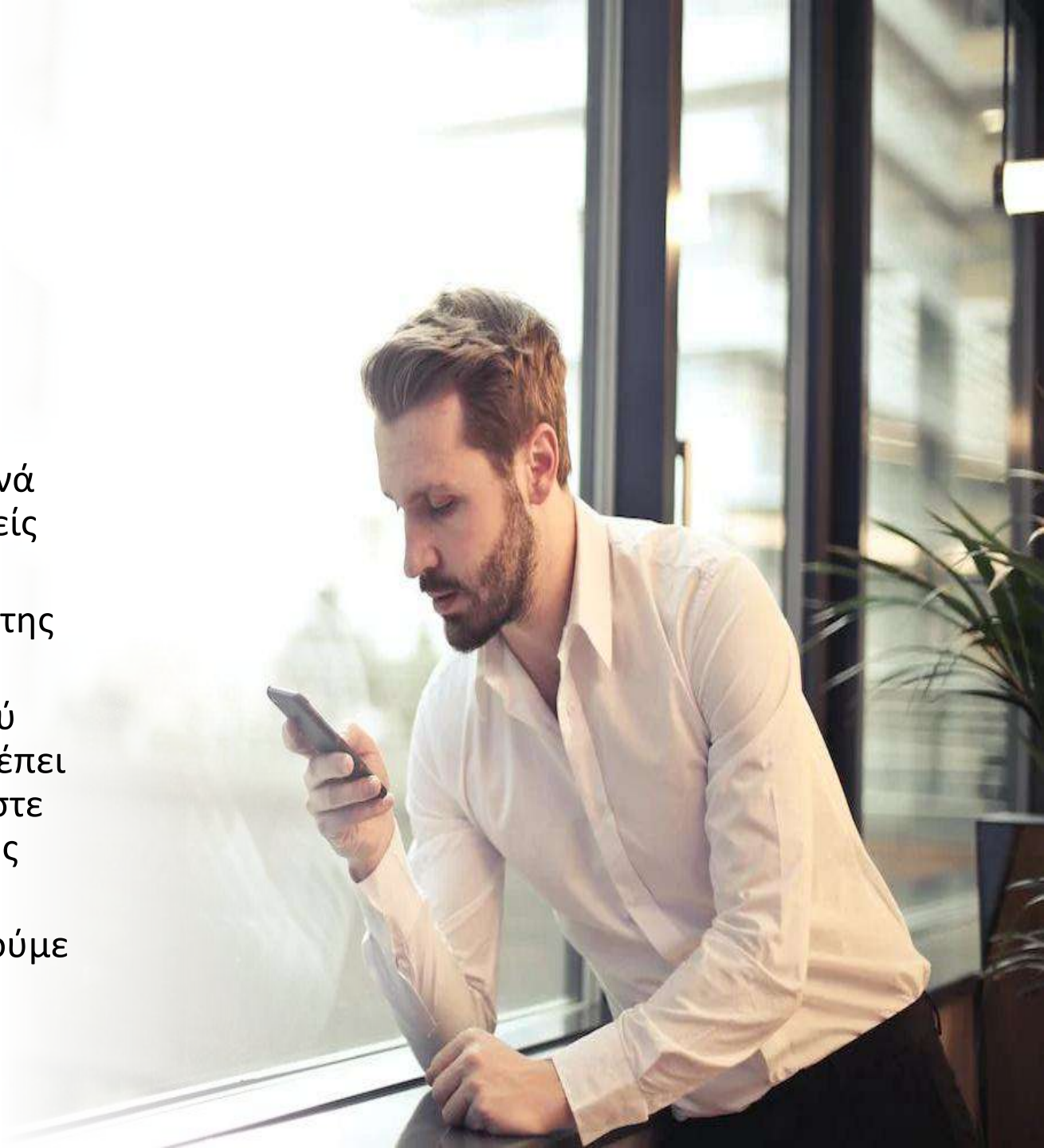
ΤΟ ΔΙΑΔΙΚΤΥΟ
(ΧΡΗΣΕΙΣ ΚΑΙ ΚΙΝΔΥΝΟΙ)

ΤΑΞΗ ΣΤ1 2023-24

ΤΟ ΔΙΑΔΙΚΤΥΟ ΣΤΗ ΖΩΗ ΜΑΣ

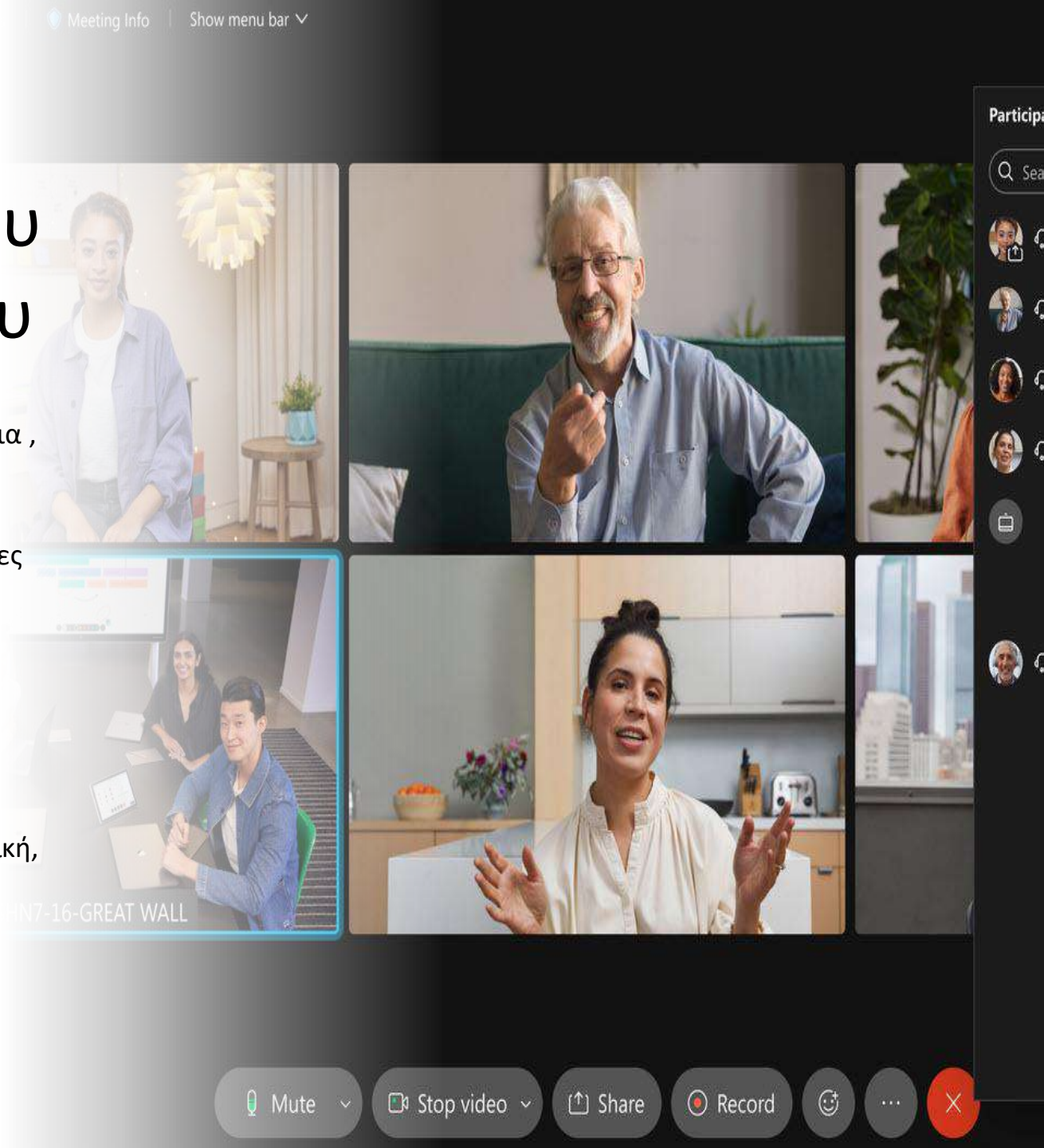
ΚΡΥΣΤΑΛΛΙΑ Μ.

