

A young woman with long brown hair is sitting at a desk in a dimly lit room. She is covering her face with her right hand, suggesting distress or frustration. A laptop is open in front of her, and the keyboard is visible. The background is dark, and the lighting is focused on her face and the laptop.

ΟΙ ΧΡΗΣΕΙΣ ΚΑΙ ΟΙ ΚΙΝΔΥΝΟΙ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

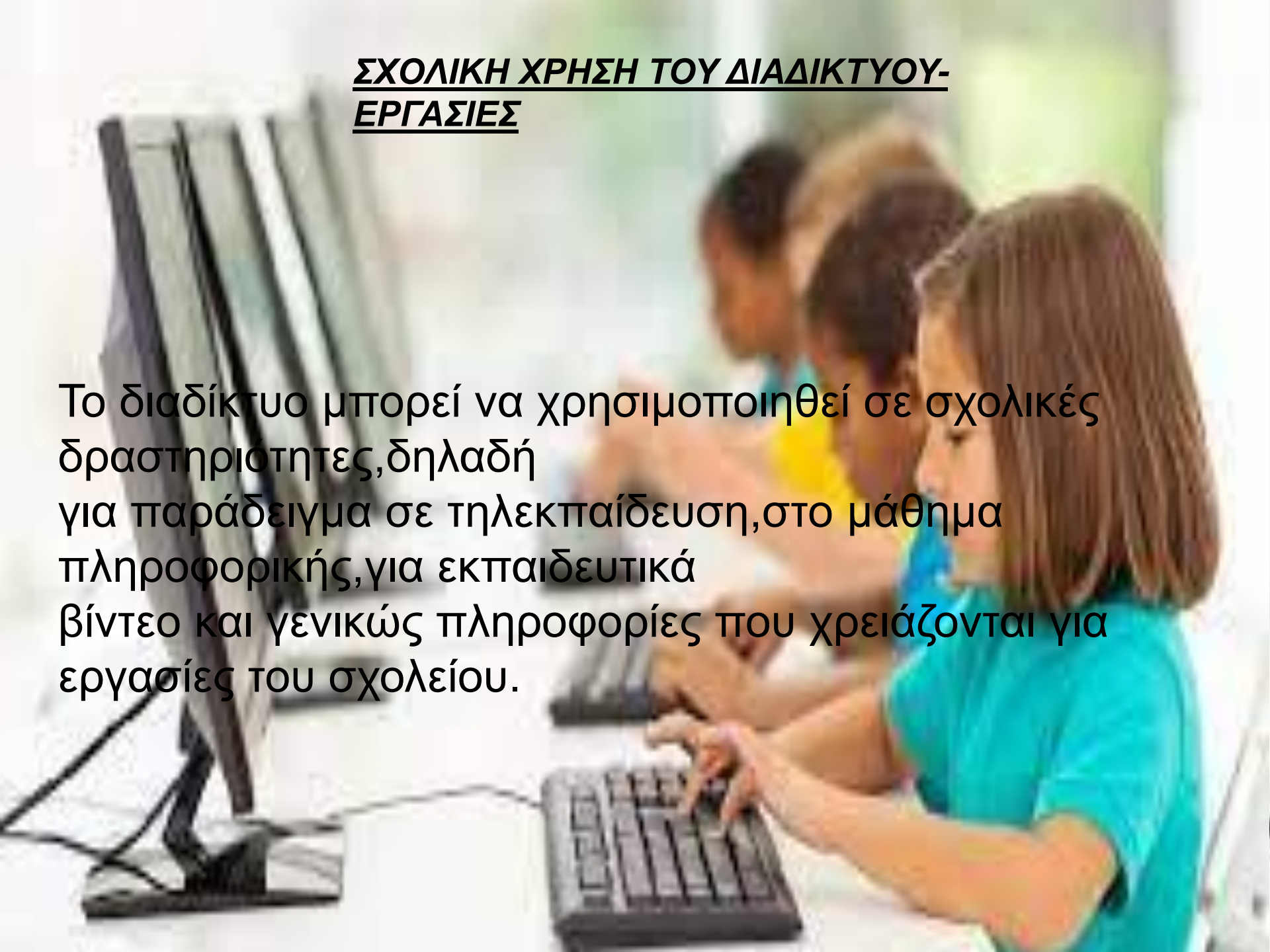
ΤΜΗΜΑ ΣΤ2

ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ ΣΕ
ΔΙΑΦΟΡΟΥΣ ΤΟΜΕΙΣ ΤΗΣ
ΖΩΗΣ ΜΑΣ

ΕΡΓΑΣΙΑ ΜΥΡΤΩ Ι.

ΣΧΟΛΙΚΗ ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ- ΕΡΓΑΣΙΕΣ

Το διαδίκτυο μπορεί να χρησιμοποιηθεί σε σχολικές δραστηριότητες, δηλαδή για παράδειγμα σε τηλεεκπαίδευση, στο μάθημα πληροφορικής, για εκπαιδευτικά βίντεο και γενικώς πληροφορίες που χρειάζονται για εργασίες του σχολείου.



ΧΡΗΣΗ ΣΕ ΕΠΙΧΕΙΡΗΣΕΙΣ

- Το διαδίκτυο μπορεί να χρησιμοποιηθεί στα καταστήματα ηλεκτρονικών ειδών, στα καταστήματα με ρούχα, παπούτσια, αξεσουάρ κ.ά. στην μορφή των e-shop και με αυτόν τον τρόπο μπορείς να κάνεις παραγγελίες και διαδικτυακά.
- Άλλες επιχειρήσεις που το διαδίκτυο είναι χρήσιμο είναι οι τράπεζες. Δηλαδή μέσα από την τράπεζα μπορείς να πληρώνεις διαδικτυακά τους λογαριασμούς ρεύματος κλπ, όπως επίσης παρέχει και συστήματα ασφαλείας.



ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ ΓΙΑ ΕΠΙΚΟΙΝΩΝΙΑ

- Το διαδίκτυο είναι χρήσιμο στην επικοινωνία από μεγάλες αποστάσεις με ανθρώπους από όλο τον κόσμο, είτε πρόκειται για παιχνίδι, είτε για δουλειά.
- Άλλη χρήση του διαδικτύου στην επικοινωνία είναι η ανταλλαγή απόψεων, ιδεών, πληροφοριών και σκέψεων.



ΟΙΚΙΑΚΗ ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ

- Το διαδίκτυο είναι χρήσιμο στα βιντεοπαιχνίδια, στην δουλειά από το σπίτι, στην πληρωμή ενοικίου, ρεύματος κλπ χωρίς να χρειάζεται να πηγαίνεις πουθενά.
- Άλλη χρήση του οικιακού διαδικτύου, είναι η πληροφόρηση για τον καιρό, τις ειδήσεις σε όλο τον κόσμο, ταινίες, σειρές, ντοκιμαντέρ και νέα από ηθοποιούς, δημοσιογράφους κ.ά.

Το Διαδίκτυο στη ζωή μας . Χρήσεις σε διαφορετικούς τομείς της ζωής μας .

Το διαδίκτυο δεν χρησιμοποιείται μόνο για να αναζητήσουμε κάτι χρησιμοποιείται σε επαγγελματικούς τομείς και σε ψυχαγωγικούς τομείς για παράδειγμα σε σχολεία ,φροντιστήρια και νηπιαγωγεία.

Κωνσταντίνος Π.

Το διαδίκτυο σε επαγγελματικούς τομείς .

- Αρκετοί εργαζόμενοι αν για παράδειγμα αρρωστήσουν μπορούν αντί για να πάρουν άδεια να κάνουν τηλεργασία (εάν τους αφήνει το αφεντικό τους) και να μην χρειαστεί να χάσουν πολύτιμα χρήματα .

Το Διαδίκτυο στα σχολεία .

Επίσης το διαδίκτυο χρησιμοποιείται και για τα σχολεία ,τα νηπιαγωγεία και ακόμα και τα φροντιστήρια .Οι λόγοι που το διαδίκτυο χρησιμοποιείται από τα σχολεία είναι για να προβάλλονται τα ηλεκτρονικά βιβλία και εκπαιδευτικά βίντεο .

Το Διαδίκτυο στην αγορά.

- Αρκετοί πελάτες επιλέγουν να κάνουν τα ψώνια τους online για να βρίσκουν πάντα τις καλύτερες τιμές της αγοράς και να μην πληρώνουν μεταφορικά και τελωνείο εάν είναι το κατάστημα έξω από τα σύνορα της χώρας τους .

Το Διαδίκτυο και το εμπόριο .

- Σχεδόν όλοι οι έμποροι επιλέγουν να παίρνουν τα εμπορεύματα τους από διάφορες χώρες γιατί συνήθως έχουν μεγαλύτερη ποικιλία και πολύ καλύτερες τιμές .

Το Διαδίκτυο και η αστυνόμευση .

- Το διαδίκτυο μπορεί να βοηθήσει πολύ την αστυνομία γιατί μπορούν να δουν ποια άτομα πουλάνε παράνομα όπλα και γενικά κάνουν διάφορες απάτες και ποιοι γράφουν fake news .

ΧΡΗΣΕΙΣ ΔΙΑΔΙΚΤΥΟΥ

ΧΡΗΣΤΟΣ Χ.



Εισαγωγή

Το διαδίκτυο είναι παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι χρησιμοποιούν καθιερωμένη ομάδα πρωτοκόλλων, η οποία συχνά αποκαλείται "TCP/IP" (αν και αυτή δεν χρησιμοποιείται από όλες τις υπηρεσίες του Διαδικτύου) για να εξυπηρετεί δισεκατομμύρια χρήστες καθημερινά σε ολόκληρο τον κόσμο. Η εμφάνιση του διαδικτύου αποτελεί μια πολύ σημαντική καινοτομία στην τεχνολογία. Το διαδίκτυο μας βοηθάει σε διάφορους τομείς της ζωής μας όπως:

Επικοινωνία

- Το διαδίκτυο και η κοινωνική δικτύωση αποτελεί μέρος της καθημερινότητας πολλών παιδιών και εφήβων. Στόχος της κοινωνικής δικτύωσης είναι η δημιουργία μιας διαδικτυακής παγκόσμιας κοινότητας ατόμων με σκοπό την επικοινωνία και τη μεταξύ τους αλληλεπίδραση «δημιουργώντας» μια νέα μορφή επικοινωνίας. Επιπλέον, το «social networking» ως νέος τρόπος κοινωνικής διαδραστικότητας και συμμετοχής, επιτρέπει στους χρήστες να δημιουργούν οι ίδιοι περιεχόμενο στο Διαδίκτυο και να το μοιράζονται με άλλους χρήστες χωρίς να έχουν εξειδικευμένες τεχνικές γνώσεις.

-

Γνώσεις

- Οι γνώσεις που αποκομίζονται από το Διαδίκτυο είναι αρκετές, κάτι που ωφελεί τα νέα παιδιά. Αρχικά μπορεί να βετλιώσουν την ξένη γλώσσα που γνωρίζουν, μέσω της συχνής συνομιλίας με άτομα από όλο τον κόσμο. Επίσης, συχνές απορίες τους θα λυθούν μέσω αναζητήσεων και ανάγνωσης άρθρων ή επιστημονικών πηγών. Οι έφηβοι θα αναγκαστούν να μάθουν να ψάχνουν για να βρίσκουν αυτό που τους ενδιαφέρει. Με τον τρόπο αυτό αποκτούν και κίνητρο να ενημερωθούν και να αποκομίσουν γνώσεις, καθώς είναι κάτι που ανακάλυψαν μόνοι τους.

Κοινωνικοποίηση

- Το Διαδίκτυο και τα μέσα κοινωνικής δικτύωσης έχουν κατηγορηθεί για απομόνωση των νέων, αλλά αντίθετα απ' ότι πιστεύεται, το διαδίκτυο δίνει τη δυνατότητα ανάπτυξης της επικοινωνίας στους νέους και μάλιστα τους δίνεται η δυνατότητα για την ανάπτυξη καλύτερης κοινωνικοποίησης.
- Μέσω των online παιχνιδιών, blogs ή chats, οι έφηβοι έρχονται σε επαφή και με άτομα διαφορετικών χαρακτηριστικών και αντίθετων απόψεων απο αυτές που έχουν συνηθίσει.

Δεξιότητες σχετικές με τον υπολογιστή


- Οι νέοι, δεδομένου ότι ασχολούνται με το διαδίκτυο, γίνονται
- «άριστοι» στις βασικές λειτουργίες του υπολογιστή, οι οποίες γίνονται «κτήμα τους» αβίαστα, αφού είναι αναγκασμένοι να ανταπεξέλθουν στις απαιτήσεις χρήσης του, όπως επίσης, σε ενδεχόμενους «ιούς», σε αναβαθμίσεις και άλλα σχετικά. Όσο περισσότερο ασχολούνται και εξερευνούν τον υπολογιστή, τόσο πιο οικείος γίνεται.
- Επίσης, αποκτούν «εξ ανάγκης» την ικανότητα δακτυλογράφησης, αφού θέλουν να απάντουν άμεσα και γρήγορα σε «chat», που τους οδηγεί στην εκμάθηση τυφλού συστήματος πληκτρολογήσεως.

ΔΙΑΣΚΕΔΑΣΗ

- Όλοι έχουμε βρεθεί σε μία θέση όπου χρειαζόταν να περιμένουμε χωρίς να έχουμε κάτι να κάνουμε.
- Έτσι με την βοήθεια του ίντερνετ μπορούμε να περνάμε αυτή την ώρα διασκεδάζοντας είτε παίζοντας κάποιο παιχνίδι, είτε παρακολουθώντας κάποιο βίντεο. Ακόμα μπορούμε να δούμε online σειρές και ταινίες που δεν προλάβαμε στην τηλεόραση ή που δεν προβάλλονται στην χώρα μας.



ΨΥΧΑΓΩΓΙΑ

- Η ψυχαγωγία μέσω Internet την εποχή μας είναι ο πιο διαδεδομένος τρόπος ψυχαγωγίας, για όλες τις ηλικίες. Μπορεί κάποιος να δει βίντεο με ότι θέμα αυτός επιλέξει ή ακόμα και να παίξει παιχνίδια.
- 

Συναλλαγές στο Διαδίκτυο

- Οι εφαρμογές παρέχουν τη δυνατότητα ηλεκτρονικών πληρωμών και συναλλαγών μέσω Διαδικτύου. Η διασφάλιση των συναλλαγών απαιτεί αξιοποίηση πρωτοκόλλων κρυπτογράφησης και κωδικοποίησης για την εξακρίβωση της ταυτότητας του χρήστη και τη μεταφορά των στοιχείων της συναλλαγής. Η ολοκλήρωση μιας συναλλαγής επιτυγχάνεται με την αξιοποίηση ενός συνόλου υπηρεσιών που διατίθενται από τραπεζικά συστήματα και άλλες εταιρείες.

