χρήστης σχετικά με τις πληροφορίες που δημοσιοποιεί στα μέσα κοινωνικής δικτύωσης, δεν είναι πάντα σε θέση να ελέγξει τις πληροφορίες που άλλοι χρήστες δημοσιοποιούν γι' αυτόν. Για παράδειγμα, ένας φίλος σας μπορεί να δημοσιεύσει στο προφίλ του μια φωτογραφία που μεταξύ άλλων περιλαμβάνει και εσάς, σε άσεμνες πόζες ή σε ένα μέρος που δεν θα θέλατε να ξέρουν άλλοι ότι έχετε επισκεφθεί. Επίσης, δηλώνοντας κάποιος ότι είναι συμμαθητής σας και γνωστοποιώντας το σχολείο που πηγαίνει, αυτομάτως αποκαλύπτει μια διεύθυνση όπου μπορεί κάποιος να σας εντοπίσει.

# ΚΙΝΔΥΝΟΙ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

**Παραχώρηση των δεδομένων σε τρίτες εταιρείες.**
Οι εταιρείες που κατέχουν τις ιστοσελίδες κοινωνικής δικτύωσης έχουν πρόσβαση στις πληροφορίες που δημοσιεύετε σε αυτές, αλλά και σε δεδομένα που προκύπτουν από τη σύνδεσή σας, όπως η διεύθυνση IP, η γεωγραφική περιοχή όπου ανήκετε, και ο browser που χρησιμοποιείτε. Οι πληροφορίες αυτές μπορούν να παραχωρηθούν σε τρίτες εταιρείες και να χρησιμοποιηθούν σε μεθόδους στοχευμένης διαφήμισης.

**Παραχώρηση στοιχείων σε εφαρμογές.**
Σε αρκετές πλατφόρμες κοινωνικής δικτύωσης, πέρα από τη δημοσίευση πληροφορίας στο προφίλ του, ο χρήστης έχει τη δυνατότητα να χρησιμοποιήσει εφαρμογές. Καθώς οι εφαρμογές δεν πιστοποιούνται πάντα για την ασφάλειά τους, ενδέχεται να αποκτούν πρόσβαση σε προσωπικές πληροφορίες από το προφίλ σας, όπως τα στοιχεία διεύθυνσής σας, ή να περιέχουν κακόβουλο λογισμικό (ιούς κ.τ.λ.).

**Εξειδικευμένες απάτες.**
Οι πληροφορίες που δημοσιεύετε στο προφίλ σας μπορούν να χρησιμοποιηθούν από επιτήδειους, ώστε να εξειδικεύσουν τις επιθέσεις ηλεκτρονικού «ψαρέματος» (phishing) τους και να έχουν μεγαλύτερη πιθανότητα να εξαπατήσουν εσάς ή τους φίλους σας.

# ΣΥΜΒΟΥΛΕΣ ΠΡΟΣΤΑΣΙΑΣ

**Προσωπικά δεδομένα**
- Μη δημοσιεύετε πληροφορίες που μπορεί να βοηθήσουν κάποιον άγνωστο να σας εντοπίσει. Η διεύθυνση και το τηλέφωνό σας, η επιχείρηση όπου εργάζεστε ή το σχολείο στο οποίο φοιτάτε, μπορεί να χρησιμοποιηθούν από αγνώστους για να σας πλησιάσουν.
- Μην ξεχνάτε ότι τη διεύθυνσή σας μπορεί να προδώσουν και οι προσωπικές πληροφορίες των γειτόνων ή των συμμαθητών σας. Μη δημοσιεύετε φωτογραφίες με ευκρινή τα στοιχεία διεύθυνσής σας.
- Μη χρησιμοποιείτε τα μέσα κοινωνικής δικτύωσης ως ημερολόγιο. Το προφίλ σας δεν είναι ανάγκη να περιέχει όλες τις πληροφορίες για την καθημερινή σας δραστηριότητα.
- Ελέγξτε τις ρυθμίσεις ασφαλείας και απορρήτου για το προφίλ σας. Ρυθμίστε τες έτσι ώστε οι πληροφορίες σας να είναι ορατές μόνο στους φίλους σας.
- Μην επιτρέπετε σε εφαρμογές (applications) που δε γνωρίζετε να χρησιμοποιούν τα στοιχεία του λογαριασμού σας πέρα από το ονοματεπώνυμό σας, εάν δεν είναι απολύτως απαραίτητο για την παρεχόμενη υπηρεσία, ή να δημοσιεύουν σχόλια στο λογαριασμό σας.

**Αποφυγή Καταστάσεων Αμηχανίας**
- Σκεφτείτε πριν δημοσιεύσετε ένα σχόλιο ή μια φωτογραφία. Μήπως θα σας έφερνε σε δύσκολη θέση εάν το έβλεπαν τα μέλη της οικογένειάς σας ή ο μελλοντικός εργοδότης σας;
- Πριν δημοσιεύσετε μια πληροφορία στα μέσα κοινωνικής δικτύωσης, σκεφτείτε ότι δε σβήνεται ποτέ από το Διαδίκτυο. Μήπως θα μπορούσε να επηρεάσει αρνητικά τη μελλοντική σας ζωή;
- Ελέγξτε το περιεχόμενο που δημοσιεύουν οι φίλοι σας στα μέσα κοινωνικής δικτύωσης. Μήπως δεν αρμόζει στο προφίλ που θέλετε να προβάλλετε στον υπόλοιπο κόσμο; Θυμηθείτε: «Δείξε μου το φίλο σου, να σου πω ποιος είσαι».
- Σεβαστείτε τους φίλους σας. Εάν η πληροφορία που πρόκειται να δημοσιεύσετε αφορά κάποιο φίλο σας, π.χ. πρόκειται για μια κοινή σας φωτογραφία, επικοινωνήστε μαζί του και ζητήστε την άδειά του για τη δημοσίευση.

**Όχι εμπιστοσύνη σε αγνώστους**
- Μη δέχεστε αιτήματα φιλίας από αγνώστους. Μην εμπιστεύεστε τα στοιχεία που δηλώνει κάποιος στο προφίλ του στα μέσα κοινωνικής δικτύωσης. Το όνομα, η ηλικία, ακόμη και οι φωτογραφίες του προφίλ μπορεί να μην είναι αληθινά.
- Δώστε ιδιαίτερη σημασία στα παιδιά. Μιλήστε τους για τους κινδύνους στα μέσα κοινωνικής δικτύωσης και μην τους επιτρέπετε να συναντούν άτομα που γνώρισαν μέσα από αυτά.
- Όταν δέχεστε αιτήματα φιλίας από άτομα που γνωρίζετε στην πραγματική σας ζωή, επικοινωνήστε τηλεφωνικά μαζί τους και ρωτήστε αν το προφίλ τούς ανήκει, πριν αποδεχθείτε το αίτημα.



**Απόπειρες Απάτης**
- Αν κάποιος φίλος σας επικοινωνήσει μαζί σας και σας ζητήσει χρήματα, επικοινωνήστε πρώτα μαζί του τηλεφωνικά. Ενδέχεται να έχει κλαπεί το προφίλ του από απατεώνες.
- Καμία ιστοσελίδα κοινωνικής δικτύωσης δεν πρόκειται να σας αποστείλει e-mail ζητώντας να επιβεβαιώσετε τον κωδικό σας, συμπληρώνοντάς τον σε κάποια φόρμα. Εάν λάβετε ένα τέτοιο e-mail, πιθανόν να πρόκειται για επίθεση ηλεκτρονικού «ψαρέματος» (phishing).

**Ασφάλεια Λογαριασμού**
- Σιγουρευτείτε ότι ο κωδικός ασφαλείας για το λογαριασμό σας είναι «δυνατός». Μη χρησιμοποιείτε κωδικούς που εύκολα μπορεί κανείς να μαντέψει, όπως η ημερομηνία γέννησής σας.
- Μη χρησιμοποιείτε τον ίδιο κωδικό με άλλους λογαριασμούς, όπως το e-mail σας, και θυμηθείτε να αλλάζετε τον κωδικό σας σε τακτά χρονικά διαστήματα.
- Όπως με κάθε άλλο κωδικό ασφαλείας, μην αποκαλύπτετε τον κωδικό ασφαλείας του προφίλ σας σε τρίτα άτομα και μην τον συμπληρώνετε σε φόρμες στο Διαδίκτυο, εκτός από τη σελίδα του log in. Θυμηθείτε ότι καμία ιστοσελίδα κοινωνικής δικτύωσης δεν πρόκειται να σας αποστείλει e-mail ζητώντας να επιβεβαιώσετε τον κωδικό σας, συμπληρώνοντάς τον σε κάποια φόρμα.
- Αν αντιληφθείτε ότι ο λογαριασμός σας έχει κλαπεί, αναφέρετέ το το συντομότερο στο διαχειριστή του μέσου κοινωνικής δικτύωσης, μέσω της προτεινόμενης από αυτό διαδικασίας (report).
- Μελετήστε τις διαδικασίες προστασίας της ιδιωτικότητας και ασφάλειας λογαριασμού που παρέχει το μέσο κοινωνικής δικτύωσης, και ενεργοποιήστε τες. Εάν μπορείτε να επιλέξετε εναλλακτικούς τρόπους για ανάκτηση του λογαριασμού σας ή περιορισμό των ατόμων που βλέπουν το προφίλ σας, επιλέξτε το όταν δημιουργείτε το λογαριασμό σας. Επισκεφτείτε τις ρυθμίσεις του λογαριασμού σας ανά τακτά χρονικά διαστήματα για να ανακαλύψετε νέες προσφερόμενες υπηρεσίες.

**Όροι χρήσης**
- Πριν δημιουργήσετε λογαριασμό σε κάποια σελίδα κοινωνικής δικτύωσης, διαβάστε προσεχτικά τους όρους χρήσης και την πολιτική ασφαλείας της. Σε αυτά μπορεί να περιλαμβάνεται ο όρος ότι αποποιείστε των πνευματικών δικαιωμάτων για το περιεχόμενο που δημοσιεύετε, ή το δικαίωμα της εταιρείας να παραχωρεί σε τρίτες εταιρείες στοιχεία που σας αφορούν. Αν δεν συμφωνείτε με τους όρους χρήσης, μην προχωρήσετε στη δημιουργία του λογαριασμού.
- Ξαναδιαβάστε τους όρους χρήσης και την πολιτική ασφαλείας ανά τακτά χρονικά διαστήματα. Κατά τη δημιουργία του λογαριασμού σας έχετε αποδεχθεί ότι ενδέχεται να αλλάξουν χωρίς προειδοποίηση.

# FACEBOOK

Είναι η πιο γνωστή ιστοσελίδα κοινωνικής δικτύωσης, με πάνω από 1 δισεκατομμύριο χρήστες σε όλο τον κόσμο.

- Ξεκίνησε το 2004 ως μια σελίδα για να επικοινωνούν φίλοι και συγγενείς. Εξελίχθηκε σε εταιρεία παγκόσμιου βεληνεκούς με αποκορύφωμα την εισαγωγή της στο χρηματιστήριο της Νέας Υόρκης τον Μάιο 2012.
- Η έδρα της εταιρείας βρίσκεται στην Καλιφόρνια των Η.Π.Α. Παρόλο που το περιεχόμενο της σελίδας έχει μεταφραστεί στα Ελληνικά, δεν υπάρχει αντιπρόσωπος της εταιρείας στην Ελλάδα.
- Βάσει των όρων χρήσης της ιστοσελίδας, συμφωνείτε στη μεταβίβαση και επεξεργασία των δεδομένων σας στις Η.Π.Α.
- Οι βασικές υπηρεσίες που παρέχει η πλατφόρμα της Facebook αφορούν τη δημιουργία ενός προφίλ ή χρονολογίου (timeline) από κάθε χρήστη και τη σύνδεσή του με άλλους χρήστες που ονομάζονται «φίλοι».

# ΧΡΗΣΙΜΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

- Κάθε χρήστης έχει τη δυνατότητα να οργανώνει τους φίλους του σε ομάδες και να ρυθμίζει ποιες από τις πληροφορίες του θα βλέπουν. Εάν δεν ορίσει κάτι διαφορετικό στις ρυθμίσεις απορρήτου τού λογαριασμού του, τότε αυτές οι πληροφορίες μπορεί να είναι δημόσια ορατές.
- Βάσει των όρων χρήσης του, το Facebook επιτρέπει μόνο σε χρήστες άνω των 13 ετών να γίνουν μέλη του.
- Κάθε χρήστης που δημιουργεί προφίλ στο Facebook αποδέχεται τους όρους χρήσης, στους οποίους αναλύονται μια σειρά από θέματα που αφορούν τη νομική του σχέση με την εταιρεία Facebook. Μέσα σε αυτά αποδέχεται και ότι η εταιρεία διατηρεί το δικαίωμα να αλλάξει τους όρους χρήσης, χωρίς να τον ενημερώσει.
- Σύμφωνα με τους όρους χρήσης του Facebook κάθε χρήστης εισάγει το πραγματικό του ονοματεπώνυμο και τα πραγματικά του στοιχεία. Στην πραγματικότητα όμως δεν υπάρχει μηχανισμός που να ελέγχει την ταυτότητα ενός νέου χρήστη. Σε περίπτωση που η εταιρεία ανακαλύψει ότι κάποιος χρήστης έχει δηλώσει ψεύτικα στοιχεία, διατηρεί το δικαίωμα να κλείσει το προφίλ του.
- Η εταιρεία Facebook δηλώνει ρητά στους όρους χρήσης ότι δεν μπορεί να εγγυηθεί για την ασφάλεια του λογαριασμού κάθε χρήστη.
- Μέσα από την πλατφόρμα του Facebook κάθε χρήστης μπορεί να χρησιμοποιήσει εφαρμογές από τρίτες οντότητες. Με αυτό τον τρόπο δίνει πρόσβαση στα προσωπικά του στοιχεία σε εταιρείες εκτός της Facebook.
- Η Facebook διατηρεί το δικαίωμα να χρησιμοποιήσει το προφίλ ενός χρήστη σε διαφημίσεις που λαμβάνουν χώρα στη σελίδα της, εάν εκείνος δεν δηλώσει ρητά ότι δεν το επιθυμεί. Επίσης, επιφυλάσσεται του δικαιώματός της να παραχωρήσει στο μέλλον το όνομα και τη φωτογραφία ενός χρήστη σε άλλες εταιρείες, για διαφημίσεις εκτός του Facebook.
- Παράλληλα με τις πληροφορίες που δηλώνει κανείς στο προφίλ του, η Facebook διατηρεί το δικαίωμα να συγκεντρώνει και άλλα στοιχεία για κάθε λογαριασμό, όπως η IP διεύθυνση από τις συνδέσεις του και ο browser που χρησιμοποιεί. Με αυτό τον τρόπο μπορεί να εξαγάγει περισσότερη πληροφορία, όπως π.χ. τη γεωγραφική θέση ενός χρήστη.
- Η Facebook συνεργάζεται με τις αστυνομικές Αρχές σε όλο τον κόσμο, έπειτα από επίσημη νομική διαδικασία (αίτημα δικαστικής συνδρομής ή υπό περιπτώσεις με εισαγγελική παραγγελία). Η παροχή στοιχείων βασίζεται στις αρχές της αστυνομικής συνεργασίας και στο νομικό πλαίσιο της Καλιφόρνιας.

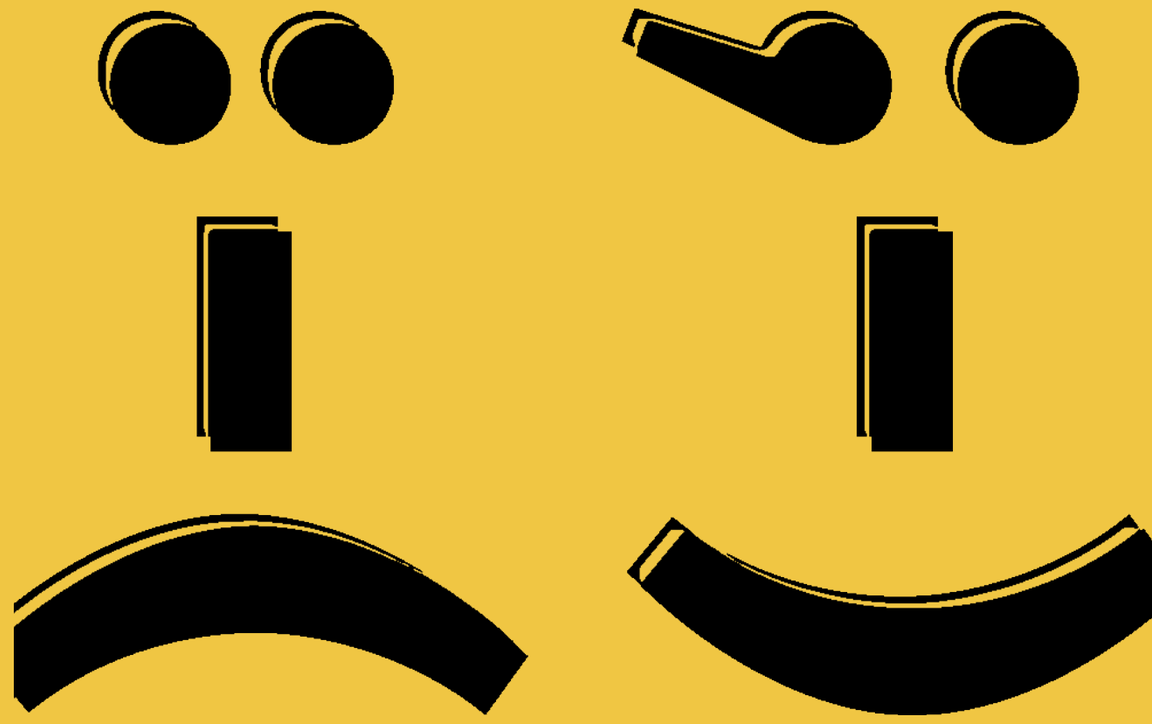


# ΣΥΜΒΟΥΛΕΣ

- Διαβάστε αναλυτικά τους όρους χρήσης πριν δημιουργήσετε ένα λογαριασμό (sign up). Εάν δεν συμφωνείτε με κάποιον από τους όρους χρήσης, μην προχωρήσετε στη δημιουργία του λογαριασμού. Επισκεφτείτε ξανά τους όρους χρήσης ανά τακτά χρονικά διαστήματα, ώστε να ενημερωθείτε για τυχόν αλλαγές **(www.facebook.com/page_guidelines.php)**.
- Σε κάθε ανάρτηση που πραγματοποιείτε, είτε πρόκειται για σχόλιο είτε για δημοσίευση φωτογραφίας, επιλέξτε το σύνολο των ατόμων στα οποία θα είναι ορατή. Υπάρχει επιλογή δίπλα από το κουμπί «Δημοσίευση», στην οποία ορίζετε αν θα είναι δημόσια ορατή ή μόνο στους φίλους σας. Επίσης, μπορείτε να ορίσετε μόνο συγκεκριμένα άτομα ή λίστες ατόμων από τους φίλους σας που θα μπορούν να δουν τη συγκεκριμένη δημοσίευση.
- Επιλέξτε από τις ρυθμίσεις λογαριασμού εάν επιθυμείτε πληροφορίες όπως το όνομα και η φωτογραφία τού προφίλ σας να εμφανίζονται σε διαφημίσεις που λαμβάνουν χώρα στο Facebook. Επίσης, επιλέξτε αν θέλετε στο μέλλον να χρησιμοποιούνται τα στοιχεία σας σε διαφημίσεις εκτός του Facebook.
- Πριν επιτρέψετε σε μια εφαρμογή (Facebook app) να αποκτήσει πρόσβαση στο προφίλ σας, διαβάστε προσεκτικά τις πληροφορίες στις οποίες θα έχει πρόσβαση και τις ενέργειες που θα μπορεί να πραγματοποιήσει στο προφίλ σας.
- Εάν κάποιος χρήστης σάς ενοχλεί στο Facebook, αναφέρετέ τον στο διαχειριστή της ιστοσελίδας πατώντας την επιλογή «Αναφορά/Μπλοκάρισμα» (Report/Block) που βρίσκεται στο προφίλ του. Στο μενού ενεργειών της αναφοράς μπορείτε να δηλώσετε την αιτία για την οποία σας παρενοχλεί, π.χ. παριστάνει εσάς (κλοπή ταυτότητας), σας προσβάλλει. Μπορείτε, επίσης, να επιλέξετε να μπλοκάρετε κάποιον χρήστη που σας ενοχλεί, ώστε να μη λαμβάνετε μηνύματά του.
- Προστατέψτε τον κωδικό ασφαλείας (password), όπως κάθε άλλον κωδικό σας. Μη γνωστοποιείτε τον κωδικό σας σε τρίτα άτομα, καθώς μπορεί στο μέλλον να παριστάνουν εσάς. Εάν σας κλέψουν τον κωδικό του λογαριασμού σας, ακολουθήστε τη διαδικασία της σελίδας για να «ασφαλίσετε» και να ανακτήσετε το λογαριασμό σας **(www.facebook.com/hacked)**.
- Χρησιμοποιήστε τη βοήθεια για κάθε ερώτηση που μπορείτε να έχετε σχετικά με τη χρήση του Facebook **(www.facebook.com/help)**.