- Το διαδίκτυο μας βοηθάει καθημερινά σε διάφορους τομείς της ζωής μας.
- Αποτελεί κομμάτι της ζωής μας.
- Σίγουρα είναι πολύ χρήσιμο , όμως πρέπει να προστατευόμαστε από τους κινδύνους του.
- Να το χρησιμοποιούμε με ασφάλεια.



Κάποιες χρήσεις του διαδικτύου

- Διασκέδαση (π.χ. παιχνίδια , βίντεο κ.λπ..)
- Εργασία – τηλεργασία
- Ενημέρωση – πληροφορίες
- Επικοινωνία
- Εκπαίδευση
- Αγορές –πωλήσεις
- Οικιακή χρήση
- Τέχνες-μουσική – κινηματογράφος
- Επιστήμες (ιατρική , φυσική, μαθηματικά)



ΕΠΙΚΟΙΝΩΝΙΑ

- Το διαδίκτυο και η κοινωνική δικτύωση αποτελεί μέρος της καθημερινότητας πολλών παιδιών , εφήβων και ενηλίκων . 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.

- Καθημερινά επικοινωνούμε με τους φίλους, συνεργάτες, οικογένειά κ.λπ.

ΔΙΑΣΚΕΔΑΣΗ – ΨΥΧΑΓΩΓΙΑ

- Βιντεοπαιχνίδια
- Βίντεο
- Ταινίες
- Μουσική
- Κινηματογράφος

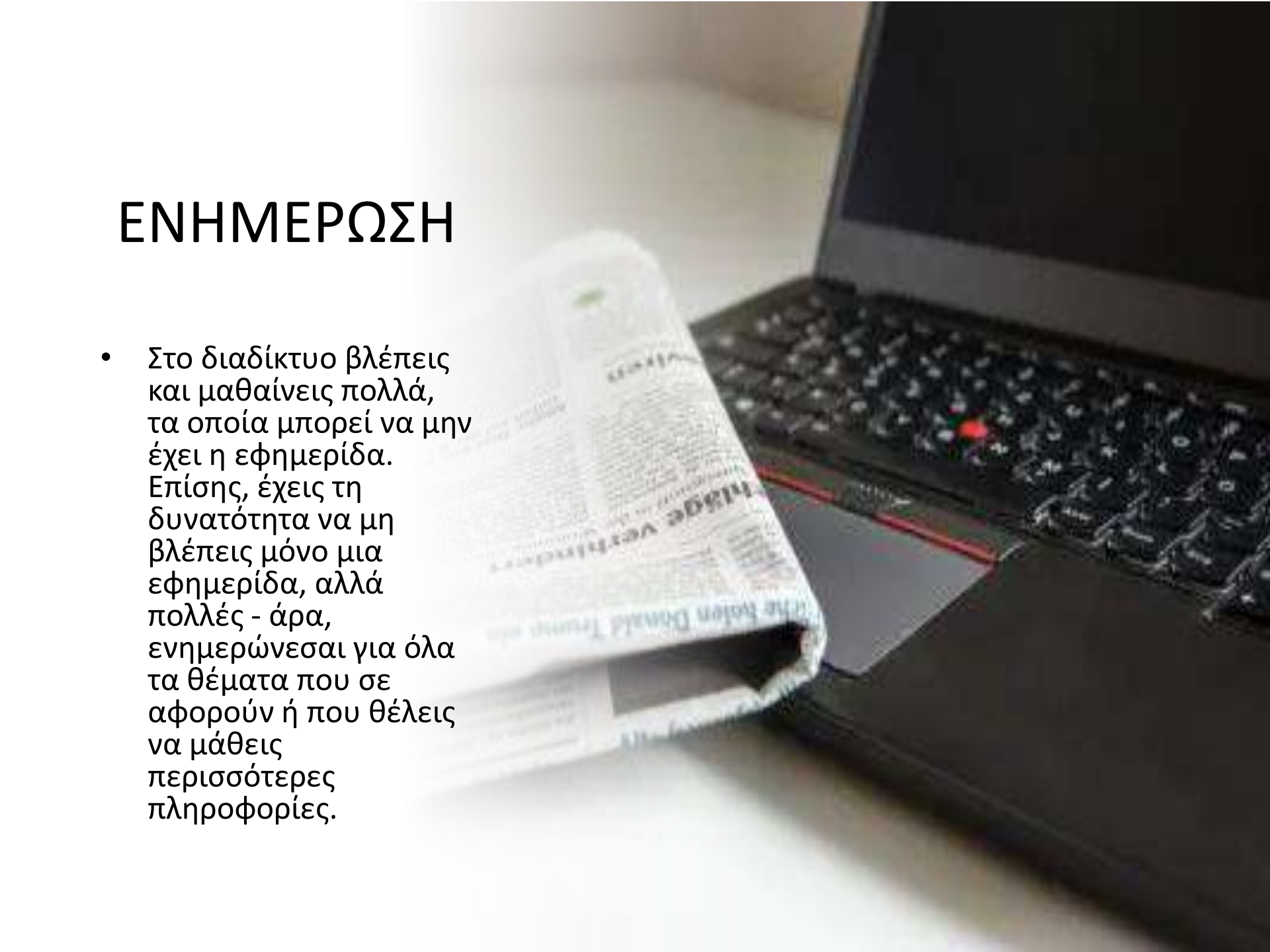
- Χρησιμοποιούμε τα βιντεοπαιχνίδια, τα βίντεο, την μουσική, τον κινηματογράφο και της ταινίες ως μέρος της ψυχαγωγίας – διασκέδασής μας. Είναι σημαντικό καθημερινά να μπορούμε να κάνουμε τα παραπάνω πράγματα.