ONLINE SHOPPING



- Βρεθήκατε ποτέ σε μια θέση που έπρεπε να βγείτε έξω και να αγοράσετε κάτι αλλά δεν ήταν στη διάθεση σας ή δεν είχατε το χρόνο να βγείτε έξω και να το πάρετε;
- Αν, ναι το ίντερνετ στις μέρες μας σου επιτρέπει να αγοράσεις ένα αντικείμενο από οπουδήποτε στον κόσμο, απ' την
- γειτονιά σου μέχρι και από μια άλλη χώρα, ακόμα κι από άλλη ήπειρο.

ΑΜΕΣΗ ΕΝΗΜΕΡΩΣΗ - SOCIAL MEDIA

- Μέσω του διαδικτύου, στις μέρες μας είναι πολύ εύκολο για όλους να μαθαίνουμε σύντομα και δωρεάν ό,τι είδους πληροφορία χρειαζόμαστε, και έτσι ενημερωνόμαστε γρηγορά και με απόλυτη ασφάλεια.



ΕΡΓΑΣΙΑ



- Ο σχεδιασμός Ιστού, ο τεχνικός υπολογιστών και ο προγραμματιστής, είναι μεταξύ πολλών που βρίσκονται στη μέγιστη ζήτησή τους για τους εργοδότες. Σχεδόν κάθε επιχείρηση σήμερα, πρέπει να έχει έναν ιστιοχώρο που προωθεί τα προϊόντα και τα διπλώματα ευρεσιτεχνίας του ότι οι σχεδιαστές Ιστού είναι μεταξύ των ο πιο ιδιαίτερα ζητούμενων επαγγελματιών που απαιτούνται. Επιπλέον, οι σύμβουλοι, οι πωλητές, οι έμποροι και όλα τα είδη των επαγγελματιών απαιτούνται για να προαγάγουν και να βοηθήσουν τους ανθρώπους μέσω του Διαδικτύου. Οι νοικοκυρές, μητέρες και με ειδικές ανάγκες άτομα, μπορούν τώρα να έχουν μια πιθανότητα να εργαστούν από το σπίτι τους και να κερδίσουν τα χρήματα που ειδώλλως θα ήταν δύσκολο να ληφθούν.

ΚΙΝΔΥΝΟΙ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Αργυρώ Π.

ΕΙΣΑΓΩΓΉ

- ◉ Το διαδίκτυο είναι ένα παγκόσμιο σύστημα που χρησιμεύει αρκετά στην καθημερινότητά μας. Στο διαδίκτυο μας βοήθα σε αρκετά πράγματα όπως να βρούμε διάφορες πληροφορίες για σημαντικά πράγματα για διάφορους ήρωες της επανάστασης. Όμως έχει και πολλούς κινδύνους.



ΚΙΝΔΥΝΟΙ

- ⊙ Διαδικτυακός εκφοβισμός
- ⊙ Απάτες
- ⊙ Εθισμός
- ⊙ Σελίδες που δεν γνωρίζουμε
- ⊙ αγορές στο διαδίκτυο
- ⊙ Προσωπικά στοιχεία
- ⊙ διαδικτυακά παιχνίδια

ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ

- Ο διαδικτυακός εκφοβισμός αφορά την απειλή , τον εκφοβισμό και την παρενόχληση παιδιών αλλά και μεγάλων που συνομιλούν με άγνωστους ανθρώπους διαδικτυακά . Είδη εκφοβισμού είναι : bullying , Σχολικός εκφοβισμός , **Διαδικτυακός εκφοβισμός** , Παρενόχληση , Ηθική παρενόχληση , Προσωπική επίθεση.

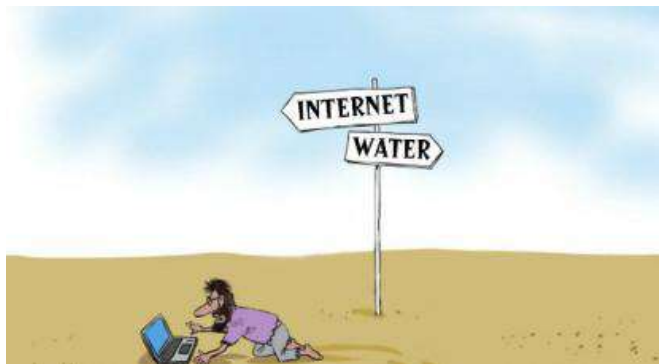
ΑΠΑΤΕΣ

- Οι απάτες στο διαδίκτυο είναι αρκετά συχνές. Οι διαδικτυακές απάτες μπορεί να συμβούν σε όλους. Υπάρχουν διάφορες απάτες π.χ. μπορούν να σου πάρουν προσωπικά στοιχεία ή να σε κοροϊδέψουν όταν κάνεις αγορές ή συναλλαγές με τράπεζες ή άλλους οργανισμούς



ΕΘΙΣΜΌΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

- ◉ Ο εθισμός στο διαδίκτυο είναι μια σχετικά νέα μορφή εξάρτησης. Αναφέρεται στη περίπτωση όπου το διαδίκτυο αποκτά μεγαλύτερη σημασία και προτεραιότητα στη ζωή σου από τους φίλους, την οικογένεια και την εργασία σου, κυριαρχεί στη καθημερινότητά σου και είναι ένα στοιχείο της που δεν θέλουμε να αποχωριστείς.



ΆΓΝΩΣΤΕΣ ΣΕΛΪΔΕΣ

- ◉ Άγνωστες σελίδες στο διαδίκτυο μπορούν να γίνουν πολύ επικίνδυνες. Καλό είναι να αποφεύγουμε τέτοιου είδους σαιτ γιατί πολλές φορές δεν ξέρουμε τι περιέχουν. Γενικότερα πρέπει να είμαστε πολύ προσεκτικοί με τέτοια πράγματα. Υπάρχουν σαιτ που μπορεί να περιέχουν ακατάλληλο περιεχόμενο ή σαιτ που μπορεί να περιέχουν ιούς και να επηρεάσουν τον υπολογιστή ή το ηλεκτρονικό μέσο σου.



ΑΓΟΡΈΣ ΣΤΟ ΔΙΑΔΊΚΤΥΟ

- Οι αγορές στο μέσο διαδικτύου μπορούν να γίνουν πολύ επικίνδυνες. Μπορούν να σου πάρουν τα στοιχεία ή να μην σου φέρουν ποτέ τα πράγματα που παρήγγειλες. Επίσης μπορούν να πάρουν λεφτά από την κάρτα σου και να μην στα επιστρέψουν ή να κρατήσουν τους κωδικούς της κάρτας σου.



ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ

- Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα .Στο διαδίκτυο υπάρχει αρκετός κίνδυνος για αυτό δεν πρέπει να ξέρει κανείς και να προσεχείς πολύ με τα προσωπικά σου στοιχεία.

ΔΙΑΔΙΚΤΥΑΚΑ ΠΑΙΧΝΙΔΙΑ

- ◉ Υπάρχει μεγάλος κίνδυνος που άφορα τα παιχνίδια στο διαδίκτυο
- ◉ Το διαδίκτυο έχει ανοίξει νέους ορίζοντες πληροφόρησης και επικοινωνίας στη ζωή μας, αλλά ταυτόχρονα ελλοχεύουν σε αυτό και σοβαροί κίνδυνοι, ειδικά για παιδιά και έφηβους. Επικίνδυνα διαδικτυακά παιχνίδια έχουν εισβάλλει στην καθημερινή πραγματικότητα της «ιντερνετικής» ζωής, κυρίως ανήλικων, απειλώντας ακόμη και τη ζωή τους.

Κίνδυνοι του διαδικτύου και τρόποι αντιμετώπισής τους

Ελισάβετ Λ.



ΕΙΣΑΓΩΓΗ

- Το διαδίκτυο στις μέρες μας συμβάλει στην καθημερινότητα μας και μας βοηθάει σε πολλά πράγματα. Όμως όσο χρήσιμο κι' αν είναι το διαδίκτυο κρύβει πολλούς κινδύνους που εμείς πρέπει να προφυλακτούμε.



ΤΙ ΕΙΝΑΙ Ο ΚΙΝΔΥΝΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

- Στο διαδίκτυο υπάρχουν πολλοί κίνδυνοι όπως ιοί, ηλεκτρονικές απάτες, εκφοβισμός, επικίνδυνα παιχνίδια κ.α. όλα αυτά συμβάλλουν ως κίνδυνοι στο διαδίκτυο.



ΕΙΔΟΙ ΚΙΝΔΥΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

1. Εθισμός στο διαδίκτυο
2. Διαδικτυακή παρενόχληση
3. Σεξουαλική Παρενόχληση στο διαδίκτυο
4. Διαδικτυακή απάτη
5. Διαδικτυακά παιχνίδια
6. Ιοί



Βασικοί Κίνδυνοι στο διαδίκτυο

- Αποπλάνηση Ανηλίκων
- Ηλεκτρονική Παρενόχληση
- Διαδικτυακά Παιχνίδια
- Υπερβολική Χρήση και Εθισμός
- Ανεπιθύμητη Αλληλογραφία



Τι πρέπει να προσέχουμε ώστε να μείνουμε ασφαλείς

- 2) Προσοχή στους Κοινωνικούς ιστότοπους
- 3) Προσοχή στα online games
- 4) Προσοχή στο Phishing
- 5) Προσοχή στις αγορές στο διαδίκτυο
- 6) Σε σελίδες που δεν γνωρίζουμε
- 7) Στους ιούς που κυκλοφορούν στο διαδίκτυο (χρειαζόμαστε οπωσδήποτε ένα antivirus)
- 8) Στα προγράμματα που κατεβάζουμε.
- 9) Πρέπει να δίνουμε μεγάλη προσοχή με το ποιους μιλάμε και τα προσωπικά στοιχεία μας δημοσιεύουμε στο διαδίκτυο για να πέσουμε θύματα εκβιασμού, εκφοβισμού ή οτιδήποτε.
- 10) Πρέπει να προσέχουμε ιδιαίτερα τους «ξένους» με τους οποίους μιλάμε γιατί η σεξουαλική παρενόχληση είναι ένας από τους πιο συχνούς κινδύνους.

SITES/ΠΗΓΕΣ

ΈΝΑ ΜΕΓΑΛΟ ΕΥΧΑΡΙΣΤΩ ΣΤΟΥΣ

ereunitis.gr

wikipedia.org

[SaferInternet4kids](http://SaferInternet4kids.org)

UOP.KEP BlogsPorta





ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ ΚΑΙ ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗ

Μαριλένα Γ. ΣΤ 2

Εισαγωγή

Σε αυτή τη παρουσίαση θα εξετάσουμε:

- **τι είναι ο διαδικτυακός εκφοβισμός**
- **και θα δούμε κάποιους τρόπους αντιμετώπισης του.**



Τι είναι ο διαδικτυακός εκφοβισμός

- **Διαδικτυακός εκφοβισμός** συμβαίνει όταν κάποιος κακόβουλος παρενοχλεί ένα άτομο με τη χρήση της τεχνολογίας. Η παρενόχληση αυτή μπορεί να γίνεται σε τακτικά ή άτακτα χρονικά διαστήματα μέσω οποιασδήποτε πράξης εκφοβισμού, επιθετικότητας ή αυταρχικής συμπεριφοράς.
- Ο **Διαδικτυακός Εκφοβισμός συνήθως έχει τη μορφή** ενός εκφοβιστικού, ρατσιστικού, προσβλητικού ή πρόστυχου ηλεκτρονικού μηνύματος, φωτογραφίας ή βίντεο. Κάποιες φορές ο εκφοβισμός μπορεί να οδηγήσει στο να περιθωριοποιηθούν και να αποκλειστούν άτομο ή άτομα από άλλους.
- Ο **Διαδικτυακός Εκφοβισμός διαφέρει** από τα άλλα είδη εκφοβισμού αφού επεμβαίνει στον προσωπικό χώρο του παραλήπτη. Ο εκφοβισμός αυτός είναι δύσκολο να περιοριστεί, αφού δεν υπάρχει περιορισμός ούτε των μηνυμάτων που διανέμονται ηλεκτρονικά, ούτε του αριθμού των παραληπτών που μπορούν να γίνουν δέκτες αυτών των μηνυμάτων.

Τι προκαλεί ο διαδικτυακός εκφοβισμός

- Ο Διαδικτυακός Εκφοβισμός, μπορεί να προκαλέσει πολύ **σοβαρές συνέπειες στη ζωή του θύματος.**
- Η **καθημερινότητα** και η **αξιοπρέπεια** του θύματος προσβάλλονται ή/και δυσφημούνται.
- Η **αυτοεκτίμηση του πλήττεται έντονα.**
- Το άτομο αρχίζει να **αναπαράγει αρνητικές σκέψεις** και η **επίδοση των κοινωνικών του ικανοτήτων μειώνεται σημαντικά.**
- Οι συνέπειες από τις παραπάνω ενέργειες επιδρούν αρνητικά στη ζωή του προσβαλλόμενου ατόμου κι **επιφέρουν κοινωνική απομόνωση, απότομη πτώση στις επιδόσεις, κατάθλιψη, φόβο, αίσθηση ανασφάλειας ή απομόνωσης, απώλεια εμπιστοσύνης στον εαυτό** κ.α.
- Εάν η παρενόχληση είναι συνεχής, επίμονη κι έντονη **μπορεί να οδηγήσει πιθανή τάση αυτοκτονίας λόγω της αίσθησης δυστυχίας.**

Μορφές διαδικτυακού εκφοβισμού

- **Απειλές και εκφοβισμός** μέσω ηλεκτρονικών μηνυμάτων.
- **Παρενόχληση ή καταδίωξη** – η επαναλαμβανόμενη αποστολή ανεπιθύμητων μηνυμάτων
- **Εξύβριση / δυσφήμιση**. Ένα παράδειγμα αυτού του τύπου διαδικτυακού εκφοβισμού είναι όταν το άτομο δέχεται επίθεση μέσω διαδικτύου για μια συμπεριφορά που κάποιος θεώρησε μη αποδεκτή. Ο απώτερος στόχος είναι το θύμα να ταπεινωθεί δημοσίως και να έρθει σε δύσκολη θέση.
- **Κλοπή ταυτότητας / μη εξουσιοδοτημένη πρόσβαση και πλαστοπροσωπία**
- **Δημόσια ανάρτηση, αποστολή ή προώθηση προσωπικών ή ιδιωτικών πληροφοριών και εικόνων**
- **Roasting** – μια ομάδα ανθρώπων κάνει συμμορία εναντίον ενός ατόμου και δημοσιεύει προσβλητικό περιεχόμενο μέχρι το θύμα να «σπάσει».
- **Flaming** – λέγεται συχνά ότι οι θύτες ψάχνουν για μία αντίδραση ή αντιπαράθεση με το θύμα.