# #παιδική_ πορνογραφία_ στο_διαδίκτυο

Όταν η παιδική αξιοπρέπεια κινδυνεύει και ηλεκτρονικά




Από τα συχνότερα αδικήματα που αντιμετωπίζει η Υπηρεσία μας με την πάροδο των τελευταίων ετών, λαμβάνοντας υπ' όψη α) την ανάπτυξη της τεχνολογίας στους ηλεκτρονικούς υπολογιστές και τα κινητά, β) την εξέλιξη του Διαδικτύου με τη δημιουργία αμέτρητων ιστοσελίδων και εφαρμογών κοινωνικής δικτύωσης, ηλεκτρονικής συνδιάλεξης (chat), με δυνατότητα χρήσης κάμερας, ανταλλαγής αρχείων, cloud, e-mail, και γ) την ανωνυμία που προσφέρει το Διαδίκτυο, είναι αυτά της πορνογραφίας ανηλίκων (άρθρο 348Α ΠΚ), της προσβολής γενετήσιας αξιοπρέπειας ανηλίκων (άρθρο 337 ΠΚ) και της αποπλάνησης ανηλίκων (άρθρο 339 ΠΚ).
Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος έχει πιστοποιηθεί από την Interpol ως επίσημη Υπηρεσία αναγνώρισης θυμάτων σεξουαλικής κακοποίησης από όλο τον κόσμο (VICTIM IDENTIFICATION via INTERPOL'S ICSE DATABASE).

Η παραγωγή υλικού παιδικής πορνογραφίας είναι ένα παγκόσμιο φαινόμενο με τεράστια κέρδη.

Οργιάζουν καθημερινά σε όλο τον κόσμο τα κυκλώματα παιδικής πορνογραφίας, ενώ αποτελεί τη δεύτερη πιο προσοδοφόρα εγκληματική δραστηριότητα μετά το εμπόριο ναρκωτικών. Αυτό συμβαίνει διότι η παιδική πορνογραφία κρύβει ένα πολύ μεγάλο χρηματοοικονομικό κέρδος, ενώ υπάγεται στην ομπρέλα του οργανωμένου εγκλήματος.

Μόνο στις ΗΠΑ εκτελούνται καθημερινά 700.000 συναλλαγές γύρω από την παιδική πορνογραφία και διακινούνται δύο τρισεκατομμύρια δολάρια, ενώ σε παγκόσμιο επίπεδο διακινούνται καθημερινά πέντε τρισεκατομμύρια δολάρια κατά μέσο όρο.

**Η παιδική πορνογραφία στην Ελλάδα**

Τα τελευταία χρόνια έχει υπάρξει ραγδαία αύξηση του αριθμού των χρηστών του Διαδικτύου που κατεβάζουν βίντεο και φωτογραφίες με παιδικό πορνογραφικό υλικό.
Πλην όμως, έως σήμερα, δεν έχει διακριβωθεί η ύπαρξη κάποιου οργανωμένου κυκλώματος που να βιντεοσκοπεί πράξεις ασέλγειας σε ανηλίκους, παρά μόνο μεμονωμένες περιπτώσεις.



## ΠΩΣ ΛΕΙΤΟΥΡΓΟΥΝ ΤΑ «ΑΡΠΑΚΤΙΚΑ»
### (GROOMING = ΑΠΟΠΛΑΝΗΣΗ ΑΝΗΛΙΚΟΥ)

Διαδικασία κατά την οποία τα «αρπακτικά», προσποιούμενα ότι είναι έφηβοι, χρησιμοποιούν τα δωμάτια ανοιχτής επικοινωνίας (chat rooms), τις ιστοσελίδες κοινωνικής δικτύωσης και άλλους χώρους διαδικτυακής επικοινωνίας για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν. Τα θύματα του grooming μπορεί να υποστούν σοβαρά τραύματα που έχουν ψυχολογικό και συναισθηματικό αντίκτυπο, με πολύ βλαβερές επιπτώσεις στην υγεία τους. Η κακοποίηση που δέχεται ένα παιδί το οποίο εμπλέκεται σε grooming, δεν είναι μόνο σεξουαλικής φύσεως αλλά και συναισθηματικής, καθώς τα παιδιά βρίσκουν πολύ δύσκολο να ανταπεξέλθουν στις απαιτήσεις και την πίεση των «αρπακτικών».

Επισημαίνεται ότι κατά την περίοδο της εφηβείας τα νεαρά άτομα κάνουν την «προσωπική τους επανάσταση». Αυτή η στάση ανεξαρτησίας και η αναζήτηση νέων γνωριμιών μέσω Διαδικτύου καθιστούν τους εφήβους την πιο ευαίσθητη ομάδα στο ζήτημα της πορνογραφίας αλλά και της σεξουαλικής παρενόχλησης.

Συχνά τέτοιου είδους ιστοχώροι θεωρούνται από τα παιδιά ασφαλείς τόποι συνομιλίας στο Διαδίκτυο, τόσο εξαιτίας της δημόσιας φύσης της συζήτησης, όσο και της λανθασμένης εκτίμησης των παιδιών ότι διατηρείται η ανωνυμία τους. Τα «αρπακτικά» ξεκινούν συζητήσεις με τα πιθανά θύματα, με σκοπό να αναπτύξουν φιλική σχέση με αυτά και να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, τα ενδιαφέροντα, τα χόμπι και τις σεξουαλικές τους εμπειρίες.

Οι συζητήσεις μπορεί να διαρκέσουν ημέρες, εβδομάδες, ακόμη και μήνες, μέχρι το «αρπακτικό» να αποκτήσει την εμπιστοσύνη του παιδιού. Στη συνέχεια, προκαλεί σιγά σιγά συζητήσεις σεξουαλικής φύσεως και του στέλνει φωτογραφίες ως κάτι το αποδεκτό και φυσιολογικό. Αυτή η τακτική αποσκοπεί στο να υπονομεύσει την απροθυμία των παιδιών να λάβουν μέρος σε σεξουαλική επαφή αλλά και να αποτρέψει το θύμα από το να ζητήσει προστασία από τους γονείς και τους δασκάλους του, αφού καταλήγει να νιώθει ένοχο που έχει ανταλλάξει τέτοιου είδους φωτογραφίες.

Τα «αρπακτικά» συνήθως είναι άτομα υπεράνω πάσης υποψίας, που πιθανόν να έχουν και δική τους οικογένεια: φιλήσυχοι, ευυπόληπτοι, μορφωμένοι, επιφανείς, οικονομικά ευκατάστατοι π.χ. επιστήμονες, δάσκαλοι, επιχειρηματίες κ.ά. **Δεν διστάζουν να εκμεταλλευτούν τη θέση τους αλλά και τη σχέση τους (συγγενείς) για να ικανοποιήσουν το αρρωστημένο πάθος τους.**

**Συνήθως τα «αρπακτικά» έχουν παιδοφιλικές τάσεις. Οι παιδόφιλοι που δεν μπορούν να έχουν πρόσβαση σε ανήλικα παιδιά ικανοποιούν τις ανάγκες και το πάθος τους μέσα από το Διαδίκτυο, που τους δίνει πρόσβαση σε παιδικό πορνογραφικό υλικό.**

# ΠΩΣ ΛΕΙΤΟΥΡΓΟΥΝ ΤΑ ΚΥΚΛΩΜΑΤΑ

Πρόκειται για «κλειστές ομάδες», οι οποίες επικοινωνούν μέσω ομάδων συζήτησης (news groups), μέσω δωματίων επικοινωνίας (chat rooms) ή μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail). Πάγια τακτική των κυκλωμάτων που διακινούν υλικό, είναι η χρήση παραπλανητικών φωτογραφιών στην αρχική σελίδα των ιστοσελίδων. Οι ιστοσελίδες στις οποίες «ανεβάζουν» πορνογραφικό υλικό ανηλίκων είναι «καμουφλαρισμένες», ώστε να μην εντοπίζονται (είναι αδύνατον με τη χρήση μιας μηχανής αναζήτησης). Δημιουργούν βίντεο στα οποία αναμειγνύουν πορνογραφία ενηλίκων μαζί με ανηλίκων για να δυσκολεύουν τον εντοπισμό τους.

### Συμβουλές για παιδιά

- Συμβουλευτείτε τους γονείς σας, όταν έχει προκύψει κάποιο πρόβλημα με κάποιον ο οποίος σας προσέγγισε στο Διαδίκτυο, μέσω ιστοσελίδας ή εφαρμογής.
- Αν διαθέτετε λογαριασμό σε κάποια ιστοσελίδα κοινωνικής δικτύωσης (μετά την ηλικία των δεκατριών), αποφεύγετε να βάζετε τα προσωπικά σας στοιχεία (ονοματεπώνυμο, διεύθυνση, τηλέφωνο, σχολείο), καθώς επίσης και φωτογραφίες σας ή των συμμαθητών σας.
- Αν θέλετε να βάλετε φωτογραφίες σας σε διάφορες σελίδες, καλό είναι να μην απεικονίζουν ευαίσθητα σημεία του σώματός σας ή το πρόσωπό σας και να είναι με μακρινή λήψη.
- Χρησιμοποιήστε σύνθετο κωδικό πρόσβασης στο λογαριασμό σας και όχι κάποιον τον οποίο μπορεί να μαντέψει κάποιος. Καλό, επίσης, είναι τον κωδικό πρόσβασης να τον γνωρίζουν οι γονείς σας, για λόγους ασφαλείας.
- Μην αποδέχεστε αιτήματα φιλίας από αγνώστους.
- Αποφεύγετε να μπαίνετε σε σελίδες στις οποίες συνομιλείτε με αγνώστους ή δεν εμφανίζεται το username τους ή απαιτείται η χρήση κάμερας.
- Μην ανοίγετε ποτέ την κάμερα σε αγνώστους.
- Αν κάποιος χρήστης σε μια συνομιλία σάς ζητήσει να βγάλετε κάποια φωτογραφία που να δείχνει το σώμα σας ή γενικότερα εσάς, και να τη στείλετε, μην το κάνετε σε καμία περίπτωση και ειδοποιήστε αμέσως τους γονείς σας.
- Μην ανοίγετε μηνύματα/e-mail και κυρίως συνδέσμους (link) που υπάρχουν σε αυτά, κι ας τα έχει στείλει κάποιος φίλος ή φίλη σας, αφού δεν ξέρετε σε ποια σελίδα σας οδηγούν. Μπορεί, για παράδειγμα, πίσω από το σύνδεσμο αυτό να κρύβεται κάποιος ιός.
- Αν κάποιος άγνωστος χρήστης σάς προσέγγισε σε μια συνομιλία και μιλάει πονηρά και με σεξουαλικά υπονοούμενα, μη συνεχίσετε να μιλάτε μαζί του.
- Αν για οποιονδήποτε λόγο αισθάνεστε ανασφάλεια ή φόβο, καλό είναι να ειδοποιήσετε τους γονείς σας ή την Υπηρεσία μας στο τηλέφωνο 11188 για οποιαδήποτε βοήθεια.
- Ο χώρος του Διαδικτύου προσφέρει μια πλασματική πραγματικότητα. Συνεπώς, δεν σας δίνει τη δυνατότητα να διαλέξετε τους φίλους σας έχοντας μια ολοκληρωμένη άποψη για το ποιοι είναι, μιας και δεν υπάρχει άμεση επαφή μαζί τους, όποτε να είστε πολύ επιφυλακτικοί σχετικά με το με ποιους μιλάτε και τι μοιράζεστε μαζί τους.

Σημαντικό είναι να σκεφτείτε ότι στο Διαδίκτυο σχεδόν πάντα δεν ξέρετε με ποιο άτομο συνομιλείτε εκείνη τη στιγμή, αν ανοίγοντας την κάμερα του υπολογιστή ή του τηλεφώνου σας το άτομο αυτό σας καταγράφει, ή ακόμα πώς θα χρησιμοποιήσει ή και πού θα στείλει μετέπειτα μια φωτογραφία που του στείλατε.

### Συμβουλές για γονείς

**Ανεξάρτητα του πώς μπορεί να λειτουργεί κάποιο άτομο που σκοπεύει να προσεγγίσει τα παιδιά και παραβαίνει τις διατάξεις των ανωτέρω αναφερόμενων άρθρων, παρατηρούνται τα εξής:**

1. Τα παιδιά πολλές φορές, μη λαμβάνοντας υπόψη τους κινδύνους που μπορεί να διατρέχουν, καθώς δεν γνωρίζουν το άτομο με το οποίο συνομιλούν εκείνη τη στιγμή, ή νομίζοντας ότι μιλάνε με κάποιο γνωστό τους, ενώ στην πραγματικότητα μπορεί να είναι κάποιος που έχει παραβιάσει το προφίλ φίλου/φίλης για την προσέγγιση των παιδιών, ή με κάποιον ο οποίος με τεχνάσματα στον γραπτό λόγο κερδίζει την εμπιστοσύνη τους, αποστέλλουν τα προσωπικά τους στοιχεία (ονοματεπώνυμο, διευθύνσεις, τηλεφωνικούς αριθμούς), ανεβάζουν (upload) ή αποστέλλουν (send) μέσω του ηλεκτρονικού υπολογιστή και των κινητών τηλεφώνων (Smartphones) φωτογραφίες τους, πολλές φορές με προκλητικό περιεχόμενο, ή ακόμα συναντιούνται με τα άτομα αυτά.
Ακολούθως, τα παιδιά μπορεί να γίνονται στόχοι διαδικτυακού εκφοβισμού (bullying), δηλαδή με απειλές και εκβιασμούς να τους ζητείται η αποστολή κι άλλων φωτογραφιών με προκλητικό περιεχόμενο, όχι απαραίτητα από την αρχική ιστοσελίδα ή εφαρμογή από την οποία έχει προηγηθεί η οποιαδήποτε συνομιλία, αλλά από οποιαδήποτε άλλη ιστοσελίδα, υπηρεσία ή εφαρμογή όπου τους έχει υποδειχθεί να εισέλθουν για να πραγματοποιήσουν αυτές τις ενέργειες.
Ιστοσελίδες και εφαρμογές όπου μπορεί να παρατηρηθούν τέτοιες ενέργειες είναι τα μέσα κοινωνικής δικτύωσης αλλά και διαδικτυακά παιχνίδια με πλατφόρμες επικοινωνίας (chat).
2. Τα παιδιά θέλοντας να περάσουν τον ελεύθερο χρόνο τους, να διασκεδάσουν, να λύσουν τις απορίες τους ή ακόμα και να ακολουθήσουν τη «μόδα» της εποχής, για παράδειγμα φωτογραφίες του εαυτού τους (selfie) και άλλα, πραγματοποιούν ενέργειες που ουσιαστικά τα στοχοποιούν και τα παγιδεύουν. Ενέργειες όπως αυτή που προαναφέρθηκε, καθώς επίσης το άνοιγμα συνδέσμων (link) αγνώστου περιεχομένου, είτε από κάποια ιστοσελίδα είτε από κάποια εφαρμογή είτε από κάποια υπηρεσία όπως e-mail, πίσω από τους οποίους μπορεί να κρύβεται κάποια άλλη ιστοσελίδα με περιεχόμενο ακατάλληλο για τα παιδιά ή ακόμα και κάποιο κακόβουλο λογισμικό για τον υπολογιστή ή το κινητό, οδηγούν σε απρόσμενα αποτελέσματα για το παιδί.
3. Με δεδομένα τα ανωτέρω ενδεικτικά αναφερόμενα και γενικευμένα παραδείγματα:
- Η επίτευξη σωστής επικοινωνίας μεταξύ γονέα-κηδεμόνα και παιδιού είναι πρωταρχικός παράγοντας, ενώ σε περίπτωση οποιασδήποτε απορίας ή αδυναμίας καλό είναι να ζητηθεί η συμβουλή ειδικού ψυχολόγου.
- Οι γονείς και οι κηδεμόνες θα πρέπει να έχουν την εποπτεία των συσκευών και των αποθηκευτικών μέσων, με τα οποία τα παιδιά εισέρχονται σε ιστοσελίδες, εφαρμογές και υπηρεσίες για οποιονδήποτε σκοπό. Αν δεν υπάρχει η απαραίτητη τεχνογνωσία από πλευράς γονέων και κηδεμόνων, καλό είναι να ληφθεί υπόψη η συμβουλή ειδικού.
- Οι γονείς και οι κηδεμόνες καλό είναι να γνωρίζουν από πριν τους κωδικούς πρόσβασης στα εκάστοτε προφίλ-λογαριασμούς στα οποία εισέρχεται το παιδί, με σκοπό την πλήρη εποπτεία.
- Καλό είναι παιδιά νεαρής ηλικίας (κάτω των δεκατριών ετών) να μη διαθέτουν λογαριασμούς σε ιστοσελίδες κοινωνικής δικτύωσης ή, εφόσον δεν μπορεί να αποφευχθεί αυτό, να υπάρχει καλή επικοινωνία και η κατάλληλη ρύθμιση για την πρόσβαση από τρίτα άτομα σε αυτούς, π.χ. δυνατότητα αναζήτησης, προβολή μόνο σε φίλους κ.λπ.
- Να αποφεύγεται το «ανέβασμα» (upload) ή η αναφορά σε κάποια συζήτηση προσωπικών στοιχείων (ονοματεπώνυμα, διευθύνσεις κατοικίας, τηλεφωνικοί αριθμοί, σχολεία κ.λπ.), φωτογραφιών, ακόμα και e-mail στις εκάστοτε ιστοσελίδες, εφαρμογές και υπηρεσίες.
- Να αποφεύγεται το «ανέβασμα» ή η αποστολή φωτογραφιών με άσεμνο περιεχόμενο.
- Σε περίπτωση «ανεβάσματος» απλής φωτογραφίας με κανονικό περιεχόμενο, να μην απεικονίζονται ευδιάκριτα σε αυτήν τα πρόσωπα των παιδιών ή να είναι με μακρινή λήψη, πολύ περισσότερο δε όταν τα παιδιά είναι κάτω των δεκατριών ετών.
- Να μη γίνεται αποδοχή άγνωστων ατόμων ως φίλων σε προφίλ ή λογαριασμούς που τυχόν διαθέτουν τα παιδιά.
- Οι φίλοι που διαθέτει το παιδί σε κάποιο προφίλ να είναι μόνο οι φίλοι του και στην πραγματική ζωή.
- Να αποφεύγεται είσοδος σε σελίδες, εφαρμογές ηλεκτρονικής συνδιάλεξης (chat) άγνωστες προς τα παιδιά και στις οποίες δίνεται η δυνατότητα συνομιλίας με αγνώστους, καθώς και σε αυτές όπου γίνεται χρήση κάμερας.
- Να αποφεύγεται το άνοιγμα οποιουδήποτε συνδέσμου (link) αγνώστου προελεύσεως.
- Συμβουλεύουμε τα παιδιά για την αποφυγή χρήσης κάμερας, κυρίως όταν η συνομιλία γίνεται με άγνωστα άτομα ή χωρίς την παρουσία των γονέων και των κηδεμόνων.