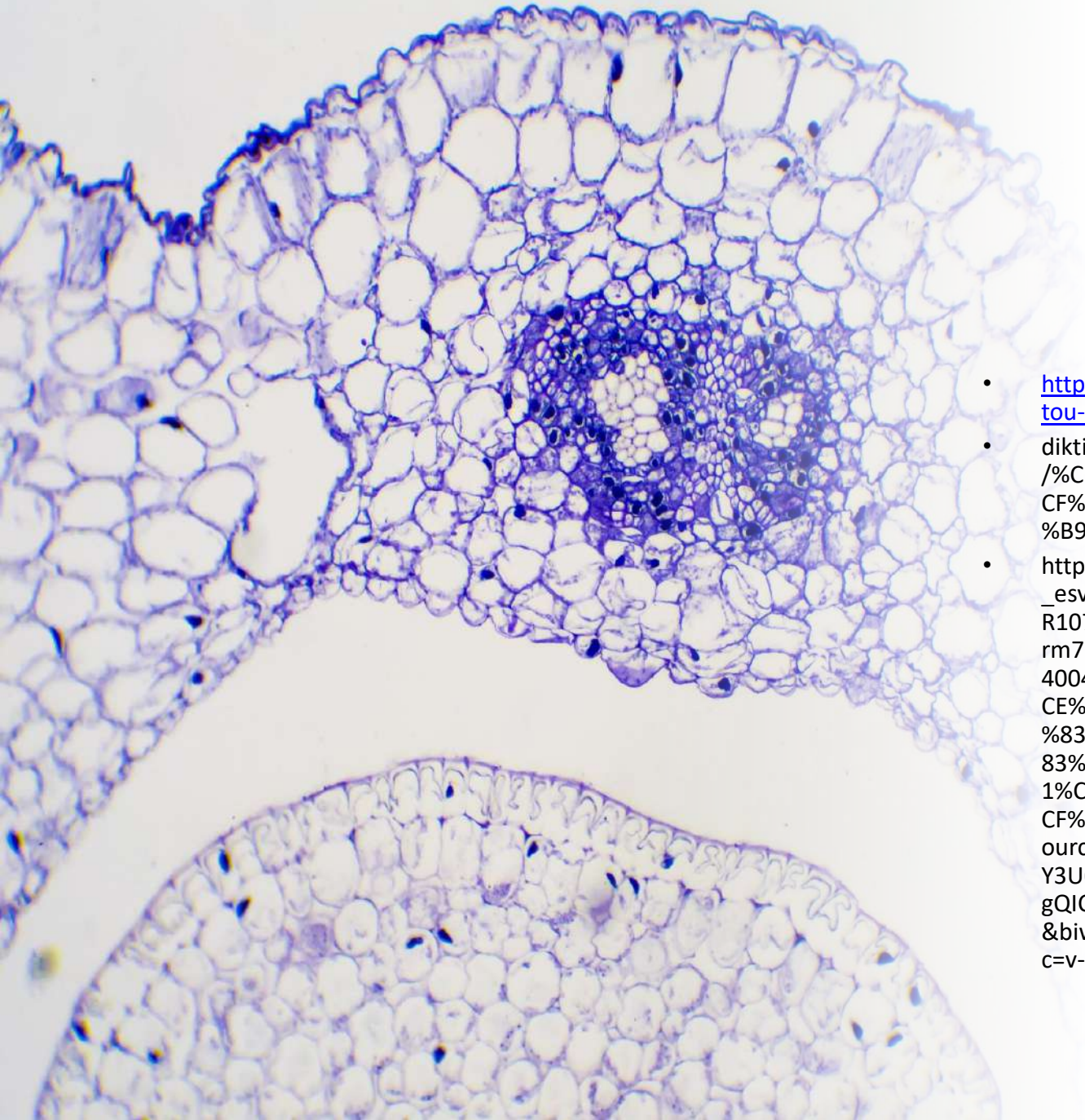
ΤΗΛΕΙΑΤΡΙΚΗ

- Η τηλεϊατρική αναφέρεται στην εφαρμογή των σύγχρονων τεχνολογιών, των τηλεπικοινωνιών και της πληροφορικής, για να προσφέρει σε ασθενείς κλινική βοήθεια από απόσταση. Η τηλεϊατρική βοηθάει περισσότερο εκείνους που βρίσκονται σε απομακρυσμένες περιοχές, όπως οι αγρότες, όταν ο ιατρός τους βρίσκεται σε άλλη περιοχή. Η χρήση των νέων τεχνολογιών επιτρέπει την εύκολη επικοινωνία του ιατρού με τον ασθενή μέσω της μετάδοσης ήχου και εικόνας.

ΕΝΗΜΕΡΩΣΗ

- Στο διαδίκτυο βλέπεις και μαθαίνεις πολλά, τα οποία μπορεί να μην έχει η εφημερίδα. Επίσης, έχεις τη δυνατότητα να μη βλέπεις μόνο μια εφημερίδα, αλλά πολλές - άρα, ενημερώνεσαι για όλα τα θέματα που σε αφορούν ή που θέλεις να μάθεις περισσότερες πληροφορίες.