Αληθινά περιστατικά διαδικτυακού εκφοβισμού

Μπορούμε να αναφέρουμε την περίπτωση του Βρετανού **Ryan Halligan το 2003**, που αυτοκτόνησε όταν οι συμμαθητές του διακινούσαν μέσω του instant messaging κοροϊδευτικά σχόλια ότι είναι ομοφυλόφιλος.

Ο **15χρονος Ghyslain Raza από το Quebec**, ίσως είναι το πιο διάσημο θύμα του cyber bullying. Δημιούργησε ένα δίλεπτο φιλμ μιμούμενος μία σκηνή της ταινίας «Ο πόλεμος των άστρων» χειριζόμενος μια μπάλα του γκολφ. Κάποιοι συμμαθητές του το «ανέβασαν» στο διαδίκτυο, όπου το είδαν εκατομμύρια χρήστες, ενώ τα μέσα τον αποκάλεσαν «Star wars kid». Η ανεπιθύμητη διασημότητα που βίωσε, τον οδήγησε να νοσηλευτεί σε ψυχιατρική κλινική.

Η **Megan Meier**, η οποία αυτοκτόνησε μετά από μια σειρά προσβλητικών μηνυμάτων που δέχτηκε στο MySpace.

Αντιμετώπιση του Διαδικτυακού εκφοβισμού

- **Αγνόηση ενοχλητικών μηνυμάτων**, σε περίπτωση ωστόσο απειλών συνιστάται αναφορά των μηνυμάτων και λήψη προληπτικών μέτρων .
- **Αποκλεισμός του αποστολέα** που στέλνει απειλητικά ή ενοχλητικά μηνύματα
- **Προειδοποίηση του αποστολέα**
- **Αναφορά του περιστατικού στην Αστυνομία** είτε σε κάποια αρμόδια υπηρεσία Δίωξης Ηλεκτρονικού εγκλήματος
- **Αναγκαία η κινητοποίηση όλων των φορέων κοινωνικοποίησης:** οικογένεια, σχολείο, κοινωνία
- Πρόληψη: ενημέρωση, ευαισθητοποίηση



ΠΗΓΕΣ

- **Wikipedia**, "Διαδικτυακός εκφοβισμός",
https://el.wikipedia.org/wiki/Διαδικτυακός_εκφοβισμός#
- **Γενικό Λύκειο Τυχερού**, Πρόγραμμα Αγωγής Υγείας
<https://blogs.sch.gr/lyktycher/files/2016/06/ΔΙΑΔΙΚΥΤΑΚΟΣ-ΕΚΦΟΒΙΣΜΟΣ.pdf>
- **Weebly**, Αντιμετώπιση του Διαδικτυακού εκφοβισμού,
<https://cyberbullyinga1.weebly.com/>

ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ

◆ ΑΘΗΝΑ Μ.

ΤΙ ΕΙΝΑΙ ΔΙΑΔΙΚΤΥΑΚΟΣ Εκφοβισμός

- ◆ Ο διαδικτυακός εκφοβισμός αφορά τον εκφοβισμό, την απειλή, την ταπείνωση και την παρενόχληση κυρίως σε παιδιά και εφήβους που δέχονται μέσω της χρήσης του Διαδικτύου, κινητών τηλεφώνων είτε άλλων ψηφιακών τεχνολογιών.

Αιτίες

Συχνά οι νέοι εκτίθενται στον Διαδικτυακό εκφοβισμό εξαιτίας της βίωσης έντονων συναισθημάτων όπως θυμός, απόγνωση είτε πάλι και εκδίκηση, που μπορεί να προέρχεται τόσο από τις προβληματικές σχέσεις που υπάρχουν στο οικογενειακό περιβάλλον όσο και εξαιτίας μιας ευρύτερης κοινωνικής δυσλειτουργικότητας που παρουσιάζει το άτομο. Σε μερικές περιπτώσεις ο Διαδικτυακός εκφοβισμός αποτελεί μορφή ψυχαγωγίας[εκκρεμεί παραπομπή] στοχεύοντας στην εκδήλωση ποικίλων αντιδράσεων και στην ικανοποίηση αναγκών που σχετίζονται με την επιβολή εξουσίας και ελέγχου.[εκκρεμεί παραπομπή] Σπανιότερα, η αποστολή μηνυμάτων σε λάθος παραλήπτες μπορεί να αποτελέσει αιτία του φαινομένου.

Μορφές

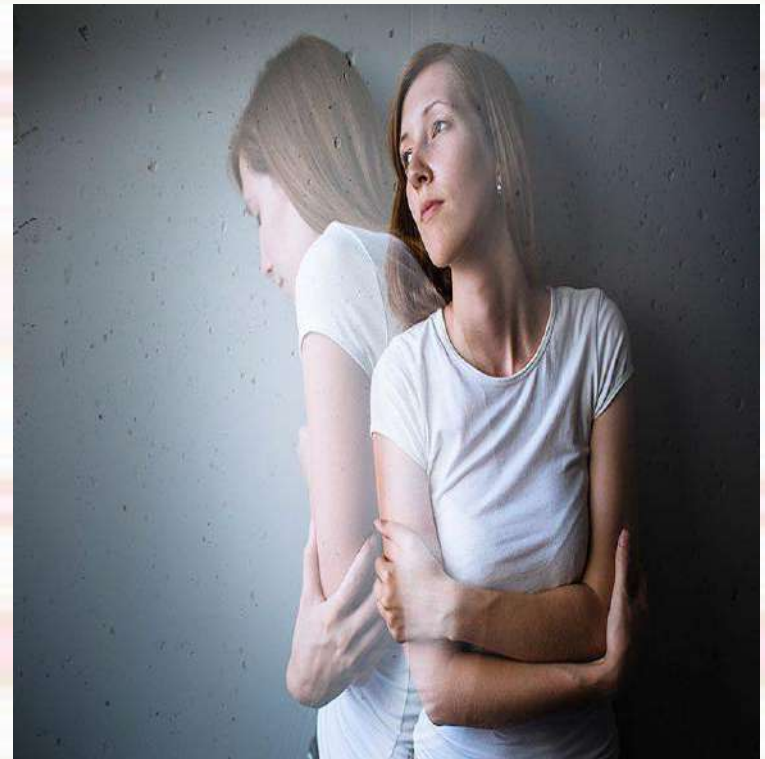
- ◆ Επαναλαμβανόμενη αποστολή ηλεκτρονικών ή τηλεφωνικών μηνυμάτων
- ◆ Παρέμβαση και παρενόχληση οποιασδήποτε διαδικτυακής δραστηριότητας του ατόμου
- ◆ Είσοδος σε προσωπικούς διαδικτυακούς λογαριασμούς του ατόμου
- ◆ Αποστολή φωτογραφιών του ατόμου ή αλλού είδους μαγνητοσκοπημένου υλικού
- ◆ Αποστολή προσωπικών πληροφοριών του ατόμου σε πολλαπλούς παραλήπτες
- ◆ Αποστολή απειλητικών μηνυμάτων σε αλλά άτομα υποκρινόμενοι το άτομο που εκφοβίζεται
- ◆ Υποκίνηση τρίτων για διαδικτυακή παρακολούθηση και παρενόχληση του ατόμου

ΣΥΝΕΠΕΙΕΣ

- ◆ Το φαινόμενο του Διαδικτυακού εκφοβισμού εγκυμονεί σοβαρές επιπτώσεις για την ψυχική υγεία του θύματος, αλλά και του θύτη. Η αυτοεκτίμηση του ατόμου που υφίσταται Διαδικτυακό εκφοβισμό πλήττεται έντονα τόσο ώστε σε μερικές περιπτώσεις συνδέεται με το αίσθημα της ενοχής. Το άτομο αρχίζει να αναπαράγει αρνητικές σκέψεις και η επίδοση των κοινωνικών του ικανοτήτων μειώνεται σημαντικά. Κάποιες φορές, κυρίως κατά την εφηβική ηλικία η αποχή από το σχολείο και από τις παρέες των συνομηλίκων αποτελεί προσωρινό καταφύγιο, ενώ ταυτόχρονα η αυτοκτονία θεωρείται ως η μοναδική λύση στο πρόβλημα. Άτομα που δέχτηκαν έντονα Διαδικτυακό εκφοβισμό ενδέχεται στο μέλλον να παρουσιάσουν μεγαλύτερη αστάθεια στις διαπροσωπικές τους σχέσεις συνοδευόμενη από την κοινωνική απομόνωση.
- ◆ Από την άλλη, οι εκφοβιστές τείνουν να είναι άτομα με έντονη αντικοινωνική συμπεριφορά, επιρρεπή στο αλκοόλ και απομονωμένα από τους συνομηλίκους. Μακροπρόθεσμα αντιλαμβάνονται ότι ο εκφοβισμός δεν αποτελεί μορφή ικανοποίησης και αναγνώρισης, βιώνοντας έτσι έντονη προσωπική απογοήτευση.

Τρόποι Αντιμετώπισης

Τα θύματα που δέχονται «ηλεκτρονικό εκφοβισμό» πρέπει να προβούν άμεσα σε μια σειρά από κινήσεις. Να απαιτήσουν από τον δράστη να σταματήσει να τους παρενοχλεί. Να αγνοήσουν τις επιθέσεις και να μπλοκάρουν κάθε επικοινωνία μαζί του. Να ζητήσουν βοήθεια είτε από τους γονείς, είτε από την δίωξη ηλεκτρονικού εγκλήματος, είτε από ειδικούς που το αντικείμενο τους είναι το cyberbullying ή η προστασία των παιδιών. Από τη μεριά τους οι γονείς, μόλις αντιληφθούν το παιδί τους έχει πέσει θύμα ιντερνετικού εκφοβισμού, θα πρέπει να το προσεγγίσουν, μιλώντας μαζί του, και ζητώντας βοήθεια ειδικού.



Αθηνά Μ.

- ◆ Digital id
- ◆ iekdelta_ligo
- ◆ ΒΙΚΙΠΑΙΔΕΙΑ

Cost Analysis

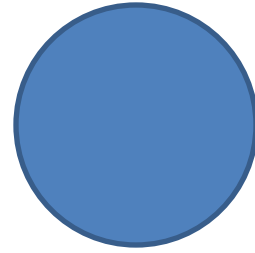
- ◆ Indicate the financial advantages for the customer
- ◆ Compare quality and price with those of the competition

Strengths and Advantages

- ◆ Summarize the special features and advantages of the product being introduced

Next Steps of Action

- ◆ Explain the steps that now need to be taken



Διαδικτυακός Εκφοβισμός

Αντριάνα Σ.



Μορφές Διαδικτυακού εκφοβισμού

- . Επαναλαμβανόμενη αποστολή ηλεκτρονικών ή τηλεφωνικών μηνυμάτων
- Παρέμβαση και παρενόχληση οποιασδήποτε διαδικτυακής δραστηριότητας του ατόμου
- Είσοδος σε προσωπικούς διαδικτυακούς λογαριασμούς του ατόμου
- Αποστολή φωτογραφιών του ατόμου ή άλλου είδους μαγνητοσκοπημένου υλικού
- Αποστολή προσωπικών πληροφοριών του ατόμου σε πολλαπλούς παραλήπτες
- Αποστολή απειλητικών μηνυμάτων σε άλλα άτομα υποκρινόμενοι το άτομο που εκφοβίζεται
- Υποκίνηση τρίτων για διαδικτυακή παρακολούθηση και παρενόχληση του ατόμου

Αντιμετώπιση του Διαδικτυακού εκφοβισμού

- Αγνόηση ενοχλητικών μηνυμάτων, σε περίπτωση ωστόσο απειλών συνιστάται αναφορά των μηνυμάτων και λήψη προληπτικών μέτρων .
- Αποκλεισμός του αποστολέα που στέλνει απειλητικά ή ενοχλητικά μηνύματα
- Προειδοποίηση του αποστολέα
- Αναφορά του περιστατικού στην [Αστυνομία](#) είτε σε κάποια αρμόδια υπηρεσία Δίωξης Ηλεκτρονικού εγκλήματος
- Αναφορά της περίπτωσης στον γονέα ή τον κηδεμόνα του ατόμου.
- Στατιστικά στοιχεία

Στατιστικά στοιχεία

- Περίπου 15-35% των νέων έχει πέσει θύμα Διαδικτυακού εκφοβισμού
- 10-20% των νέων παραδέχεται την ανάμειξή του σε Διαδικτυακό εκφοβισμό
- Τα κορίτσια ενδέχεται να εμπλακούν συχνότερα από ότι τα αγόρια σε περιστατικά Διαδικτυακού εκφοβισμού
- Η πλειοψηφία των ατόμων που υφίστανται είτε ασκεί Διαδικτυακό εκφοβισμό είναι ηλικίας 12-16 ετών.

ΣΥΝΕΠΕΙΕΣ

- Το φαινόμενο του Διαδικτυακού εκφοβισμού εγκυμονεί σοβαρές επιπτώσεις για την ψυχική υγεία του θύματος, αλλά και του θύτη. Η αυτοεκτίμηση του ατόμου που υφίσταται Διαδικτυακό εκφοβισμό πλήττεται έντονα τόσο ώστε σε μερικές περιπτώσεις συνδέεται με το αίσθημα της ενοχής. Το άτομο αρχίζει να αναπαράγει αρνητικές σκέψεις και η επίδοση των κοινωνικών του ικανοτήτων μειώνεται σημαντικά. Κάποιες φορές, κυρίως κατά την εφηβική ηλικία η αποχή από το σχολείο και από τις παρέες των συνομηλίκων αποτελεί προσωρινό καταφύγιο, ενώ ταυτόχρονα η [αυτοκτονία](#) θεωρείται ως η μοναδική λύση στο πρόβλημα. Άτομα που δέχτηκαν έντονα Διαδικτυακό εκφοβισμό ενδέχεται στο μέλλον να παρουσιάσουν μεγαλύτερη αστάθεια στις διαπροσωπικές τους σχέσεις συνοδευόμενη από την κοινωνική απομόνωση. Από την άλλη, οι εκφοβιστές τείνουν να είναι άτομα με έντονη αντικοινωνική συμπεριφορά, επιρρεπή στο αλκοόλ και απομονωμένα από τους συνομηλίκους. Μακροπρόθεσμα αντιλαμβάνονται ότι ο εκφοβισμός δεν αποτελεί μορφή ικανοποίησης και αναγνώρισης, βιώνοντας έτσι έντονη προσωπική απογοήτευση.

