3Ο ΓΕΛ ΚΟΜΟΤΗΝΗΣ| ΒΡ6

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
ΚΙΝΔΥΝΟΙ & ΠΡΟΣΤΑΣΙΑ

Ασφάλεια των νέων στο διαδίκτυο

Το Διαδίκτυο είναι σήμερα καθημερινό εργαλείο στη ζωή μας:

- για την αναζήτηση πληροφοριών
- για επικοινωνία
- για αγορές
- για ψυχαγωγία

Η έρευνα δείχνει ότι τα παιδιά στην πλειοψηφία τους χρησιμοποιούν το Διαδίκτυο πολλές φορές την ημέρα, ενώ η χρήση του Διαδικτύου και των κινητών τηλεφώνων είναι σχεδόν αυτονόητη για την ευρωπαϊκή νεολαία.

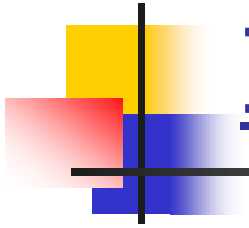
Κίνδυνοι που διατρέχει ο υπολογιστής μας

Ο κυριότερος κίνδυνος είναι το λογισμικό κακόβουλης λειτουργίας

Το **λογισμικό κακόβουλης λειτουργίας** είναι ένας όρος που χρησιμοποιείται για κακόβουλο λογισμικό το οποίο έχει σχεδιαστεί για να προκαλεί βλάβες ή να εκτελεί ανεπιθύμητες ενέργειες στο σύστημα ενός υπολογιστή.

Είδη κακόβουλων λογισμικών είναι τα παρακάτω:

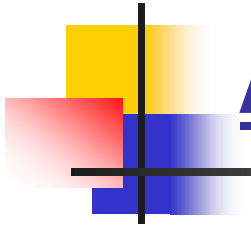
- Ιοί
- Ιοί τύπου worm
- Δούρειοι ίπποι
- Λογισμικό κατασκοπίας - spyware



Ιός

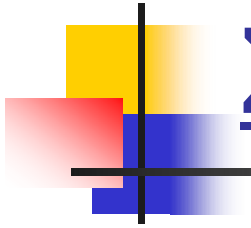
Ο ιός του υπολογιστή είναι ένα κομμάτι προγράμματος, το οποίο αντιγράφει τον εαυτό του και επισυνάπτεται σε ένα νομότυπο πρόγραμμα με σκοπό να «μολύνει» άλλα προγράμματα.

Δούρειος Ίππος (Trojan horse)

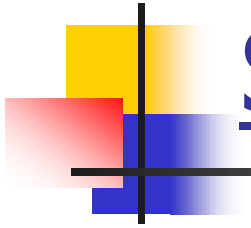


- Πρόκειται για ένα είδος προγράμματος, το οποίο δεν αναπαράγεται, αλλά δρα «υπογείως», χωρίς ο χρήστης του υπολογιστή να αντιλαμβάνεται αρχικά την ύπαρξή του.
- Το πρόγραμμα αυτό ενεργεί ως μέσο μεταφοράς άλλων μορφών επιβλαβούς λογισμικού (malware), ενεργοποιείται σε συγκεκριμένο χρόνο και δημιουργεί ένα αντίγραφο του αυθεντικού προγράμματος που χρησιμοποιείται από το χρήστη, το οποίο θα δουλεύει κανονικά, σα να ήταν το αυθεντικό.
- Όταν ο χρήστης εκτελέσει το συγκεκριμένο πρόγραμμα χρησιμοποιεί την έκδοση του Δούρειου Ίππου, ο οποίος δρα καταστροφικά.

Σκουλήκια (worms)



- Πρόκειται για προγράμματα υπολογιστών τα οποία αντιγράφουν τον εαυτό τους σε δίκτυα Η/Υ.
- Χρησιμοποιούν το Internet ως μέσο διάδοσής τους (emails, irc chat κ.ά.).
- Αναπαράγονται από υπολογιστή σε υπολογιστή, εκμεταλλευόμενα τα σφάλματα των λειτουργικών προγραμμάτων των υπολογιστών.
- Οι μολυσμένοι υπολογιστές μετά από κάποιο διάστημα κατακλύζονται από αντίγραφα του «σκουληκιού» και δε μπορούν να λειτουργήσουν.



Spyware

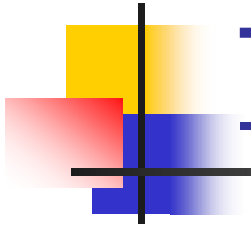
Με τον όρο **Spyware (Λογισμικό Κατασκοπίας)** αναφερόμαστε σε ένα είδος κακόβουλου λογισμικό το οποίο φορτώνεται κρυφά σε έναν υπολογιστή χωρίς να το ξέρει ο χρήστης και εκτελείται στο παρασκήνιο.

Τι κάνει συνήθως ένα Spyware

- Αλλαγή της αρχικής σελίδας του browser
- Τροποποίηση της λίστας αγαπημένων (σελιδοδεικτών) του browser
- Προσθήκη νέων γραμμών εργαλείων στο browser
- Εμφανίζουν συνεχώς παράθυρα με ανεπιθύμητες διαφημίσεις
- Ξεκινάνε μαζί με τον υπολογιστή κατά την εκκίνηση του και πιάνουν μνήμη και υπολογιστική ισχύ.
- Το spyware κάποιες φορές απενεργοποιεί το firewall, αφαιρεί ανταγωνιστικό λογισμικό κατασκοπίας και εκτελεί άλλες κακόβουλες ενέργειες.