Σημαντικό είναι οι γονείς να μην ξεχνάνε ότι εκτός από τα παιδιά τους πρέπει να προστατεύουν και τους εαυτούς τους. Δεν πρέπει να ανεβάζουν (upload) φωτογραφίες των ανήλικων παιδιών τους καθώς και προσωπικές και οικογενειακές τους στιγμές.
1. Περιπτώσεις στις οποίες οι γονείς των παιδιών διαπιστώνουν την ύπαρξη προβλήματος:
- Συνομιλούμε με το παιδί για την πλήρη διερεύνηση του προβλήματος, την πηγή αυτού και του τι ακριβώς έχει γίνει. Διαπιστώνουμε αν έχει γίνει μόνο συνομιλία ή, σε περίπτωση που το παιδί έχει

# ΠΩΣ ΛΕΙΤΟΥΡΓΟΥΝ ΤΑ ΚΥΚΛΩΜΑΤΑ

στείλει φωτογραφίες, τι είδους, πόσες και πού, και, σε περίπτωση που του έχουν στείλει φωτογραφίες, τι είδους, πόσες και ποιος, αν έχει γίνει χρήση ή προτροπή χρήσης κάμερας και μέσω ποιας εφαρμογής.
- Συμβουλευόμαστε αρμόδιο ψυχολόγο σε περίπτωση αδυναμίας σωστής επικοινωνίας με το παιδί για τον οποιονδήποτε λόγο αλλά και τη μετέπειτα διαχείριση της συμπεριφοράς αυτού.

Για τη συλλογή αποδεικτικών στοιχείων πριν από οποιονδήποτε αποκλεισμό (block) ή διαγραφή της επικοινωνίας (συμπεριλαμβανομένης της συνομιλίας και των φωτογραφιών) με το άγνωστο άτομο-δράστη, για τη σωστή λήψη αυτών, για τον εντοπισμό τους ή για το τι πρέπει να κάνετε γενικότερα και για συμβουλές αναφορικά με το νομικό κομμάτι του προβλήματος, μπορείτε να καλέσετε την Υπηρεσία μας στο 11188.

**Μερικές από τις διεθνείς επιχειρήσεις στις οποίες έχει συμμετάσχει η Υπηρεσία μας:**

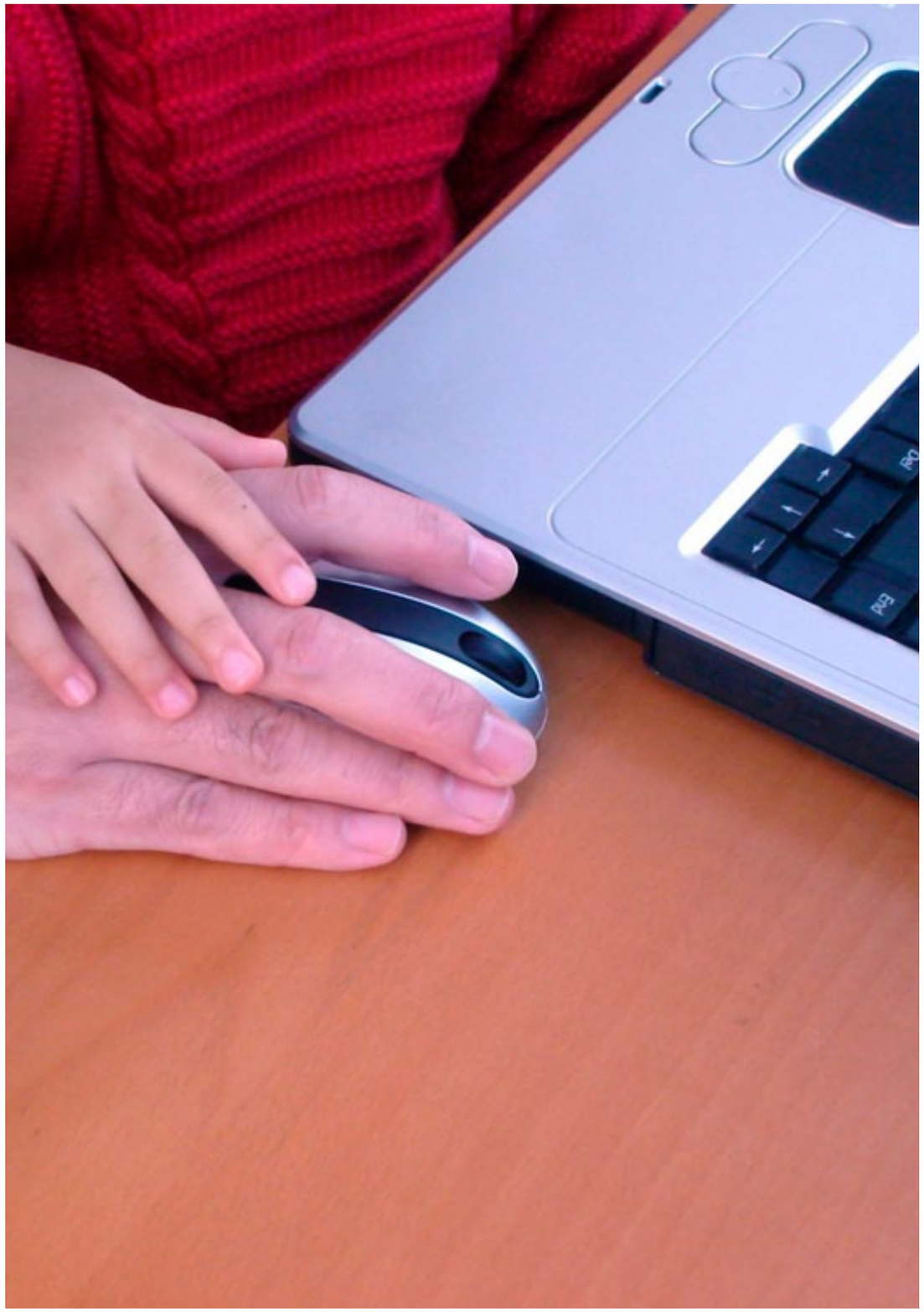
- **CAROUSELL I & II**
- **KOALA**
- **STORM**
- **PURITY**
- **MYOSIS**
- **TWINS**
- **CHARLY**
- **SPIDER WEB**
- **ICARUS**
- **ANGELS**
- **Hydra** (Κατά τη διάρκεια της επιχείρησης εντοπίστηκαν από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος συνολικά 78 χρήστες-δράστες σε 32 διαφορετικές χώρες του κόσμου.)
- **Depletion**
- **Depletion 2**
- **Sornyak**
- **Rina**

- Chat scanning [Σάρωση διαδικτυακών εικονικών δωματίων επικοινωνίας στα πλαίσια της οποίας πραγματοποιήθηκε **στοχευμένη διαδικτυακή έρευνα-ανακριτική διείσδυση σε δωμάτια εικονικής διαδικτυακής επικοινωνίας** (chat rooms). Κατά τη διάρκειά της με τη χρήση προφίλ-λογαριασμών σε πρόγραμμα ηλεκτρονικής συνδιάλεξης αστυνομικοί «υποδύθηκαν» τους ανηλίκους κάτω των δεκατριών ετών. Επίσης, δόθηκε στη δημοσιότητα ο «Κώδικας Επικοινωνίας Παιδοφίλων» στο Διαδίκτυο, προς ενημέρωση και ευαισθητοποίηση των γονιών. **Ο «Κώδικας Επικοινωνίας» προέκυψε από σχετικό εγχειρίδιο που εντοπίστηκε στο Σκοτεινό Διαδίκτυο (Dark Web), ύστερα από πολύμηνες και στοχευμένες έρευνες εξειδικευμένων Αξιωματικών της Δίωξης Ηλεκτρονικού Εγκλήματος].**

Το υλικό πορνογραφίας ανηλίκων που έχει βρεθεί προκαλεί απδία και φρίκη. **Βρέφη από λίγων μηνών έως και παιδιά 17 ετών** είναι οι τραγικοί πρωταγωνιστές των άρρωστων σεξουαλικών βίντεο και φωτογραφιών, ανήλικοι, οι οποίοι με τη χρήση ναρκωτικών ουσιών υποχρεώνονται σε ερωτικές περιπτύξεις είτε μεταξύ τους, είτε με ενήλικες, είτε και με ζώα.

Οι περισσότερες φωτογραφίες και βίντεο προέρχονται από χώρες της Λατινικής Αμερικής, της νοτιοανατολικής Ασίας και της Αφρικής, όπως η Βενεζουέλα, η Βραζιλία, η Ταϊλάνδη, η Σιγκαπούρη και η Αλγερία.

Το κόστος για την απόκτηση των φωτογραφιών και των βίντεο από τα «αρπακτικά» κατηγοριοποιείται ανάλογα με την ηλικία των παιδιών ή το περιεχόμενό τους.



# #ασφάλεια_πληροφοριών_&_βιομηχανική_κατασκοπεία

Όταν κάθε επιχείρηση
βάλλεται ηλεκτρονικά

# Ο ΠΟΛΥΤΙΜΟΣ ΔΕΚΑΛΟΓΟΣ ΤΗΣ ΕΠΙΧΕΙΡΗΣΗΣ ΣΑΣ

### Antivirus - Antimalware
Θα πρέπει να υπάρχει πρόγραμμα προστασίας από ιούς (Antivirus) και πρόγραμμα προστασίας από κακόβουλο λογισμικό (Antimalware), τα οποία θα πρέπει να είναι ενημερωμένα για όλες τις τρέχουσες απειλές.

### Firewall
Με τη χρήση του firewall, μπορείτε να παρακολουθείτε και να εντοπίζετε τυχόν ασυνήθιστη συμπεριφορά ενός επιμέρους προγράμματος. Το firewall αποτελεί την καρδιά της πολιτικής ασφαλείας γιατί φιλτράρει την κίνηση του δικτύου της επιχείρησης.

### Intrusion Prevention System
Το σύστημα Ελέγχου Επιθέσεων (Intrusion Prevention System), ψάχνει για ιούς αλλά και παρακολουθεί τα συστήματά σας για οποιαδήποτε ασυνήθιστη δραστηριότητα.

### Χρήστες
**Πολιτική πρόσβασης χρηστών στο δίκτυο της επιχείρησης.** Έλεγχος της πρόσβασης των χρηστών στο δίκτυο της επιχείρησης μέσω:

Authentication: Επιβεβαίωση της ταυτότητας των χρηστών.
Authorization: Καθορισμός επιτρεπόμενων ενεργειών για κάθε χρήστη.
Accounting: Δημιουργία αρχείου ενεργειών για τον κάθε χρήστη (τι ενέργειες έκανε και πότε).

**Απομακρυσμένη πρόσβαση χρηστών.** Οποιοσδήποτε χρήστης θα πρέπει να συνδέεται στο δίκτυό σας μέσω κατάλληλου Εικονικού Ιδιωτικού Δικτύου **(Virtual Private Network-VPN)** με τα ακολουθούμενα επίπεδα ασφαλείας.

**Εκπαίδευση χρηστών, ώστε όλοι οι χρήστες να καταλαβαίνουν τη σπουδαιότητα της πιστής εφαρμογής των κανόνων ασφαλείας**. Κάποιοι κανόνες ασφαλείας, ενδεικτικά, μπορεί να είναι: Να σβήνουν τον υπολογιστή πριν την απομάκρυνση από το γραφείο τους και να χρησιμοποιούν ισχυρούς κωδικούς ασφαλείας (passwords). Επιπλέον, το σύστημα δεν θα πρέπει να επιτρέπει σε ένα χρήστη να έχει πρόσβαση στο δίκτυο αν δεν έχει χρησιμοποιήσει ισχυρό password.



**Έλεγχος των αδειών χρήσης λογισμικού.** Οι χρήστες δεν θα πρέπει να κατεβάζουν οποιοδήποτε λογισμικό κατά βούληση γιατί μπορεί να θέσουν σε κίνδυνο το δίκτυο της επιχείρησής σας.
**Εφαρμογή πολιτικής πρόσβασης των χρηστών και στο έντυπο υλικό της επιχείρησης.**
**Εφαρμογή κυρώσεων σε όποιο χρήστη** δεν εφαρμόζει την πολιτική ασφαλείας της επιχείρησης.

### Πολιτική ασφαλείας στις χρησιμοποιούμενες συσκευές
**Διαμόρφωση κρίσιμων συσκευών** ώστε να μην υποστηρίζουν τη χρήση φορητών συσκευών μεταφοράς δεδομένων, π.χ. USB.
**Μην επιτρέπετε σε άτομα εκτός επιχείρησης**, όπως επισκέπτες, να συνδέονται στο δίκτυο της επιχείρησής σας. Σε αντίθετη περίπτωση, θα πρέπει να ακολουθούν το δικό σας επίπεδο ασφαλείας. Θα πρέπει, δηλαδή, να γίνεται έλεγχος της πρόσβασης στο δίκτυο από φορητές ασύρματες συσκευές, όπως κινητά τηλέφωνα ή ταμπλέτες (tablets), κ.τ.λ.
**Χρήση λογισμικού Data Loss Prevention (DLP)** για την αποφυγή περιπτώσεων διαρροής κρίσιμων δεδομένων της επιχείρησης.

### Περιορισμός της έκτασης πρόσβασης
Θα πρέπει να υπάρχουν δικλείδες ασφαλείας ώστε, αν κάποιος εισβολέας καταφέρει να εισχωρήσει σε κάποιο τμήμα του δικτύου σας, να μην μπορεί αυτομάτως να εισχωρήσει και σε όλο το δίκτυο.

### Γνώση των αδυναμιών του δικτύου σας
Δεν υπάρχει το τέλειο σύστημα ασφαλείας, γι' αυτό θα πρέπει ο υπεύθυνος ασφαλείας της επιχείρησης να γνωρίζει τα τρωτά σημεία του και τις περιοχές που παρουσιάζουν τον μεγαλύτερο κίνδυνο, και να απαγορεύεται η πρόσβαση σε αυτές.

### Κατοχύρωση Διπλωμάτων Ευρεσιτεχνίας
Διασφάλιση των κρίσιμων δεδομένων της επιχείρησης με Διπλώματα Ευρεσιτεχνίας, όπου είναι εφικτό.

### Παρακολούθηση του φυσικού χώρου της επιχείρησής σας με χρήση καμερών ασφαλείας

### Εκτίμηση του κόστους
Θα πρέπει να δίνεται ιδιαίτερη σημασία στην εκτίμηση του κόστους για την ασφάλεια της επιχείρησης και να συνυπολογίζεται στον προϋπολογισμό της επιχείρησης, αφού είναι κρίσιμο στοιχείο για την υπόστασή της.

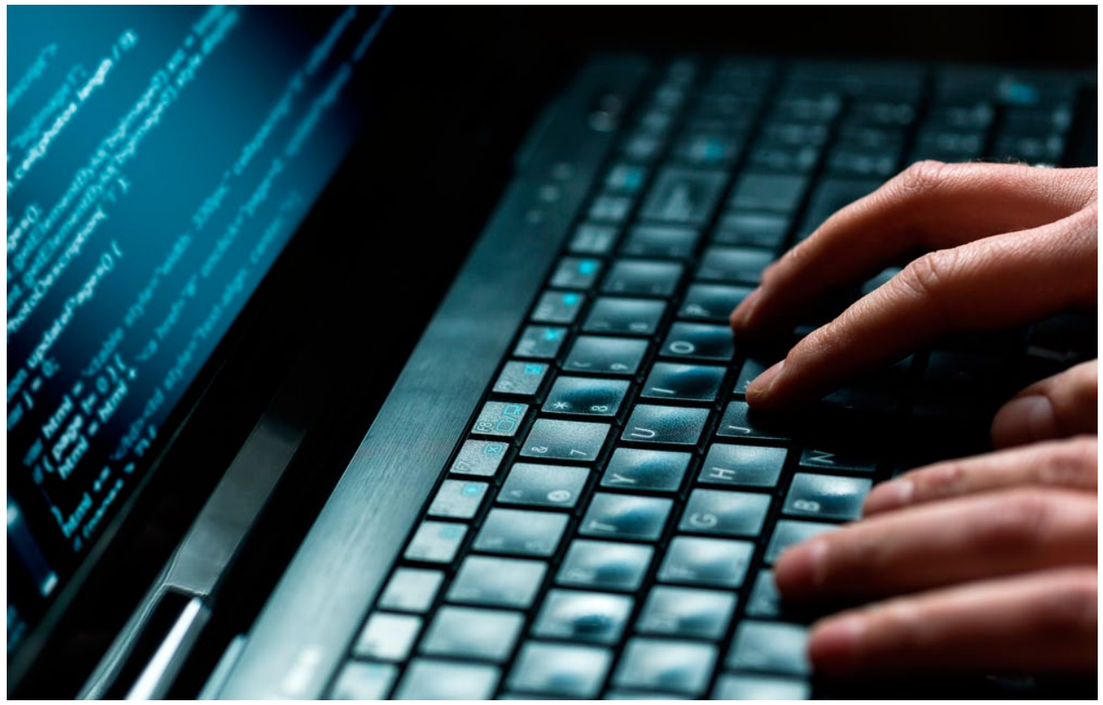
Αν πέσετε θύμα βιομηχανικής κατασκοπείας, ενημερώστε αμέσως την Υπηρεσία μας καλώντας στο τηλέφωνο 11188 ή μέσω e-mail **ccu@cybercrimeunit.gov.gr.**

**Ορισμός.**

Με τον όρο βιομηχανική κατασκοπεία, σε επίπεδο επιχειρήσεων, εννοούμε τη **συλλογή πολύτιμων δεδομένων εταιρειών είτε από άλλες εταιρείες που αποσκοπούν στη βελτίωση των συγκριτικών πλεονεκτημάτων τους είτε από ιδιώτες-hackers.**

# #απάτες_μέσω_διαδικτύου

Και οικονομικά εγκλήματα



## ΑΠΑΤΕΣ ΜΕΣΩ ΔΙΑΔΙΚΤΥΟΥ

Βασική αρχή στις απάτες που διαπράττονται μέσω Διαδικτύου είναι να πείσουν το θύμα να καταβάλει ένα μικρό αρχικό ποσό με σκοπό να εξασφαλίσει ένα πολύ μεγαλύτερο στο μέλλον, όπως για παράδειγμα οι νιγηριανές απάτες, ή γενικότερα να πείσουν το θύμα για την ασφάλεια των διαδικτυακών συναλλαγών, με σκοπό στη συνέχεια να του αποσπάσουν μεγάλα χρηματικά ποσά (απάτες με πιστωτικές κάρτες, κ.τ.λ).