Πηγές

- https://web.archive.org/web/20111013221951/http://mblog.lib.umich.edu/cyberbullying/archives/2007/03/what_are_the_so.html
- <http://www.cyberbully.org/cyberbully/docs/cbcteducator.pdf> Αρχείοθηκε 2010-10-10 στο [Wayback Machine](http://www.waybackmachine.org/).
- http://www.stopcyberbullying.org/why_do_kids_cyberbully_each_other.html
- http://www.stopcyberbullying.org/what_is_cyberbullying_exactly.html
- <http://www.stopcyberbullying.org/parents/guide.html>
- http://www.stopcyberbullying.org/lawenforcement/telling_the_difference.html
- https://web.archive.org/web/20150325054625/http://www.pi.ac.cy/InternetSafety/sec_kindinoi_ekfobismos.html

Εθισμός στο Διαδίκτυο

Γιώργος Π.



Εισαγωγή



- Ο εθισμός στο **διαδίκτυο** μια σχετικά νέα μορφή εξάρτησης, και έγινε δημοφιλής με την καινοτόμο έρευνα της Young (1996), αναφέρεται στην «καταναγκαστική, υπερβολική χρήση του διαδικτύου και τον εκνευρισμό ή δυσθυμική συμπεριφορά που παρουσιάζεται κατά τη στέρησή της» Ο εθισμός στο **Διαδίκτυο**, αν και δεν έχει επισήμως αναγνωρισθεί ως κλινική οντότητα παρά μόνο στην Κίνα, Ν.Κορέα και Ταϊβάν, αποτελεί μια κατάσταση που προκαλεί σημαντική έκπτωση στην κοινωνική και επαγγελματική ή ακαδημαϊκή λειτουργικότητα του ατόμου.



Τι είναι ο εθισμός στο διαδίκτυο

- Το Διαδίκτυο έχει την ικανότητα να καλύψει συγκεκριμένες ψυχολογικές ανάγκες ενός ατόμου. Ένα από τα χαρακτηριστικά του μέσου που προκύπτει από τη φύση του είναι ότι μπορεί να δημιουργήσει μια «ιδανική κατάσταση εαυτού», όπου το άτομο μπορεί να εξερευνησει διάφορες πτυχές της προσωπικότητάς του χωρίς να έχει περιορισμούς και συνέπειες. Στο Διαδίκτυο δεν υπάρχουν άμεσες συνέπειες των πράξεων, ο χρήστης μπορεί να μπει και να βγει όποτε θέλει, ενώ μπορεί να καλύψει την όποια εξωτερική εμφάνιση, αφού δεν υπάρχει οπτική επαφή. Ταυτόχρονα, ο έφηβος μπορεί να ενσαρκώσει διαφορετικούς ρόλους ή να υιοθετήσει διαφορετικές ταυτότητες ανάλογα με την εκάστοτε διαδικτυακή εμπειρία, εξαιτίας της ανωνυμίας, που συνιστά κατεξοχήν χαρακτηριστικό του Διαδικτύου. Συνήθως, τα παιδιά που αντιμετωπίζουν το πρόβλημα του εθισμού στο διαδίκτυο είναι αγόρια και μεγαλώνουν σε δύσκολες καταστάσεις (δυσλειτουργικές οικογένειες). Πρόσφατες έρευνες στην Ελλάδα κατέδειξαν τη σημασία της γονικής μέριμνας και φροντίδας στην ανάπτυξη του εθισμού στο Διαδίκτυο. Η βέλτιστη παροχή γονικής μέριμνας χαρακτηρίζεται από φροντίδα και υγιή προστατευτικότητα, ούτως ώστε το παιδί να κατευθύνεται και να καθοδηγείται με επάρκεια σε ένα ασφαλές περιβάλλον, χωρίς να παρεμποδίζονται οι προσπάθειές του για την ανάδειξη προσωπικής ταυτότητας και αυτονομίας. Αντίθετα, υπερπροστατευτικότητα των γονέων και χαμηλά επίπεδα φροντίδας συνιστούν το πρότυπο μέριμνας 'affectionless control' (έλεγχος χωρίς στοργή), το οποίο συνδέθηκε με υψηλότερες βαθμολογίες εθισμού στο Διαδίκτυο.



Τα είδη του εθισμού στο διαδίκτυο

- Ο εθισμός των εφήβων στο διαδίκτυο μπορεί, επίσης να είναι το αποτέλεσμα άλλων ψυχικών διαταραχών, όπως κατάθλιψη, αγχώδεις διαταραχές, διαταραχές προσωπικότητας, υπερκινητικότητα και κοινωνική φοβία. Συχνά όμως η ανάπτυξη καταθλιπτικού συναισθήματος ή άγχους έπεται της εμφάνισης του εθισμού, όπως συμβαίνει και με άλλες εθιστικές συμπεριφορές. Αυτό καταδεικνύει την αναγκαιότητα εκτίμησης κάθε περίπτωσης από ειδικό ψυχικής υγείας, ο οποίος θα είναι σε θέση να κρίνει την ύπαρξη ή μη συννοσηρών καταστάσεων.
- Η διαταραχή εθισμού στο διαδίκτυο δεν συμπεριλαμβάνεται στο τελευταίο εγχειρίδιο DSM το οποίο χρησιμοποιείται τακτικά από ψυχιάτρους. Ο προβληματικός τζόγος είναι η μόνη (μη σχετιζόμενη με ουσίες) διαταραχή η οποία συμπεριλαμβάνεται στο DSM. Ωστόσο, η διαταραχή διαδικτυακών παιγνίων καταγράφεται σε ένα παράρτημα του εν λόγω εγχειριδίου, ως μια διαταραχή η οποία χρήζει περαιτέρω μελέτης.
- Ο Τζέραλντ Τζ. Μπλοκ έχει επιχειρηματολογήσει ότι ο εθισμός στο διαδίκτυο θα πρέπει να συμπεριληφθεί ως διαταραχή. Ωστόσο, ο Μπλοκ παρατήρησε ότι η διάγνωση είναι περίπλοκη επειδή 86% των μελετούμενων υποκειμένων εμφανίζουν συμπτώματα τα οποία παρουσιάζονται και σε άλλες διαγνώσιμες διαταραχές ψυχικής υγείας.



Γνωστοί τρόποι εθισμού

- Ο συμπεριφορικός εθισμός συχνά συγχέεται με τον υψηλό βαθμό εμπλοκής με τη συγκεκριμένη δραστηριότητα. Ο υψηλός βαθμός εμπλοκής δεν διακρίνεται από μικρότερο βαθμό ενασχόλησης με όρους χρονικής διάρκειας, όμως διαφέρει από τον εθισμό στο ότι οι αρνητικές συνέπειες είναι απύσες. Αναταραχή του ατόμου να επαναλάβει τη συμπεριφορά, ώστε να απαλύνει δυσφορία που νιώθει όταν τη διακόπτει. Αντίθετα το άτομο με υψηλό βαθμό εμπλοκής προβαίνει στη δραστηριότητα, επειδή τη βρίσκει ευχάριστη. Ο υψηλός βαθμός εμπλοκής στη χρήση Διαδικτύου μπορεί να είναι μια θετική συμπεριφορά, ειδικά καθώς η χρήση του προάγεται κοινωνικά και είναι απαραίτητη ώστε να ολοκληρωθεί η διαδικασία μάθησης επαγγελματικών δεξιοτήτων.



Γνωστοί τρόποι αντιμετώπισης

Για την αντιμετώπιση του φαινομένου έχει προταθεί η κινητοποιητική συνέντευξη, το γνωστικό- συμπεριφορικό μοντέλο θεραπείας, η συμβουλευτική παρέμβαση στην οικογένεια, οι ομάδες απεξάρτησης, ενώ υπάρχουν κάποια δεδομένα και για το ρόλο της φαρμακοθεραπείας στη θεραπεία. Ιδιαίτερα σημαντική για την αντιμετώπιση του εθισμού στα παιδιά και στους εφήβους είναι η ύπαρξη κοινής στάσης των γονέων, η παροχή υποστήριξης αλλά όχι κάλυψης και η τοποθέτηση του υπολογιστή σε ένα ορατό σημείο στο σπίτι και όχι στο δωμάτιο του παιδιού. Σημαντικό ρόλο στην αντιμετώπιση του εθισμού στο Διαδίκτυο έχει και η συμβουλευτική στην οικογένεια, έτσι ώστε να δημιουργηθεί ένα υποστηρικτικό πλαίσιο, που θα δράσει ευεργετικά στη θεραπεία. Η κινητοποιητική συνέντευξη μπορεί να είναι ιδιαίτερα αποτελεσματική στον χειρισμό της άρνησης του προβλήματος, ένα συχνό εμπόδιο που παρατηρείται σε όλες τις ηλικίες. Στα πλαίσια της γνωστικο- συμπεριφορικής θεραπείας,, προωθείται η γνωσιακή αναδόμηση και ένας πιο ισορροπημένος και προσαρμοστικός τρόπος σκέψης. Παράλληλα χρησιμοποιούνται μια σειρά από συμπεριφορικές στρατηγικές, όπως η αναγνώριση του πρότυπου χρήσης του Διαδικτύου και η εφαρμογή ενός διαμετρικά αντίθετου προγράμματος χρήσης, η οριοθέτηση των περιόδων χρήσης με διάφορα εξωτερικά μέσα, παρακίνηση για ενασχόληση με ευχάριστες εναλλακτικές δραστηριότητες, η χρήση καρτών υπενθύμισης, η πλήρης αποχή από ιδιαίτερα προβληματικές διαδικτυακές εφαρμογές, η ενσωμάτωση καθορισμένων διαστημάτων χρήσης στο εβδομαδιαίο πρόγραμμα του χρήστη. Οι ομάδες απεξάρτησης χρησιμοποιούν τις πρακτικές των ομάδων απεξάρτησης από άλλους εθισμούς, όπως το πρόγραμμα των 12 βημάτων ή βασίζονται στις αρχές της ομαδικής ψυχοθεραπείας.

ΠΗΓΕΣ

- Test Young. Ένα απλό τεστ που βοηθά στη διάγνωση του εθισμού στο διαδίκτυο
- Ασφάλεια στο Διαδίκτυο
- Για ένα ασφαλέςτερο διαδίκτυο
- Ελληνική Εταιρεία Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο
- Μονάδα απεξάρτησης 18 Άνω - Τμήμα Παθολογικής Χρήσης Διαδικτύου
- Συμβουλευτική υπηρεσία φοιτητών προς αντιμετώπιση της παθολογικής χρήσης Η/Υ και Διαδικτύου
- Wikipedia

- ΕΥΧΑΡΙΣΤΟΥΜΕ ΓΙΑ ΤΗΝ ΠΑΡΑΚΟΛΟΥΘΗΣΗ

ΕΘΙΣΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΝΑΣΤΑΣΙΑ Β.

Ο εθισμός στο Διαδίκτυο, αν και δεν έχει επισήμως αναγνωρισθεί ως κλινική οντότητα παρά μόνο στην Κίνα, Ν.Κορέα και Ταϊβάν, αποτελεί μια κατάσταση που προκαλεί σημαντική έκπτωση στην κοινωνική και επαγγελματική ή ακαδημαϊκή λειτουργικότητα του ατόμου.



ΑΙΤΙΑ

- Το Διαδίκτυο έχει την ικανότητα να καλύψει συγκεκριμένες ψυχολογικές ανάγκες ενός ατόμου. Ένα από τα χαρακτηριστικά του μέσου που προκύπτει από τη φύση του είναι ότι μπορεί να δημιουργήσει μια «ιδανική κατάσταση εαυτού», όπου το άτομο μπορεί να εξερευνήσει διάφορες πτυχές της προσωπικότητάς του χωρίς να έχει περιορισμούς και συνέπειες. Στο Διαδίκτυο δεν υπάρχουν άμεσες συνέπειες των πράξεων, ο χρήστης μπορεί να μπει και να βγει όποτε θέλει, ενώ μπορεί να καλύψει την όποια εξωτερική εμφάνιση, αφού δεν υπάρχει οπτική επαφή. Ταυτόχρονα, ο έφηβος μπορεί να ενσαρκώσει διαφορετικούς ρόλους ή να υιοθετήσει διαφορετικές ταυτότητες ανάλογα με την εκάστοτε διαδικτυακή εμπειρία, εξαιτίας της ανωνυμίας, που συνιστά κατεξοχήν χαρακτηριστικό του Διαδικτύου.

Ο εθισμός των εφήβων στο διαδίκτυο μπορεί, επίσης να είναι το αποτέλεσμα άλλων ψυχικών διαταραχών, όπως [κατάθλιψη](#), [αγχώδεις διαταραχές](#), [διαταραχές προσωπικότητας](#), [υπερκινητικότητα](#) και [κοινωνική φοβία](#). Συχνά όμως η ανάπτυξη καταθλιπτικού συναισθήματος ή άγχους έπεται της εμφάνισης του εθισμού, όπως συμβαίνει και με άλλες εθιστικές συμπεριφορές. Αυτό καταδεικνύει την αναγκαιότητα εκτίμησης κάθε περίπτωσης από ειδικό ψυχικής υγείας, ο οποίος θα είναι σε θέση να κρίνει την ύπαρξη ή μη συννοσηρών καταστάσεων.

ΣΥΜΠΤΩΜΑΤΑ

Συμπτώματα συνδρόμου απόσυρσης, όπως ψυχοκινητική διέγερση, εκούσια ή ακούσια κίνηση δακτυλογράφησης των δακτύλων του χεριού, άγχος, έμμονη σκέψη για το διαδίκτυο και όνειρα για το διαδίκτυο.

Κατανάλωση υπερβολικού χρόνου ή και χρήματος σε δραστηριότητες σχετικές με το διαδίκτυο (λογισμικά, σκληροί δίσκοι κ.λ.π)

Έκπτωση λειτουργικότητας του ατόμου σε κοινωνικό, οικογενειακό αλλά και προσωπικό επίπεδο.

Μειωμένη επίδοση στο σχολείο λόγω των πολλών ωρών που περνάει ο έφηβος στο διαδίκτυο.

