Ασφάλεια στο Διαδίκτυο

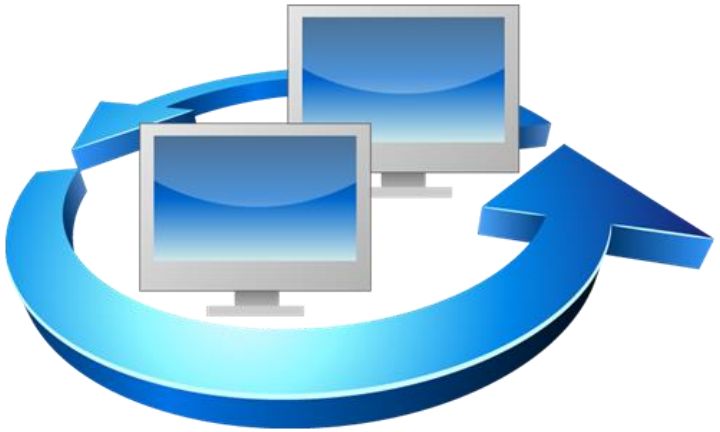
Παντελής Μπάγκος
Καθηγητής
Πανεπιστήμιο Θεσσαλίας

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ
ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΒΙΟΪΑΤΡΙΚΗ

http://dib.uth.gr
http://icb.sci.uth.gr
http://www.compgen.org

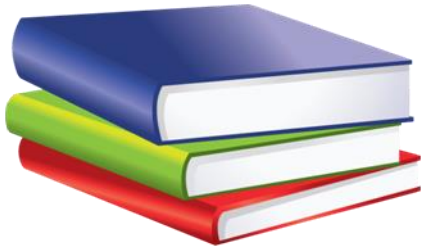
Διαδίκτυο

- Το **μεγαλύτερο** δίκτυο υπολογιστών στον **κόσμο**!
- **Πρόσβαση** και με **κινητό τηλέφωνο**!
- **Συνδέεσαι** από **παντού**!



Θετικά του Διαδικτύου

- ✓ Γνώση
- ✓ Εκπαίδευση
- ✓ Πληροφορίες



- ✓ Ψυχαγωγία
- ✓ Διασκέδαση

- ✓ Επικοινωνία
- ✓ Ενημέρωση

- ✓ Αγορές
- ✓ Ταξίδια

Διαδίκτυο

- Ταχύτητες συνεχώς αυξάνονται

Πληροφορία πιο προσβάσιμη!

- Παγκόσμιος Ιστός σαν μια κοινωνία!

- Οι πληροφορίες δεν είναι πάντα έγκυρες

- Όποιο αρχείο δημοσιεύεται, μένει στο Διαδίκτυο για πάντα!

ΕΙΔΙΚΑ ΓΙΑ ΤΑ ΠΑΙΔΙΑ:

- Μη ενδεδειγμένη χρήση
- Χρήση χωρίς επιτήρηση από τους γονείς
- Χρήση για περισσότερη από 1,5 ώρα την ημέρα

Ελλοχεύει σοβαρούς κινδύνους και μπορεί να έχει επιπτώσεις..

Μύθοι και πραγματικότητα

Μύθος: Στο διαδίκτυο είμαστε ανώνυμοι…

Πραγματικότητα: Κάθε ενέργεια στο διαδίκτυο αφήνει ηλεκτρονικά ίχνη!

Μύθος: Ό,τι δημοσιεύουμε στο διαδίκτυο μπορούμε όποτε θέλουμε να το διαγράψουμε…

Πραγματικότητα: Ό,τι ανεβαίνει στο διαδίκτυο δεν διαγράφεται ποτέ!

Μύθος: Ό,τι διαβάζουμε στο διαδίκτυο είναι αλήθεια…

Πραγματικότητα: Πρέπει πάντα να επαληθεύουμε την πηγή!

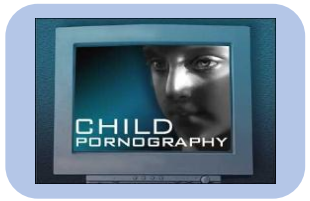
Μύθος: Στο διαδίκτυο αν χρησιμοποιήσουμε τα κατάλληλα εργαλεία μπορούμε να είμαστε απόλυτα προστατευμένοι…

Πραγματικότητα: Δεν υπάρχει 100% προστασία στο διαδίκτυο!