## SPAMMING-SCAMMING

Η λέξη «spam» περιγράφει τη μαζική αποστολή μηνυμάτων ηλεκτρονικού υπολογιστή (e-mails), τα οποία έχουν συνήθως απρόκλητο και εμπορικό χαρακτήρα και αποστέλλονται αδιακρίτως. Όταν ο στόχος του αποστολέα των μηνυμάτων αυτών είναι να εξαπατήσει τον αποδέκτη και να χρησιμοποιήσει με κακόβουλο τρόπο τα δεδομένα που θα υποκλέψει, τότε κάνουμε λόγο για τη διαδικασία «scamming».

Πρόκειται για τον πλέον διαδεδομένο τρόπο δράσης σε πολλά είδη ηλεκτρονικών οικονομικών εγκλημάτων (νιγηριανές απάτες, ισπανικό λόττο, phishing, απατηλές θέσεις εργασίας στο εξωτερικό, διαφημίσεις για χάσιμο βάρους κ.τ.λ.). Επιπλέον, η μαζική αποστολή κακόβουλων μηνυμάτων γίνεται και προς κινητά τηλέφωνα, σε μια εποχή που οι χρήστες των Smart-phones αυξάνονται ραγδαία.



## «ΝΙΓΗΡΙΑΝΕΣ» ΑΠΑΤΕΣ

Πρόκειται για e-mail που μας ενημερώνουν ότι κάποιος (συνήθως πρώην υψηλόβαθμο στέλεχος της νιγηριανής κυβέρνησης) χρειάζεται τη βοήθειά μας για να μεταφέρει ένα υψηλό χρηματικό ποσό (π.χ. 30 εκατ. δολάρια), έναντι υψηλής υποσχόμενης αμοιβής (ποσοστό επί του κεφαλαίου), το οποίο δεν μπορεί να διοχετευτεί εκτός της χώρας με το όνομα του δικαιούχου-αποστολέα του e-mail. Ζητείται δηλαδή στον παραλήπτη να βοηθήσει λειτουργώντας ως αποδέκτης του εν λόγω ποσού, αφού παράλληλα ενημερωθεί ότι η επιλογή του δεν έγινε τυχαία αλλά βάσει πληροφόρησης για τη φερεγγυότητά του (συχνά αναφέρεται κάποιο επιμελητήριο ή επαγγελματική ένωση). Παράλληλα δίνεται ιδιαίτερη έμφαση στην εμπιστευτικότητα που θα πρέπει να τηρηθεί. Σε πρώτη φάση, ζητείται από το υποψήφιο θύμα η συγκατάθεσή του και η παροχή στοιχείων που αφορούν τους τραπεζικούς του λογαριασμούς, και οποιωνδήποτε πληροφοριών κρίνονται απαραίτητες για την πραγματοποίηση των συναλλαγών. Πολλές φορές και ύστερα από απαίτηση του θύματος, προσκομίζονται και έγγραφα τα οποία δείχνουν αυθεντικά και επίσημα, εξαλείφοντας έτσι κάθε αμφιβολία του θύματος. Από τη στιγμή, λοιπόν, που το θύμα θα ανταποκριθεί, αρχίζει μια ατελείωτη διαδικασία ανταλλαγής e-mail, τηλεφωνημάτων και επιστολών κάνοντάς το να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του εν λόγω ποσού. Ακριβώς, όμως, πριν την τελική μεταβίβαση των χρημάτων εμφανίζεται από πλευράς του αξιωματούχου κάποιο προσωρινό πρόβλημα (έκτακτος φόρος, απρόβλεπτο τέλος, πληρωμή κάποιου ενδιάμεσου υπαλλήλου κ.τ.λ.). Ο αξιωματούχος, βέβαια, προφασίζεται αδυναμία πληρωμής του ποσού λόγω του ότι έχει ήδη προχωρήσει σε μεταβίβαση των χρημάτων, με αποτέλεσμα τη δέσμευση αυτών έως ότου λυθεί το πρόβλημα που προέκυψε. Στα πλαίσια συνεργασίας τους, ζητείται από το θύμα να καταβάλει το ποσό, το οποίο φυσικά θα του επιστραφεί με την ολοκλήρωση της συναλλαγής. Αυτή βέβαια είναι η αρχή μιας σειράς «προβλημάτων» που προφασίζεται ο δράστης, καταφέρνοντας να αποσπάσει χρηματικό ποσό που μπορεί να φτάσει μέχρι και τα 500.000€. Η εμπειρία έχει δείξει πως κάποια από τα θύματα πείθονται να ταξιδέψουν μέχρι τη Νιγηρία για την ολοκλήρωση της συναλλαγής και, ενώ τους έχουν διαβεβαιώσει ότι δεν απαιτείται visa, καταλήγουν να βρίσκονται παράνομα στη χώρα, γεγονός που χρησιμοποιείται εκβιαστικά από το κύκλωμα των δραστών.

Δεν είναι λίγες οι περιπτώσεις συνανθρώπων μας που το κύκλωμα των δραστών πείθει να ταξιδέψουν στο εξωτερικό και οδηγεί σε θυρίδα τράπεζας δείχνοντάς τους τα λεφτά, ενώ εκείνοι έχουν ήδη καταβάλει κάποια χρηματικά ποσά για την αποδέσμευση του κεφαλαίου. Η παραμονή τους γίνεται σε ξενοδοχείο 5 αστέρων, με το κύκλωμα να τους παρακινεί να κάνουν για 4 ημέρες πολυτελή ζωή, την οποία και προφασίζονται ότι θα καλύψουν, χωρίς βεβαίως να το κάνουν.

## ΙΣΠΑΝΙΚΟ ΛΟΤΤΟ

Η εν λόγω μορφή απάτης πραγματοποιείται με τη μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας σε τυχαίους χρήστες του Διαδικτύου. Τα μηνύματα αυτά τους ενημερώνουν ότι έχουν κερδίσει ένα μεγάλο χρηματικό ποσό της τάξεως των εκατομμυρίων δολαρίων σε ηλεκτρονική κλήρωση του Διαδικτύου, στην οποία όμως ποτέ δεν δήλωσαν συμμετοχή! Οι δράστες, για να γίνουν πιστευτοί, χρησιμοποιούν παραπλήσια ονόματα μεγάλων εταιρειών (π.χ. Microsoft, Yahoo κ.λπ.) και συνοδεύουν τα μηνύματα που αποστέλλουν με πλαστά πιστοποιητικά όσον αφορά την υποτιθέμενη ηλεκτρονική κλήρωση. Η απάτη έγκειται στο γεγονός ότι ζητούν από τους υποτιθέμενους νικητές την προπληρωμή κάποιων φόρων ή/και εξόδων εκταμίευσης των χρημάτων, ποσό που συνήθως είναι της τάξης των μερικών χιλιάδων δολαρίων.

## PHISING ΠΡΟΣΩΠΙΚΩΝ ΣΤΟΙΧΕΙΩΝ

Το «phishing» πραγματοποιείται συνήθως με την αποστολή μαζικών spam e-mails, τα οποία υποτίθεται ότι αποστέλλονται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κ.λπ.). Σκοπός είναι να παραπλανηθεί ο παραλήπτης και να του εκμαιευθούν απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, οι εγκέφαλοι της απάτης χρησιμοποιούν τα στοιχεία αυτά για την πραγματοποίηση αξιόποινων πράξεων. Συγκεκριμένα, ο αποστολέας ζητάει στον παραλήπτη να ενημερώσει ή να επαληθεύσει κάποια προσωπικά στοιχεία του για λόγους ασφαλείας και τον οδηγεί στο τέλος μέσω συνδέσμων σε κάλπικες ιστοσελίδες, οι οποίες και μιμούνται στο μέγιστο τις επίσημες. Τα κέρδη των δραστών παγκοσμίως υπερβαίνουν το 1 δις ευρώ σε ετήσια βάση.

## PHARMING

Η διαδικασία «pharming» αποτελεί μια παραλλαγή του «phishing». Περιγράφει την παρέμβαση τρίτων στον εξυπηρετητή DNS (DNS server) μιας ιστοσελίδας, που στόχο έχει την ανακατεύθυνση του προγράμματος περιήγησης σε άλλες ψεύτικες ιστοσελίδες. Το pharming μπορεί να πραγματοποιηθεί επιφέροντας αλλοίωση:

- Του host's file ενός Η/Υ με αποτέλεσμα την ανακατεύθυνση ενός ονόματος χώρου σε ψευδή προορισμό.
- Του «router» ενός δικτύου LAN: Με την αλλοίωση των ρυθμίσεων ή ακόμη και του firmware ενός router ο δράστης μπορεί να πετύχει την ανακατεύθυνση ενός ονόματος χώρου για όλους τους Η/Υ του δικτύου.
- Ενός DNS server: Οι δράστες αποκτούν πρόσβαση σε έναν κεντρικό DNS server αλλοιώνοντας την κίνηση όλων των χρηστών του Διαδικτύου που εξυπηρετείται από αυτούς.

Με πιο απλά λόγια, όταν ο χρήστης του Διαδικτύου πληκτρολογεί την ιστοσελίδα κάποιου διαδικτυακού καταστήματος, εν αγνοία του μεταφέρεται σε έναν ψεύτικο ιστότοπο, ο οποίος προσομοιάζει στην πραγματική ιστοσελίδα τού εν λόγω καταστήματος, που έχει δημιουργηθεί για να παραπλανήσει το χρήστη. Στη συνέχεια, ο δράστης υφαρπάζει τα προσωπικά στοιχεία που ο ανυποψίαστος χρήστης θα καταχωρήσει κατά τη διαδικασία της συναλλαγής (ονοματεπώνυμο, κωδικοί πιστωτικών καρτών κ.τ.λ.), προκειμένου να τα χρησιμοποιήσει με κακόβουλο τρόπο.
Το φαινόμενο του «pharming» έχει παρουσιαστεί πρόσφατα σε δύο τραπεζικούς οργανισμούς. Με την ανακατεύθυνση των σελίδων του web banking, μέσω μόλυνσης του προσωπικού τους Η/Υ, οι χρήστες οδηγούνταν σε ψευδείς ιστοσελίδες όπου και υποκλέπτονταν τα προσωπικά τους δεδομένα.

## ΑΠΑΤΕΣ ΜΕ ΠΙΣΤΩΤΙΚΕΣ ΚΑΡΤΕΣ

Τα περιστατικά απάτης με τη χρήση πιστωτικών καρτών σε online αγορές αυξάνονται με ραγδαίο ρυθμό. Υπολογίζεται ότι οι τράπεζες μετρούν απώλειες εκατομμυρίων ευρώ από ανθρώπους που κατασκευάζουν, παραχαράσσουν, υποκλέπτουν αριθμούς πιστωτικών καρτών, ή που κάνουν εικονικές αγορές μέσω Internet χρησιμοποιώντας αριθμούς καρτών που είναι σχετικά εύκολο να βρει ο απατεώνας ή να τους κατασκευάσει με τη βοήθεια κατάλληλων αλγοριθμικών προγραμμάτων με ηλεκτρονικούς υπολογιστές. Επιπλέον, η έλλειψη επαφής πρόσωπο με πρόσωπο στο Διαδίκτυο τείνει να κάνει τους απατεώνες πιο τολμηρούς. Online αγορές προϊόντων που ποτέ δεν παραδόθηκαν, υπέρογκες χρεώσεις πιστωτικών καρτών για υπηρεσίες που ποτέ δεν ζητήθηκαν ή είχαν αρχικά παρουσιαστεί ότι προσφέρονται δωρεάν, παραπλανητική πληροφόρηση για προϊόντα που αγοράζονται μέσω Διαδικτύου, είναι μόνο μερικές από τις καταγγελίες πολιτών που δέχονται καθημερινά οι διωκτικές αρχές της χώρας μας.

Χαρακτηριστικά αναφέρουμε περιπτώσεις ανθρώπων οι οποίοι ενδιαφερόμενοι να αγοράσουν κάποιο αυτοκίνητο, τρακτέρ, μηχανή κ.τ.λ. αναζητούν στο Διαδίκτυο την αγγελία που θα καλύψει τις ανάγκες τους. Στη συνέχεια και αφού έχουν αναπτύξει σχετική επικοινωνία με τον κάτοχο-δράστη, καταβάλλουν κάποια προκαταβολή, συνήθως μέσω εταιρείας πληρωμών (π.χ. Western Union). Εκεί ξεκινούν τα προβλήματα, καθώς ο δράστης προφασίζεται πλέον διάφορες δικαιολογίες για να εισπράξει επιπλέον χρήματα, να καθυστερήσει και τελικά να μην παραδώσει ποτέ το προϊόν.

### Πυραμιδικά Συστήματα Εργασίας

Στις απάτες που διαπράττονται μέσω Διαδικτύου συμπεριλαμβάνονται και τα διαδικτυακά πυραμιδικά συστήματα εργασίας από το σπίτι. Πρόκειται για απάτες που υπόσχονται υψηλές αμοιβές και ασυνήθιστα υψηλά κέρδη από επενδύσεις που στην πραγματικότητα δεν υφίστανται. Τελικά, το σύστημα καταρρέει αφού οι επενδυτές δεν πληρώνονται ούτε τα υποσχόμενα μερίδια ούτε τις προσυμφωνημένες αποδόσεις, με αποτέλεσμα να χάνουν και την αρχική τους επένδυση.

### Θέσεις εργασίας

Η παγκόσμια οικονομική κατάσταση έχει φέρει στο προσκήνιο ένα ακόμη είδος απάτης. Πρόκειται για απατηλές διαδικτυακές αγγελίες που αναρτώνται σε ιστοσελίδες εύρεσης εργασίας ή αποστέλλονται μέσω e-mail στο θύμα και περιγράφουν ιδιαίτερα ελκυστικές θέσεις εργασίας συνήθως στο εξωτερικό, ενώ οι δράστες δεν διστάζουν να δημιουργήσουν ιστοσελίδα της εταιρείας-εργοδότη, στην οποία αναρτούν πληροφορίες για την απατηλή αγγελία προκειμένου να γίνουν ακόμη πιο πειστικοί. Ζητείται από τους ανυποψίαστους υποψήφιους εργαζόμενους να γνωστοποιήσουν τα προσωπικά τους στοιχεία, ακόμη και να αποστείλουν αντίγραφα εγγράφων τους όπως το δίπλωμα οδήγησης, την ταυτότητά τους και όποιο άλλο θεωρηθεί «χρήσιμο» και «απαραίτητο» για τη διεκδίκηση της εν λόγω θέσης εργασίας. Στη συνέχεια, ο εργαζόμενος ενημερώνεται ότι μιας και η εργοδότρια εταιρεία δεν κατέχει τραπεζικό λογαριασμό στη δική του χώρα, ένας από τους πιστωτές της θα του χορηγήσει επιταγή για τα έξοδα και το μισθό του. Η επιταγή συνήθως υπερβαίνει κατά πολύ τα συμφωνηθέντα και ζητείται από τον υποψήφιο να αποστείλει με έμβασμα το επιπλέον ποσό στον εργοδότη. Αφού η διαδικασία ολοκληρωθεί, ο εργαζόμενος αντιλαμβάνεται ότι η επιταγή είναι πλαστή. Σε άλλες περιπτώσεις, το θύμα πείθεται να καταβάλει ένα ποσό για να κατοχυρώσει την εν λόγω «κάλπικη» θέση εργασίας.

## ΑΠΑΛΕΙΨΗ ΧΡΕΟΥΣ (DEBT ELIMINATION)

Επιπλέον, η ισχύουσα οικονομική κατάσταση έχει οδηγήσει στην άνθηση ενός ακόμη είδους απάτης. Πρόκειται για ιστοσελίδες που υπόσχονται τη διαχείριση και εξάλειψη του χρέους των νοικοκυριών και επιχειρηματιών, διαφημίζοντας νόμιμους τρόπους για την αντιμετώπιση των στεγαστικών δανείων και του χρέους από πιστωτικές κάρτες. Συνήθως, το μόνο που ζητείται είναι η καταβολή ενός αρχικού ποσού, η αποστολή όλων των απαραίτητων πληροφοριών που αφορούν τα επίμαχα δάνεια ή τις πιστωτικές κάρτες και, βέβαια, μια εξουσιοδότηση προς το άτομο που θα φέρει εις πέρας τη διαδικασία. Ο διαμεσολαβητής τότε εκδίδει ομόλογα και γραμμάτια προς τους δανειστές που φιλοδοξούν να ικανοποιήσει νόμιμα όλα τα χρέη. Σε αντάλλαγμα, το θύμα είναι υποχρεωμένο να καταβάλει ένα ποσοστό της αξίας των χρεών που θα καλύψει ο διαμεσολαβητής.
Η προαναφερθείσα διαδικασία είναι ιδιαίτερα συνδεδεμένη με τα εγκλήματα που σχετίζονται με την κλοπή ταυτότητας, καθώς οι συμμετέχοντες παρέχουν όλες τις προσωπικές πληροφορίες τους προς τους διαμεσολαβητές.