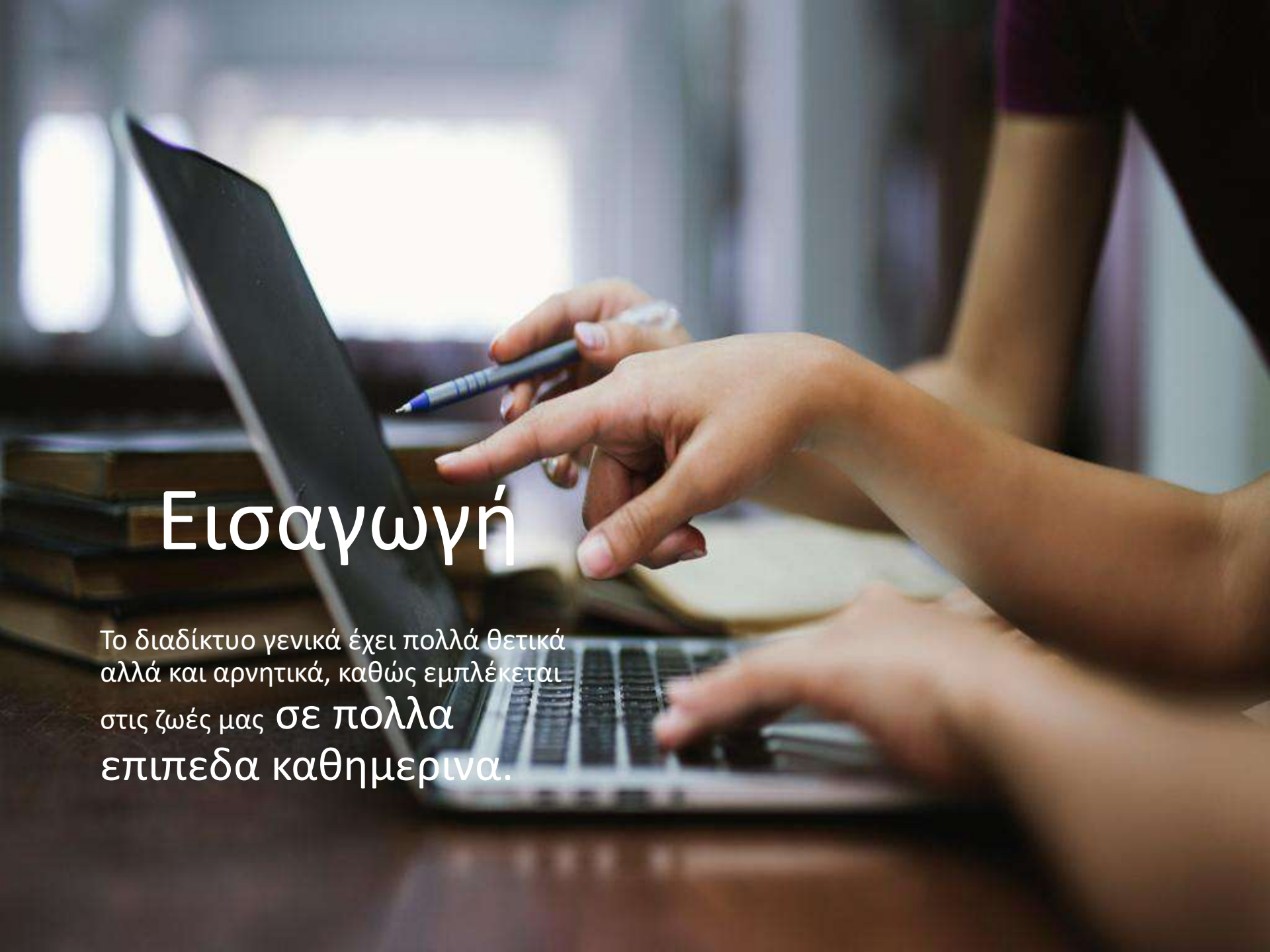
ΠΗΓΕΣ

- https://europalso.gr/goneis/ta-ofeli-tou-diadiktiou-ton-meson-koinonikis-
- diktiosis/https://el.wikipedia.org/wiki/%CE%A4%CE%B7%CE%BB%CE%B5%CF%8A%CE%B1%CF%84%CF%81%CE%B9%CE%BA%CE%AE
- https://www.google.com/search?sca_esv=587420702&rlz=1C1ONGR_enGR1073GR1073&sxsrf=AM9HkKlfDf0Ajrm7rSxwZ30y2xnYxk2GJA:1701591594004&q=%CE%B5%CE%BD%CE%B7%CE%BC%CE%AD%CF%81%CF%89%CF%83%CE%B7+%CE%BC%CE%B5%CF%83%CF%89+%CE%B4%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%85%CE%BF%CF%85&tbm=isch&source=lnms&sa=X&ved=2ahUKEwiJqY3U6vKCAxXoSfEDHWxmC0kQ0pQJegQICxAB&cshid=1701591738968478&biw=1536&bih=739&dpr=1.25#imgrc=v-xdb5XGOWNPJ


The End

ΤΟ ΔΙΑΔΙΚΤΥΟ ΣΤΗ ΖΩΗ ΜΑΣ

ΦΑΝΗ Π.



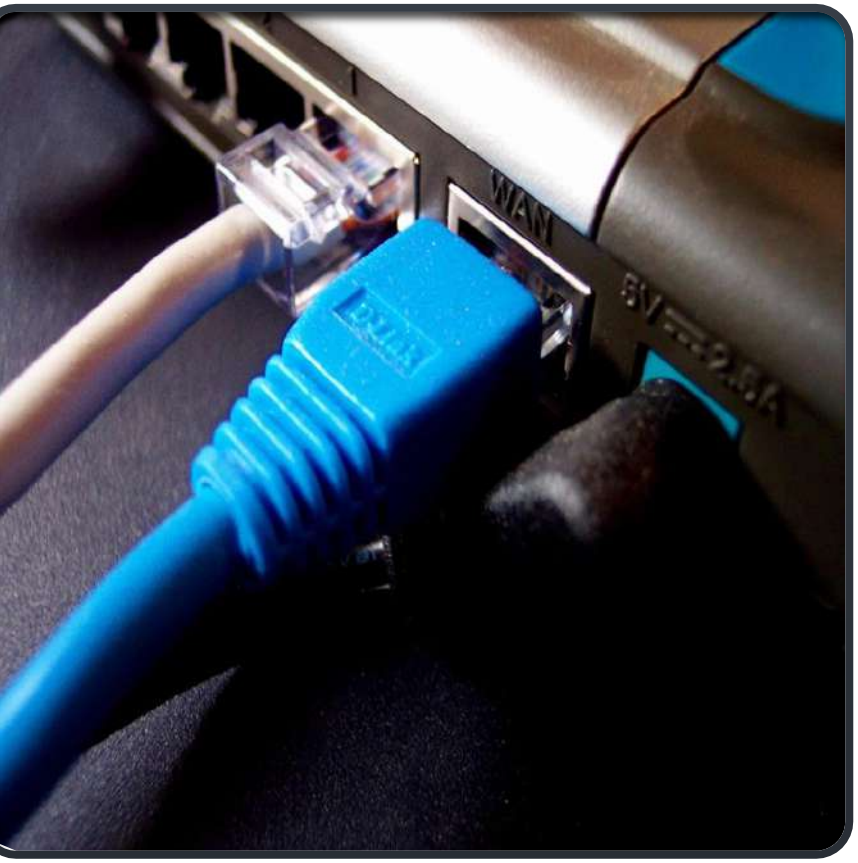
Εισαγωγή

Το διαδίκτυο γενικά έχει πολλά θετικά αλλά και αρνητικά, καθώς εμπλέκεται στις ζωές μας σε πολλα επιπεδα καθημερινα.

Τι είναι το διαδικτύο προς τη ζωή μας;

- Αδιαμφισβήτητα, τα τελευταία χρόνια το διαδίκτυο έχει εισβάλλει στην καθημερινότητα μας. Πλέον, έχουμε πρόσβαση σε αυτό από τα «έξυπνα τηλέφωνα μας», οπουδήποτε κι αν βρισκόμαστε. Είναι κάτι που θεωρείται τόσο δεδομένο, ώστε δεν αναλογιζόμαστε τις αρνητικές συνέπειες αυτού του φαινομένου. Σίγουρα το διαδίκτυο και η ευκολότερη πρόσβαση σε αυτό έχουν διευκολύνει τις ζωές μας. Ωστόσο, κατά πόσο είμαστε σε θέση να μην υποπέσουμε στην παγίδα της κατάχρησης; Η χρήση του διαδικτύου έχει εξαπλωθεί σε όλους τους τομείς της ζωής μας: στην εργασία, στις κοινωνικές σχέσεις, στην ψυχαγωγία. Το χρησιμοποιούμε από το πρωί μέχρι το βράδυ.

Σε τι τομείς χρησιμοποιούμε το διαδικτυο στη ζωή μας ;



- **Υπάρχουν πολλοί τομείς που χρησιμοποιούμε το διαδίκτυο στη ζωή μας για παράδειγμα:**

- **Για διασκέδαση**
- **Για εργασία-τηλεργασία**
- **Για ενημέρωση**
- **Για επικοινωνία**
- **Για εκπαίδευση**
- **Για αγορές-πωλήσεις**
- **Για οικιακές χρήσεις**
- **Τέχνες –μουσική**
- **Για επιστήμες**
- **Ηλεκτρονικές υπηρεσιες**
- **Για συγκοινωνίες**

- Το διαδικτυο όμως δεν εχει μονο θετικα αποτελεσματα αλλα και αρνητικα.για παραδειγμα:
- Προβληματα υγειας
- Απατεσ
- Προσωπικα στοιχεια
- Διαδικτυακοσ εκφοβισμοσ
- Υπερπληροφορηση-Μη αξιοπιστη πληροφορηση
- Ακαταληλο περιεχομενο
- Τυχερα παιχνιδια (τζογοσ)
- Ιοι
- εθισμος

- Συμπερασματικά, το διαδίκτυο είναι ένα αναπόσπαστο κομμάτι της ζωής μας και σίγουρα έχει πολλά θετικά που μπορεί να μας προσφέρει. Το ζήτημα λοιπόν, δεν είναι σε καμία περίπτωση να αποκοπούμε τελείως από αυτό, αλλά να το χρησιμοποιούμε μόνο προς όφελος και διευκόλυνση μας. Με λίγα λόγια ο σκοπός είναι… Να χρησιμοποιούμε εμείς το διαδίκτυο κι όχι αυτό εμάς!