Άλλα κακόβουλα λογισμικά…

- **Rootkits**
- **Ransomware**
- **Bots – zombies**
- **Scareware**
- **Βακτήρια (bacteria)**
- **Dialers**



Τρόποι Μετάδοσης

- Από μολυσμένο αποθηκευτικό μέσο (flash disk, memory card, κ.λπ.)
- Από εκτέλεση ή άνοιγμα μολυσμένων αρχείων του υπολογιστή
- Από εκτέλεση ή άνοιγμα μολυσμένων αρχείων που επισυνάπτονται σε μηνύματα ηλεκτρονικής αλληλογραφίας
- Από άνοιγμα ή ανάγνωση αγνώστων μηνυμάτων ηλεκτρονικής αλληλογραφίας που περιέχουν καταστροφικό κώδικα (malicious code)
- Από άνοιγμα ή ανάγνωση μολυσμένων ιστοσελίδων .htm και .html

Πώς μπορώ να διαπιστώσω εάν ο υπολογιστής μου έχει ιό;

- Η λειτουργία του Η/Υ είναι πολύ αργή.
- Λήψη παράξενων μηνυμάτων και μη αναμενόμενη εκκίνηση προγραμμάτων.
- Λειτουργία μόντεμ ή σκληρού δίσκου για υπερβολικά μεγάλα χρονικά διαστήματα.

Ο πρώτος ιός υπολογιστή και ο ιός Koobface

- **Ο πρώτος ιός** υπολογιστών εμφανίσθηκε στα μέσα της δεκαετίας του **1980** και ήταν δημιούργημα δύο Πακιστανών ονόματι Basit και Amjad Alvi, Για την ιστορία, ο ιός έμεινε γνωστός με το όνομα **Brain**.

- Ο **Koobface** είναι ένας ιός τύπου worm που είχε αρχικά προσβάλει χρήστες των ιστοσελίδων δικτύωσης όπως το **Facebook** , το Skype , Yahoo Messenger και το e-mail ιστοσελίδες όπως το Google Mail, το Yahoo Mail και AOL Mail,MySpace, hi5, Bebo , Friendster και το Twitter.

Hackers & Crackers

- Ένας καλός **hacker** πρέπει να μην μοιάζει με αυτό που είναι, να περνάει την εντύπωση ότι είναι έμπιστο άτομο και να συμπεριφέρεται έξυπνα. Πέρα από τις τεχνικές γνώσεις, οι άνθρωποι αυτοί έχουν και κοινωνικές δεξιότητες.

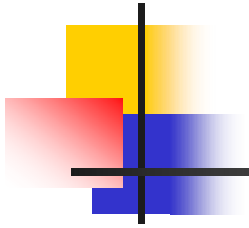
- Αντίθετα, οι ***crackers*** *(criminal hackers)* θεωρούνται ως οι κακόβουλοι hackers και έχουν ως στόχο την πρόκληση ζημιάς σε δίκτυα υπολογιστών, την εισβολή σε υπολογιστές χρηστών χωρίς εξουσιοδότηση, την δημιουργία ιών, την παραβίαση κωδικών ασφαλείας, την καταστροφή ή και την αλλοίωση δικτυακών τόπων.

Πλεονεκτήματα χρήσης νόμιμου λογισμικού

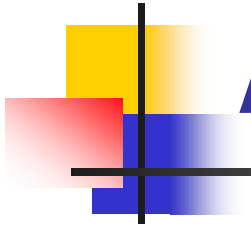
- Μπορούμε να τα χρησιμοποιήσουμε νόμιμα, για να παράγουμε και εμείς με τη σειρά μας τη δική μας πνευματική εργασία.
- Έχουμε τεχνική υποστήριξη από τους κατασκευαστές
- Μας παρέχονται τα απαραίτητα εγχειρίδια χρήσης,για να μάθουμε να χρησιμοποιούμε σωστά το νέο πρόγραμμα.
- Το προϊον που παίρνουμε είναι ελεγμένο και δοκιμασμένο.
- Είμαστε βέβαιοι ότι το CD ή DVD που κρατάμε στα χέρια μας δεν περιέχει ιούς ή κακόβουλα προγράμματα.

ΠΡΟΣΤΑΤΕΨΕ ΤΟΝ ΥΠΟΛΟΓΙΣΤΗ ΣΟΥ

Ποια είναι τα κατάλληλα μέτρα προστασίας για τον υπολογιστή μας για να έχουμε ασφαλή πλοήγηση στο διαδίκτυο;



1. Διατηρήστε το λειτουργικό σύστημα ενημερωμένο.
2. Χρησιμοποιείτε πρόγραμμα προστασίας από τους ιούς.
3. Χρησιμοποιείτε τείχος προστασίας.
4. Δημιουργείτε αντίγραφα ασφαλείας των σημαντικών αρχείων.
5. Προσέχετε όταν κάνετε λήψη περιεχομένου.



Αντιμετώπιση Ιών

Κοινά προβλήματα λογισμικού, όπως σφάλματα εκτέλεσης του προγράμματος και κατεστραμμένα αρχεία, μπορεί να δημιουργήσει συμπτώματα που φαίνεται να σχετίζονται με ιούς.

Αν ο υπολογιστής σας αρχίζει να ενεργεί παράξενα ή συμπεριφέρεται διαφορετικά από ό, τι στο παρελθόν , μπορεί να έχει μολυνθεί με έναν ιό.

Προγράμματα Αντιμετώπισης Ιών

- Η χρήση λογισμικού αντιβιοτικού είναι η πιο συνηθισμένη μέθοδος αντιμετώπισης τους.
- Ένα τέτοιο πρόγραμμα που πρέπει να είναι εγκατεστημένο σε κάθε ηλεκτρονικό υπολογιστή επιτελεί τρείς βασικές λειτουργίες:
  1. Ανίχνευση των ιών
  2. Προσδιορισμός ταυτότητας ιών,
  3. Καθαρισμός των ιών

Γνωστά Antivirus που μπορούμε να αγοράσουμε

- **ESET NOD32 Antivirus**
- **Norton Antivirus**
- **Kaspersky Antivirus**

Δωρεάν Antivirus

- Avira Free Antivirus
- Avast Free Antivirus
- AVG Antivirus Free

Δωρεάν **Anti-malware**

- **Malwarebytes Anti-Malware**
- **Dr.Web CureIt**
- **Wormblaster Malware Protector**

Δωρεάν Antispyware

-  SuperAntiSpyware Free
-  Spyware Terminator
-  Spybot - Search & Destroy

Firewall

- Το Firewalls είναι ένα σύστημα που έχει σχεδιαστεί για να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση προς ή από ένα ιδιωτικό δίκτυο.
- Τα Firewalls μπορούν να εφαρμοστούν τόσο σε υλικό και λογισμικό, ή ένας συνδυασμός και των δύο.
- Το Firewall δεν προστατεύει από ιούς! Αυτό που πετυχαίνει μέσα από τον έλεγχο της κυκλοφορίας των πληροφοριών είναι κυρίως την προστασία από προγράμματα τύπου backdoor που χρησιμοποιούν οι ερασιτέχνες hackers.