## BOTNETS

Εκατομμύρια υπολογιστές έχουν μετατραπεί σε υποχείρια οργανωμένων hackers, εν αγνοία των χρηστών τους, απειλώντας τη συνολική λειτουργία του Διαδικτύου. Έως και το ένα τέταρτο των υπολογιστών που συνδέονται στο Διαδίκτυο είναι μολυσμένοι με κρυφό λογισμικό που τους επιστρατεύει σε κακόβουλα δίκτυα, γνωστά ως botnets, ανέφερε ο «πατέρας του Internet» Βιντ Σερφ (επινόησε το πρωτόκολλο TCP/IP). Το φαινόμενο φαίνεται να αποκτά επιδημικές διαστάσεις, καθώς περίπου ένας στους έξι υπολογιστές με σύνδεση στο Διαδίκτυο έχουν μετατραπεί σε «ζόμπι» των botnets.
Ένας ηλεκτρονικός υπολογιστής θεωρείται ότι είναι υπολογιστής-ζόμπι όταν είναι συνδεδεμένος στο Διαδίκτυο και ελέγχεται από κάποιον εξωτερικό χρήστη. Αυτός ο εξωτερικός χρήστης είναι συνήθως κάποιος hacker που, εξαπολύοντας επιτυχημένη επίθεση ενάντια στον υπολογιστή, καταφέρνει να τον μετατρέψει σε υπολογιστή-ζόμπι. Η επίθεση αυτή περιλαμβάνει μεταξύ άλλων τη μόλυνση του υπολογιστή-θύματος από κάποιον ιό ή δούρειο ίππο. Οι υπολογιστές-ζόμπι χρησιμοποιούνται κυρίως για την αποστολή άχρηστων ή κακόβουλων ηλεκτρονικών μηνυμάτων (spam-scam). Με τον τρόπο αυτό οι spammers μπορούν να αποφύγουν τον εντοπισμό τους και χρησιμοποιούν το εύρος ζώνης (bandwidth) των ιδιοκτητών των υπολογιστών-ζόμπι για τους δικούς τους σκοπούς. Τα botnets χρησιμοποιούνται και για την εκτέλεση DDoS Attacks και brute force attacks σε πληροφοριακά συστήματα και για τη χρήση κατά τη διάρκεια απάτης pharming με τη συνεχή δημιουργία απατηλών κλώνων σε διαφορετικά σημεία ανά τον κόσμο. Μέχρι στιγμής, τα μεγαλύτερα botnets που έχουν καταγραφεί αριθμούσαν έως και 30.000.000 Η/Υ!
Στην Ελλάδα, μεγάλος βιομηχανικός οργανισμός έπεσε θύμα επίθεσης botnet που εκδηλώθηκε με την υποκλοπή όλων των ηλεκτρονικών συνομιλιών κατόπιν επίθεσης στον mail server με τη χρήση botnet, ενώ τραπεζικός οργανισμός δέχθηκε ισχυρό πλήγμα, όταν οι χρήστες των υπηρεσιών διαδικτυακής εξυπηρέτησής του έπεσαν θύματα απάτης τη στιγμή που οι Η/Υ τους κατέστησαν «ζόμπι» με τη χρήση ειδικού προγράμματος «Trojan».

### Ιός ransomware

Ένα ακόμη χαρακτηριστικό παράδειγμα της μεθόδου phishing αποτελεί και ο ιός ransomware ή, όπως είναι πλέον γνωστός, «ο ιός των 100€». Οι δράστες, εκμεταλλευόμενοι τις αδυναμίες του Η/Υ του θύματος, του μεταφέρουν κακόβουλο λογισμικό, καθώς εκείνο περιηγείται στο Διαδίκτυο. Το λογισμικό αυτό «κλειδώνει» όλες τις λειτουργίες του Η/Υ και εμφανίζει στην οθόνη του ένα μήνυμα που υποτίθεται ότι προέρχεται από τη Δίωξη Ηλεκτρονικού Εγκλήματος, ενημερώνοντας το χρήστη ότι του επιβάλλεται το πρόστιμο των 100€ για αδικήματα του Ποινικού Κώδικα που υποτίθεται ότι διέπραξε. Η καταβολή του προστίμου δύναται να πραγματοποιηθεί με τη χρήση προπληρωμένων καρτών paysafe ή ucash. Πρόκειται για έναν ιό με πανευρωπαϊκή παρουσία, που χρησιμοποιεί τα εμβλήματα της εκάστοτε αστυνομίας της χώρας από την οποία ο Η/Υ του θύματος έχει πρόσβαση στο Διαδίκτυο. Χιλιάδες χρήστες έχουν πέσει θύματα αυτού, ενώ δεν είναι λίγοι κι εκείνοι που έχουν τελικά καταβάλει το επίμαχο χρηματικό ποσό. Πρόκειται για ένα άριστα οργανωμένο κύκλωμα, το οποίο μέσα από μια πολύπλοκη διαδικασία και μέσα από μηχανισμούς ξεπλύματος μαύρου χρήματος, καταφέρνει να διασπά τις προπληρωμένες κάρτες των 100€ σε κάρτες αξίας 10€, τις οποίες και διανέμει σε όλο τον κόσμο.



### Κινητά τηλέφωνα και διαδικτυακές παγίδες

Η χρήση των κινητών τηλεφώνων και δη των Smartphones αυξάνεται συνεχώς και όλο και περισσότεροι χρήστες τα θεωρούν ως απαραίτητα εργαλεία στην καθημερινότητά τους. Επιτήδειοι, εκμεταλλευόμενοι την τάση αυτή, προκαλούν απάτες αρκετών εκατομμυρίων ευρώ από την αγοραπωλησία εφαρμογών software για κινητά τηλέφωνα, όπως για παράδειγμα για τον εντοπισμό του κινητού τηλεφώνου κάποιου αγαπημένου προσώπου. Συνήθως ζητείται από τον ανυποψίαστο χρήστη να εισαγάγει το κινητό του τηλέφωνο, προκειμένου να αποκτήσει την εφαρμογή που έχει επιλέξει. Στη συνέχεια, ξεκινούν οι υπέρογκες χρεώσεις στον αριθμό του, τις οποίες ο ίδιος αποδέχτηκε καθώς αυτές περιγράφονται στα ψιλά γράμματα των όρων χρήσης που η πλειοψηφία των καταναλωτών δεν διαβάζει.

## ΗΛΕΚΤΡΟΝΙΚΕΣ ΔΗΜΟΠΡΑΣΙΕΣ (AUCTIONS)

Ένα είδος απάτης που είναι ιδιαίτερα διαδεδομένο σε χώρες του εξωτερικού αφορά τις διαδικτυακές δημοπρασίες. Αυτού του είδους οι απάτες εστιάζουν κυρίως στη διαστρεβλωμένη παρουσίαση ή στη μη παράδοση του δημοπρατούμενου προϊόντος. Οι καταναλωτές θα πρέπει να είναι ιδιαίτερα προσεκτικοί όταν οι πωλητές τούς ζητούν να καταβάλουν το συμφωνημένο χρηματικό ποσό σε λογαριασμό κάποιου τρίτου ή επικαλούνται έκτακτους λόγους που τους αναγκάζουν να εγκαταλείψουν τη χώρα τους, καθώς επίσης, όταν η καταβολή του ποσού ζητείται να πραγματοποιηθεί μέσω Western Union ή MoneyGram.

## ΟΙ ΝΟΜΟΙ ΣΤΗΝ ΠΡΑΞΗ

Τα στελέχη της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος για την αντιμετώπιση των παραβατικών πράξεων που συντελούνται μέσα από το Διαδίκτυο και συνιστούν το αδίκημα της «Απάτης», καθοδηγούνται από δύο βασικά άρθρα του κοινού Ποινικού Κώδικα (Π.Κ.): α) άρθρο 386 «Απάτη», και β) άρθρο 386Α «Απάτη με υπολογιστή», τα οποία περιληπτικά περιγράφονται ως εξής:

### Άρθρο 386 «Απάτη»

**1.** Όποιος, με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και, αν η ζημιά που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών.

**3.** Επιβάλλεται κάθειρξη μέχρι δέκα ετών: α) αν ο υπαίτιος διαπράττει απάτες κατ' επάγγελμα ή κατά συνήθεια και το συνολικό όφελος ή η συνολική ζημιά υπερβαίνουν το ποσό των τριάντα χιλιάδων (30.000) ευρώ, ή β) εάν το περιουσιακό όφελος ή η προξενηθείσα ζημία υπερβαίνει συνολικά το ποσό των εκατό είκοσι χιλιάδων (120.000) ευρώ.

### Άρθρο 386Α «Απάτη με υπολογιστή»

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του άρθρου 386. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα πρόσωπα.

## ΠΟΣΟ ΑΡΑΓΕ ΚΟΣΤΙΖΕΙ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ;

Μια από τις μεγαλύτερες εταιρείες τεχνολογίας στον κόσμο παρουσίασε περί τα τέλη του 2012 μια νέα έρευνα, η οποία αναδεικνύει ότι το κόστος και η συχνότητα του κυβερνοεγκλήματος συνέχισαν να αυξάνονται για τρίτη συνεχόμενη χρονιά. Σύμφωνα με την τρίτη ετήσια έρευνα, που αφορούσε πολυεθνικές εταιρείες των Η.Π.Α., η συχνότητα των κυβερνοεπιθέσεων έχει σημειώσει ραγδαία αύξηση μέσα σε τρία χρόνια, ενώ οι οικονομικές τους επιπτώσεις αυξήθηκαν περίπου κατά 40%. Η έρευνα για το Κόστος του Κυβερνοεγκλήματος για το 2012 (Cost of Cyber Crime Study 2012), η οποία διενεργήθηκε από το **«Ponemon Institute»**, κατέδειξε ότι το **μέσο ετήσιο κόστος του κυβερνοεγκλήματος** για ένα ενδεικτικό δείγμα επιχειρήσεων στις Η.Π.Α. ανήλθε στα **8,9 εκατ. δολάρια**. Το ποσό αυτό παρουσιάζει αύξηση 6% σε σχέση με το μέσο κόστος για το 2011 και 38% σε σχέση με το αντίστοιχο μέγεθος για το 2010. Επίσης, η φετινή έρευνα κατέγραψε μια αύξηση 42% στον αριθμό των κυβερνοεπιθέσεων, με τους οργανισμούς να αντιμετωπίζουν κατά μέσο όρο **102 ολοκληρωμένες επιθέσεις την εβδομάδα**, ενώ αντιμετώπιζαν 72 και 50 επιθέσεις την εβδομάδα το 2011 και το 2010 αντίστοιχα. Ανώτατο στέλεχος της εταιρείας που πραγματοποίησε την έρευνα δήλωσε:

*«Οι οργανισμοί ξοδεύουν συνεχώς περισσότερο χρόνο, χρήμα και ενέργεια για να ανταποκριθούν στις κυβερνοαπειλές, φτάνοντας σε επίπεδα που σύντομα θα καταστούν μη βιώσιμα. Υπάρχουν στοιχεία που ξεκάθαρα δείχνουν ότι η χρήση προηγμένων λύσεων "security intelligence" βοηθά στην ουσιαστική μείωση του κόστους, της συχνότητας και των επιπτώσεων αυτών των επιθέσεων.»*

Και φέτος, το **μεγαλύτερο κόστος** για τις επιχειρήσεις προήλθε από κυβερνοεγκλήματα όπως η χρήση κακόβουλων κωδικών, οι επιθέσεις άρνησης υπηρεσίας, η χρήση κλεμμένων ή παραβιασμένων συσκευών και η κακόβουλη δραστηριότητα προσώπων που βρίσκονται μέσα σε έναν οργανισμό. **Συνδυαστικά**, το **κόστος** που προέρχεται από αυτές τις απειλές αντιστοιχεί σε **περισσότερο από το 78% του ετήσιου κόστους του κυβερνοεγκλήματος ανά οργανισμό**. Επίσης, η έρευνα κατέληξε στα παρακάτω **βασικά ευρήματα**:

- Η κλοπή πληροφοριών και η διακοπή των εργασιών συνεχίζουν να αντιστοιχούν στο μεγαλύτερο εξωτερικό κόστος για τις επιχειρήσεις. Σε ετήσια βάση, **η υποκλοπή πληροφοριών ισοδυναμεί με το 44% του συνολικού εξωτερικού κόστους**, σημειώνοντας άνοδο 4% σε σχέση με το 2011. Η διακοπή των εργασιών ή η μείωση της παραγωγικότητας αντιστοιχεί στο 30% του εξωτερικού κόστους, σημειώνοντας άνοδο 1% από το 2011.
- Η χρήση **προηγμένων λύσεων ασφάλειας πληροφοριών και διαχείρισης περιστατικών (Security Information & Event Management –SIEM)** μπορεί να περιορίσει τις επιπτώσεις των κυβερνοαπειλών. Οι οργανισμοί που χρησιμοποίησαν τέτοιες λύσεις εξοικονόμησαν περίπου 1,6 εκατ. δολάρια το χρόνο. Γι' αυτούς τους οργανισμούς, το κόστος για την ανάκτηση των συστημάτων, τον εντοπισμό και τον περιορισμό των απειλών ήταν σημαντικά μικρότερο σε σχέση με το κόστος που αντιμετώπισαν όσοι δεν αξιοποίησαν λύσεις SIEM.
- Οι κυβερνοεπιθέσεις μπορεί να κοστίσουν ακριβά, αν δεν αντιμετωπιστούν γρήγορα. Ο **μέσος χρόνος αντιμετώπισης** μιας κυβερνοεπίθεσης είναι **24 μέρες**, αλλά μπορεί να φτάσει μέχρι και τις 50, σύμφωνα με τη φετινή μελέτη. Το μέσο κόστος που προέκυψε για την περίοδο των 24 ημερών ανερχόταν σε 591.780$, καταγράφοντας αύξηση 42% σε σχέση με το μέσο εκτιμώμενο κόστος των 415.748$ για την ίδια περίοδο πέρυσι.
- Η ανάκτηση δεδομένων και ο εντοπισμός των απειλών παραμένουν οι πιο δαπανηρές εσωτερικές δραστηριότητες σε σχέση με το κυβερνοέγκλημα. Σε ετήσια βάση, αυτές οι δραστηριότητες αντιστοιχούν στο **μισό σχεδόν του συνολικού εσωτερικού κόστους**, με τα λειτουργικά έξοδα και το κόστος εργασίας να αντιστοιχούν στο μεγαλύτερο μέρος του.

Ο Πρόεδρος και ιδρυτής του Ponemon Institute, **Dr Larry Ponemon**, δήλωσε ότι σκοπός αυτής της έρευνας είναι να ποσοτικοποιήσει τις οικονομικές επιπτώσεις των κυβερνοεπιθέσεων και να καταγράψει τις διαχρονικές τάσεις που αφορούν το σχετικό κόστος, και ότι η καλύτερη κατανόηση του κόστους τού κυβερνοεγκλήματος θα βοηθήσει τους οργανισμούς να καθορίσουν τις κατάλληλες επενδύσεις και τους πόρους που χρειάζονται, ώστε να μετριάσουν τις καταστροφικές συνέπειες μιας επίθεσης.

Αντίστοιχες μελέτες για το κόστος του κυβερνοεγκλήματος έχουν πραγματοποιηθεί στην Αυστραλία, τη Γερμανία, την Ιαπωνία και το Ηνωμένο Βασίλειο με παρόμοια αποτελέσματα. Για παράδειγμα, η εταιρεία λύσεων τεχνολογίας ασφάλειας πληροφοριακών συστημάτων RSA δημοσίευσε για το 1ο εξάμηνο του 2012 έρευνα σχετικά με την αύξηση του κόστους που επέφερε το phishing σε εταιρείες του Η.Β., του Καναδά και των Η.Π.Α. Το phishing υφίσταται ως φαινόμενο για τα τελευταία 16 χρόνια και εξακολουθεί να αποτελεί έναν από τους μεγαλύτερους κινδύνους που κρύβει το Διαδίκτυο. Το κόστος του σημείωσε αύξηση κατά 19% σε σχέση με το αντίστοιχο του 1ου εξαμήνου του 2011 και προκάλεσε ζημιά ύψους 687 εκατ. δολαρίων για τις αμερικάνικες εταιρείες. Η έρευνα κατέδειξε ότι το Η.Β., οι Η.Π.Α., ο Καναδάς, η Βραζιλία και η Νότια Αφρική συγκαταλέγονται στις χώρες με τις περισσότερες επιθέσεις phishing διεθνώς. Συγκεκριμένα στον Καναδά τα φαινόμενα phishing σημείωσαν αύξηση κατά 400% κατά το 1ο εξάμηνο του 2012 σε σχέση με το αντίστοιχο περυσινό, γεγονός που ενδεχομένως οφείλεται στην οικονομική σταθερότητα της χώρας αλλά και στην ισοτιμία σχεδόν 1:1 σε σχέση με το αμερικάνικο δολάριο, καθώς οι «απατεώνες» αρέσκονται να ακολουθούν το χρήμα. Όπως και να έχει τελικά, παρά το γεγονός ότι το phishing ήδη μετρά 16 χρόνια ζωής και θεωρείται «παλαιό» φαινόμενο, κανείς δεν μπορεί να αγνοήσει ζημιά 687 εκατ. δολαρίων.