Σε προχωρημένες περιπτώσεις ο έφηβος δεν κοιμάται, παραμελεί την προσωπική του υγιεινή, μπορεί να σταματήσει ακόμα και το σχολείο. Ακόμη, απομονώνεται από την οικογένεια και τους φίλους του, γίνεται επιθετικός, μπορεί να κλέβει χρήματα από τους γονείς για να παίζει. Τέλος, φτάνει σε σημείο να μην τρώει ή και το αντίθετο.

ΗΛΙΚΙΕΣ ΠΟΥ ΕΜΦΑΝΙΖΟΥΝ ΣΥΧΝΟΤΕΡΑ ΕΞΑΡΤΗΣΗ

Το φαινόμενο συνήθως εμφανίζεται αρχικά σε εφήβους κατά την πρώιμη εφηβεία (10-14 ετών) ή και σε μικρότερη ακόμη ηλικία. Είναι πιο έντονο κατά την μέση εφηβεία (15-17 ετών), κατά την οποία οι έφηβοι πειραματίζονται και σταδιακά αυτονομούνται, καθώς και κατά την όψιμη εφηβεία (> 17 ετών). Ένας ακόμα πληθυσμός υψηλού κινδύνου είναι αυτός των φοιτητών, οι οποίοι καλούνται πολλές φορές για πρώτη φορά να οριοθετήσουν οι ίδιοι τη χρήση Διαδικτύου στην οποία προβαίνουν μακριά από οικογενειακό έλεγχο, αλλά και χωρίς το ξεκάθαρα δομημένο πλαίσιο υποχρεώσεων του σχολείου μέσης εκπαίδευσης. Σποραδικά εμφανίζεται το πρόβλημα και σε μεγαλύτερες ηλικίες, όπου κυρίως αφορά περιπτώσεις υπέρμετρης ενασχόλησης με κοινωνική δικτύωση, αλλά και διαδικτυακό τζόγο, όπως και διαδικτυακή πορνογραφία.

Θέλεις να βγείς έξω
να παίξεις που έχει
υπέροχη μέρα;



ΡΟΛΟΣ ΓΟΝΕΩΝ

Ο ρόλος των γονέων είναι ιδιαίτερα σημαντικός τόσο για την πρόληψη, όσο και για την αντιμετώπιση του εθισμού των παιδιών τους από το Διαδίκτυο. Όσον αφορά την πρόληψη, το σημαντικότερο πράγμα που χρειάζεται να κάνουν οι γονείς προκειμένου να μπορούν να ελέγχουν αποτελεσματικά τη χρήση του Διαδικτύου από τα παιδιά τους, είναι να γνωρίσουν οι ίδιοι το μέσο. Προς το παρόν, οι γονείς δε γνωρίζουν το μέσο και επιπλέον δε φαίνονται διατεθειμένοι να έλθουν σε επαφή με το Διαδίκτυο, ενώ ταυτόχρονα δεν ενδιαφέρονται για τις δραστηριότητες των παιδιών τους στο Ίντερνετ. Ταυτόχρονα, οι γονείς θα πρέπει κάποιες φορές να χρησιμοποιούν το Διαδίκτυο μαζί με το παιδί, ώστε να του δίνουν τις απαραίτητες κατευθύνσεις, ενώ η εγκατάσταση κάποιων φίλτρων στον υπολογιστή μπορεί να αποτρέψει την εμφάνιση ακατάλληλων για το παιδί ιστοσελίδων. Επιπλέον, είναι απαραίτητο να έχουν τεθεί κάποιες βάσεις όταν το παιδί φτάνει στην [εφηβεία](#), να υπάρχουν δηλαδή όρια. Για να υπάρξουν ωστόσο όρια θα πρέπει οι γονείς να μπορούν να διαθέσουν τον απαραίτητο χρόνο, αφού είναι δύσκολο για ενοχικούς γονείς να θέσουν όρια. Σε πιο πρακτικό επίπεδο, ο υπολογιστής είναι καλό να βρίσκεται σε κοινόχρηστο χώρο και όχι στο δωμάτιο του παιδιού, ώστε να ελέγχεται διακριτικά η δραστηριότητα του παιδιού στο Διαδίκτυο. Ενώ, τέλος, οι γονείς θα πρέπει να συζητούν για τις διαδικτυακές διαδρομές του παιδιού τους, ώστε να έχουν πάντοτε ενημέρωση για τις ιστοσελίδες που επισκέπτεται, τα άτομα με τα οποία συνομιλεί και τις πληροφορίες που ανταλλάσσει με άλλα άτομα.

ΑΝΤΙΜΕΤΩΣΗ

- . Ιδιαίτερα σημαντική για την αντιμετώπιση του εθισμού στα παιδιά και στους εφήβους είναι η ύπαρξη κοινής στάσης των γονέων, η παροχή υποστήριξης αλλά όχι κάλυψης και η τοποθέτηση του υπολογιστή σε ένα ορατό σημείο στο σπίτι και όχι στο δωμάτιο του παιδιού. Σημαντικό ρόλο στην αντιμετώπιση του εθισμού στο Διαδίκτυο έχει και η συμβουλευτική στην οικογένεια, έτσι ώστε να δημιουργηθεί ένα υποστηρικτικό πλαίσιο, που θα δράσει ευεργετικά στη θεραπεία. Η κινητοποιητική συνέντευξη μπορεί να είναι ιδιαίτερα αποτελεσματική στον χειρισμό της άρνησης του προβλήματος, ένα συχνό εμπόδιο που παρατηρείται σε όλες τις ηλικίες. Στα πλαίσια της γνωστικο- συμπεριφορικής θεραπείας, εντοπίζονται οι γνωστικές διαστρεβλώσεις που εκλύουν και διατηρούν την προβληματική χρήση του Διαδικτύου, προωθείται η γνωσιακή αναδόμηση και ένας πιο ισορροπημένος και προσαρμοστικός τρόπος σκέψης. Παράλληλα χρησιμοποιούνται μια σειρά από συμπεριφορικές στρατηγικές, όπως η αναγνώριση του πρότυπου χρήσης του Διαδικτύου και η εφαρμογή ενός διαμετρικά αντίθετου προγράμματος χρήσης, η οριοθέτηση των περιόδων χρήσης με διάφορα εξωτερικά μέσα, παρακίνηση για ενασχόληση με ευχάριστες εναλλακτικές δραστηριότητες, η χρήση καρτών υπενθύμισης, η πλήρης αποχή από ιδιαίτερα προβληματικές διαδικτυακές εφαρμογές, η ενσωμάτωση καθορισμένων διαστημάτων χρήσης στο εβδομαδιαίο πρόγραμμα του χρήστη. Οι ομάδες απεξάρτησης χρησιμοποιούν τις πρακτικές των ομάδων απεξάρτησης από άλλους εθισμούς, όπως το πρόγραμμα των 12 βημάτων ή βασίζονται στις αρχές της ομαδικής ψυχοθεραπείας. Σε ό,τι αφορά τη φαρμακοθεραπεία, η χρήση της εσιταλοπράμης φάνηκε αποτελεσματική σε μικρή ανοικτή μελέτη, έχει προταθεί η ναλτρεξόνη λόγω του μηχανισμού δράσης της στα κέντρα ανταμοιβής του εγκεφάλου, ενώ η μεθυλφενιδάτη αποδείχθηκε αποτελεσματική σε μια ανοικτή μελέτη σε παιδιά με Διαταραχή Ελλειμματικής Προσοχής-Υπερκινητικότητα (ΔΕΠΥ) και εθισμό σε διαδικτυακά παιχνίδια. Σε κάθε περίπτωση, ο εθισμός στο Διαδίκτυο, ως ψυχική διαταραχή, χρήζει αντιμετώπισης από επαγγελματίες ψυχικής υγείας εξειδικευμένους στο συγκεκριμένο αντικείμενο.

ΑΝΑΣΤΑΣΙΑ Β. ΕΘΙΣΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΠΗΓΕΣ

[Εθισμός στο Διαδίκτυο - Βικιπαίδεια
\(wikipedia.org\)](#)

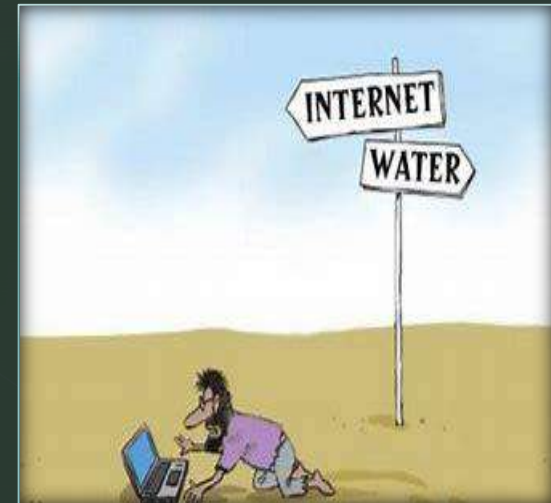


Εθισμός του διαδικτύου.

Τζωρτζίνα Μ.

Παρουσίαση του κινδύνου

Ο Εθισμός στο διαδίκτυο είναι μια σχετικά νέα μορφή εξάρτησης. Είναι μάλιστα γεγονός ότι το ηλικιακό όριο των παιδιών που κάνουν κατάχρηση της ενασχόλησής τους με το διαδίκτυο μικραίνει όλο και περισσότερο. Η πιο συχνή μορφή εξάρτησης από το διαδίκτυο για τα παιδιά, τους εφήβους και τους νεαρούς ενήλικες είναι ο εθισμός στα video games. Αρκετά συχνή είναι και η ενασχόληση των νέων, εφήβων και νεαρών ενηλίκων με τα social media. Το Διαδίκτυο έχει την ικανότητα να καλύψει συγκεκριμένες ψυχολογικές ανάγκες ενός ατόμου. Στο Διαδίκτυο δεν υπάρχουν άμεσες συνέπειες των πράξεων, ο χρήστης μπορεί να μπει και να βγει όποτε θέλει, ενώ μπορεί να καλύψει την όποια εξωτερική εμφάνιση, αφού δεν υπάρχει οπτική επαφή. Ταυτόχρονα, ο έφηβος μπορεί να ενσαρκώσει διαφορετικούς ρόλους ή να υιοθετήσει διαφορετικές ταυτότητες ανάλογα με την εκάστοτε διαδικτυακή εμπειρία, εξαιτίας της ανωνυμίας, που συνιστά κατεξοχήν χαρακτηριστικό του Διαδικτύου. Η βέλτιστη παροχή γονικής μέριμνας χαρακτηρίζεται από φροντίδα και υγιή προστατευτικότητα, ούτως ώστε το παιδί να κατευθύνεται και να καθοδηγείται με επάρκεια σε ένα ασφαλές περιβάλλον, χωρίς να εμποδίζονται οι προσπάθειές του για την ανάδειξη προσωπικής ταυτότητας και αυτονόμησης.



Τρόποι αντιμετώπισης του εθισμού

- Συνήθως η θεραπευτική προσέγγιση περιλαμβάνει διαγνωστική συνέντευξη, οικογενειακή θεραπεία, συμβουλευτική υποστήριξη και ατομική ή και ομαδική ψυχοθεραπεία και σε κάποιες περιπτώσεις όπου κρίνεται απαραίτητο μπορεί να χορηγηθεί και φαρμακευτική αγωγή (συνήθως αντικαταθλιπτική). Η κάθε περίπτωση είναι διαφορετική και μοναδική και ως τέτοια πρέπει να αντιμετωπίζεται. Σε πολλές περιπτώσεις μπορεί να αποτελεί μια καταθλιπτική καταφυγή. Δηλαδή, εμφανίζεται σε ένα καταθλιπτικό άτομο, το οποίο στρέφεται προς το gaming χρησιμοποιώντας το ως αποκούμπι για να αντλήσει ικανοποίηση και χαρά. Αυτό μπορεί να συμβαίνει είτε στα παιδιά είτε στους ενήλικες. Στα παιδιά η κατάθλιψη μπορεί να εκδηλώνεται ως έντονη και διαρκής γκρίνια ή ακόμη και όταν βαριούνται συνεχώς. Μέσα από το gaming ένα παιδί βρίσκει την απόλαυση που του λείπει και το βοηθά να νιώσει ευχαρίστηση.

ΠΑΡΑΒΙΑΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Θάνος Μ.



ΕΙΣΑΓΩΓΗ

Είναι πολύ σημαντικό να προστατεύουμε τα προσωπικά μας δεδομένα. Όμως, υπάρχουν κάποιοι άνθρωποι που μπορεί να προσπαθήσουν να πάρουν αυτά τα δεδομένα χωρίς την άδειά μας. Αυτό μπορεί να συμβαίνει και στο διαδίκτυο, όταν παίζουμε παιχνίδια ή ψάχνουμε πράγματα στον υπολογιστή. Είναι σημαντικό να μάθουμε πώς να προστατευόμαστε, ώστε να μπορούμε να είμαστε ασφαλείς στο διαδίκτυο.

Ποια είναι τα προσωπικά δεδομένα

Προσωπικά δεδομένα είναι κάθε πληροφορία που χαρακτηρίζει κάποιο άτομο, όπως για παράδειγμα το όνομά του, η διεύθυνσή του, το τηλέφωνό του, ο αριθμός ταυτότητας και διαβατηρίου του, η διεύθυνση του ηλεκτρονικού του ταχυδρομείου, τα ενδιαφέροντά του, οι φωτογραφίες του, οι απόψεις του, το θρήσκευμά του, οι πολιτικές του πεποιθήσεις και άλλα σημαντικά στοιχεία της ιδιωτικής του ζωής.

Παιδιά
βοηθήστε με να
ξεχωρίσω ποιές από
αυτές τις πληροφορίες
είναι προσωπικά μου
δεδομένα!



Οι φωτογραφίες μου

Το όνομά μου

Το τηλέφωνό μου

Τι καιρό κάνει
σήμερα;

Το όνομα του
σκύλου μου

Προσωπικά
Δεδομένα

Το βιβλίο
που διαβάζω

Η διεύθυνση μου

Ο παιδότοπος
που συχνάζω

Το πολίτευμα
της Ελλάδας

Το σχολείο που πηγαίνω

Τι προκαλεί η παραβίαση προσωπικών δεδομένων;

Με την παραβίαση προσωπικών δεδομένων αποκαλύπτονται και διαρρέουν ιδιωτικές ή εμπιστευτικές πληροφορίες και δεδομένα σε μη αξιόπιστο περιβάλλον.