Γνωστά **Firewall**

- **Online Armor Free**
- **Agnitum Outpost Firewall Free**
- **Comodo Firewall**

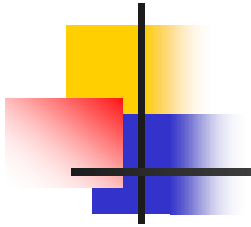
Αντίγραφα Ασφαλείας

- Καλύτερα είναι να προγραμματίσετε τακτική, αυτόματη δημιουργία αντιγράφων ασφαλείας έτσι ώστε να μην χρειάζεται καν να το σκεφτείτε. Μπορείτε να επιλέξετε την καθημερινή, εβδομαδιαία ή μηνιαία δημιουργία αντιγράφων ασφαλείας. Μπορείτε επίσης να δημιουργείτε αντίγραφα ασφαλείας με μη αυτόματο τρόπο.

Ρυθμίσεις γονικού ελέγχου

- Μπορείτε να χρησιμοποιήσετε το **Γονικό έλεγχο** για να διαχειριστείτε καλύτερα τον τρόπο, με τον οποίο τα παιδιά σας χρησιμοποιούν τον υπολογιστή.
- Για παράδειγμα, μπορείτε να θέσετε **όρια** στην πρόσβαση των παιδιών στο Web, στις ώρες κατά τις οποίες μπορούν να συνδεθούν με τον υπολογιστή, στα παιχνίδια που μπορούν να παίζουν και στα προγράμματα που μπορούν να εκτελούν.

Απειλές και ποινικά αδικήματα μέσω Internet



- **Υποκλοπή Προσωπικών Δεδομένων**
- **Cyberbulling**
- **Grooming: Σεξουαλική Αποπλάνηση**
- **Sexting**
- **Παιδική Πορνογραφία μέσω Διαδικτύου**

Ποια είναι τα Προσωπικά Δεδομένα;

- Προσωπικά δεδομένα είναι κάθε πληροφορία που σε χαρακτηρίζει, όπως για παράδειγμα το **όνομά σου, η διεύθυνσή σου, το τηλέφωνό σου**, τα **ενδιαφέροντά** σου, οι **επιδόσεις σου στο σχολείο**, οι **φωτογραφίες** σου, οι απόψεις σου, κ.α.
- Μερικές φορές τα προσωπικά σου δεδομένα αφορούν ιδιαίτερα ευαίσθητα στοιχεία της ιδιωτικής σου ζωής, όπως στο θρήσκευμά σου, στις πολιτικές σου πεποιθήσεις, στην κατάσταση της υγείας σου ή στην ερωτική σου ζωη.

Πώς χρησιμοποιούνται τα προσωπικά μου δεδομένα;

- Το ίδιο συμβαίνει και κατά την εγγραφή σου σε ένα διαδικτυακό (on-line) κατάστημα βιβλίων.
- Το σχολείο σου τηρεί δεδομένα για τους βαθμούς και τις επιδόσεις σου.
- Το προφίλ σου στο Facebook περιέχει πληροφορίες για τους φίλους σου, τα ενδιαφέροντά σου, αλλά και άλμπουμ με φωτογραφίες σου.
- Το ηλεκτρονικό φόρουμ για μουσική που παρακολουθείς περιέχει στοιχεία για τις μουσικές προτιμήσεις σου και τους καλλιτέχνες που σε ενδιαφέρουν.

Είναι δυνατόν τα προσωπικά μου δεδομένα να χρησιμοποιηθούν... εναντίον μου;

- Αν δεν προσέξεις πώς και πού δημοσιοποιείς τα προσωπικά δεδομένα ή αν πέσουν σε λάθος χέρια, τα προσωπικά σου δεδομένα μπορούν να χρησιμοποιηθούν από κάποιους για να σε δυσφημίσουν ή να σε φέρουν σε δύσκολη θέση, αποκαλύπτοντας ιδιωτικές σου στιγμές...
- Οι πληροφορίες αυτές είναι δυνατόν να δυσκολέψουν τη ζωή σου στο μέλλον, π.χ. όταν θα ψάχνεις για δουλειά ή να πάρεις δάνειο από μία τράπεζα.
- Σε ακραίες περιπτώσεις μπορεί να πέσεις ακόμα και θύμα υποκλοπής ταυτότητας ή θύμα παρενόχλησης και εξαπάτησης.

Ελληνική Νομοθεσία.

- Στο Σύνταγμα της Ελλάδος:
  - Η θεμελιώδης διάταξη του άρθρου 2 παρ. 1, αναφέρει ότι «ο σεβασμός και η προστασία της αξίας του ανθρώπου αποτελούν πρωταρχική υποχρέωση της πολιτείας».
  - Στο άρθρο 9, αναφέρεται ότι «η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη» διάταξη που απαγορεύει τη δημοσιοποίηση της ζωής του ατόμου.
  - Το άρθρο 19 προστατεύει το απόρρητο των επιστολών και την ελεύθερη ανταπόκριση και επικοινωνία. Βασικό στοιχείο της επικοινωνίας αποτελεί η μυστικότητα του περιεχομένου της.