## ONLINE ΣΥΝΑΛΛΑΓΕΣ ΚΑΙ ΑΣΦΑΛΕΙΑ

Με την πάροδο του χρόνου, όλο και περισσότερες επιχειρήσεις δραστηριοποιούνται μέσω του Διαδικτύου, αυξάνοντας τα έσοδά τους, μειώνοντας το κόστος τους και διευκολύνοντας τους χρήστες. Με τον τρόπο αυτό ο καθένας δύναται να έχει πρόσβαση όλο το 24ωρο στον κατάλογο μιας επιχείρησης και να αγοράσει ό,τι επιθυμεί. Οι περισσότερες ιστοσελίδες που πουλούν προϊόντα, χρησιμοποιούν συστήματα πληρωμών-συναλλαγών, όπως το Paypal, διατραπεζικά συστήματα, κ.λπ. Πώς μπορούμε να είμαστε βέβαιοι ότι δεν θα εξαπατηθούμε και πώς μπορούμε να υποψιαστούμε απάτες ώστε να τις αποφύγουμε;

**Είναι όμως οι online συναλλαγές ασφαλείς;**
Πώς μπορούμε να είμαστε βέβαιοι ότι δεν θα εξαπατηθούμε και πώς μπορούμε να υποψιαστούμε απάτες ώστε να τις αποφύγουμε;

## ΤΙ ΘΑ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΕΧΕΙ ΚΑΝΕΙΣ ΟΣΟΝ ΑΦΟΡΑ ΤΙΣ ΣΥΝΑΛΛΑΓΕΣ ΤΟΥ

**1)** Να μην κάνει τις συναλλαγές του χρησιμοποιώντας **δημόσιους υπολογιστές** (από net cafe, καφετέριες, βιβλιοθήκες, κ.λπ.). Μπορεί να έχουν keyloggers ή spy-wares, χωρίς να το γνωρίζει το προσωπικό του χώρου αυτού. Έτσι, κακόβουλοι χρήστες μπορούν εύκολα να υποκλέψουν τα ευαίσθητα προσωπικά στοιχεία κάποιου και να προβούν σε συναλλαγές αντ' αυτού.
**2)** Όταν πραγματοποιεί συναλλαγές από τον υπολογιστή του, θα πρέπει να είναι σίγουρος ότι έχει λάβει όλα τα **απαραίτητα μέτρα ασφαλείας πρόσφατα ενημερωμένα** (firewall, antivirus, anti-spyware, κ.λπ.).
**3)** Όταν συγκρίνει προϊόντα από διάφορες ιστοσελίδες, μπορεί να βρει σε κάποιες εξ αυτών **τα ίδια προϊόντα φθηνότερα σε σχέση με άλλες ιστοσελίδες**. Καλό θα ήταν, λοιπόν, να ψάξει μήπως οι ιστοσελίδες αυτές είναι φαντάσματα (μια αναζήτηση στο Google με την επωνυμία της ιστοσελίδας με τα πολύ φθηνά προϊόντα αρκεί).
**4)** Πάντα να κάνει τις συναλλαγές του **πληκτρολογώντας ο ίδιος τη διεύθυνση της ιστοσελίδας**. Να μην κλικάρει πάνω σε links από e-mail, καθώς μπορεί να είναι απατηλά.
**5)** Να πραγματοποιεί τις πληρωμές-συναλλαγές του μόνο μέσω ιστοσελίδων που έχουν το **εικονίδιο ασφαλείας** (μια κλειδαριά πάνω αριστερά στον browser). Το εικονίδιο αυτό μας ενδιαφέρει ουσιαστικά εκεί που πληκτρολογούμε π.χ. αριθμό κάρτας και τα υπόλοιπα ευαίσθητα προσωπικά στοιχεία και κλικάρουμε αποστολή.
**6)** Να επαληθεύει ότι εκεί που πληκτρολογεί τα ευαίσθητα στοιχεία του, στον browser δεν γράφει http αλλά **https**.
**7)** Προτού πραγματοποιήσει κάποια συναλλαγή μέσω μιας ιστοσελίδας, θα πρέπει να **καλέσει** στο ηλεκτρονικό κατάστημα, προκειμένου να επιβεβαιώσει εάν λειτουργεί η επιχείρηση. Εάν δεν απαντήσουν, το πιθανότερο είναι να μην αποστείλουν ούτε το αγορασθέν προϊόν, ακόμη κι αν έχει πληρωθεί.
**8)** Πάντα να τηρεί κάπου στον υπολογιστή του ή να εκτυπώνει τις **αποδείξεις** από τις αγορές του.
**9)** Να είναι ιδιαίτερα προσεκτικός όσον αφορά συναλλαγές μέσω **εταιρειών μεταφοράς χρημάτων και διεθνών πληρωμών** (Western Union, Money-Gram, BidPay κ.λπ.).
**10)** Να είναι βέβαιος ότι οι κωδικοί του, οι αριθμοί των καρτών του (χρεωστικών-πιστωτικών) και τα άλλα ευαίσθητα προσωπικά στοιχεία του είναι **φυλαγμένα επαρκώς**, ώστε να μην μπορεί κάποιος να τα υποκλέψει ή να τα απομνημονεύσει.
**11)** Να φροντίζει να **αλλάζει** τους **κωδικούς** του σε τακτά χρονικά διαστήματα και αυτοί να αποτελούνται από πεζά και κεφαλαία γράμματα, αριθμούς και σύμβολα.

## ΤΙ ΘΑ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΕΧΕΙ ΚΑΝΕΙΣ ΟΣΟΝ ΑΦΟΡΑ ΤΙΣ ΑΓΟΡΕΣ ΤΟΥ

**1)** Ποτέ να μην πληρώνει προκαταβολικά σε πωλητή που δεν γνωρίζει, ακόμη κι αν αυτός αποκαλύπτει τα προσωπικά του στοιχεία ή τον αριθμό του τραπεζικού του λογαριασμού.
**2)** Να αναζητά πληροφορίες-αναρτήσεις σχετικά με το πώς το διαδικτυακό κατάστημα διαχειρίζεται τυχόν παράπονα πελατών του.
**3)** Να ζητά την αυθεντική απόδειξη ή γραπτή απόδειξη αγοράς.
**4)** Να προσέχει ιδιαιτέρως όταν η προσφορά φαίνεται πολύ καλή για να είναι αληθινή, και το άλλο μέρος ασκεί συνεχώς πίεση για την ολοκλήρωση της αγοραπωλησίας.
**5)** Να προσέχει όταν του ζητείται η πληρωμή μεγάλων ποσών σε ανθρώπους που δεν γνωρίζει: θα πρέπει να πραγματοποιείται συνάντηση σε κάποιο κατάστημα ή δημόσιο χώρο.
**6)** Να προσέχει εάν κατά την αγορά επώνυμων προϊόντων αυτά είναι όντως αυθεντικά.

### Πώς να προστατεύσει κανείς τις συναλλαγές μέσω κινητού τηλεφώνου;

**1)** Διατηρήστε το λογισμικό προστασίας του κινητού τηλεφώνου σας επικαιροποιημένο και όλες τις συσκευές που συνδέονται με αυτό προφυλαγμένες από κακόβουλες επιθέσεις και ιούς.
**2)** Χρησιμοποιήστε έναν ισχυρό κωδικό προκειμένου να κλειδώνετε τη συσκευή του κινητού σας τηλεφώνου.
**3)** Μελετήστε προσεκτικά τις εφαρμογές που επιθυμείτε να εγκαταστήσετε πριν το κάνετε.
**4)** Δώστε τον αριθμό του κινητού σας τηλεφώνου μόνο σε άτομα της εμπιστοσύνης σας και μη δίνετε τον αριθμό του κινητού άλλων χωρίς την έγκρισή τους.
**5)** Ενεργοποιήστε την υπηρεσία γεωεντοπισμού του κινητού σας σε περίπτωση που το χάσετε.
**6)** Να είστε προσεκτικοί με τα δίκτυα Wi-Fi Hotspot στα οποία συνδέεστε με το κινητό σας τηλέφωνο.
**7)** Όταν γίνεστε αποδέκτης μηνυμάτων τον αποστολέα των οποίων δεν γνωρίζετε, μην ανταποκρίνεστε.
**8)** Μπλοκάρετε τους χρήστες των οποίων τον αριθμό και το e-mail δεν γνωρίζετε, χρησιμοποιώντας CALLER ID.
**9)** Επιβάλετε σε όσους προσπαθούν να σας τραβήξουν φωτογραφία ή βίντεο να λαμβάνουν πρώτα την άδειά σας.

## ΜΠΟΡΟΥΝ ΟΙ ΕΠΙΧΕΙΡΗΣΕΙΣ ΝΑ ΑΝΤΙΜΕΤΩΠΙΣΟΥΝ ΤΗΝ ΚΥΒΕΡΝΟΑΠΑΤΗ ΚΑΙ ΜΕ ΠΟΙΟΝ ΤΡΟΠΟ;

Οι επιχειρήσεις θα πρέπει, εκτός από την εφαρμογή λογισμικών προστασίας και ασφάλειας των πληροφοριακών τους συστημάτων, να εκπαιδεύουν το προσωπικό τους, έτσι ώστε να αποκτήσει «Κουλτούρα Ασφάλειας» (Culture of Security). Είναι αρκετά συχνό το φαινόμενο, κατά την πρόσληψη των υπαλλήλων της, μια επιχείρηση να τους ζητά να υπογράψουν όρους και πολιτικές ασφαλείας που θα πρέπει να τηρούν, ώστε να προστατεύεται τόσο το πελατολόγιο της εταιρείας όσο και τα πληροφοριακά δεδομένα της. Στην προσπάθειά της αυτή μια επιχείρηση θα πρέπει να εφαρμόζει κάποια μέτρα, τα οποία συνοψίζονται στα εξής:

**1)** Να εντοπίσει ποια δεδομένα είναι εκτεθειμένα σε μεγαλύτερο κίνδυνο, εφόσον τα πληροφοριακά της συστήματα έχουν πρόσβαση στο Διαδίκτυο (π.χ. στοιχεία πελατών της ή λογιστικά δεδομένα και οικονομικά στοιχεία).
**2)** Να έχει εγκατεστημένα σε όλους τους Η/Υ ειδικά λογισμικά (π.χ. προγράμματα antivirus, προγράμματα anti-spyware, firewalls) και οι κωδικοί πρόσβασης και συναλλαγών να αλλάζουν κάθε 60 ή 70 μέρες.
**3)** Να εγκαθιστά πρόγραμμα που θα τηρεί back-ups (π.χ. σε εξωτερικό σκληρό δίσκο) όλων των σημαντικών δεδομένων, και να το αναβαθμίζει σε τακτά χρονικά διαστήματα, έτσι ώστε να μην υπάρχει απώλεια δεδομένων σε περίπτωση φυσικής καταστροφής ή κυβερνοεπίθεσης. Καλό θα ήταν να κρυπτογραφούνται όλα τα ευαίσθητα και υψίστης σημασίας δεδομένα.
**4)** Να έχει ήδη σχεδιασμένο πλάνο επείγουσας επέμβασης ή εναλλακτικών ενεργειών σε περίπτωση κυβερνοεπίθεσης, το οποίο θα πρέπει να ελέγχεται ετησίως.
**5)** Να εκπαιδεύει το προσωπικό της για την επίδραση που θα έχει σε όλους μια κυβερνοεπίθεση με τη μορφή της απάτης. Η εκπαίδευση μπορεί να γίνει με σεμινάρια πάνω σε πρακτικές του Διαδικτύου ή και τεχνολογικές λύσεις που θα πείθουν τους εργαζομένους ότι θα πρέπει να είναι ιδιαιτέρως προσεκτικοί απέναντι σε διαδικτυακές απάτες, καθώς μπορεί να εξαπατηθούν και να ζημιωθούν στην προσωπική τους ζωή μέσα από το Διαδίκτυο.
**6)** Να υπογράφει συμβόλαια με τους εργαζομένους της, τους οποίους θα δεσμεύει να αναφέρουν προς τις αρμόδιες αρχές τυχόν υποψία αλλά και πραγμάτωση διαδικτυακής απατηλής συναλλαγής.

### Μερικές συμβουλές:

**1)** Συνεργαστείτε μόνο με εταιρείες που γνωρίζετε ή στα στοιχεία των οποίων μπορείτε να έχετε άμεση πρόσβαση από επίσημες βάσεις δεδομένων.
**2)** Κατανοήστε όλες τις λεπτομέρειες σχετικά με τις προσφερόμενες υπηρεσίες ή προϊόντα.
**3)** Ελέγξτε προσεκτικά όλα τα τιμολόγια και τους λογαριασμούς που καλείστε να πληρώσετε.
**4)** Διαφυλάξτε τα οικονομικά και τραπεζικά δεδομένα σας και μην τα αποκαλύπτετε σε άγνωστους τρίτους.
**5)** Καταστήστε το προσωπικό σας υπεύθυνο για τυχόν λανθασμένες ενέργειες, αφού πρώτα το εκπαιδεύσετε σχετικά.

### Συμβουλές για Ηλεκτρονικές Δημοπρασίες (Auctions):

- Πριν δώσετε προσφορά, επικοινωνήστε με τον πωλητή και ξεκαθαρίστε αμφισβητούμενα σημεία σχετικά με το δημοπρατούμενο προϊόν.
- Να είστε ιδιαίτερα προσεκτικοί όσον αφορά αντισυμβαλλόμενους στο εξωτερικό.
- Επιβεβαιώστε τις πολιτικές επιστροφής και εγγύησης του προϊόντος, καθώς και τα μεταφορικά έξοδα.
- Ασφαλίστε τα δημοπρατηθέντα κατά τη μεταφορά τους.

### Συμβουλές για Απάτες σχετικές με Πιστωτικές Κάρτες (credit card fraud):

- Επιβεβαιώστε ότι η ιστοσελίδα όπου δηλώνετε τα στοιχεία της πιστωτικής σας κάρτας είναι ασφαλής και γνωστή στο ευρύ κοινό.
- Επιβεβαιώστε και το κατάστημα που προβάλλεται μέσω της ιστοσελίδας.
- Ελέγχετε συχνά τις κινήσεις της πιστωτικής σας κάρτας μέσω της τράπεζάς σας ή μέσω web-banking.

### Συμβουλές για εξάλειψη χρέους:

- Ελέγχετε εάν είναι υπαρκτά το όνομα, η διεύθυνση και ο τηλεφωνικός αριθμός της εταιρείας ή του φυσικού προσώπου που προβάλλεται ως «σωτήρας».
- Ελέγξτε τους όρους της συμφωνίας πριν υπογράψετε.
- Προσέξτε εταιρείες που δηλώνουν μόνο ταχυδρομικές θυρίδες για επικοινωνία.
- Προσέξτε μήπως αυτά που υπόσχονται είναι πολύ καλά για να είναι αληθινά.

### Συμβουλές για θέσεις εργασίας:

- Προσέξτε μήπως υπόσχονται πολλά έσοδα ή κέρδη.
- Προσέξτε μήπως σας ζητήσουν να προκαταβάλετε χρήματα για διαδικαστικά θέματα.
- Προσέξτε αγγελίες εργασίας που δεν ζητούν προϋπηρεσία ως απαραίτητο προσόν.
- Επιβεβαιώστε ότι η εταιρεία-εργοδότης είναι υπαρκτή.

# ΜΠΟΡΟΥΝ ΟΙ ΕΠΙΧΕΙΡΗΣΕΙΣ ΝΑ ΑΝΤΙΜΕΤΩΠΙΣΟΥΝ ΤΗΝ ΚΥΒΕΡΝΟΑΠΑΤΗ ΚΑΙ ΜΕ ΠΟΙΟΝ ΤΡΟΠΟ;

**Συμβουλές για νιγηριανές επιστολές:**

- Προσέξτε μήπως αυτά που σας υπόσχονται είναι πολύ καλά για να είναι αληθινά.
- Μην απαντάτε σε e-mail που σας ζητούν στοιχεία τραπεζικού λογαριασμού.
- Μην εξαπατάστε από άτομα που παρουσιάζονται ως κυβερνητικοί υπάλληλοι μιας ξένης χώρας.
- Προσέξτε όταν σας ζητούν να βοηθήσετε στην τοποθέτηση χρημάτων σε υπεράκτιους λογαριασμούς.
- Μην εμπιστεύεστε όσους σας υπόσχονται μεγάλα χρηματικά ποσά σε περίπτωση συνεργασίας.

**Συμβουλές για phishing:**

- Να είστε καχύποπτοι όταν σας ζητούν μέσω απομονωμένων e-mail προσωπικές πληροφορίες.
- Μη συμπληρώνετε φόρμες με τα προσωπικά σας στοιχεία όταν σας αποστέλλονται από άγνωστες διευθύνσεις ηλεκτρονικών ταχυδρομείων.
- Πληκτρολογήστε στον browser τη διεύθυνση της ιστοσελίδας και μην μπαίνετε σε αυτή μέσω συνδέσμων.

**Συμβουλές για spamming:**

- Μην ανοίγετε τα μηνύματα spam.
- Μην απαντάτε στα μηνύματα spam, ώστε ο αποστολέας να μην αντιληφθεί ότι η διεύθυνσή σας είναι υπαρκτή και ενεργή.
- Διατηρείτε δύο e-mail διευθύνσεις, μία για τους οικείους σας και μία για κάθε άλλο σκοπό.
- Ποτέ μην αγοράζετε κάτι που σας αποστέλλεται μέσω ενός απομονωμένου e-mail.

Συνοψίζοντας, δεν θα πρέπει να κυριεύεται κανείς από το αίσθημα του φόβου πριν προβεί σε online πληρωμές και συναλλαγές.
ΟΛΟΙ θα πρέπει να απολαμβάνουμε τα πλεονεκτήματα που μας παρέχουν αυτού του τύπου οι συναλλαγές και να πραγματοποιούμε τις αγορές μας πιο φθηνά, πιο ξεκούραστα, με μεγαλύτερη ποικιλία και τη δυνατότητα να επιλέξουμε και να αγοράσουμε όποτε και οτιδήποτε επιθυμούμε. Η Υπηρεσία μας αντιμετωπίζει θετικά τις online συναλλαγές, αρκεί να διαθέτει κανείς τα χρυσά εργαλεία για όλων των τύπων τις συναλλαγές και να μπορεί να τις ελέγχει πλήρως. Ποια είναι αυτά;

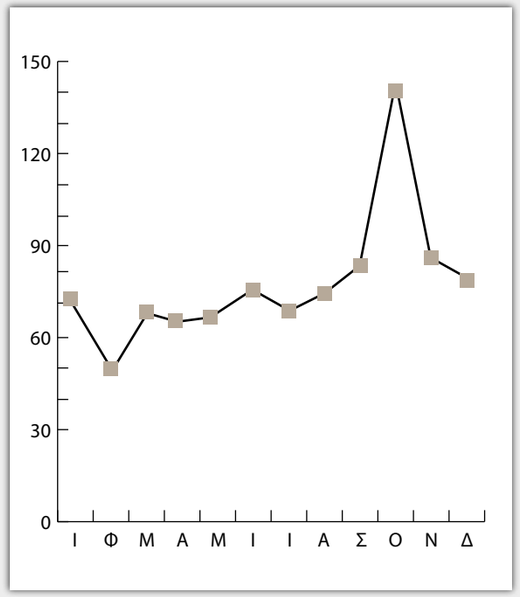
**α)** Μια **προπληρωμένη κάρτα** που θα έχει εκδότη ένα έγκριτο χρηματοπιστωτικό ίδρυμα.
**β)** Ένας λογαριασμός **Paypal** συνδεδεμένος με μια κάρτα ανάληψης.
**γ) E-banking** για την άμεση πρόσβαση στις κινήσεις των λογαριασμών και των καρτών, αλλά και για την άμεση πραγματοποίηση πληρωμών.



# ΑΠΟΛΟΓΙΣΤΙΚΑ ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΕΞΙΧΝΙΑΣΗΣ ΑΠΑΤΩΝ ΑΠΟ ΤΗ ΔΙΕΥΘΥΝΣΗ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΓΙΑ ΤΟ 2015

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος διαχειρίστηκε με επιτυχία εννιακόσιες είκοσι (920) περιπτώσεις διαδικτυακών απατών και παράνομης νομιμοποίησης εσόδων (money laundering), η μηνιαία εξέλιξη των οποίων περιγράφεται στο κατωτέρω διάγραμμα.