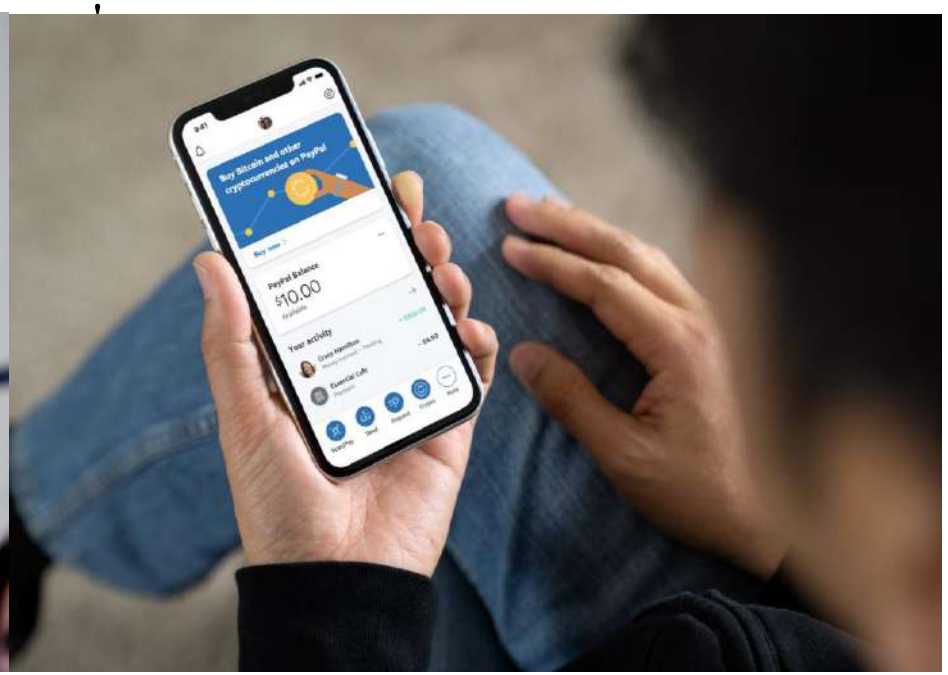
Πηγές

- https://thessculture.gr/arthrografia/to-diadiktyo-sti-zoi-mas/
- https://aggelikikavallieratou.gr/


#
Thank you
Menu
Ctrl


ΧΡΗΣΗ
ΔΙΑΔΥΚΤΙΟΥ
Ελένη Σ.

-Το διαδίκτυο καθιστά εφικτή την **άμεση διεκπεραίωση οικονομικών συναλλαγών**, όπως είναι η μεταφορά χρημάτων ή η πληρωμή λογαριασμών, με τη χρήση ενός απλού υπολογιστή, γεγονός που αποδεσμεύει πολύτιμο χρόνο για τους πολίτες, αφού δεν είναι απαραίτητη πλέον η πολύωρη αναμονή σε καταστήματα τραπεζών ή άλλων υπηρεσιών. Η δυνατότητα αυτή,



- Το διαδίκτυο προσφέρει εκπληκτικές δυνατότητες διαφήμισης και προώθησης προϊόντων και υπηρεσιών, παρέχοντας σε εταιρείες και επιχειρήσεις ένα ισχυρό μέσο για την αύξηση των πωλήσεών τους. Κάθε επιχείρηση διαθέτει πλέον τη δική της ιστοσελίδα, όπου όχι μόνο προβάλλει τα προϊόντα της, αλλά μπορεί και να πραγματοποιεί απευθείας πωλήσεις μέσω αυτής. Παραλλήλως, με τη χρήση των μέσων κοινωνικής δικτύωσης, ακόμη και μικρές εταιρείες έχουν τη δυνατότητα να προωθούν ανέξοδα τα προϊόντα ή τις υπηρεσίες που παρέχουν.

- Το διαδίκτυο έχει αποτελέσει έναν ιδανικό τρόπο διακίνησης πληροφοριών σε κάθε άκρη της γης, επιτρέποντας στους πολίτες πρόσβαση σε πηγές γνώσης που άλλοτε ήταν απρόσιτες. Βιβλιοθήκες, πανεπιστημιακά και εκπαιδευτικά ιδρύματα, έχουν ψηφιοποιήσει και θέσει στη διάθεση του κοινού πλήθος βιβλίων, επιστημονικά άρθρα και διαλέξεις, μελέτες και έρευνες, επιτρέποντας σε κάθε πολίτη που το επιθυμεί να ενημερωθεί κατά τρόπο έγκυρο για κάθε επιστημονικό αντικείμενο που του κινεί το ενδιαφέρον.

Το διαδίκτυο αυξάνει θεαματικά τις πηγές λήψης πληροφοριών και εκπαιδευτικού υλικού για τους μαθητές, καθώς έχουν πια πρόσβαση σε μεγάλες βιβλιοθήκες (ψηφιακά βιβλία), σε ιστοσελίδες εκπαιδευτικού και ενημερωτικού χαρακτήρα, σε ιστορικά αρχεία, αλλά και αρχεία εφημερίδων και περιοδικών. Είναι ουσιαστικά εφικτή η εύρεση πληροφοριών και στοιχείων για κάθε γνωστικό αντικείμενο, γεγονός που εκτείνει σημαντικά το εύρος ενημέρωσης των μαθητών και βοηθά στην έμπρακτη αποδέσμευση από τους περιορισμούς του ενός διδακτικού βιβλίου. Καλύπτονται, έτσι, τυχόν ελλείψεις ή παραλείψεις του σχολικού εγχειριδίου και προσφέρεται στους φίλεργους μαθητές πληθώρα πληροφοριακού υλικού.

- Η συνεισφορά του διαδικτύου στον τομέα της επικοινωνίας υπήρξε καταλυτικής σημασίας, εφόσον τόσο με τα Μέσα Κοινωνικής Δικτύωσης όσο και με τις υπηρεσίες κλήσεων και συνομιλίας με τη χρήση κάμερας, άλλαξε πλήρως τον τρόπο με τον οποίο επικοινωνούν οι άνθρωποι στις μέρες μας. Ιδίως τα Μέσα Κοινωνικής Δικτύωσης με την ιδιαίτερη διάδοσή τους στα άτομα νεανικής ηλικίας έχουν διαμορφώσει νέους κώδικες επικοινωνίας, φέρνοντας σ' επαφή ανθρώπους απ' όλα τα μέρη του κόσμου. Οι χρήστες των μέσων αυτών δεν περιορίζουν τις συνομιλίες τους μόνο μεταξύ των ατόμων που γνωρίζουν δια ζώσης· προσεγγίζουν άτομα από κάθε πιθανό μέρος του κόσμου με βάση τα κοινά ενδιαφέροντά τους, και διευρύνουν έτσι κατά τρόπο εντυπωσιακό τον κύκλο γνωριμιών τους.