Τι είναι το cyberbulling;

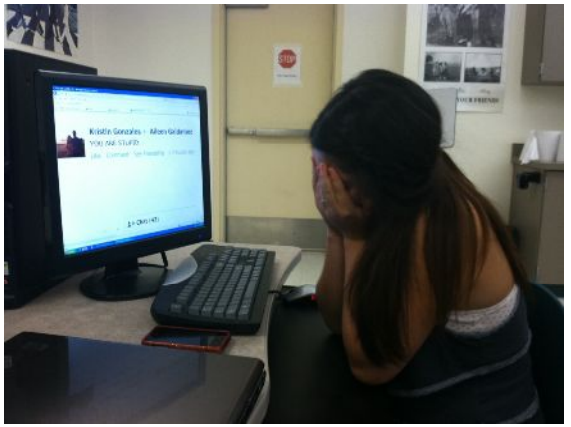
- Ο όρος **διαδικτυακός εκφοβισμός** (Cyber-bullying) αφορά τον εκφοβισμό που είναι δυνατό να πραγματοποιηθεί μέσω του Διαδικτύου και περιλαμβάνει **εσκεμμένη, επαναλαμβανόμενη και εχθρική συμπεριφορά** απέναντι σε συγκεκριμένο άτομο ή ομάδα ατόμων με σκοπό την **πρόκληση συναισθηματικής και ψυχολογικής βλάβης**.

Συνέπειες στα παιδιά

- Τα νέα άτομα νιώθουν μοναχικά, δυστυχή και φοβισμένα.
- Αισθάνονται μια διαρκή πίεση, έντονο άγχος και φόβο και βρίσκονται σε συναισθηματικό αδιέξοδο.
- Χάνουν την εμπιστοσύνη στον εαυτό τους και μπορεί να θέλουν να μην ξαναπάνε στο σχολείο.
- Σε ακραίες περιπτώσεις έχει οδηγήσει σε πρόθεση αυτοκτονίας.

Τι πρέπει να κάνει ένας έφηβος όταν πέσει θύμα cyberbulling;

- Εάν πέσουμε θύμα εκφοβισμού, σταματάμε αμέσως την επικοινωνία με το θύτη.
- Εμπιστευόμαστε στους γονείς μας ή σε κάποιο ενήλικα τον εκφοβισμό που έχουμε δεχθεί.
- Δεν προωθούμε εκφοβιστικά μηνύματα.
- Φιλτράρουμε ηλεκτρονικά μηνύματα από άτομα που μάς παρενοχλούν και μπλοκάρουμε την πρόσβασή τους σε προσωπικούς δικτυακούς χώρους (π.χ., ιστολόγιο).



Τι ονομάζουμε grooming;

- Ο όρος **Grooming** αναφέρεται στην αποπλάνηση και συμβαίνει όταν άγνωστοι εκμεταλλεύονται κακόβουλα το στοιχείο της ανωνυμίας στο Διαδίκτυο για να προσεγγίσουν ανήλικους με στόχο να αναπτύξουν φιλική σχέση και να αποσπάσουν όσο το δυνατό περισσότερες πληροφορίες (π.χ., τόπο διαμονής, τα ενδιαφέροντά τους, τις σεξουαλικές τους εμπειρίες κλπ) και απώτερο σκοπό τη σεξουαλική παρενόχληση.

Grooming

- Το Grooming αποτελεί ένα είδος ψυχολογικού χειρισμού και για το λόγο αυτό είναι σημαντικό **να εξηγήσουμε στους γονείς** πως οφείλουν να είναι ενημερωμένοι για τις **διαδικτυακές γνωριμίες** των παιδιών τους ώστε, όταν παρατηρήσουν κάτι ύποπτο, να μπορέσουν να τα συμβουλέψουν αποτελεσματικά και να δράσουν άμεσα.

Πώς τα κυκλώματα παιδοφιλίας χρησιμοποιούν το Διαδίκτυο;

- Υπάρχει μια ισχυρή εντύπωση ότι το Διαδίκτυο έχει γίνει ένας ισχυρός παράγων στην εξέλιξη των παιδοφιλικών κυκλωμάτων παγκοσμίως.
- Τα δίκτυα παιδοφιλίας χρησιμοποιούν εξελιγμένες τεχνολογίες τηλεπικοινωνιών, κάνοντας χρήση κρυπτογράφησης και κωδικών ονομασιών, γίνεται συνεχώς δυσκολότερη η ανακάλυψή τους από τις αρχές.

Παραδείγματα διακίνησης πορνογραφικού υλικού στην Ελλάδα και στην Ευρώπη

- Μια ιδιαίτερη περίπτωση παιδικής πορνογραφίας απασχόλησε το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής τον Μάρτιο του 2009 καθώς εντοπίστηκαν ένας Σκοτσέζος στο Ηράκλειο Κρήτης και ένας επιχειρηματίας στην Αθήνα να συμμετέχουν σε κύκλωμα όπου παρουσιάζονταν ζωντανές μεταδόσεις βιασμού και σεξουαλικής κακοποίησης μικρών παιδιών.

Τι είναι το sexting;

- Το **sexting** ορίζεται ως η πράξη αποστολής, λήψης και διατήρησης μηνυμάτων σεξουαλικού περιεχομένου με φωτογραφικό ή οπτικοακουστικό υλικό μέσω κινητού τηλεφώνου ή άλλου μέσου ψηφιακής τεχνολογίας.
- Τυπικά το sexting, στα πλαίσια του σχολείου, εμφανίζεται περισσότερο μέσα από τη χρήση κινητών τηλεφώνων.
- Οι εμπλεκόμενοι έφηβοι, συχνά δεν μπορούν να διανοηθούν ότι ένα sext μπορεί να προωθηθεί σε πολλαπλούς αποδέκτες.