**ΑΠΑΤΕΣ (ΜΗΝΙΑΙΑ ΕΞΕΛΙΞΗ)**




**ΒΙΒΛΙΟΓΡΑΦΙΑ**
http://www.ic3.gov
http://www.fraud.org
http://www.staysafeonline.org
http://www.rsa.com
http://www.businessweek.com
http://www.acfe.gr
http://www.interpol.int

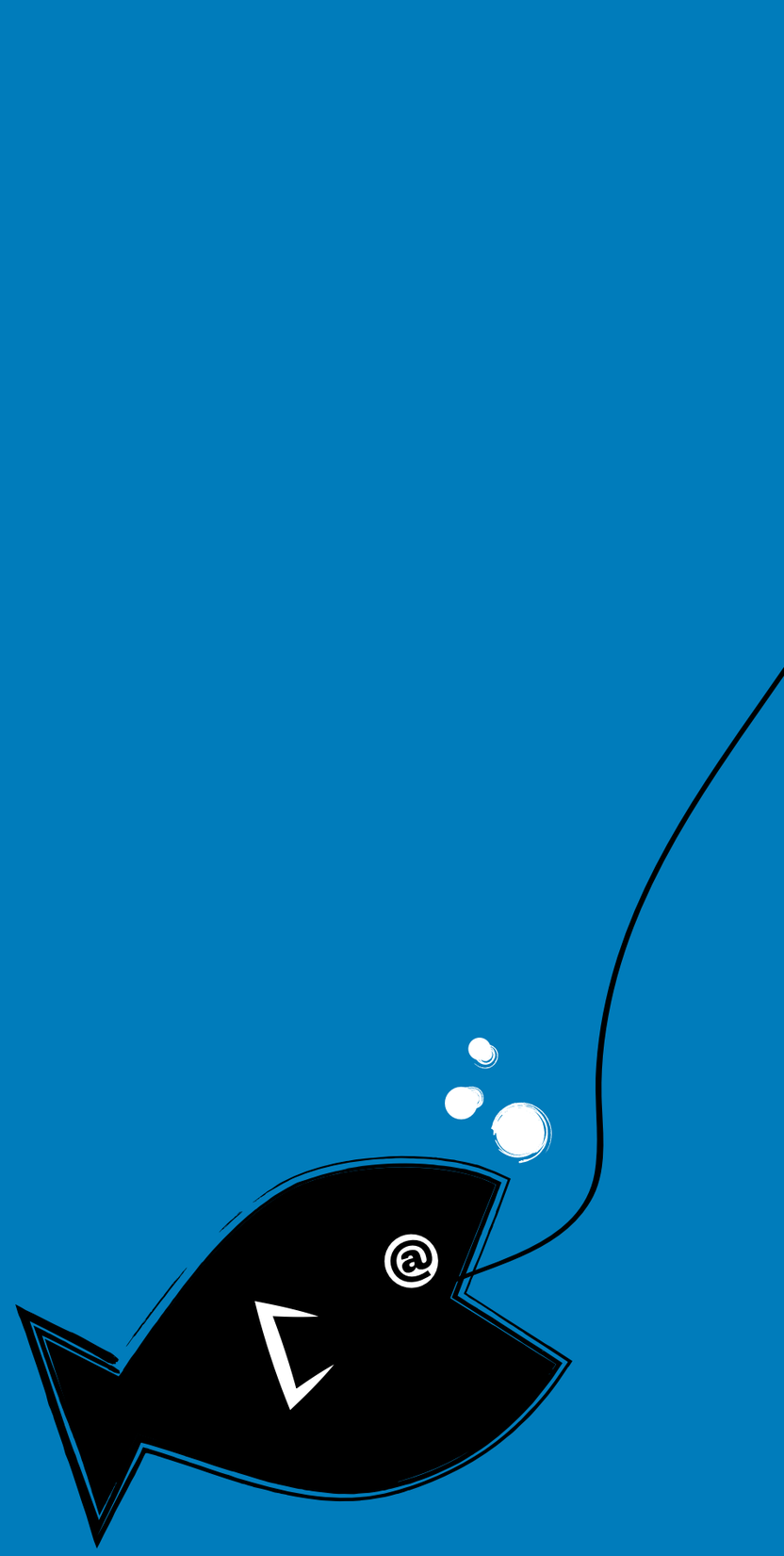
ΕΜΜΑΝΟΥΗΛ ΣΦΑΚΙΑΝΑΚΗΣ,
ΚΩΝΣΤΑΝΤΙΝΟΣ ΣΙΩΜΟΣ,
ΓΕΩΡΓΙΟΣ ΦΛΩΡΟΣ,
ΕΘΙΣΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
ΚΑΙ ΑΛΛΕΣ ΔΙΑΔΙΚΤΥΑΚΕΣ
ΣΥΜΠΕΡΙΦΟΡΕΣ ΥΨΗΛΟΥ ΚΙΝΔΥΝΟΥ,
ΕΚΔΟΣΕΙΣ ΛΙΒΑΝΗ 2012.

ΑΝΑΣΤΑΣΙΑ Κ. ΜΑΛΛΕΡΟΥ,
ΤΟ ΔΙΚΑΙΟ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΧΡΗΜΑΤΟΣ,
ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ 2007.

ΘΕΟΔΩΡΟΣ Ν. ΚΡΙΘΑΡΑΣ,
ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΔΙΑΔΙΚΤΥΟ,
ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ 2009.

# #ηλεκτρονικό_ψάρεμα

Όταν ένα «κλικ» μπορεί να είναι παγίδα




Βασική αρχή στις απάτες που διαπράττονται μέσω Διαδικτύου είναι να πείσουν το θύμα να καταβάλει ένα μικρό αρχικό ποσό με σκοπό να εξασφαλίσει ένα πολύ μεγαλύτερο στο μέλλον, όπως για παράδειγμα οι νιγηριανές απάτες, ή γενικότερα να πείσουν το θύμα για την ασφάλεια των διαδικτυακών συναλλαγών, με σκοπό στη συνέχεια να του αποσπάσουν μεγάλα χρηματικά ποσά (απάτες με πιστωτικές κάρτες, κ.τ.λ.).

# ΗΛΕΚΡΟΝΙΚΕΣ ΣΥΣΚΕΥΕΣ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

## Ασφαλής χρήση κινητών συσκευών

iPhone & iPad

### 1. Συμβουλές ασφαλούς χρήσης προσωπικών iPhone & iPad

Στην παρακάτω ενότητα, θα βρείτε μερικές βασικές συμβουλές για την ασφαλή χρήση του iPhone και του iPad που χρησιμοποιούν το λειτουργικό σύστημα iOS 4. Οι οδηγίες δεν αφορούν συσκευές οι οποίες λειτουργούν σε εταιρικό περιβάλλον, αλλά μόνο συσκευές των οποίων τον έλεγχο έχει ο χρήστης. Πληροφορίες σχετικά με εταιρική σύνδεση και με θέματα όπως το VPN μπορούν να αναζητηθούν στην ιστοσελίδα της Apple
http://www.apple.com/support/iphone/enterprise

### 2. Ασφάλεια της συσκευής

Πρέπει συνεχώς να προστατεύουμε τη φορητή ηλεκτρονική συσκευή από τυχόν επιτήδειους που θα θελήσουν να προσθέσουν κάποιο ύποπτο λογισμικό ή απλώς να διαβάσουν προσωπικά στοιχεία μας. Υπάρχουν αρκετοί τρόποι με τους οποίους κάποιος μπορεί να παρακάμψει τους μηχανισμούς ασφαλείας μιας συσκευής, έχοντας αποκτήσει πρόσβαση σε αυτήν. Ιδιαίτερα για τα κινητά τηλέφωνα, είναι αυξημένος ο κίνδυνος να αποκτήσει κάποιος πρόσβαση σε αυτά. Ο καλύτερος τρόπος προφύλαξης είναι να εξασφαλίσουμε ότι οι συσκευές μας με λειτουργικό iOS δεν θα βρεθούν σε χέρια ανθρώπων που θέλουν να μας βλάψουν. Αν αναλογιστούμε τον ιδιαίτερα υψηλό κίνδυνο να διαρρεύσουν ευαίσθητα δεδομένα που είναι αποθηκευμένα στη συσκευή μας, μπορούμε να αντιληφθούμε πόσο σημαντικό θέμα είναι η προστασία της. Τα δεδομένα που αποθηκεύονται μπορεί να είναι από συνθηματικές λέξεις που χρησιμοποιούνται σε κοινωνικά δίκτυα, μέχρι κωδικοί πιστωτικών καρτών. Αν το κινητό σας τηλέφωνο βρεθεί σε λάθος χέρια, σκεφτείτε σε πόσες πληροφορίες θα μπορεί κάποιος να έχει πρόσβαση!

### 3. Αναβάθμιση – Ενημέρωση Λογισμικού

Κάθε φορά η αναβάθμιση του κινητού τηλεφώνου θα πρέπει να γίνεται με το πιο πρόσφατο λογισμικό του iOS.
Οι αναβαθμίσεις αυτές θα πρέπει να γίνονται μέσω ενός προσωπικού υπολογιστή συνδεδεμένου με το διαδίκτυο, στον οποίο έχουμε εγκαταστήσει το πρόγραμμα iTunes. Τόσο η ενημέρωση του λογισμικού της κινητής συσκευής όσο και η εγκατάσταση του iTunes αποτελούν αποκλειστική ευθύνη του χρήστη. Προτείνεται να γίνεται ενημέρωση του λογισμικού από ηλεκτρονικό υπολογιστή τον οποίο γνωρίζουμε.

### 4. Μη χρησιμοποιείτε τεχνικές «Jailbreak»

Ο όρος «Jailbreak» αναφέρεται στη διαδικασία αλλαγής του λειτουργικού συστήματος μιας συσκευής iOS, κατά παράβαση της άδειας χρήσης του τελικού χρήστη. Με τη διαδικασία του «Jailbreak» μειώνεται σημαντικά η ικανότητα της συσκευής να αντιμετωπίσει επιθέσεις, γιατί αναστέλλεται η εφαρμογή των υπογραφών κώδικα, οι οποίες αποτελούν σημαντικό στοιχείο ασφαλείας. Με τη διαδικασία του «Jailbreak» είναι κατά πολύ ευκολότερο να έχει κανείς πρόσβαση σε ένα iPhone ή iPad. Οι περισσότερες δημόσιες επιθέσεις με στόχο συσκευές iOS απαιτούν να έχει γίνει πρώτα «Jailbreak». Μια ακόμα παρεμφερής ανησυχία που εκφράζεται, αφορά την ποιότητα των εργαλείων και των εφαρμογών που προσφέρει η κοινότητα του «Jailbreak». Αυτές οι δωρεάν εφαρμογές κατασκευάζονται με ελάχιστη επίβλεψη και περιορισμένες δοκιμές. Ενδέχεται να περιλαμβάνουν ιούς ή άλλο κακόβουλο λογισμικό, και μπορεί να προκαλέσουν σοβαρές, ανεπανόρθωτες βλάβες στη συσκευή σας, καταστρέφοντας τα δεδομένα σας.

### 5. Ενεργοποίηση του Αυτόματου Κλειδώματος και του Κλειδώματος Συνθηματικού

Η ενεργοποίηση του Αυτόματου Κλειδώματος κλειδώνει αυτόματα την οθόνη του κινητού μετά από μια εκ των προτέρων ορισμένη περίοδο αδράνειας του κινητού τηλεφώνου. Θα πρέπει να βεβαιωθούμε ότι το Αυτόματο Κλείδωμα είναι ενεργοποιημένο.
Προτεινόμενος χρόνος κλειδώματος του τηλεφώνου είναι τα 3 λεπτά, περίπου.
- Πηγαίνουμε στα Settings → General → Auto Lock.
- Ορίζουμε το χρόνο Αυτόματου Κλειδώματος στα 3 λεπτά.

Για να είναι αποτελεσματικό το Αυτόματο Κλείδωμα, θα πρέπει να συνδυάζεται με το Κλείδωμα Συνθηματικού. Με τη χρήση του Αυτόματου Κλειδώματος και του Κλειδώματος Συνθηματικού μπορούμε να έχουμε καλύτερη προστασία. Το συνθηματικό θα πρέπει να έχει 4 ψηφία και θα πρέπει να δίνεται κάθε φορά που κλειδώνει η οθόνη. Για να γίνει αυτό, πρέπει να γίνουν οι παρακάτω ρυθμίσεις:
- Πηγαίνουμε στα Settings → General → Passcode Lock.
- Θέτουμε σε λειτουργία (ON) το «Passcode Lock».
- Ορίζουμε το «Require Passcode» σε Immediately.

**Σημείωση:** Στην ίδια οθόνη θα πρέπει να τεθεί εκτός λειτουργίας το Simple Passcode, ούτως ώστε να μπορούν να οριστούν συνθηματικά που συνδυάζουν γράμματα και αριθμούς.

Για να έχετε περισσότερη ασφάλεια, ενεργοποιήστε την Αυτόματη Διαγραφή Δεδομένων για να διαγράψετε όλα τα δεδομένα που έχουν δημιουργηθεί από το χρήστη, μετά από δέκα αποτυχημένες προσπάθειες πρόσβασης με συνθηματικό στη συσκευή.
- Πηγαίνουμε στα Settings → General → Passcode Lock.
- Θέτουμε σε λειτουργία (ON) το «Erase Data».

### 6. Μη συνδέεστε με ασύρματα δίκτυα που δεν εμπιστεύεστε

Όσο είναι δυνατόν, να αποφεύγετε ή να περιορίζετε τη χρήση ασύρματων δικτύων. Όταν δεν τα χρησιμοποιείτε, θα πρέπει να απενεργοποιείτε τη συσκευή για να μην είναι εκτεθειμένη.
- Πηγαίνουμε στα Settings → Wi-Fi.
- Θέτουμε εκτός λειτουργίας (OFF) τα Wi-Fi.

Αντισταθείτε στον πειρασμό να χρησιμοποιήσετε σημεία δωρεάν ασύρματης πρόσβασης στο διαδίκτυο. Τα περισσότερα από αυτά δεν προσφέρουν καμιά προστασία σε δεδομένα που μεταδίδονται ασύρματα, κάτι που σημαίνει ότι οποιοσδήποτε βρίσκεται κοντά, μπορεί να τα υποκλέψει. Αν, παρ' όλα αυτά, είναι απολύτως απαραίτητο να χρησιμοποιήσετε ασύρματο δίκτυο, διαλέξτε κάποιο που να το ξέρετε, και φροντίστε τα δεδομένα που ανταλλάσσετε με άλλους να είναι κρυπτογραφημένα. Στη λίστα των διαθέσιμων

δικτύων, όσα είναι προστατευμένα συνοδεύονται από το εικονίδιο κλειδαριάς δίπλα στο όνομά τους.

Για να απενεργοποιηθεί η αυτόματη σύνδεση σε ασύρματα δίκτυα, κάνουμε τις παρακάτω ενέργειες:
- Πηγαίνουμε στα Settings → Wi-Fi.
- Θέτουμε την εντολή «Ask to join Networks» στο OFF.

**Σημαντική Σημείωση.** Ακόμα κι αν τεθεί εκτός λειτουργίας η αυτόματη σύνδεση σε ασύρματο δίκτυο, η συσκευή θα συνδεθεί αυτομάτως με δίκτυα τα οποία έχει επισκεφθεί προηγουμένως και τα οποία εξακολουθούν να υπάρχουν στη μνήμη της.

Ένα άλλο μέτρο προστασίας που μπορούμε να πάρουμε, είναι να επιλέξουμε την εντολή «Forget this Network» μετά από κάθε ασύρματη σύνδεση. Αυτό θα μειώσει τις πιθανότητες να συνδεθεί η συσκευή μας με λειτουργικό σύστημα iOS με κάποιο άλλο ασύρματο δίκτυο που έχει το ίδιο όνομα. Είναι σημαντικό να επιλέξουμε αυτή την εκδοχή πριν βγούμε από το βελινεκές του συγκεκριμένου δικτύου. Σε διαφορετική περίπτωση, το δίκτυο δεν θα εμφανίζεται στη λίστα των διαθέσιμων δικτύων και δεν θα είναι δυνατόν να το αφαιρέσουμε.
- Πηγαίνουμε στα Settings → Wi-Fi.
- Επιλέγουμε δίκτυο από τη λίστα.
- Επιλέγουμε την εντολή «Forget this Network».

### 7. Απενεργοποιήστε το Bluetooth, εκτός αν το χρειάζεστε

Το Bluetooth θα πρέπει να είναι ενεργοποιημένο μόνο όταν μας είναι απολύτως απαραίτητο. Όταν δεν το χρησιμοποιούμε, θα πρέπει να το έχουμε κλειστό, ώστε να μην μπορούν άλλες συσκευές να ανακαλύψουν την iOS συσκευή μας και να προσπαθήσουν να συνδεθούν μαζί της.
- Πηγαίνουμε στα Settings → General → Bluetooth.
- Θέτουμε το «Bluetooth» στο OFF.

### 8. Απενεργοποιήστε τις Υπηρεσίες Εντοπισμού, εκτός αν τις χρειάζεστε

Οι Υπηρεσίες Εντοπισμού μπορεί να χρησιμοποιηθούν από εφαρμογές στη συσκευή σας με σκοπό να ανακαλύψουν το σημείο στο οποίο είστε. Οι Υπηρεσίες Εντοπισμού θα πρέπει να είναι σε λειτουργία μόνο αν υπάρχει κάποια επείγουσα ανάγκη και οι εφαρμογές πρέπει να γνωρίζουν πού βρίσκεστε. Διαφορετικά, απενεργοποιήστε τες ή κάντε περιορισμένη χρήση τους. Για να απενεργοποιήσουμε τις Υπηρεσίες Εντοπισμού, κάνουμε τα ακόλουθα:
- Πηγαίνουμε στα Settings (Settings → General σε iPads).
- Θέτουμε το «Location Services» στο OFF.

Οι εφαρμογές που χρησιμοποιούν την υπηρεσία «Location Services» θα ζητήσουν να κάνουν χρήση της την πρώτη φορά που θα τις θέσετε σε λειτουργία. **Σκεφτείτε προσεκτικά αυτά τα αιτήματα και επιτρέψτε τη λειτουργία των Υπηρεσιών Εντοπισμού μόνο όταν αυτό είναι απολύτως απαραίτητο.**

### 9. Ασφαλής Χρήση του Safari

Η δυνατότητα «Autofill» θα πρέπει να απενεργοποιηθεί στο Safari. Με αυτό τον τρόπο το Safari δεν θα μπορεί να αποθηκεύει κρίσιμες ενδεχομένως πληροφορίες που υπάρχουν στη συσκευή σας, όπως username και password.
- Πηγαίνουμε στα Settings → Safari.
- Θέτουμε το «Autofill» στο OFF.

Επιπλέον, η τεχνολογία JavaScript μπορεί να απενεργοποιηθεί, προκειμένου να εμποδίσουμε τυχόν κακόβουλο λογισμικό να βλάψει τη συσκευή μας. Ωστόσο, η απενεργοποίηση αυτή ενδέχεται να καταστήσει άχρηστες ορισμένες ιστοσελίδες, επομένως είναι αναγκαίο να εξακαλουθήσει το JavaScript να βρίσκεται σε λειτουργία. Αν θελήσουμε να το απενεργοποιήσουμε:
- Πηγαίνουμε στα Settings → Safari.
- Θέτουμε τα «JavaScripts» στο OFF.