- Το διαδίκτυο, ιδίως για τις νεότερες γενιές, προσφέρει πάρα πολλές δυνατότητες διασκέδασης και ψυχαγωγίας, εφόσον παρέχει πρόσβαση σε άφθονο ψυχαγωγικό υλικό, όπως: τηλεοπτικές σειρές, κινηματογραφικές ταινίες, τραγούδια, λογοτεχνικά έργα, ηλεκτρονικά παιχνίδια κ.ά. Καίριο στοιχείο της διαδικτυακής ψυχαγωγίας είναι η δυνατότητα αλληλεπίδρασης, καθώς οι πιθανοί διαδικτυακοί συνομιλητές ή συμπαίκτες προέρχονται από οποιαδήποτε περιοχή της χώρας ή άλλου κράτους.

- Με τις δυνατότητες ενημέρωσης και πληροφόρησης του διαδικτύου κάθε πολίτης είναι σε θέση να γνωρίσει καλύτερα την κουλτούρα και τις αντιλήψεις των άλλων λαών, παύοντας να τους αντιμετωπίζει ως κάτι το άγνωστο. Οι άλλοι λαοί γίνονται πλέον οικείοι και γνώριμοι, αποκτούν μια σαφέστερη ταυτότητα και δεν αποτελούν πηγή ανησυχίας ως κάτι το ανοίκειο.

Κίνδυνοι του διαδικτύου

Θανάσης Λ.

Μερικοί κίνδυνοι του διαδικτύου είναι:

- Ακατάλληλο Περιεχόμενο Ο όρος ακατάλληλο περιεχόμενο είναι υποκειμενικός σε σχέση με την ηλικία ή και την ψυχική κατάσταση του κάθε ατόμου.

  Αποπλάνηση (Grooming)

  Εθισμός (Internet Addiction)

  Ηλεκτρονικός Τζόγος

  Παραβίαση Ιδιωτικότητας

  Υποκλοπή Προσωπικών Δεδομένων (Phishing

Τι είναι οι κίνδυνοι του διαδικτύου;

- Με τους κίνδυνους του διαδικτύου μπορούμε να χάσουμε τα προσωπικά μας στοιχεία, την περιουσία μας, να δεχόμαστε απειλές κ.λ.π

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiJm_yN-OuCAxWIVPEDHeG7BukQFnoECBIQAw&url=https%3A%2F%2Finternetsafety.pi.ac.cy%2Fkids%2Fkids-danger%2F&usg=AOvVaw0FcQhNg0zyQDpK_iVszMvu&opi=89978449

ΚΙΝΔΥΝΟΙ ΔΙΑΔΙΚΤΥΟΥ

Μιράντα Γ.

- Εργασία της Μιράντας Γ. για το μάθημα της πληροφορικής
- Τάξη ΣΤ1

- Το διαδίκτυο έχει βοηθήσει την ανθρωπότητα, μέσω της παγκοσμιοποίησης και της πληροφορίας αλλά έχει και πολλές αρνητικές συνέπειες.

ΑΡΝΗΤΙΚΕΣ ΣΥΝΕΠΕΙΕΣ

1. Παιδική πορνογραφία: Άτομα υπεράνω υποψίας αποκτούν την εμπιστοσύνη των ανηλίκων και προκαλούν συζητήσεις σεξουαλικής φύσης.

- 2. Ψηφιακή παρενόχληση: παρενόχληση, δυσφήμιση και διάδοση ψευδών πληροφοριών.

- 3. Αυτοκτονίες: Στην Ελλάδα σε πέντε χρόνια πάνω από 400 άτομα έχουν εκδηλώσει πρόθεση στο διαδίκτυο να αυτοκτονήσουν.

- 4. Οικονομικές απάτες: Απατεώνες μπορούν να υποκλέψουν κωδικούς ασφαλείας και να σας χρεώσουν υπέρογκα ποσά.

- 5. Παραβίαση προσωπικών δεδομένων

- 6. Εθισμός στο διαδίκτυο

Τρόποι αντιμετώπισης

1. Είμαστε προσεκτικοί όταν δίνουμε την ηλεκτρονική μας διεύθυνση και ρυθμίζουμε την υπηρεσία φιλτραρίσματος του ηλεκτρονικού μας ταχυδρομείου.

- 2. Δεν δίνουμε τα προσωπικά μας στοιχεία σε ένα δωμάτιο συνομιλίας.

- 3.Ενημερωνόμαστε για το φαινόμενο του εθισμού και χρησιμοποιούμε το διαδίκτυο με μέτρο, συμπεριλαμβάνοντας στο πρόγραμμά μας άλλες δραστηριότητες, όπως χορό.

- 4. Αξιολογούμε τις πληροφορίες που βρίσκουμε στο διαδίκτυο και ελέγχουμε τον συγγραφέα. Εγκαθιστούμε φίλτρα λογισμικού που μπορούν να αποκλείσουν πηγές που περιέχουν μίσος, ρατσισμό και γενικά προπαγάνδα.

- Εθισμός στο διαδικτύο

Οικονομικές απάτες στο Ίντερνετ

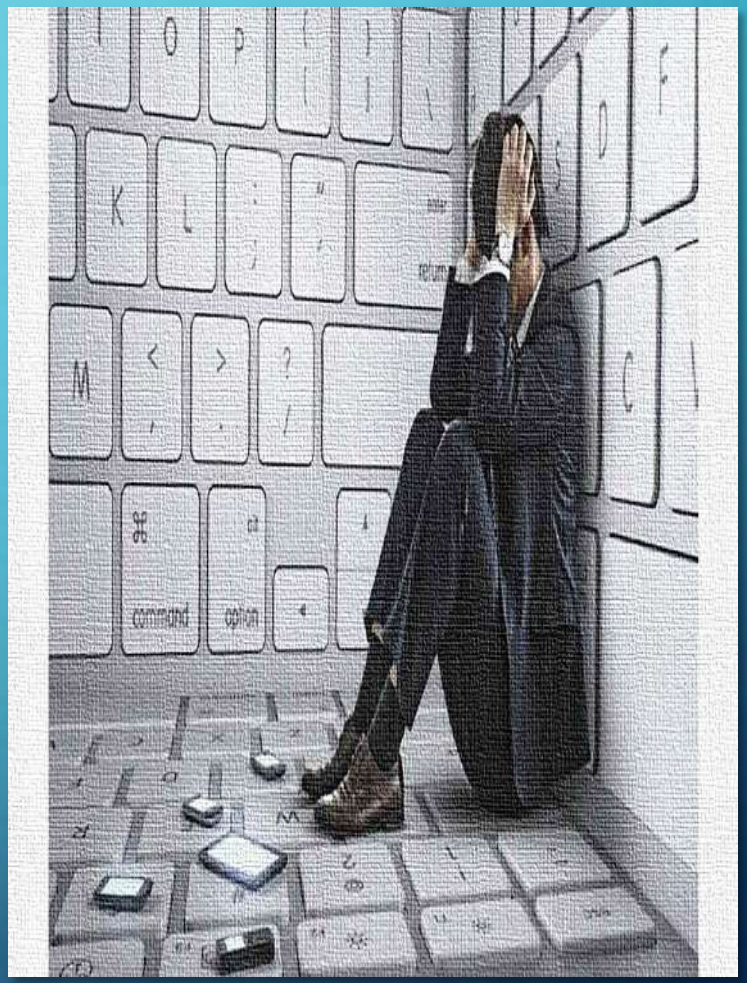
ΕΘΙΣΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΡΙΑΔΝΗ Κ.

Το **Διαδίκτυο** είναι ένα από τα σημαντικότερα εργαλεία του ανθρώπου στη σημερινή κοινωνία. Όλοι μας το έχουμε ακουστά ή και ακόμα το χρησιμοποιούμε συχνά. Αλλά πόσοι από εμάς πραγματικά το γνωρίζουμε; Μας παρέχει πρόσβαση σε μία στοίβα πληροφοριών και υπηρεσιών χωρίς να μετακινούμαστε. Όλα σχεδόν τα σχολεία έχουν υπολογιστές και τα περισσότερα παιδιά σήμερα χρησιμοποιούν τον υπολογιστή ή το διαδίκτυο. Οι υπολογιστές έχουν μπει σε κάθε πλευρά της καθημερινής ζωής των ανθρώπων άλλες φορές σωστά και άλλες προκαλώντας προβλήματα.

Ο ΕΘΙΣΜΟΣ

Ο εθισμός είναι μια κατάσταση κατά την οποία το άτομο λαμβάνει μια ουσία ή συμμετέχει σε μια δραστηριότητα, η οποία μπορεί να είναι ευχάριστη, αλλά της οποίας η χρήση γίνεται καταναγκαστική και επηρεάζει σημαντικά την λειτουργικότητα του (εργασία,



ΤΙ ΕΙΝΑΙ Ο ΕΘΙΣΜΟς ΣΤΟ **ΔΙΑΔΙΚΤΥΟ**

Ο εθισμός στο διαδίκτυο είναι μια κατάσταση όπου κάποιος αποκτά μια υπερβολική εξάρτηση του διαδικτύου , προτιμώντας να περνάει πολλές ώρες σερφάροντας αντί να ασχολείται με άλλες δραστηριότητες της καθημερινής του ζωής.

ΤΙ ΠΡΟΒΛΗΜΑΤΑ ΠΡΟΚΑΛΕΙ

Ο εθισμος στο διαδικτυο μπορει να οδηγησει σε :

- Απώλεια ενδιαφεροντος για τις καθημερινες δραστιριοτητες.
- Προβληματα υπνου.
- Καταθλιψη , αυξημενο αγχος.
- Μειωση της προσωπικης

ΠΑΡΑΓΟΝΤΕΣ ΠΟΥ ΣΥΜΒΑΛΛΟΥΝ ΣΤΗΝ ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΕΘΙΣΜΟΥ ΑΠΟ ΤΟ ΔΙΑΔΙΚΤΥΟ

Στα πλαίσια της πρόληψης αρκετοί παράγοντες είναι εκείνοι που θα μπορούσαν να συμβάλλουν στην αντιμετώπιση του προβλήματος:

Ενημέρωση των νέων από το οικογενειακό και σχολικό περιβάλλον. Συγκεκριμένα:

- Το **οικογενειακό περιβάλλον** μέσα από το οποίο θα πρέπει να τεθούν τα πρώτα όρια χρήσης του υπολογιστή, όσον αφορά τον χρόνο αλλά και το είδος της χρήσης του.
- Το **σχολείο** μέσα από το οποίο ενημερωμένοι εκπαιδευτικοί αναλαμβάνουν την πληροφόρηση μαθητών και γονέων σχετικά με τους κινδύνους του διαδικτύου. Προτείνοντας μέτρα πρόληψης ώστε να γίνουν αντιληπτές οι θετικές πλευρές της χρήσης Η/Υ όπως η χρήση τους για τις σχολικές εργασίες των μαθητών.
- Η συνδρομή καταρτισμένων επιστημόνων όπως **ψυχολόγων** αποτελεί ουσιαστικής σημασίας για την πρόληψη και την παροχή άμεσης βοήθειας όταν υπάρχει υπερβολική έκθεση στο διαδίκτυο.

ΠΗΓΕς:

- WEEBLY
- DIMPAPP
- PAIDI-OIKOGENEIA.GR
- PHYCHOPEDIA.GR

ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ

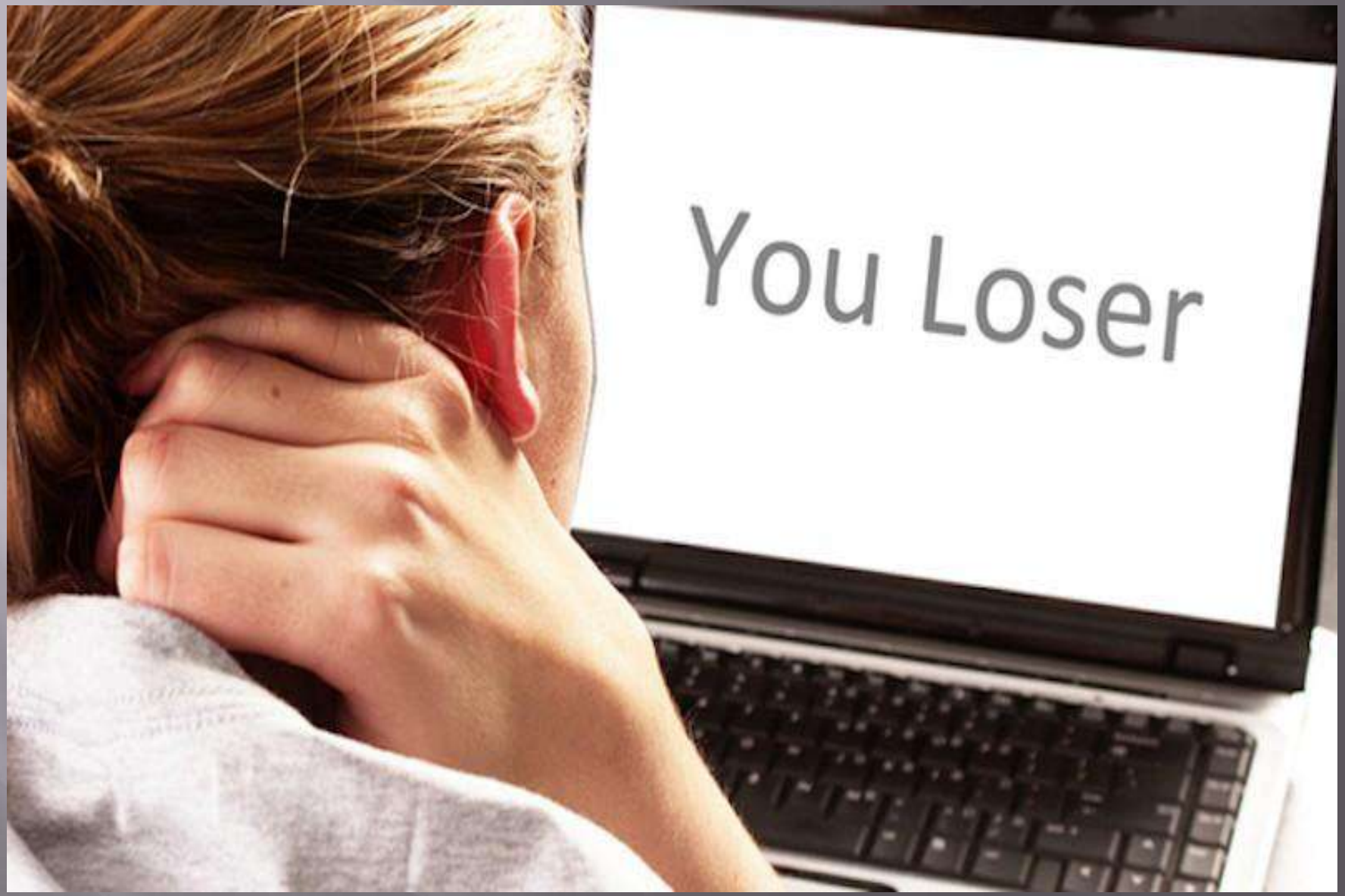
Από Φωτεινή Α.