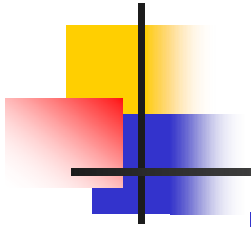
οδηγίες και συμβουλές προς γονείς και παιδιά

Το **παιδί** πρέπει να κατανοήσει ότι

1. Σε χώρους όπως τα chat room δεν μπορούμε ποτέ να είμαστε σίγουροι για την ταυτότητα του άλλου.
2. Πρέπει να αντιμετωπίζει τις διαδικτυακές γνωριμίες με αρκετή επιφυλακτικότητα, καθώς ακόμη και άτομα που έχουν κερδίσει την εμπιστοσύνη του μπορεί να έχουν σκοπό να το βλάψουν.
3. Δεν είναι ασφαλές να δίνει τα προσωπικά στοιχεία επικοινωνίας.

Οι **γονείς** οφείλουν να είναι ενημερωμένοι για τις διαδικτυακές γνωριμίες των παιδιών τους ώστε όταν παρατηρήσουν κάτι ύποπτο να μπορέσουν να τα συμβουλέψουν αποτελεσματικά.

ΆΛΛΟΙ ΚΙΝΔΥΝΟΙ ΠΟΥ ΜΠΟΡΕΙ ΝΑ ΣΥΝΑΝΤΗΣΟΥΜΕ ΣΤΟ ΔΙΑΔΙΚΤΥΟ



- Phishing
- Spam email
- Μηνύματα Hoaxes
- Ψεύτικα profil
- Εθισμός στο διαδίκτυο
- Διαδικτυακά παιχνίδια & online gambling
- Τι κρύβεται πίσω από τα Social media
- Οικονομικές συναλλαγές - εξαπάτηση

Τι ονομάζεται phishing-οικονομική εξαπάτηση;

- Πρόκειται για μια ιδιαίτερα διαδεδομένη τεχνική οικονομικής εξαπάτησης μέσω του «ψαρέματος» προσωπικών δεδομένων και ειδικότερα στοιχείων που αφορούν οικονομικές συναλλαγές (αριθμό λογαριασμού, κωδικό πιστωτικής κάρτας κ.λπ.).

Τι πρέπει να κάνουμε όταν λαμβάνουμε ένα μήνυμα phishing;

1. Αποφύγετε την κοινοποίηση προσωπικών και ευαίσθητων στοιχείων σας μέσω τηλεφώνου, e-mail ή/και ηλεκτρονικής φόρμας, εφόσον δεν έχετε επιβεβαιώσει ότι το αίτημα έχει προέλθει από την ίδια την εταιρεία με την οποία συνεργάζεστε και η οποία παρουσιάζεται ως αποστολέας.
2. Βεβαιωθείτε ότι η διεύθυνση στη συγκεκριμένη σελίδα είναι σωστή και κάντε κλικ σε οποιεσδήποτε εικόνες ή συνδέσμους, για να επαληθεύσετε ότι σας οδηγούν στις σωστές σελίδες μέσα στο site.

Τι είναι τα spam email;

- Η ανεπιθύμητη αλληλογραφία ή spamming είναι η μαζική αποστολή μεγάλου αριθμού μηνυμάτων ηλεκτρονικού ταχυδρομείου που απευθύνονται σε ένα σύνολο παραληπτών του διαδικτύου χωρίς αυτοί να έχουν προκαλέσει συνειδητά την αλληλογραφία με τον εν λόγω αποστολέα.

Πώς να αποφύγετε τα spam email;

1. Μη δημοσιεύετε την διεύθυνση ηλεκτρονικού ταχυδρομείου σας.
2. Μη δίνετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας, σε οργανισμούς που δεν εμπιστεύεστε.
3. Μην απαντάτε στο spam.
4. Αναφέρετε κάθε μήνυμα Spam που λαμβάνετε.

Τι είναι τα μηνύματα απατηλού περιεχομένου- hoaxes;

Τα Hoaxes διακινούνται στο δίκτυο μέσω του ηλεκτρονικού ταχυδρομείου και η δημοφιλέστερη κατηγορία τους είναι τα προειδοποιητικά μηνύματα σχετικά με ιούς (π.χ. μη διαβάσετε email με το subject "Good Times" διότι θα καταστραφεί ο Η/Υ σας).

Ποιοι είναι οι παράγοντες που οδηγούν τους νέους σε εθισμό στο διαδίκτυο;

1. Συνήθως, τα παιδιά που αντιμετωπίζουν το πρόβλημα του εθισμού στο διαδίκτυο είναι αγόρια και μεγαλώνουν σε δύσκολες καταστάσεις (δυσλειτουργικές οικογένειες).
2. Επίσης, ο εθισμός των εφήβων στο διαδίκτυο μπορεί, να είναι το αποτέλεσμα άλλων ψυχικών διαταραχών, όπως κατάθλιψη, αγχώδεις διαταραχές, διαταραχές προσωπικότητας, υπερκινητικότητα και κοινωνική φοβία.
3. Το φαινόμενο αυτό, μπορεί να εμφανιστεί σε εφήβους κατά την πρώιμη εφηβεία (10-14 ετών) ή και σε μικρότερη ακόμη ηλικία.

Ποιά είναι τα συμπτώματα του εθισμού στο διαδίκτυο;

1. Κατανάλωση υπερβολικού χρόνου ή και χρήματος σε δραστηριότητες σχετικές με το διαδίκτυο (λογισμικοί, σκληροί δίσκοι κ.λ.π)
2. Μειωμένη επίδοση στο σχολείο λόγω των πολλών ωρών που περνάει ο έφηβος στο διαδίκτυο.
3. Σε προχωρημένες περιπτώσεις ο έφηβος δεν κοιμάται,
4. Παραμελεί την προσωπική του υγιεινή, μπορεί να σταματήσει ακόμα και το σχολείο.
5. Απομονώνεται από την οικογένεια και τους φίλους τους, γίνονται επιθετικοί, μπορεί να κλέβουν χρήματα από τους γονείς για να παίζουν.
6. Τέλος, φτάνουν σε σημείο να μην τρώνε ή και το αντίθετο (να παχύνουν πολύ).