@σφαλώς πλοηγήσου!

Προβλήματα και Μορφές Εγκληματικότητας

- Διαδικτυακή Αποπλάνηση
- Cyberbullying
- Εθισμός
- Προσωπικά δεδομένα
- Απάτες μέσω διαδικτύου



Διαδικτυακή Παρενόχληση

- Να κοροϊδέψει ένα άτομο σε ένα chat-room.
- Να αποστείλει αισχρά, προσβλητικά ή απειλητικά μηνύματα μέσω του διαδικτύου.
- Να στείλει αισχρό υλικό κατά τις συνομιλίες.
- Να εξευτελίσει κάποιον με το να φτιάξει ένα ψεύτικο προφίλ με εξευτελιστικές πληροφορίες.
- Να βάλει προσωπικό υλικό στο διαδίκτυο δίχως την άδεια του άλλου.
- Να αποκλείσει κάποιον από ομάδα ή διαδικτυακή δραστηριότητα

Διαδικτυακή Παρενόχληση

πρώτος στόχος είναι να κερδηθεί η εμπιστοσύνη

- Η επίδειξη ενδιαφέροντος για ένα συγκεκριμένο άτομο και η επιδίωξη συνάντησης.
- Η αποστολή πορνογραφικού υλικού σε έφηβο.
- Η μεταφορά του θέματος μιας συνομιλίας σε σεξουαλικό περιεχόμενο.
- Η απαίτηση αποστολής προσωπικών φωτογραφιών.

Στο διαδίκτυο κάποια πράγματα δεν είναι αυτό που φαίνεται να είναι

https://www.youtube.com/watch?v=cZAiW61p9DQ

Cyberbullying

Εκείνοι που συμμετέχουν στο cyber bullying είναι συνήθως μια ομάδα φίλων οι οποίοι κακοποιούν ψυχικά ή και σωματικά τα θύματά τους!

Cyberbullying

- Αποστολή ειδικών προγραμμάτων trojan horses για την υποκλοπή κωδικών.
- Αποστολή κειμένων με προσβλητικό περιεχόμενο.
- Κακόβουλη δημοσίευση φωτογραφιών σε μέσα κοινωνικής δικτύωσης.
- Ανώνυμες κλήσεις και μηνύματα με σκοπό τον φόβο και την ταραχή.
- Διάδοση φημών και ψευδών γεγονότων με σκοπό την δυσφήμιση.

Cyberbullying

- Αγνόησε (αρχικά) τα ενοχλητικά μηνύματα, σε περίπτωση απειλών συνιστάται αναφορά και λήψη προληπτικών μέτρων.

- Απόκλεισε τον αποστολέα των μηνυμάτων.
- Αποθήκευσε τις Αποδείξεις.
- Μίλα σε πρόσωπα που εμπιστεύεσαι (γονείς, εκπαιδευτικούς)
- Μην απαντήσεις και μην προσπαθήσεις να συναντήσεις τον δράστη.
- Κάλεσε ΑΜΕΣΑ τη **Δίωξη Ηλεκτρονικού Εγκλήματος**, εάν η ηλεκτρονική παρενόχληση περιλαμβάνει απειλές βίας, καταναγκασμού, ή κάθε μορφής σεξουαλικής εκμετάλλευσης.

Εκδήλωση Πρόθεσης Αυτοκτονίας

Γραμμές υποστήριξης:

- 1107, 197 (ΕΚΚΑ)
- 1056 (Χαμόγελο Παιδιού)
- 11525 (Μαζί για το Παιδί)
- 8001132000 (Συνήγορος Παιδιού)
- 15900 (Γραμμή ΣΟΣ)
- 1034 (Βοήθεια για την Κατάθλιψη)