Παραδείγματα παραβίασης προσωπικών δεδομένων

- **Κλοπή Ταυτότητας:** Κάποιοι μπορούν να χρησιμοποιήσουν τις προσωπικές πληροφορίες για να πραγματοποιήσουν απάτες και να ανοίξουν λογαριασμό στο όνομα του θύματος.
- **Διακίνηση Δεδομένων:** Οι προσωπικές πληροφορίες μπορούν να πωλούνται ή να διακινούνται σε άλλες εταιρείες χωρίς την άδεια ενός ατόμου.
- **Δυσφήμιση:** Κακόβουλοι μπορούν να χρησιμοποιήσουν τις προσωπικές πληροφορίες για να προκαλέσουν πρόβλημα όπως δυσφήμιση ή απειλές.
- **Οικονομική Ζημία:** Η παραβίαση μπορεί να οδηγήσει σε οικονομική ζημία για το θύμα, ειδικά εάν υπάρξουν απώλειες χρημάτων λόγω απάτης ή κλοπής ταυτότητας.

Γνωστή υπόθεση παραβίασης προσωπικών δεδομένων

Τον Σεπτέμβριο 2016, ο τότε γίγαντας στην παροχή διαδικτυακών υπηρεσιών **Yahoo** αποκάλυψε ότι το **2014** υπέστη την μεγαλύτερη παραβίαση δεδομένων χρηστών στην ιστορία, πιθανώς από χάκερ που είχε κυβερνητική στήριξη.

Στην πρώτη της δήλωση, η εταιρεία ανακοίνωσε ότι η διαδικτυακή αυτή επίθεση επηρέασε **500 εκατομμύρια χρήστες** και πως κατά την διάρκειά της εκτέθηκαν ονόματα, email, ημερομηνίες γέννησης και τηλέφωνα.

Παρόλα αυτά, έσπευσε να καθησυχάσει τους χρήστες ότι η πλειονότητα των κωδικών είχαν προστατευτεί μέσω της χρήσης αλγόριθμου.

Τρεις μήνες αργότερα, η **Yahoo!** εξέδωσε νέα ανακοίνωση και παραδέχτηκε ότι το 2013 μια άλλη ομάδα χάκερ εξασφάλισε πρόσβαση στα δεδομένα 1 δισ. χρηστών, τα οποία περιλάμβαναν όχι μόνο ονόματα, email, ημερομηνίες γέννησης και κωδικούς πρόσβασης αλλά και ερωτήσεις ασφαλείας των χρηστών με τις αντίστοιχες απαντήσεις.

Τον Οκτώβριο του 2017, η **ίδια εταιρεία παραδέχτηκε ότι στην πραγματικότητα** κατά την κυβερνοεπίθεση αυτή διέρρευσαν τα δεδομένα 3 δισ. χρηστών της πλατφόρμας.

Τρόποι προστασίας προσωπικών δεδομένων

- Μην κοινοποιείτε τα προσωπικά σας δεδομένα όπως την ημερομηνία γέννησης, τη διεύθυνση και τον τραπεζικό λογαριασμό σας
- Εντοπίστε τις ενδεχόμενες από
- Χρησιμοποιείτε όνομα χρήστη κωδικούς και ασφαλίστε τον υπολογιστή σας
- Κλειδώνετε τις φορητές σας συ
- Προσοχή στα δημόσια δίκτυα Wi-Fi
- Διατηρείτε ενημερωμένα τα λειτουργικά σας συστήματα



ΠΗΓΕΣ

- <https://el.wikipedia.org>
- www.dpa.gr
- <http://europa.eu>
- <https://saferinternet4kids.gr>
- www.newsbeast.gr

ΠΑΡΑΒΙΑΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Μυρτώ Γ.

ΕΙΣΑΓΩΓΗ

- Η παραβίαση των προσωπικών δεδομένων είναι κάτι που μπορεί να συμβεί στον καθένα. Όμως, υπάρχουν τρόποι αντιμετώπισης.

ΤΙ ΕΙΝΑΙ Η ΠΑΡΑΒΙΑΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

- Παραβίαση δεδομένων είναι η σκόπιμη ή ακούσια διαρροή ασφαλών ή ιδιωτικών / εμπιστευτικών πληροφοριών σε μη αξιόπιστο περιβάλλον.

ΤΙ ΠΡΟΚΑΛΕΙ Η ΠΑΡΑΒΙΑΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

- Η ανεξέλεγκτη καταχώριση και επεξεργασία των προσωπικών δεδομένων σε ηλεκτρονικά και χειρόγραφα αρχεία υπηρεσιών, εταιρειών και οργανισμών μπορεί να δημιουργήσει προβλήματα στην ιδιωτική ζωή του πολίτη . Οι κίνδυνοι αυτοί αυξάνονται με τις νέες δυνατότητες ταχύτατης μεταφοράς πληροφοριών παγκοσμίως μέσω του Διαδικτύου.

ΤΑ ΕΙΔΗ ΤΩΝ ΠΑΡΑΒΙΑΣΕΩΝ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

- Τα είδη των παραβιάσεων αναφέρονται σε προσωπικά δεδομένα που έχουν σχέση με την ταυτότητα του ατόμου, με ιατρικά δεδομένα, οικονομικά στοιχεία, προσωπικές και οικογενειακές φωτογραφίες και videos.

ΓΝΩΣΤΕΣ ΠΑΡΑΒΙΑΣΕΙΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

- Κατά την περίοδο 2008-2010 έλαβε χώρα περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα μεγάλου αριθμού συνδρομητών του ΟΤΕ. Αν και δεν διαπιστώθηκε πότε συνέβη, φαίνεται ότι συνέβη τουλάχιστον μία φορά, κατά πάσα πιθανότητα σε τέσσερις διαφορετικές περιόδους. Τα δεδομένα αφορούν σε πάνω από 8.000.000 παλιούς ή υφιστάμενους συνδρομητές. Τα δεδομένα βρέθηκαν μετά από έρευνα της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος το 2013 στα πλαίσια έρευνάς της στην εταιρεία InfoCredit ΑΕ. Για την παραβίαση επιβλήθηκε πρόστιμο 60.000 ευρώ από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.[198]
- Τον Απρίλιο 2009 εκλάπησαν τέσσερις υπολογιστές από μονάδα του Ινστιτούτου Υγείας του Παιδιού στους οποίους ήταν καταχωρημένα ευαίσθητα προσωπικά δεδομένα υγείας 2.050 παιδιών.[199]
- Το 2011 χάκερ υπέκλεψε και δημοσίευσε στο διαδίκτυο προσωπικά δεδομένα 8.500 χρηστών από το διαδικτυακό τόπο της ελληνικής Sony BMG.[200]

ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

- Προσφυγή στην Αρχή Προστασίας Προσωπικών Δεδομένων.

- Η πληροφορίες είναι από την wikipedia.

Παραβίαση προσωπικών δεδομένων

Πέτρος Σ.

A decorative graphic element consisting of several horizontal lines of varying lengths and colors (teal, white, and light blue) extending from the right side of the slide.

Τι είναι;

- Παραβίαση δεδομένων προσωπικού χαρακτήρα επέρχεται όταν υπάρξει παραβίαση ασφαλείας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που υποβλήθηκαν σε επεξεργασία.

- Παραβίαση δεδομένων προσωπικού χαρακτήρα επέρχεται όταν υπάρξει παραβίαση ασφαλείας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που υποβλήθηκαν σε επεξεργασία.

Παραδείγματα

- Κάνετε κράτηση για ένα ταξί μέσω διαδικτυακής εφαρμογής. Η εταιρεία ταξί υπέστη μαζική παραβίαση δεδομένων προσωπικού χαρακτήρα και έχουν κλαπεί δεδομένα οδηγών και χρηστών. Υπάρχουν ενδείξεις ότι δεν είχε τεθεί σε ισχύ κανένα συγκεκριμένο μέτρο ασφαλείας για την προστασία των δεδομένων προσωπικού χαρακτήρα. Η εταιρεία όφειλε να σας ενημερώσει σχετικά με την παραβίαση. Σε αυτήν την περίπτωση, μπορείτε να υποβάλετε καταγγελία κατά της εταιρείας ταξί στην εθνική αρχή προστασίας δεδομένων

Τι κάνουμε σε περίπτωση παραβίασης των προσωπικών μας δεδομένων.

- Εάν η παραβίαση των δεδομένων δημιουργεί υψηλό κίνδυνο για τα άτομα που πλήττονται τότε πρέπει όλοι να ενημερωθούν, εκτός εάν υπάρχουν αποτελεσματικά μέτρα τεχνικής και οργανωτικής προστασίας που έχουν τεθεί σε εφαρμογή ή άλλα μέτρα που εξασφαλίζουν ότι ο κίνδυνος δεν είναι πλέον πιθανό να υλοποιηθεί .
- Εάν αυτό συμβεί, ο οργανισμός που κατέχει τα δεδομένα προσωπικού χαρακτήρα πρέπει να ειδοποιήσει την εποπτική αρχή χωρίς αδικαιολόγητη καθυστέρηση. Εάν η παραβίαση των δεδομένων προσωπικού χαρακτήρα είναι πιθανό να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες σας και ο κίνδυνος δεν έχει περιοριστεί, τότε εσείς, ως άτομο, πρέπει επίσης να ενημερωθείτε.

- Το μέγεθος του, μπορεί να είναι αβέβαιο και παράγωγο πολλών διαφορετικών συνθηκών. Παρά την αβεβαιότητα του, ένα τέτοιο κόστος μπορεί να ιχνηλατηθεί και να μας επιτρέψει να καταλάβουμε τις πηγές του, τα κρίσιμα στοιχεία που το διογκώνουν και στο τέλος έναν από τους πλέον αποδοτικούς τρόπους διαχείρισής του. Για να το κάνουμε αυτό είναι καλό να ξεδιπλώσουμε το πώς μπορεί να εκδηλωθεί ένα περιστατικό παραβίασης προσωπικών δεδομένων, μπαίνοντας στη θέση ενός συνετού χάκερ.

Άρθρα για την παραβίαση

- Δημοσιεύθηκε το τελικό κείμενο των νέων Κατευθυντηρίων Γραμμών 9/2022 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων με αντικείμενο τη γνωστοποίηση της παραβίασης δεδομένων προσωπικού χαρακτήρα. Το κείμενο φιλοδοξεί να παράσχει συνδρομή σε υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία ως προς τη συμμόρφωσή τους με τις απαιτήσεις των άρθρων 33-34 ΓΚΠΔ.

- Υπενθυμίζεται ότι, σύμφωνα με το άρθρο 33 ΓΚΠΔ, «σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια σύμφωνα με το άρθρο 55, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση». Αντίστοιχα, ως προς τα υποκείμενα των δεδομένων. «Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.»

Αποφυγή δημοσίευσης των προσωπικών δεδομένων μας

- Πόσες φορές την ημέρα δημοσιεύουμε κάτι από την προσωπική μας ζωή στα κοινωνικά δίκτυα; Πολλές φορές αυτό μπορεί να κρύβει κινδύνους. Η Αστυνομία αναφέρει τα πέντε βασικά σημεία που πρέπει να λαμβάνουμε υπόψη για τη δική μας ασφάλεια, προτού κοινοποιούμε στα μέσα κοινωνικής δικτύωσης¹. Ημερομηνία γέννησης Αν είναι αναρτημένη δημόσια η ημερομηνία γέννησης μας στο Facebook, ελλοχεύουν διάφοροι κίνδυνοι. Μπορεί να αισθανόμαστε ωραία βλέποντας δεκάδες «φίλους» να μας εύχονται για τα γενέθλιά μας, αλλά την ίδια ώρα δίνουμε χαρά σε κάθε επιτήδειο, ο οποίος μπορεί με όλα τα στοιχεία που απλόχερα του δίνουμε, να πλαστογραφήσει (ημερομηνία γέννησης, όνομα, φωτογραφία προφίλ κλπ), διάφορα προσωπικά μας έγγραφα, (από άδεια οδηγού μέχρι και το διαβατήριό μας).² Μόνος ή μόνη στο σπίτι Από τα χειρότερα αλλά και καθημερινά μας λάθη να δημοσιοποιούμε, ότι είμαστε μόνοι στο σπίτι. Ο κίνδυνος μπορεί να είναι ελάχιστος, αλλά πάντα παραμονεύει.,

Τι πρέπει να αποφεύγουμε;

- Σύμφωνα με τους ειδικούς, μικροί και μεγάλοι όταν χρησιμοποιούμε το διαδίκτυο δεν θα πρέπει να δημοσιοποιούμε υλικό με προσωπικά δεδομένα, φωτογραφίες δικές μας και φίλων μας. Δεν πρέπει επίσης να δημοσιοποιούμε δραστηριότητες στο ίντερνετ.

- Πηγες :
- European Commission[https://commission.europa.eu > reform > rights-citizens](https://commission.europa.eu/reform-rights-citizens)
- <https://saferinternet4kids.gr/nea/databreach/>
- <https://www.alphanews.live/cyprus/pente-pragmata-poy-den-prepei-na-demosieyete-sta-koinonika-diktya>



Παιχνίδια στο διαδίκτυο .



Γιάννης Δ.

Τα παιδιά και τα παιχνίδια .

- Τα τελευταία χρόνια εκατοντάδες παιδιά χρησιμοποιούν πολλά παιχνίδια για να περάσει η ώρα τους .



Τα είδη των παιχνιδιών

- Μπορείς να παίξεις παιχνίδια μόνος σου αλλά και online με άλλους χρήστες

Υπάρχουν διάφορες κατηγορίες παιχνιδιών όπως:

Massive multiplayer online role playing game)

Stand-Alone

Διαφημιστικά Παιχνίδια

Adventure games

Μίνι παιχνίδια/παιχνίδια πλοηγού

Οι κίνδυνοι των παιχνιδιών .

Διαταραχή συμπεριφοράς

Υπερβολική ενασχόληση

Έκθεση σε διαφημιστικό υλικό

Ακατάλληλο περιεχόμενο

Διαδραστικότητα

Σε ότι αφορά τα online παιχνίδια, αυτό που τα καθιστά τόσο ιδιαίτερα είναι το υψηλό επίπεδο διαδραστικότητας που δημιουργείται μεταξύ χρηστών που δεν γνωρίζονται απαραίτητα μεταξύ τους.