Τι είναι τα ψεύτικα profil σε site κοινωνικής δικτύωσης;

- Τα ψεύτικα προφίλ είναι πολυάριθμα στους χώρους κοινωνικής δικτύωσης και ειδικά στον χώρο του facebook. Πίσω από την ανωνυμία των χρηστών, κρύβεται η προώθηση ενός διαφημιστικού υλικού ή προϊόντος. Σε άλλες περιπτώσεις, τα κίνητρα είναι διαφορετικά και σχετίζονται με τον εκφοβισμό (**cyber bulling**), την ηλεκτρονική απάτη κ.α.

Πώς μπορείτε να προφυλαχθείτε από τα ψεύτικα profil; Συμβουλές

1) Ψάξτε και διαγράψτε τα ψεύτικα προφίλ από τους φίλους σας, ειδικά αν προσπαθούν να σας προσεγγίσουν.
2) Χρησιμοποιήστε τις λειτουργίες **block** (δεν μπορεί να δει το προφίλ σας) και **report** (αναφορά ψεύτικου προφίλ στο facebook), ανάλογα με την εκάστοτε περίπτωση.
3) Να αναφέρεις ελάχιστα στοιχεία σχετικά με τα προσωπικά σου δεδομένα
4) Μην κλείσετε ραντεβού με κάποιον άγνωστο χρήστη του διαδικτύου.
5) Εάν εμπιστευτείτε κάποιον άγνωστο χρήστη, το ραντεβού φροντίστε να είναι σε δημόσιο χώρο, στον οποίο θα νιώθετε και θα είστε ασφαλής.

Διαδικτυακά Παιχνίδια

- Τα διαδικτυακά παιχνίδια είναι παιχνίδια που παίζονται στον ηλεκτρονικό υπολογιστή ή στις παιχνιδομηχανές (π.χ. Playstation) και, μέσω του διαδικτύου, ο χρήστης μπορεί να παίζει και να αλληλεπιδρά με χρήστες από διάφορες χώρες, πολύ συχνά, σε έναν ενιαίο, εικονικό κόσμο.
- Η θεματολογία τους ποικίλει, όμως τα περισσότερα και πιο διαδεδομένα διαδικτυακά παιχνίδια είναι παιχνίδια ρόλων και παρουσιάζουν ένα πλαίσιο Ηρωικής Φαντασίας.
- Σε μερικά ηλεκτρονικά παιχνίδια μπορούν να παίξουν παραπάνω από ένας παίχτες που μοιράζονται την ίδια περιοχή του παιχνιδιού.

Πώς επηρεάζουν την συμπεριφορά παιδιών και εφήβων όταν γίνεται κατάχρηση των διαδικτυακών παιχνιδιών;

- Τα παιχνίδια μπορούν να δημιουργήσουν **εξάρτηση** και αν θέλει κανείς να διακριθεί σε αυτά, χρειάζεται να δαπανήσει αρκετές ώρες την εβδομάδα.
- Κάποιες φορές, οι παίκτες παρουσιάζουν μια αποκλίνουσα συμπεριφορά, η οποία τους χαρακτηρίζει, ιδίως στη σχέση τους με τους άλλους παίκτες. Οι συμπεριφορές κυμαίνονται από άκρως εγωκεντρική θέαση του παιχνιδιού, δυναστευτική συμπεριφορά, υπερβολική καχυποψία, ρατσισμό, συναισθηματική εξάρτηση από το παιχνίδι και υπερβολική επένδυση σε αυτό, καταναγκαστική συμπεριφορά κ.α.
- Σε κάθε περίπτωση πρέπει να γίνεται σαφής διάκριση μεταξύ ενασχόλησης, εντατικής ενασχόλησης και εξάρτησης.

Τι είναι online gambling?

- Ο συστηματικός τζόγος περιλαμβάνει τη συνάντηση δύο ή περισσότερων ατόμων με σκοπό την ανταλλαγή στοιχημάτων ή/και την ίδια την δραστηριότητα για την οποία γίνονται τα στοιχήματα, αν αυτό είναι δυνατό.
- Το Διαδίκτυο έχει κάνει τη συνάντηση αυτών των τζογαδόρων πολύ πιο εύκολη, είτε πρόκειται για απλό στοίχημα είτε για πόκερ, τάβλι, και σκάκι. Για παράδειγμα, στο πόκερ οι παίχτες παίζουν σε πραγματικό χρόνο σε ένα κοινό ηλεκτρονικό περιβάλλον το οποίο ο κάθε παίκτης βλέπει στην οθόνη του.

Ποιες είναι οι διαφορές ανάμεσα στα παιχνίδια και τον τζόγο;

- Τα παιχνίδια και ο τζόγος είναι δύο εντελώς διαφορετικοί όροι.
- Ενώ το παιχνίδι έχει μια μη πραγματική προσέγγιση με μόνο φανταστικούς δεσμούς με τον φυσικό κόσμο, ο τζόγος περιλαμβάνει το ρίσκο της πραγματικής οικονομικής απώλειας ή του κέρδους.

Ποιοι κίνδυνοι κρύβονται για τους εφήβους από τη χρήση social media;

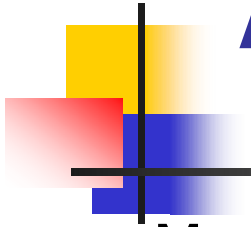
- Οι χρήστες δίνουν τα **προσωπικά τους στοιχεία** σε **αγνώστους** και υπάρχει κίνδυνος να χρησιμοποιήσουν πληροφορίες **απρόσεχτα**, εάν συνομιλούν με κάποιον συνομήλικό τους.
- Η **υποκλοπή προσωπικών** στοιχείων ενός ατόμου. Αν κάνουμε το λάθος και παραχωρήσουμε τους κωδικούς μας σε μια τέτοια περίπτωση, τότε οι επιτήδειοι που ελέγχουν αυτά τα υποτιθέμενα site θα το εκμεταλλευτούν ανάλογα.
- **Κακόβουλα προγράμματα** που αποκαλούνται "κλέφτες κωδικών πρόσβασης" (password stealers). Αυτά τα προγράμματα έχουν την δυνατότητα να εισάγουν κακόβουλο κώδικα στο πρόγραμμα περιήγησης μας.