ΠΟΛΛΟΙ ΝΕΟΙ ΣΥΝΑΝΘΡΩΠΟΙ ΜΑΣ ΠΡΟΣΠΑΘΗΣΑΝ ΝΑ ΑΥΤΟΚΤΟΝΗΣΟΥΝ ΕΩΣ ΣΗΜΕΡΑ ΜΕΣΩ ΙΝΤΕΡΝΕΤ

Εθισμός

Πιθανά κανάλια εθισμού

Ιστότοποι Κοινωνικής Δικτύωσης

facebook

Διαδικτυακά παιχνίδια

Ποια είναι τα πρώτα σημάδια εθισμού στο διαδίκτυο;

Υπερβολική Χρήση

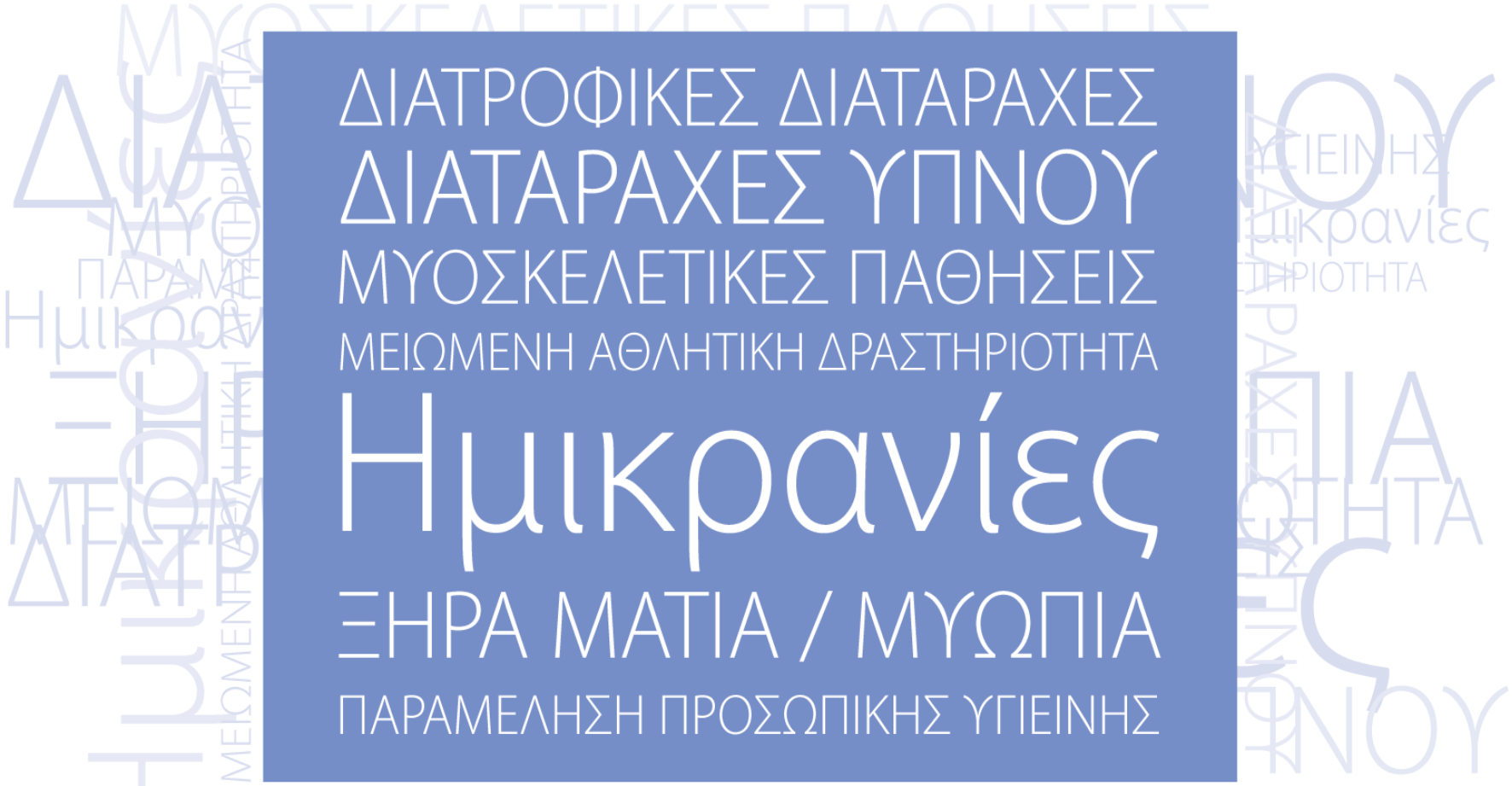