Για παιχνίδια προκαλούν κίνδυνους;

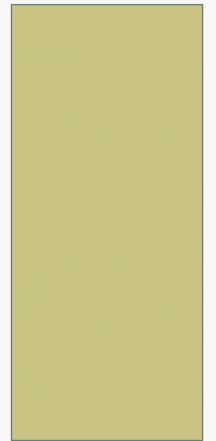
- Μερικά γνωστά παιχνίδια που έχουν προκαλέσει μεγάλα προβλήματα είναι το Fortnite, η μπλε φάλαινα, παιχνίδι του πνιγμού, το POKEMON GO! Και παιχνίδια με αλκοόλ. Μερικά από αυτά σου δίνουν εντολές με σκοπό να κάνεις ακραία πράγματα. Άλλα σε χακάρουν και σου παίρνουν τα προσωπικά δεδομένα.

Τι δεν πρέπει να κάνουμε όταν παίζουμε online παιχνίδια;

- Όταν παίζουμε online παιχνίδια δεν πρέπει να δίνουμε πληροφορίες για τον εαυτό μας. Δηλαδή να μην στέλνουμε φωτογραφίες, προσωπικά δεδομένα, διεύθυνση σπιτιού και κωδικούς. Μάλιστα δεν πρέπει να μιλάμε με ξένους διότι μπορούν να μας χακάρουν ή μπορεί να μας παρασύρουν σε επικίνδυνες καταστάσεις.

ΠΑΙΧΝΙΔΙΑ ΣΤΟ ΔΙΑΔΥΚΤΙΟ

ΑΝΑΣΤΑΣΙΑ Π.
ΣΤ'2





Τα διαδικτυακά / ηλεκτρονικά παιχνίδια είναι εξαιρετικά δημοφιλή για τα παιδιά και τους/τις νέους/ες, αποτελώντας αναπόσπαστο κομμάτι της καθημερινότητάς τους.

Στη σύγχρονη εποχή, είναι δύσκολο να εντοπίσετε παιδιά και εφήβους, που να μην απασχολούνται σε παιχνίδια σε ηλεκτρονικό υπολογιστή, στις κινητές τους συσκευές ή σε ειδικές κονσόλες.

ΘΕΤΙΚΑ

Η ενασχόληση με τα διαδικτυακά / ηλεκτρονικά παιχνίδια συμβάλλει στην απόκτηση γνώσεων και δεξιοτήτων με ένα πολύ ευχάριστο και ελκυστικό τρόπο. Τεχνολογικά νέες εξελιγμένες κονσόλες και βιντεοπαιχνίδια επιτρέπουν, αρχικά, τη ψυχαγωγία και την εξοικείωση με την τεχνολογία, αλλά, παράλληλα, συμβάλουν στην ανάπτυξη γνωστικών και άλλων δεξιοτήτων.

Ωστόσο, είναι γεγονός ότι, μέσω της ενασχόλησης με αυτά, δύναται να προκύψουν σημαντικές προκλήσεις και κίνδυνοι, οι οποίοι συνδέονται, μεταξύ άλλων, με το περιεχόμενο, τον χρόνο ενασχόλησης με αυτά, τη δυνατότητα επικοινωνίας με άλλα άτομα. Αναλυτικότερα:

- **Ακατάλληλο περιεχόμενο:** Ορισμένα παιχνίδια ενδέχεται να μην είναι κατάλληλα για την ηλικία του παιδιού, καθώς μπορεί να περιλαμβάνουν βίαιο ή ακατάλληλο περιεχόμενο ή σκηνές που αποσκοπούν στην πρόκληση τρόμου ή φόβου. Η έκθεση σε βίαιο και ακατάλληλο περιεχόμενο μπορεί να οδηγήσει στην αύξηση της επιθετικής και βίαιης συμπεριφοράς, στη χρήση χυδαίου και ακατάλληλου λεξιλογίου και να περιορίσει, σημαντικά, θετικές κοινωνικές συμπεριφορές (π.χ., ενσυναίσθηση, αποδοχή).
- **Πολύωρη ενασχόληση (εθισμός):** Τα διαδικτυακά παιχνίδια αποτελούν πιθανό κανάλι εθισμού. Η πολύωρη ενασχόληση με αυτά μπορεί να αποβεί αρνητική για τις σχολικές επιδόσεις και τις κοινωνικές δραστηριότητες, περιορίζοντας τις καθημερινές δραστηριότητες και την πραγματική και την ουσιαστική επαφή με συνομηλικούς ή και με την οικογένεια.
- **Επικοινωνία με αγνώστους (αποπλάνηση).** Οι εικονικές κοινότητες διαδικτυακών παιχνιδιών, στις οποίες συμμετέχουν τα παιδιά και οι έφηβοι, ενθαρρύνουν την πιθανή επαφή με κάποιον/α, ο/η οποίος/α να επιθυμεί, ενδεχομένως, να εκφοβίσει ή να παρενοχλήσει. Εάν κάποιος/α συμμετέχει σε παιχνίδια για πολλούς παίκτες στο Διαδίκτυο (όπου παίζει ενάντια σε άλλα άτομα, ενδεχομένως από διάφορα μέρη του κόσμου), μπορεί να κινδυνεύει να ακούσει προσβλητική γλώσσα από άλλους παίκτες, να εκφοβίζεται ή να θέτει τον εαυτό του στην ευάλωτη θέση να καταστεί θύμα σεξουαλικής παρενόχλησης.
- **Καταναλωτισμός:** Πολλά διαδικτυακά παιχνίδια ενθαρρύνουν και προωθούν την αγορά προϊόντων, αποτελώντας δαπανηρές παγίδες, διαμορφώνοντας εθιστικές υλιστικές συμπεριφορές.

ΝΑ ΘΥΜΑΣΤΕ...

Είναι σημαντικό να γνωρίζετε ότι, αναφορικά με τις προκλήσεις, που σχετίζονται με τη χρήση των διαδικτυακών παιχνιδιών και γενικότερα του Διαδικτύου, δεν είστε μόνοι/ες.

Μπορείτε να καλέσετε για σχετική υποστήριξη στη Γραμμή Βοήθειας 1480 <https://www.cybersafety.cy/helpline> και Γραμμή Καταγγελιών 1480 <https://www.cybersafety.cy/hotline>.

ΤΕΛΟΣ

ΤΕΛΟΣ



IOI

ΛΟΥΚΑΣ Γ. ΣΤ₂

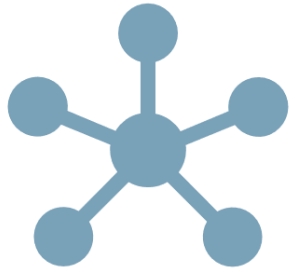
ΟΡΙΣΜΌΣ

- Ιός ενός υπολογιστή είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να «μολύνει» τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του.
- Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό.

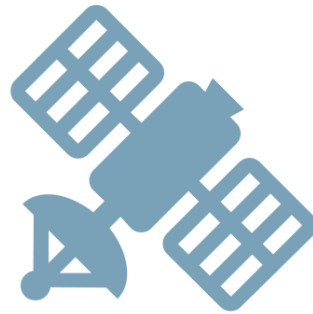


ΜΕΤΑΔΟΣΗ

- Οι ιοί διαδίδονται από τον ένα υπολογιστή στον άλλο με δύο τρόπους: Είτε μέσω φορητού μέσου αποθήκευσης, είτε μέσω δικτύου. Ο δεύτερος τρόπος είναι σήμερα ο πλέον διαδεδομένος, λόγω της ευρείας διάδοσης του Διαδικτύου διεθνώς. Η βασική υπηρεσία διάδοσης ιών είναι αυτή του ηλεκτρονικού ταχυδρομείου (e-mail).
- Για το λόγο αυτό, πολλές υπηρεσίες e-mail προσφέρουν πρώτα σάρωση των μηνυμάτων και των συνημμένων τους με κάποιο αντιβιοτικό, πριν επιτρέψουν στο χρήστη να τα λάβει.



Network



Satellite



Link

ΑΝΤΙΙΚΑ

- Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη, ορισμένοι μάλιστα ιοί είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία. Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη, ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο.

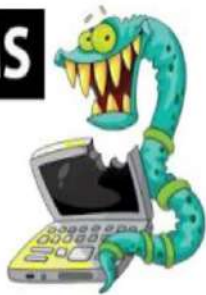
ΙΣΤΟΡΙΚΉ ΑΝΑΦΟΡΑ

- Ο πρώτος ιός που αναφέρεται ως εξαπλούμενος εκτός του συστήματος μέσα στο οποίο δημιουργήθηκε υπήρξε ο «Elk Cloner». Τον δημιούργησε το 1982 ο δεκαπεντάχρονος τότε Ρίτσαρντ Σκρέντα για υπολογιστές Apple II με λειτουργικό σύστημα το Apple DOS 3.3.
- Ο πρώτος ιός που εμφανίστηκε στους προσωπικούς υπολογιστές ήταν ο ιός Brain. Δημιουργήθηκε στο Πακιστάν το 1986 από τους αδελφούς Basit και Amjad Farooq Alvi. Προσέβαλε τον τομέα εκκίνησης (boot sector) του σκληρού δίσκου.

ΚΑΤΗΓΟΡΙΕΣ



WORMS



VIRUS



TROGAN



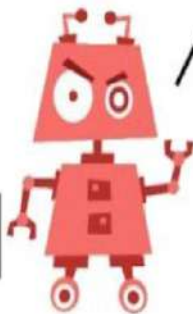
RANSOMWARE

MALWARE TYPES



ADWARE

BOTS



SPAM



SPYWARE



ΑΝΑΛΟΓΑ ΜΕ ΤΟ ΣΗΜΕΙΟ ΤΟΥ ΥΛΙΚΟΥ Ή ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ ΠΟΥ ΜΟΛΥΝΟΥΝ:

- Τομείς σκληρού δίσκου συστήματος
- Αρχεία
- Ιοί μακροεντολών
- Ιοί πηγαίου κώδικα
- Ιοί συμπλεγμάτων (σκληρού) δίσκου

ΑΝΑΛΟΓΑ ΜΕ ΤΟΝ ΤΡΟΠΟ ΜΕ ΤΟΝ ΟΠΟΙΟ ΠΡΑΓΜΑΤΟΠΟΙΟΥΝ ΤΗ ΜΪΟΛΥΝΣΗ:

- Πολυμορφικοί ιοί
- Αόρατοι ιοί
- Θωρακισμένοι ιοί
- Πολυτμηματικοί ιοί
- Ιοί πλήρωσης κενών
- Ιοί παραλλαγής



THANK
YOU

ΛΟΥΚΑΣ Γ.

ΟΙ ΙΟΙ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΖΕΣΙΚΑ Τ.

ΤΙ ΕΙΝΑΙ Ο ΙΟΣ

Ιός είναι ένα malware κατασκευασμένο ώστε να αντιγράψει τον εαυτό του σε διαφορετικά αρχεία του λειτουργικού μολύνοντας τα όπως ακριβώς κάνουν και οι βιολογικοί ιοί να αντιγράψουν τον εαυτό τους σε διαφορετικά τυχαία κύτταρα. Να επισημάνουμε ότι στους υπολογιστές υπάρχουν ιοί που είναι από εντελώς ακίνδυνοι πχ να εμφανίζουν ένα μήνυμα στην οθόνη μέχρι και ιοί που μπορούν να καταστρέψουν το λειτουργικό σύστημα ακόμα και την μητρική πλακέτα του υπολογιστή μας κάνοντας ζημιά στο bios. Άλλοι ιοί προβάλλουν διαφημίσεις ή επιβραδύνουν το σύστημα του υπολογιστή ή ακόμη να καταστρέψουν συγκεκριμένο τύπο αρχείων ή και όλα τα αρχεία. Εντός του υπολογιστή, ο ιός μολύνει είτε αυτόματα είτε κατά το άνοιγμα κάθε τύπο αρχείων που είναι προγραμματισμένος να μολύνει word, excel, exe κλπ

ΤΙ ΠΡΟΚΑΛΕΙ Ο ΙΟΣ

- **Ιός** ενός **υπολογιστή** (αγγλικά: *Virus*) είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να «μολύνει» τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφα του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν **μεταμορφικό ιό**. Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους. Π.χ. από χρήστη που στέλνει τον ιό μέσω δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB («φλασάκι»). Οι ιοί ορισμένες φορές εσφαλμένα συγχέονται με τα «σκουλήκια» υπολογιστών (worms) και τους δούρειους ίππους (trojan horses). Ένα «σκουλήκι» μπορεί να διαδοθεί σε άλλους υπολογιστές χωρίς να πρέπει να μεταφερθεί ως τμήμα ενός υπολογιστή-οικοδεσπότη (host), ενώ ένας δούρειος ίππος είναι ένα αβλαβές πρόγραμμα μέχρι να εκτελεσθεί ή μέχρι να ικανοποιηθεί κάποια συνθήκη, την οποία έχει προκαθορίσει ο δημιουργός του. Πολλοί προσωπικοί υπολογιστές συνδέονται πλέον με το Διαδίκτυο και σε τοπικά δίκτυα και διευκολύνουν έτσι τη διάδοση του κακόβουλου κώδικα. Σήμερα οι ιοί μπορούν επίσης να εκμεταλλευθούν τις υπηρεσίες του Διαδικτύου, όπως το World Wide Web, το ηλεκτρονικό ταχυδρομείο και την υπηρεσία συνομιλιών (Internet Relay Chat, IRC).

ΠΩΣ ΜΕΤΑΔΙΔΟΝΤΑΙ ΟΙ ΙΟΙ

- Οι ιοί διαδίδονται από τον ένα υπολογιστή στον άλλο με δύο τρόπους: Είτε μέσω φορητού μέσου αποθήκευσης, είτε μέσω δικτύου. Ο δεύτερος τρόπος είναι σήμερα ο πλέον διαδεδομένος, λόγω της ευρείας διάδοσης του Διαδικτύου διεθνώς. Η βασική υπηρεσία διάδοσης ιών είναι αυτή του [ηλεκτρονικού ταχυδρομείου](#) (e-mail), μέσω του οποίου αποστέλλονται είτε ως συνημμένα είτε ως τμήμα αυτού καθαυτού του μηνύματος. Για το λόγο αυτό, πολλές υπηρεσίες e-mail προσφέρουν πρώτα σάρωση των μηνυμάτων και των συνημμένων τους με κάποιο αντιβιοτικό, πριν επιτρέψουν στο χρήστη να τα λάβει.