Πως καταλαβαίνω ότι η σελίδα είναι ασφαλής?

Υπάρχουν συγκεκριμένα στοιχεία, που αποδεικνύουν ότι βρισκόμαστε υπό ασφαλή σύνδεση. Κάποια από αυτά είναι ένα μικρό εικονίδιο με **λουκέτο**, το πρόθεμα **https** που εμφανίζεται μπροστά από την διεύθυνση της ιστοσελίδας, καθώς και το **σύμβολο της εταιρίας η οποία παρέχει το πιστοποιητικό** και εγγυάται την ασφαλή ανταλλαγή δεδομένων αλλά και την ταυτότητα της ιστοσελίδας.

ΠΡΟΣΤΑΤΕΨΕ ΤΟΝ ΕΑΥΤΟ ΣΟΥ

ΒΑΣΙΚΟΙ ΚΑΝΟΝΕΣ ΧΡΗΣΗΣ ΔΙΑΔΙΚΤΥΟΥ

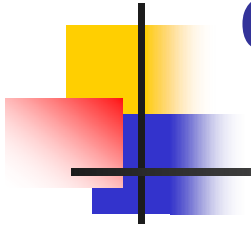


- Μ**ετριοπάθεια** Όποια άποψη και αν υποστηρίζουμε πάντα θα υπάρχει κάποιος που να υποστηρίζει το αντίθετο.
- Π**ερίσκεψη** Ξαναδιαβάστε αυτό που γράψατε πριν το στείλετε και αυτό που σας έστειλαν πριν απαντήσετε
- Ι**εραρχία** Ο list ή group owner και ο moderator είναι οι αδιαμφισβήτητοι αρχηγοί και σπανιότατα θα σας υποστηρίξει κανείς αν τους πάτε κόντρα.
- Π**ροσωπική Επαφή** Μη τσακώνεστε ποτέ μέσω δικτύου. Τα γραπτά αποθηκεύονται σε σκληρούς δίσκους και μένουν για καιρό

ΣΥΓΚΕΚΡΙΜΕΝΑ ΣΤΑ ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ

- Δεν θα πρέπει να δίνετε σε κανέναν τον κωδικό πρόσβασης στο εικονικό προφίλ σας
- Πριν εγγραφείτε σε μια ιστοσελίδα κοινωνικής δικτύωσης αναζητήστε τη δήλωση περί απορρήτου
- Αν δεχθείτε ένα προσβλητικό ή ανεπιθύμητο μήνυμα, χρησιμοποιήστε την ενσωματωμένη μέθοδο καταγγελιών της ιστοσελίδας κοινωνικής δικτύωσης που χρησιμοποιείτε. Συνήθως αναφέρεται με τη λέξη «report».
- Από τη στιγμή που δημιουργείτε το εικονικό σας προφίλ, θα πρέπει να πάτε στο μενού των ρυθμίσεων για τη διαχείριση των προσωπικών σας δεδομένων και να αλλάξετε τις προεπιλεγμένες ρυθμίσεις.
- Να γνωρίζετε ότι από τη στιγμή που προσθέτετε στη λίστα των φίλων σας κάποιο άτομο αυτό αποκτά πρόσβαση στα προσωπικά δεδομένα

Σωστή συμπεριφορά όταν κάνουμε αναζήτηση



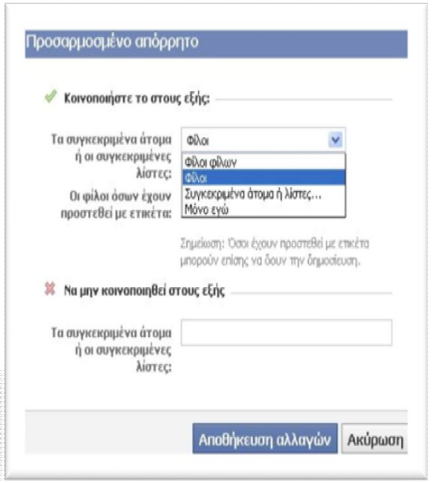
- Είναι σημαντικό να **χρησιμοποιούμε πάντα ιστοσελίδες και ιστοχώρους που είναι κατάλληλα για την ηλικία μας.**
- Τα **φίλτρα γονικού ελέγχου** μπορούν να μειώσουν αυτό τον κίνδυνο.
- **Όταν αναζητούμε μια πληροφορία στο διαδίκτυο:**
  - ελέγχουμε την αξιοπιστία του site
  - την ιδιότητα του συγγραφέα
  - τις βιβλιογραφικές αναφορές
  - τη διασταυρώνουμε με άλλες έγκυρες πηγές (π.χ. βιβλία, εγκυκλοπαίδειες, καθηγητές)

Πώς προστατευόμαστε στο Facebook

- **Μην κλικάρετε σύνδεσμο σε καμία περίπτωση από** φίλο με τον οποίο ποτέ δεν αλληλεπιδράτε ή από άγνωστο.
- **Αποφεύγετε να εξουσιοδοτείτε αναξιόπιστα παιχνίδια και εφαρμογές που σας ζητάνε** να έχουν πρόσβαση στα δεδομένα σας ανά πάσα στιγμή.