Μονομανία

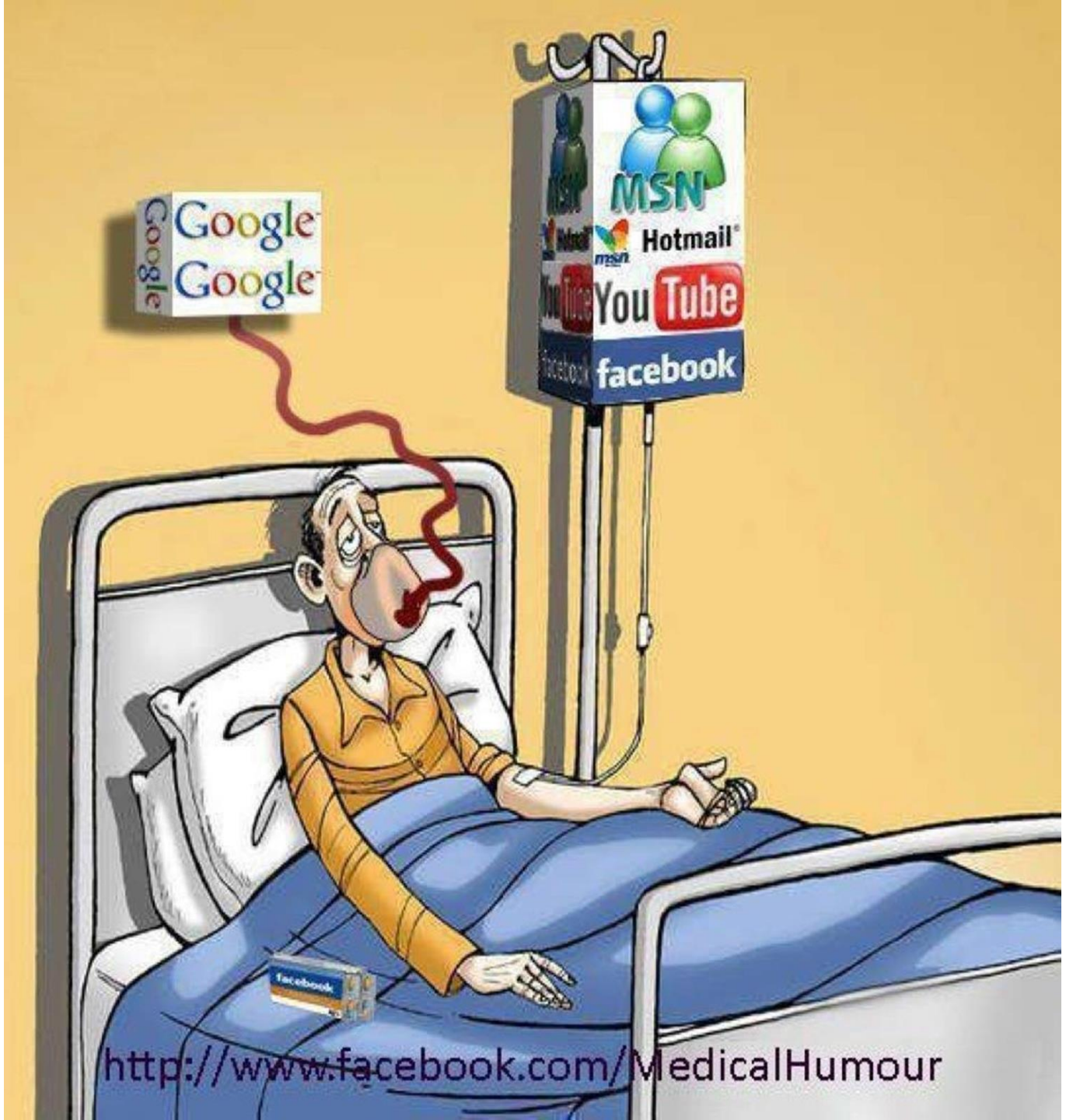
Παραμέληση Υποχρεώσεων

Απομόνωση & Αδιαφορία

Πονοκέφαλοι & ξηρότητα οφθαλμών

Σε προχωρημένο στάδιο μπορεί να εκδηλωθούν και σωματικά συμπτώματα




Google
Google
MSN
Hotmail
You Tube
facebook
http://www.facebook.com/MedicalHumour