ΑΝΤΙΜΕΤΩΠΙΣΗ

- > Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη, ορισμένοι μάλιστα ιοί είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία. Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό (antivirus). Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το [λειτουργικό σύστημα](#) του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως [διαδικασίες](#) στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν Κάθε αντιϊκό έχει τον δικό του τρόπο δράσης απέναντι στους ιούς. Ωστόσο τα περισσότερα είναι σε θέση να εργάζονται σε πραγματικό χρόνο, εντοπίζοντας τους ιούς τη στιγμή ακριβώς που αποπειρώνται να μολύνουν το σύστημα. Ορισμένα τέτοια προγράμματα προσφέρονται δωρεάν για προσωπική χρήση (δεν καλύπτουν, ωστόσο, ούτε μικρό τοπικό δίκτυο υπολογιστών) και άλλα έναντι σχετικά χαμηλής τιμής (κανένα αντιϊκό για υπολογιστές δικτύου δεν προσφέρεται δωρεάν μέχρι σήμερα). Οι δημιουργοί ιών λαμβάνουν υπόψη τις μεθόδους εντοπισμού και προσπαθούν να τις εξουδετερώσουν ακόμη και με απενεργοποίηση του αντιϊκού. τυχόν μολύνσεις σε πραγματικό χρόνο

ΓΝΩΣΤΟΣ ΙΟΣ

- **ILOVEYOU**

- Αυτός ήταν ίσως ο πιο επικίνδυνος ιός υπολογιστή που δημιουργήθηκε ποτέ που με τη μορφή ενός ατέρμονου worm – ήταν ένα αυτόνομο πρόγραμμα ικανό να αντιγράφεται μόνο του. Γνωστός ως ILOVEYOU, αυτός ο ιός ταξίδεψε αρχικά το Διαδίκτυο μέσω e-mail και κατάφερε να συντρίψει υπολογιστές σε ολόκληρο τον κόσμο. Για να καταστεί ακόμη πιο δελεαστικός, το θέμα του e-mail ήταν ένα γράμμα αγάπης από ένα μυστικό θαυμαστή. Ένα συνημμένο αρχείο στο e-mail ήταν αυτό που προκάλούσε όλα τα προβλήματα. Το αρχικό worm είχε το όνομα του αρχείου LOVE-LETTER-FOR-YOU.TXT.vbs. Τη στιγμή που κάποιος ανοίγει το αρχείο, ο ιός αποστέλλεται στις πρώτες 50 επαφές που είναι διαθέσιμες στο βιβλίο διευθύνσεων του υπολογιστή. Ο ιός προκάλεσε συνολική ζημία της τάξης των 10 δις \$ και επηρέασε σχεδόν το 10% των υπολογιστών στον κόσμο.









ΙΟΙ ΥΠΟΛΟΓΙΣΤΩΝ

Θοδωρής Μ.

Τι είναι ο ιός

- ▣ Ιός ενός υπολογιστή (αγγλικά: *Virus*) είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να «μολύνει» τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφα του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν **μεταμορφικό ιό**. Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους. Π.χ. από χρήστη που στέλνει τον ιό μέσω δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB («φλασάκι»).

Οι ιοί μπορούν να εμφανιστούν σε

...

- ▣ Μερικοί ιοί δημιουργούνται για να προξενήσουν ζημιά στον υπολογιστή, στον οποίο εγκαθίστανται, είτε με την καταστροφή των προγραμμάτων του είτε με τη διαγραφή αρχείων ή με τη διαμόρφωση (format) του σκληρού δίσκου. Μερικές, μάλιστα, φορές, δημιουργούν σε συγκεκριμένο τομέα του σκληρού δίσκου τέτοια καταστροφή, ώστε να είναι αδύνατη η ανάκτηση ολόκληρου του περιεχομένου του. Άλλοι δεν έχουν ως σκοπό να προκαλέσουν οποιαδήποτε ζημιά, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές αρκετά χιουμοριστικών. Όμως, ακόμη και αυτοί οι «καλοκάγαθοι» ιοί μπορούν να δημιουργήσουν προβλήματα στο χρήστη υπολογιστών: Καταλαμβάνουν τη μνήμη που χρησιμοποιείται από τα κανονικά προγράμματα και κατά συνέπεια προκαλούν συχνά ασταθή συμπεριφορά του συστήματος και μπορούν να οδηγήσουν σε κατάρρευσή του

Τύποι ιών

- ▣ **Ανάλογα με το σημείο του υλικού ή του λογισμικού που μολύνουν:**
 - Τομείς σκληρού δίσκου συστήματος (system sectors)
 - Αρχεία
 - Ιοί μακροεντολών (Macros)
 - Ιοί πηγαίου κώδικα (Source Code Viruses)
 - Ιοί συμπλεγμάτων (σκληρού) δίσκου ((Hard) Disk Clusters)
- ▣ **Ανάλογα με τον τρόπο με τον οποίο πραγματοποιούν τη μόλυνση:**
 - Πολυμορφικοί ιοί
 - Αόρατοι ιοί (Stealth Viruses)
 - Θωρακισμένοι ιοί (Armored Viruses)
 - Πολυτμηματικοί ιοί (Multipartite Viruses)
 - Ιοί πλήρωσης κενών (Spacefiller Viruses)
 - Ιοί παραλλαγής (Camouflage Viruses) [\[5\]](#).

Ιοί σε βιντεοπαιχνίδια



Τρόποι δράσεως

- ▣ Ανεξάρτητα από το τι και πώς μολύνει σε ένα σύστημα, ο ιός πρέπει να εξασφαλίσει ορισμένες βασικές συνθήκες, προκειμένου να δράσει. Συγκεκριμένα, πρέπει να μπορεί να εκτελέσει τον κώδικά του και να εξασφαλίσει πρόσβαση σε μέσα αποθήκευσης (κύρια στο σκληρό δίσκο, αλλά όχι μόνο). Γι' αυτό το λόγο, πολλοί ιοί προσκολλώνται σε εκτελέσιμα (executable) αρχεία είτε του λειτουργικού συστήματος είτε του κανονικού λογισμικού ενός συστήματος. Εξασφαλίζουν έτσι δύο πράγματα: Πρώτον, ότι θα μπορούν να αναπαραχθούν και δεύτερον ότι θα μπορέσουν να εκτελέσουν τον κώδικά τους.

Τι αποτελούσαν οι ιοί

- Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη, ορισμένοι μάλιστα ιοί είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να διαθέτει ειδικά προγραμματιστικά εργαλεία. Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό (antivirus). Προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη (memory resident), ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο. Κάθε αντιϊκό έχει τον δικό του τρόπο δράσης απέναντι στους ιούς. Ωστόσο τα περισσότερα είναι σε θέση να εργάζονται σε πραγματικό χρόνο, εντοπίζοντας τους ιούς τη στιγμή ακριβώς που αποπειρώνται να μολύνουν το σύστημα. Ορισμένα τέτοια προγράμματα προσφέρονται δωρεάν για προσωπική χρήση (δεν καλύπτουν, ωστόσο, ούτε μικρό τοπικό δίκτυο υπολογιστών) και άλλα έναντι σχετικά χαμηλής τιμής (κανένα αντιϊκό για υπολογιστές δικτύου δεν προσφέρεται δωρεάν μέχρι σήμερα). Οι δημιουργοί ιών λαμβάνουν υπόψη τις μεθόδους εντοπισμού και προσπαθούν να τις εξουδετερώσουν ακόμη και με απενεργοποίηση του αντιϊκού.

Τρόποι διάδοσης

- ▣ Οι ιοί διαδίδονται από τον ένα υπολογιστή στον άλλο με δύο τρόπους: Είτε μέσω φορητού μέσου αποθήκευσης, είτε μέσω δικτύου. Ο δεύτερος τρόπος είναι σήμερα ο πλέον διαδεδομένος, λόγω της ευρείας διάδοσης του Διαδικτύου διεθνώς. Η βασική υπηρεσία διάδοσης ιών είναι αυτή του ηλεκτρονικού ταχυδρομείου (e-mail), μέσω του οποίου αποστέλλονται είτε ως συνημμένα είτε ως τμήμα αυτού καθαυτού του μηνύματος. Για το λόγο αυτό, πολλές υπηρεσίες e-mail προσφέρουν πρώτα σάρωση των μηνυμάτων και των συνημμένων τους με κάποιο αντιβιοτικό, πριν επιτρέψουν στο χρήστη να τα λάβει.













Απάτες Στο Διαδίκτυο

Κατερίνα Δ.





Εισαγωγή



Τα τελευταία χρόνια , το διαδίκτυο έχει μπει στη ζωή όλων μας, είτε για εργασίες και δουριά είτε για παιχνίδια. Αλλά ανάμεσα στα χρήσιμα πράγματα που μας προσφέρει, υπάρχουν και κίνδυνοι. Πολλά είδη κινδύνων όπως διάφορες απάτες, ιοί, εκφοβισμός και άλλοι. Ευτυχώς υπάρχουν και τρόποι αντιμετώπισης.

Τι μπορεί να είναι μια απάτη στο διαδίκτυο

Στο διαδίκτυο, οι απάτες μπορεί να είναι πολλές, από email σε βιντεοπαιχνίδι. Συνήθως είναι για τραπεζικούς λογαριασμούς που σου ζητάνε κωδικό για την τράπεζα. Αν όμως δώσεις αυτόν τον κωδικό σου παίρνουν τα χρήματα από τον τραπεζικό λογαριασμό. Για αυτό χρειάζεστε προσοχή.

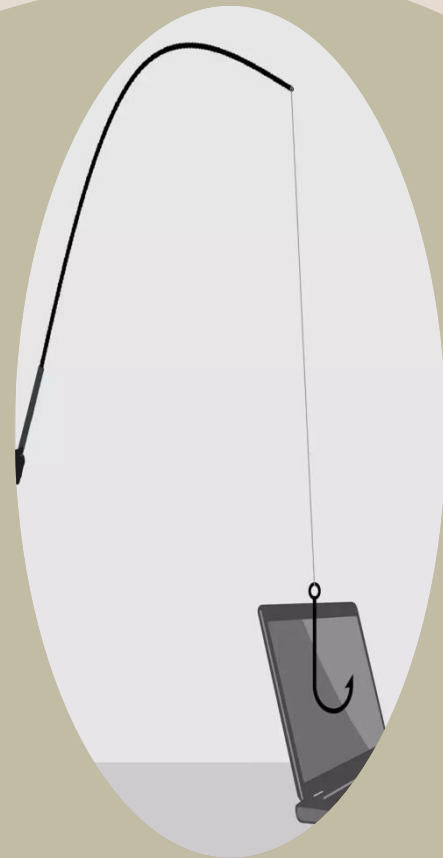


Είδη Απατών Στο Διαδίκτυο

- Φιλανθρωπική απάτη
- Απάτη με εισιτήρια μέσω διαδικτύου
- Ηλεκτρονική απάτη με δωροκάρτα
- Πλαστά ταχυδρομικά χρηματικά εντάλματα
- Απάτη αγοράς
- Απάτη λογαριασμών/Τραπεζικές
- Απάτη εκβιασμού

ΠΙΟ ΓΝΩΣΤΕΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΠΑΤΕΣ

- Απάτη με εισιτήρια μέσω διαδικτύου
 - Απάτη αγοράς
- Απάτη λογαριασμών/Τραπεζικές
 - Απάτη εκβιασμού



Ποιες Απάτες Πρέπει Να Προσέχουμε Περισσότερο

Τα τελευταία χρόνια υπάρχουν αρκετές έως πολλές απάτες αλλά πιο πολύ πρέπει να προσέχουμε τις παρακάτω

- **Απάτη με εισιτήρια μέσω διαδικτύου**
- **Ηλεκτρονική απάτη με δωροκάρτα**
- **Απάτη αγοράς**
- **Απάτη λογαριασμών/Τραπεζικές**

Τρόποι Αντιμετώπισης

Για την αντιμετώπισουμε τις απάτες πρέπει να:

- Μην παρασυρθούμε από τα άγνωστα μηνύματα
- Προσέχουμε σε τι ιστοσελίδες μπάνουμε
- Μην δίνουμε κωδικούς και προσωπικά στοιχεία
- Να ελέγχουμε από ποιον προέρχεται το μήνυμα





Κατερίνα Δ.
ΣΤ΄2

Πηγές:https://el.wikipedia.org/wiki/Διαδικτυακή_απάτη

ΑΠΑΤΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ!!

Κατερίνα Μ.



Εισαγωγή

- Όπως γνωρίζουμε καθημερινά στο διαδίκτυο γίνονται «ΑΠΑΤΕΣ» που έχουν σκοπό να σας κλέψουν τα προσωπικά σας δεδομένα (όνομα, τηλέφωνο, διεύθυνση) ή και τα χρήματά σας ! Για αυτό χρειάζεται μεγάλη προσοχή .

Τι είναι οι άπατες

- Οι απάτες είναι ένα αρκετά μεγάλο θέμα και αρκετά επικίνδυνο. Με λίγα λόγια είναι κάποια site ή μπορεί σε κάποια εφαρμογή που μπορείτε να μιλήσετε με ξένους, σας κάνουν να νομίζετε ότι μιλάτε σε κάποιον αλλά στην πραγματικότητα είναι άλλος άνθρωπος και έτσι μπορούν να σας ζητήσουν διάφορα στοιχεία και να σας εκβιάσουν μέχρι να τα δώσετε!

Τα είδη των απατών

1. Απάτες προσωπικών δεδομένων και κωδικών
2. Άπατες με αγοραπωλησίες
3. Απάτες με ρομαντικό περιεχόμενο
4. Απάτες με απειλές και εκβιασμούς
5. Απάτες με ψεύτικες φιλανθρωπίες
6. Απάτες με προσφορά εργασίας
7. Απάτες με δήθεν επενδύσεις χρημάτων
8. Απάτες με αναπάντεχα κέρδη
9. Απάτες με αναπάντεχα δώρα

Οι πιο συνηθισμένες απάτες

- Οι πιο συνηθισμένες απάτες είναι οι απάτες προσωπικών δεδομένων, απάτες και απειλές και εκβιασμού. Αυτές θα έλεγα ότι είναι οι πιο συνηθισμένες απάτες και πιστεύω πως γίνονται πολύ συχνά.

Τρόποι αντιμετώπισης

- Υπάρχουν διάφοροι τρόποι για να αντιμετωπίσεις μια απάτη αλλά εάν πιστεύετε ότι έχετε πέσει θύμα απάτης επικοινωνήστε αμέσως με τον νόμιμο οργανισμό για να τον ενημερώσετε για την απάτη, επίσης μπορείτε να ενημερώσετε άμεσα κάποιον γονέα ή κάποιον μεγαλύτερο για να σας βοηθήσουν!

Πηγες

1.SaferInternet4kids

2 .CYBERALERT

Τέλος