ΑΣΦΑΛΕΙΑ ΣΤΟ FACEBOOK

- Σε κάθε post, σε κάθε φωτογραφία, σε κάθε ετικέτα, σε κάθε δήλωση τοποθεσίας, οι χρήστες **πρέπει και μπορούν να διαλέγουν** ή να προσαρμόζουν **το κοινό** (μπορεί κανείς και να αποκλείσει αποδέκτες) ή να ορίσουν εκ των προτέρων το κοινό για όλα όσα γράφουν.
- **Επισκεφτείτε τις δικές σας ρυθμίσεις απορρήτου**
  Από τις ρυθμίσεις απορρήτου μπορείτε επίσης να ορίσετε εάν θα εμφανίζεται περιεχόμενο από ό,τι είναι δημόσιο στο προφίλ σας στο Facebook όταν κάποιος κάνει μια σχετική αναζήτηση στις μηχανές αναζήτησης, εκτός Facebook.



Τι δεν επιτρέπεται να αναρτάται στο Facebook;

- Περιεχόμενο με γυμνό ή σεξουαλικά υπονοούμενα
- Ρητορική μίσους, βάσιμες απειλές ή ευθείες επιθέσεις σε άτομα ή ομάδες
- Περιεχόμενο με σκηνές αυτοτραυματισμού ή σκληρής βίας
- Ψεύτικα ή παραπλανητικά Χρονολόγια
- Ανεπιθύμητο περιεχόμενο (σπαμ)

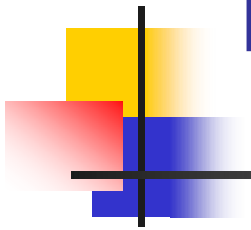
Γιατί το Facebook δεν είναι κατάλληλο για παιδιά κάτω των 13 ετών;

- Τα παιδιά αποτελούν μέρος της πιο επεκτατικής προσωπικής συλλογής δεδομένων και προφίλ στο πιο ισχυρό κοινωνικό μέσο του Διαδικτύου.
- Τα παιδιά εκτίθενται σε μια νέα γενιά εξαιρετικά πειστικών και χειραγωγίσιμων ψηφιακών πρακτικών μάρκετινγκ.
- Οι πρακτικές μάρκετινγκ του Facebook επωφελούνται από τα γνωστικό-κοινωνικά και συναισθηματικά ευάλωτα σημεία των παιδιών.
- Τα παιδιά υποβάλλονται σε μια επίθεση ανθυγιεινής εμπορίας τροφίμων – ακριβώς σε μια εποχή που η παιδική παχυσαρκία έχει γίνει μια μεγάλη κρίση.
- Δεν υπάρχουν εγγυήσεις που να προστατεύουν επαρκώς τα παιδιά από τις επιθετικές και τις επιβλαβείς πρακτικές μάρκετινγκ συλλογής δεδομένων του Facebook.

Ασφαλέστεροι κωδικοί πρόσβασης

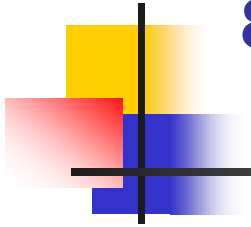
- **Χρησιμοποιείτε δυνατούς κωδικούς και όχι απλούς**
  Γενικά, να θυμάστε πως σε έναν κωδικό καλό είναι να χρησιμοποιείτε τουλάχιστον ένα **σύμβολο**, **γράμμα** (κεφαλαίο και μικρό) και **αριθμό**. Ο συνδυασμός των προηγουμένων μπορεί να δημιουργήσει έναν **ισχυρό κωδικό**. Φυσικά, αποφεύγετε ονόματα, ημερομηνίες γεννήσεις κλπ, τα οποία χαρακτηρίζουν εσάς.
- **Μη χρησιμοποιείτε τον ίδιο κωδικό παντού**
  Τουλάχιστον, προσέξτε ώστε **ο κωδικός για το email που δηλώνετε στα Κοινωνικά Δίκτυα να είναι μοναδικός**.
- **Αποφεύγετε να δίνετε τους κωδικούς** σας σε άτομα χωρίς να υπάρχει ιδιαίτερος λόγος.
- **Αλλάζετε τον κωδικό σας συχνά**

ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΗΛΕΚΤΡΟΝΙΚΗ ΕΞΑΠΑΤΗΣΗ



- Μην απαντάτε ποτέ σε μηνύματα ηλεκτρονικού ταχυδρομείου που σας ζητούν τα **προσωπικά σας στοιχεία**
- Μην κάνετε κλικ σε ύποπτες συνδέσεις
- **Συνεργαστείτε με εταιρείες που γνωρίζετε και εμπιστεύεστε.**
- Βεβαιωθείτε ότι η τοποθεσία Web χρησιμοποιεί κρυπτογράφηση
- **Παρακολουθείτε τις συναλλαγές σας**.

Πώς αντιμετωπίζεται το πρόβλημα του εθισμού στο διαδίκτυο



- Εάν το πρόβλημα αναγνωριστεί σε αρχικό στάδιο, είναι πολύ πιο εύκολο να αντιμετωπισθεί!!!
- Να βάλεις τα απαραίτητα **ΟΡΙΑ** και να απολαμβάνεις τα θετικά της τεχνολογίας χωρίς αρνητικές συνέπειες
- Να μην παραμελείς τις δραστηριότητές σου, τον ύπνο σου, τους φίλους σου και την οικογένειά σου λόγω διαδικτυακών δραστηριοτήτων (π.χ. παιχνίδια, facebook)

Ποια είναι η σωστή στάση των γονέων απέναντι στα παιδιά τους ώστε να είναι ασφαλείς στο διαδίκτυο

- Εξοικειωθείτε με το περιβάλλον των παιδιών σας.
- Εξηγήσετε ότι, αν τους συμβεί κάτι δυσάρεστο στο διαδίκτυο, δε φταίνε αυτά και θα πρέπει να το αναφέρουν άμεσα σε εσάς.
- Μάθετε στα παιδιά σας να μην απαντούν ποτέ σε πρόστυχα ή προσβλητικά μηνύματα στο διαδίκτυο.
- Χρησιμοποιήστε φίλτρα για επιβλαβείς ιστοσελίδες

ΣΩΣΤΗ ΣΤΑΣΗ ΣΩΜΑΤΟΣ