Μέσα Κοινωνικής Δικτύωσης

Δημοσιοποίηση των καθημερινών δραστηριοτήτων

…..10 – 20 Αυγούστου θα είμαι *Μύκονο*

Οι διαρρήκτες δεν χάνουν ευκαιρία και “αδειάζουν” τα σπίτια των ανυποψίαστων με την άνεσή τους …..

Όροι χρήσης του Facebook

Αλλαγή των όρων χωρίς προειδοποίηση

Δεν παρέχεται εγγύηση για την ασφάλεια των εφαρμογών

Αποποίηση των πνευματικών δικαιωμάτων για περιεχόμενο που ανεβαίνει στο facebook

Δεν παρέχεται εγγύηση για τη μυστικότητα

Συμβουλές

- Δεν δημοσιοποιούμε υλικό με προσωπικά δεδομένα.
- Δεν εμπιστευόμαστε άτομα τα οποία δεν γνωρίζουμε.
- Προσέχουμε γενικώς τι πληροφορίες δίνουμε.
- Αν αντιληφθούμε ότι μας έχουν κλέψει τον λογαριασμό, επικοινωνούμε με τη Δίωξη Ηλεκτρονικού Εγκλήματος.
- Αναφέρουμε την κλοπή του λογαριασμού στο μέσο κοινωνικής δικτύωσης που χρησιμοποιούμε μέσω της προτεινόμενης από αυτό διαδικασίας (report).
- Επιλέγουμε ασφαλέστερους κωδικούς.

Αναρτήσεις από Facebook και Instagram ως αποδεικτικά μέσα σε πολιτικά δικαστήρια - Συλλογή ελληνικής νομολογίας

Δυνατότητα αξιοποίησης αναρτήσεων σε μέσα κοινωνικής δικτύωσης ως αποδεικτικών μέσων στο πλαίσιο δικών ενώπιον πολιτικών δικαστηρίων

Lawspot.gr 09/11/2020 03/12/2020 Νέες τεχνολογίες

Οι αναρτήσεις στα ΜΚΔ έχουν χρησιμοποιηθεί στα δικαστήρια

- Διατροφή
- Επιμέλεια τέκνων
- Οφειλές
- Αντιδικίες για ενοίκια

- **Προσοχή**: έχει μεγάλη διαφορά αν μια ανάρτηση απευθύνεται σε «φίλους» ή είναι «δημόσια». Στην πρώτη περίπτωση, δεν επιτρέπεται κάποιος που δεν είναι νόμιμος αποδέκτης να κάνει χρήση της πληροφορίας αυτής (θεωρείται παραβίαση των προσωπικών δεδομένων)

Ομάδες Επικοινωνίας-Συνομιλίες

✓Η χρήση των ψευδωνύμων επιτρέπει τη διατήρηση της ανωνυμίας.

✓Η ψευδαίσθηση της ασφάλειας μπορεί να μετατρέψει τον τρόπο επικοινωνίας σε μία από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του Διαδικτύου.

✓Σε χώρες του εξωτερικού έχουν παρουσιασθεί περιπτώσεις παιδιών που εξαφανίσθηκαν, έπεσαν θύματα παιδόφιλων ή παρασύρθηκαν από αγνώστους τους οποίους «συνάντησαν» σε δωμάτια επικοινωνίας.

Είναι αληθινές αυτές οι φιλίες;

Οι μόνες αληθινές φιλίες βρίσκονται στην πραγματική ζωή και δοκιμάζονται στον πραγματικό κόσμο και τον πραγματικό χρόνο.

Ομάδες Επικοινωνίας-Συνομιλίες

✓Δε μιλάμε με κάποιον στο Διαδίκτυο που διαθέτει όνομα προφίλ που δεν αναγνωρίζουμε. Πολλές φορές οι άνθρωποι που είναι online προσποιούνται πως είναι κάποιοι άλλοι.