Επιπλέον, τα «cookies» μπορεί να θέσουν σε κίνδυνο προσωπικά δεδομένα και συνήθειες πλοήγησης στο Διαδίκτυο. Για να αποτρέψουμε κάτι τέτοιο, τα θέτουμε εκτός λειτουργίας, όταν αυτό είναι δυνατόν, ή ρυθμίζουμε την iOS συσκευή μας ώστε να δέχεται «cookies» μόνο από ιστοσελίδες τις οποίες έχουμε επισκεφθεί.

### 10. Ασφαλής Χρήση E-mail

Βεβαιωθείτε ότι όλες οι συνδέσεις e-mail που χρησιμοποιείτε είναι κρυπτογραφημένες. Προϋπόθεση για κάτι τέτοιο είναι να μπορεί ο server που χρησιμοποιείτε, να κάνει διακίνηση κρυπτογραφημένων δεδομένων: αυτό γίνεται στις περισσότερες περιπτώσεις. Αν δεν κρυπτογραφηθούν, τα μηνύματά σας θα μεταδίδονται ελεύθερα και θα είναι δυνατόν κάποιος να τα υποκλέψει και να τα διαβάσει.
- Πηγαίνουμε στα Settings → Mail, Contacts, Calendars.
- Πηγαίνουμε στο SMTP και επιλέγουμε το όνομα ενός server.
- Θέτουμε την εντολή «Use SSL» στο ON για κάθε λογαριασμό στη λίστα.
- Πηγαίνουμε στο Advanced.
- Θέτουμε την εντολή «Use SSL» στο ON για κάθε λογαριασμό στη λίστα.

Όταν ανοίγουμε το e-mail μέσω του Safari, θα πρέπει να είμαστε βέβαιοι ότι η σελίδα πιστοποίησης (login page) είναι κρυπτογραφημένη πριν δώσουμε τα στοιχεία μας. Αν είναι κρυπτογραφημένη, η διεύθυνση της σελίδας ξεκινάει με «https» αντί του «http» και το εικονίδιο μιας κλειδαριάς εμφανίζεται αριστερά από το URL.
Επιπλέον, η επιλογή «Remote Image Loading» θα πρέπει να είναι απενεργοποιημένη από τα e-mail.
Με τον τρόπο αυτό, μπορούμε να προστατεύουμε το σύστημά μας από παραποιημένες κακόβουλες εικόνες. Επίσης, δεν θα επιτρέψει σε όσους θέλουν να βλάψουν το σύστημά μας, να συνδέσουν τη διεύθυνσή μας στο δίκτυο με το λογαριασμό e-mail που έχουμε.
- Πηγαίνουμε στα Settings → Mail, Contacts, Calendars.
- Ρυθμίζουμε το «Load Remote Image» σε OFF.

### 11. Ρύθμιση του iPhone Configuration Utility

Με την έκδοση του iOS 4, κάποιες ρυθμίσεις ασφαλείας, οι οποίες μπορούσαν να τεθούν σε λειτουργία μόνο μέσω του iPhone Configuration Utility, υπάρχουν τώρα στο Settings → General → Restrictions. Στις ρυθμίσεις αυτές περιλαμβάνονται η απενεργοποίηση της κάμερας και ενσωματωμένες iOS εφαρμογές όπως το Safari και το YouTube.

### 12. Σημαντικές ρυθμίσεις ασφαλείας iPhone & iPad

Άλλες σημαντικές ρυθμίσεις ασφαλείας, όπως κρυπτογραφημένα αντίγραφα ασφαλείας, περισσότερο πολύπλοκα PIN και καθαρισμός δίσκου εξ αποστάσεως, θα βρείτε στο iPhone Configuration Utility, ένα δωρεάν εργαλείο το οποίο σας προσφέρει η Apple απευθείας από την ιστοσελίδα της (http://www.apple.com/support/iphone/enterprise), στην οποία θα βρείτε και όλες τις σχετικές οδηγίες χρήσεως.

# ΑΣΦΑΛΗΣ ΧΡΗΣΗ ΤΟΥ BLACKBERRY

### 1. 10 Συμβουλές

1. Μην αποθηκεύετε ή επεξεργάζεστε απόρρητες πληροφορίες σε μια συσκευή BlackBerry.
2. Κλείστε τη συσκευή σας και αφαιρέστε την μπαταρία πριν εισέλθετε σε χώρο υψίστης ασφαλείας.
3. Διατηρήστε το BlackBerry σε απόσταση 3 μέτρων από άλλη συσκευή επεξεργασίας απόρρητων πληροφοριών.
4. Έχετε πάντα εσείς τον έλεγχο της συσκευής σας.
5. Χρησιμοποιήστε συνθηματικό που να συνδυάζει γράμματα και αριθμούς, και να έχει τουλάχιστον 8 χαρακτήρες.
6. Αν πιστεύετε ότι η συσκευή σας έχει αλλοιωθεί από τρίτους, σταματήστε να τη χρησιμοποιείτε.
7. Όταν δεν τη χρησιμοποιείτε, κλειδώστε τη συσκευή σας με το εικονίδιο «Lock Keyboard» που βρίσκεται στην οθόνη της.
8. Μην κατεβάζετε αρχεία ή επισυναπτόμενα αρχεία από το Διαδίκτυο, εκτός κι αν είστε βέβαιοι για το περιεχόμενό τους.
9. Μη δίνετε προσωπικά στοιχεία και κωδικούς.
10. Μη συνδέετε το BlackBerry με απόρρητα δίκτυα υπολογιστών.

### 2. Απόρρητα Δεδομένα

Σε περίπτωση κατά την οποία απόρρητα δεδομένα αποθηκευτούν στη συσκευή ή μεταδοθούν μέσω αυτής, θα πρέπει η συσκευή να καταστραφεί, καθώς η εντολή «Wipe» δεν εξασφαλίζει απόλυτη ασφάλεια.

### 3. Ταξίδια

Κατά τη διάρκεια τελωνειακών ελέγχων, θα πρέπει να αφαιρούνται η μπαταρία και η κάρτα SIM από τη συσκευή BlackBerry, η οποία καλό θα ήταν να τοποθετηθεί αλλού, λ.χ. σε μια τσάντα.

### 4. Ενεργοποίηση χαρακτηριστικών ασφαλείας

Υπάρχουν διάφοροι τρόποι με τους οποίους εξασφαλίζεται η ασφαλής χρήση του BlackBerry. Μεταξύ άλλων:

- Από την αρχική οθόνη επιλέγουμε «Option» και μετά «Security».
- Το πεδίο «Password» θα πρέπει να είναι ενεργοποιημένο.
- Το πεδίο «Lock Handheld Upon Holstering» θα πρέπει να είναι ρυθμισμένο στο «Yes».
- Από την αρχική οθόνη επιλέγουμε «Option» και μετά «Firewall».
- Το πεδίο «Status» θα πρέπει να είναι ενεργοποιημένο.
- Από την αρχική οθόνη επιλέγουμε το εικονίδιο «Icon», στη συνέχεια, σκρολάροντας, επιλέγουμε «Options» και τέλος «General Options».
- Η επιλογή «Auto Answer» θα πρέπει να ρυθμιστεί σε «Never».

### 5. Φίλος ή εχθρός;

Η τεχνολογία BlackBerry είναι ένα πολυσύνθετο σύστημα λογισμικού και υλικού που προσφέρει στο χρήστη άπειρες δυνατότητες επικοινωνίας. Σε κάθε συσκευή θα πρέπει να γίνεται προσεκτική χρήση προκειμένου να προστατεύουμε τα προσωπικά μας δεδομένα. Επιπλέον πληροφορίες μπορείτε να βρείτε στην επίσημη ιστοσελίδα της BlackBerry (us.blackberry.com).

# ΠΗΓΕΣ

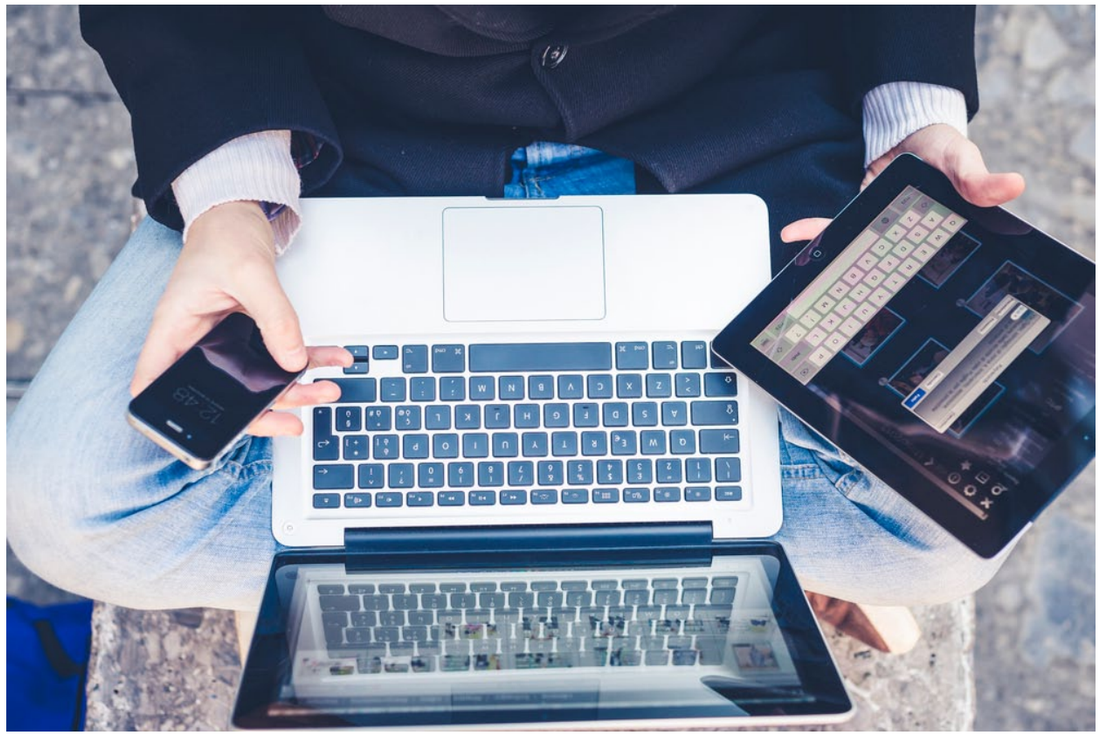
Το παραπάνω κείμενο προέρχεται από φυλλάδιο του Κέντρου Ανάλυσης Συστημάτων και Δικτύων (Systems and Networks Analysis Center) της Υπηρεσίας Εθνικής Ασφαλείας (National Security Agency) των Ηνωμένων Πολιτειών της Αμερικής. Επιπλέον πληροφορίες μπορούμε να βρούμε στην ιστοσελίδα www.nsa.gov/snac

*Το συγκεκριμένο φυλλάδιο δεν μπορεί να αντικαταστήσει την πολιτική ασφαλείας που χρησιμοποιείται, αλλά συνεισφέρει στην προστασία των χρηστών.*



# ΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ

Η κλοπή ταυτότητας είναι σπουδαία υπόθεση. Προσωπικά και οικονομικά δεδομένα που υφαρπάζονται διαδικτυακώς, πωλούνται στην υπόγεια οικονομία και χρησιμοποιούνται για παράνομους σκοπούς από εγκληματικές οργανώσεις σε όλο τον κόσμο. Η προστασία των δεδομένων σας δεν σας γλιτώνει μόνο από τη δυσάρεστη διαδικασία τού να αλλάζετε τους κωδικούς και τις πιστωτικές κάρτες σας. Βοηθάει ταυτόχρονα και στη μάχη ενάντια στο οργανωμένο έγκλημα και την τρομοκρατία.



# ΤΙ ΝΑ ΑΠΟΦΕΥΓΕΤΕ

**1. Να ανοίγετε συνημμένα αρχεία και συνδέσμους χωρίς να γνωρίζετε την αληθινή τους προέλευση.**
Αυτό που μπορεί εκ πρώτης όψεως να μοιάζει με αθώο βίντεο ή εικόνα, ενδέχεται στην πραγματικότητα να είναι κακόβουλο λογισμικό σχεδιασμένο να υποκλέπτει τα δεδομένα σας. Ακόμα και το να ανοίξετε μόνο ένα spam mail μπορεί να βάλει τη διεύθυνσή σας στη λίστα των spammers για μελλοντικές επιθέσεις.

**2. Να δίνετε περισσότερες πληροφορίες από όσες είναι απολύτως απαραίτητες.**
Η τράπεζα και ο πάροχος της πιστωτικής σας κάρτας ήδη γνωρίζουν τον κωδικό σας και τη διεύθυνσή σας. Δεν χρειάζεται να τους δώσετε αυτά τα στοιχεία μέσω e-mail, τηλεφώνου ή ιστοσελίδας.

**3. Να έχετε πρόσβαση σε διαδικτυακές τραπεζικές υπηρεσίες (online banking) από υπολογιστές με πολλαπλούς χρήστες ή από δημόσια προσβάσιμους υπολογιστές.**
Ποτέ δεν ξέρετε τι μπορεί να κρύβεται στον σκληρό τους δίσκο.

**4. Να μοιράζεστε κωδικούς, λογαριασμούς ηλεκτρονικού ταχυδρομείου ή άλλα διαδικτυακά προσωπικά δεδομένα με άλλους ανθρώπους.**
Είναι πολύ δυσκολότερο να προστατευτείτε, όταν περισσότερα από ένα άτομα έχουν πρόσβαση.

**5. Να αποθηκεύετε πιστοποιητικά σε φυλλομετρητές (browsers).**
Θα αποθηκεύατε ποτέ τον κωδικό σας σε ένα χαρτάκι Post-it; Το να τον αποθηκεύσετε σε ένα φυλλομετρητή είναι εξίσου επικίνδυνο.

**6. Να παίρνετε οτιδήποτε ως δεδομένο.**
Αν μια προσφορά σε ένα e-mail ή σε κάποιο κοινωνικό δίκτυο σας φαίνεται πολύ καλή για να είναι αληθινή, τότε μάλλον δεν είναι. Επίσης, είναι πολύ εύκολο για εγκληματίες να αντιγράψουν τα λογότυπα εταιρειών και την ταυτότητα των αποστολέων.

# ΤΙ ΝΑ ΚΑΝΕΤΕ

**1. Να είστε σε επιφυλακή.**
Να αντιμετωπίζετε τα αυτόκλητα e-mail ή σελίδες που ζητούν προσωπικές πληροφορίες, με επιφυλακτικότητα, ιδίως εκείνα που ισχυρίζονται ότι είναι από τράπεζες και εταιρείες πιστωτικών καρτών. Μια γρήγορη έρευνα στο Διαδίκτυο μπορεί να σας πει αν το e-mail που λάβατε, είναι μία από τις γνωστές απάτες. Να θυμάστε ότι πάντα μπορείτε να διασταυρώνετε με την τράπεζά σας ή την εταιρεία πιστωτικών καρτών κατά πόσο το e-mail που λάβατε, είναι πράγματι από αυτούς.

**2. Να ενημερώνετε (update) συστηματικά το λογισμικό σας.**
Πολλές κακόβουλες μολύνσεις προκύπτουν επειδή οι εγκληματίες εκμεταλλεύονται κενά ασφαλείας στο λογισμικό (σε διαδικτυακούς φυλλομετρητές, σε λειτουργικά συστήματα, σε διάφορα προγράμματα κ.τ.λ.). Η διαρκής ενημέρωσή τους θα σας βοηθήσει να είστε ασφαλείς.

**3. Να χρησιμοποιείτε αντιικό λογισμικό (anti-virus).**
Το αντιικό λογισμικό βοηθάει στο να κρατήσετε τον υπολογιστή σας καθαρό από τα πιο συνήθη κακόβουλα λογισμικά –υπάρχουν, μάλιστα, αρκετές δωρεάν επιλογές. Πάντα να ελέγχετε τα αρχεία που κατεβάζετε, με το αντιικό πρόγραμμά σας. Να μην εγκαθιστάτε προγράμματα ή εφαρμογές στον υπολογιστή σας, αν δεν ξέρετε από πού προέρχονται.



**4. Να απαγορεύετε την πρόσβαση στα προσωπικά σας στοιχεία από ιστοσελίδες κοινωνικής δικτύωσης.**
Όσο περισσότερες πληροφορίες έχουν οι εγκληματίες, τόσο πιο εύκολα μπορούν να σας στοχοποιήσουν. Περιορίζοντας την ποσότητα πληροφοριών που μοιράζεστε, και τα άτομα με τα οποία τις μοιράζεστε, δυσκολεύετε τη δράση τους.

**5. Να χρησιμοποιείτε πάντα ισχυρούς κωδικούς.**
Οι υπολογιστές μπορούν να σπάσουν τους πιο συνηθισμένους κωδικούς πολύ γρήγορα. Είναι σημαντικό να σιγουρεύετε ότι οι κωδικοί σας είναι ισχυροί (πάνω από 8 χαρακτήρες, χρησιμοποιώντας ταυτόχρονα αριθμούς, γράμματα και σύμβολα).

**6. Να παίρνετε οτιδήποτε ως δεδομένο.**
Αν μια προσφορά σε ένα e-mail ή σε κάποιο κοινωνικό δίκτυο σας φαίνεται πολύ καλή για να είναι αληθινή, τότε μάλλον δεν είναι. Επίσης, είναι πολύ εύκολο για εγκληματίες να αντιγράψουν τα λογότυπα εταιρειών και την ταυτότητα των αποστολέων.

# ΧΡΗΣΙΜΑ LINKS

**Χρήσιμες συμβουλές από τη Δίωξη Ηλεκτρονικού Εγκλήματος:**
http://www.astynomia.gr/

**Ανοικτή γραμμή για το παράνομο περιεχόμενο στο διαδίκτυο:**
http://www.safeline.gr

**Ελληνικός κόμβος ασφαλούς Διαδικτύου:**
www.saferinternet.gr

**Οργανισμός προστασίας των δικαιωμάτων των παιδιών:**
http://www.hamogelo.gr

**Συμβουλές ασφαλείας για online chatting:**
http://www.chatdanger.com

**Ιστότοπος από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος:**
www.cyberkid.gr

**Πανελλήνιο σχολικό δίκτυο:**
www.sch.gr

**Μονάδα Εφηβικής Υγείας, Β' Παιδιατρική κλινική Πανεπιστημίου Αθηνών, Νοσοκομείο Παίδων:**
www.youth-health.gr

**Ελληνική Εταιρεία Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο:**
www.hasiad.gr

**ΕΠΙΚΟΙΝΩΝΙΑ**
**Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος - Cyber Crime Division**
**Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11521**
**e-mail: ccu@cybercrimeunit.gov.gr, Τηλ.: 11188, Fax: 2106476462**

**Βρείτε μας στα:**
www.cyberkid.gr
www.facebook.com/cyberkid.gov.gr
www.cyberalert.gr
www.facebook.com/CyberAlertGR
twitter.com/cyberalertgr