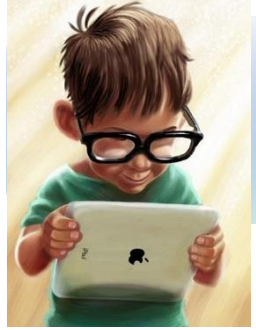
✓Εξετάζω προσεκτικά τα αιτήματα φιλίας που δέχομαι και δεν κάνω φίλο κάποιον που δε γνωρίζω και στην πραγματική ζωή.

✓Εξετάζετε προσεκτικά τα αιτήματα φιλίας προτού συμφωνήσετε. Εάν δεν θέλετε να προσθέσετε κάποιον, κάντε κλικ για να αποκλείσετε αυτή την επαφή από τον κατάλογο.

✓Ποτέ μη χρησιμοποιήσετε την υπηρεσία άμεσων μηνυμάτων για να διαδώσετε φήμες, κουτσομπολιά ή εμπαθή μηνύματα.

«Τι πρέπει να προσέχουμε στα διαδικτυακά μας ταξίδια;»

- Δεν χρησιμοποιούμε την ημερομηνία γέννησης ή άλλα βασικά προσωπικά στοιχεία.
- Δεν χρησιμοποιούμε τον ίδιο κωδικό για όλες τις περιπτώσεις.
- Φροντίζουμε ο κωδικός να αποτελείται από 8 τουλάχιστον χαρακτήρες.
- Προσπαθούμε να χρησιμοποιούμε σύμβολα, αριθμούς και γράμματα
- Αλλάζουμε συχνά τους κωδικούς.



Συμβουλές

- Μην απαντάς σε απειλητικά μηνύματα.
- Διατήρησε αποδεικτικά της δράσης (ημερομηνίες, ώρες, λογαριασμούς ηλεκτρονικού ταχυδρομείου κλπ).
- Αφαίρεσε από τις λίστες των «φίλων» αυτόν που σε παρενόχλησε και ρύθμισε το προφίλ κοινωνικής δικτύωσης ώστε να είναι «απόρρητο».
- Εάν ο θύτης είναι γνωστό σου πρόσωπο, σε αυτήν την περίπτωση ζήτησέ του να σβήσει τα μηνύματα και να αποκαταστήσει την αλήθεια σε περίπτωση διάδοσης φημών.

Συμβουλές

- Σε περίπτωση που η παρενόχληση πραγματοποιηθεί σε κάποια ιστοσελίδα κοινωνικής δικτύωσης (π.χ. Facebook) κάνε αναφορά για το περιστατικό στους διαχειριστές της ιστοσελίδας.
- Μη κρατάς τους εκφοβισμούς για τον εαυτό σου. Δεν είσαι μόνος!
- Πες το σε έναν ενήλικα που γνωρίζεις και εμπιστεύεσαι, είτε πρόκειται για τους γονείς σου είτε για κάποιον εκπαιδευτικό ή άλλο κοντινό και έμπιστο άτομο.
- Μπορείς να το καταγγείλεις καλώντας στη Δίωξη Ηλεκτρονικού Εγκλήματος.

Εφαρμογή CYBERKID για κινητά και tablets

Είναι μια διαδραστική εφαρμογή, η οποία δίνει τη δυνατότητα άμεσης επικοινωνίας με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος μέσω της γραμμής

C Y B E R A L E R T

Καθημερινή ενημέρωση για τους κινδύνους του διαδικτύου!

Παιχνίδια για τους μικρούς μας φίλους!

Απάτες μέσω διαδικτύου

Νιγηριανές Απάτες

Ενημέρωση μέσω email ότι:

- κέρδισε μεγάλη κληρονομιά.
- ότι μπορεί να γίνει συνεργάτης κάποιας ξένης εταιρείας.

PUBLISHERS CLEARING HOUSE

[redacted]

March 5, 2009

Dear [redacted]

The team at PCH is pleased to officially announce your name as the **Second place** winner of the 7 Million Dollars (**$7,000,000**) Grand Prize Draw, sponsored by Reader's Digest Magazine.

The total amount to be claimed for second place is One Million U.S. dollars (**$1,000,000**). Congratulations!

The Publishers Clearing House will make all necessary arrangements in order for you to receive your prize. Enclosed in this letter is a certified check to cover any outstanding fees that has not been paid by PCH directly.

Please contact your representative without any delay BEFORE depositing this check and for further information on this prize.

Representative: **Mrs. Sharon Mills - 1-(888)-317-4154 Ext #1**
Security Code: Q0092XQQ

It is obligated by U.S. Federal law that your **Security code and Prize information are kept highly confidential** for safety and security reasons. The Internal Revenue agent handling your file is Mr. Henry Cohen.

Congratulations again,

Christopher Porter
Chief Financial Officer

Με σκοπό να πάρουν από τον χρήστη:

- Προσωπικά τραπεζικά στοιχεία.
- Χρηματικό ποσό προκειμένου να αποδεσμευτεί ή μεταφερθεί το ποσό στο όνομά τους.

Phising

“Ψαρεύουν” τραπεζικά και άλλα προσωπικά δεδομένα των θυμάτων μέσα από πλαστές ιστοσελίδες που προσομοιάζουν τις πραγματικές φόρμες

Iός “Ransomware”

Προσοχή

- Σε πολλές περιπτώσεις η απάτη έχει στόχο τον άνθρωπο, όχι τον υπολογιστή
- Στήνονται ιστοσελίδες που μοιάζουν οπτικά με την ιστοσελίδα της τράπεζας και υποκλέπτουν τους κωδικούς. Σε αυτή την περίπτωση πρέπει να προσέχουμε το URL της ιστοσελίδας (πχ eeurobank.gr)
- Πολλές φορές βλέπουμε μια εικόνα στην οποία υπάρχει ένας σύνδεσμος. Σε αυτή την περίπτωση πρέπει να ελέγξουμε τον σύνδεσμό πριν τον επιλέξουμε.
- Σε άλλες περιπτώσεις, ζητάνε να αποστείλουμε τους κωδικούς με mail ή τελικά να τους δώσουμε και χρήματα

Γενικές οδηγίες (παιδιά)

- Αν πρόκειται να χρησιμοποιήσουν Μέσα Κοινωνικής Δικτύωσης, αυτό θα πρέπει να γίνεται με επίβλεψη των γονέων
- Δύσκολος κωδικός (συνδυασμός γραμμάτων και αριθμών)
- Προσοχή στις ρυθμίσεις ιδιωτικότητας
- Δεν αποδεχόμαστε «αιτήματα φιλίας» από άτομα που δεν γνωρίζουμε
- Προσέχουμε τους ιστότοπους που επισκεπτόμαστε
- Δεν εγκαθιστούμε άκριτα οποιοδήποτε λογισμικό βρούμε
- Αν χρειαστεί, εγκαθιστούμε λογισμικό γονικού ελέγχου (Kaspersky, KeyLogger, Qustudio, OpenDNS, Norton, Bark, Mobicip, Locategy, FamilyTime, WiFi Blocker κλπ)

Γενικές οδηγίες (ενήλικοι)

- Χρησιμοποιούμε πάντα λογισμικό προστασίας από ιούς
- Εγκαθιστούμε όλες τις «ενημερώσεις» του λειτουργικού συστήματος
- Χρησιμοποιούμε ισχυρούς κωδικούς, τόσο στα ΜΚΔ αλλά και στον ίδιο τον υπολογιστή (και όχι ίδιους). Αν χρειαστεί χρησιμοποιούμε και password manager.
- Προσέχουμε τους ιστότοπους που επισκεπτόμαστε
- Δεν εγκαθιστούμε άκριτα οποιοδήποτε λογισμικό βρούμε
- Προσέχουμε τις ρυθμίσεις ιδιωτικότητας στα ΜΚΔ

Ευχαριστώ

- Την κα Χρονά, την κα Αγγέλου και το προσωπικό του 1ου Γυμνασίου Περιστερίου για την πρόσκληση
- Την κα Παναγιώτα Κοντού που προετοίμασε μια πρώτη εκδοχή αυτής της ομιλίας
- Όλους εσάς για την παρουσία και την προσοχή σας!

http://dib.uth.gr
http://icb.sci.uth.gr
http://www.compgen.org