ΕΙΣΑΓΩΓΗ

- Στο διαδύκτιο υπάρχουν άπειρα πράγματα που μπορούμε να συναντήσουμε,όπως για παράδειγμα οι εκφοβιασμοί του διαδοκτύου που γίνονται καθημερινά.Δυστυχώς αυτό γίνεται ακόμη και σήμερα και σε άπειρεσ χώρες.

Τι είναι ο εκφοβιασμόσ διαδικτύου;

- Ο εκφοβισμός που γίνεται στο διαδίκτυο αφορά τον εκφοβισμό, την απειλή,την ταπείνωση ή την παρενόχληση παιδιών, προεφήβων και εφήβων που δέχονται μέσω της χρήσης του διαδικτύου, κινητών τηλεφώνων είτε άλλων ψηφιακών τεχνολογιών από ομηλίκους τους. Η παρενόχληση αυτή μπορεί να γίνεται σε τακτικά ή άτακτα χρονικά διαστήματα μέσω οποιασδήποτε πράξης εκφοβισμού, επιθετικότητας, τρομοκρατικής ή αυταρχικής συμπεριφοράς.


You Loser

Τι προκαλεί ο διαδικτυακόσ εκφοβισμός;

- Με λίγα λόγια όταν το παιδί είναι ανήλικο προκαλεί μεγάλο φόβο και ένταση.Διότι αυτό μπορεί να εξελιχθεί σε φυσική απειλή για ένα ανήλικο παιδί.Επίσης ο κακοποιός ταρακουνάει το παιδί με οποιονδήποτε τρόπο μόνο και μόνο για να ικανοποιήσει ο κακοποιός τις δικέσ του ανάγκες και δεν σκέφτεται τις συνέπειές του.

Τα είδη των διαδικτυακών εκφοβισμών

- Ο διαδικτυακός εκφοβισμός περιλαμβάνει καταστάσεις όπως
- 1. Η αποστολή ανήθικων μυνημάτων.
- 2. Ο αποκλεισμός ατόμων από εφαρμογές συνομιλιών.
- 3. Το hacking ενός ξένου λογαριασμού.
- 4. Η διμοσίευση ενοχλητικών φωτογραφιών.
- 5. Διάδοση προσβλητικών φημών κ.ά.

Γνωστοί διαδικτυακοί εκφοβισμοί

- 1. Φωτογραφίες ακατάλληλου περιεχομένου.
- 2. Αποστολή απειλητικών μυνημάτων
- 3. Απειλή προσωπικών δεδομένων.
- 4. Ψεύτικα στειχοία ταυτότητας.

Τρόπους αντιμετώπισης

- 1. Αναγνώριση πραγματικών στοιχείων.
- 2. Το λέμε πάντα σε έναν μεγαλύτερο άνθρωπο π.χ. στους γονείς μας,στην δασκάλα μας ή ακόμη και στην αστυνομία.
- 3. Κάνουμε διαγραφή τον χρήστη ή το προφίλ μας.
- 4. Δεν αποκαλύπτουμε ποτέ το όνομα,το τηλέφωνό μας,ταχυδρομικό κώδικα κ.λ.

Τα sites όπου αναζήτησα

- 1. Stop-bullying
- 2.Wikipedia
- 3.Cyberbullying
- 4.SaferInternet4kids
- 5.Dimpapp

Διαδικτυακος εκφοβισμος

Παρουσιαση του κινδυνου αυτου και τροποι αντιμετωπισης

Συλβια Δ.

ΤΙ ΕΊΝΑΙ ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ

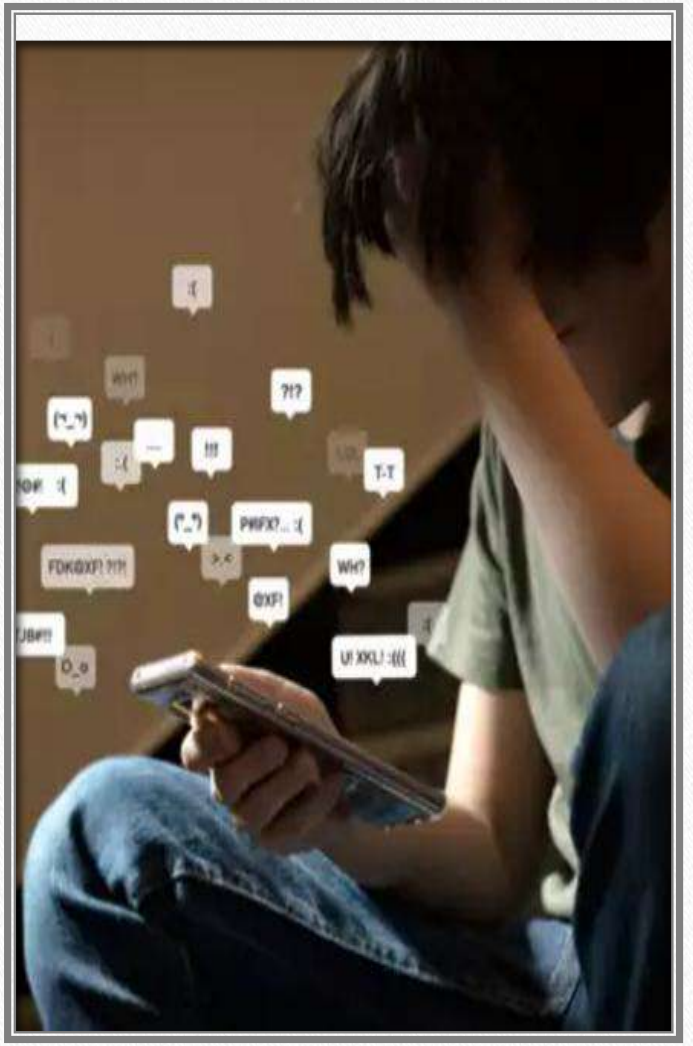
Ο όρος **διαδικτυακός εκφοβισμός** αφορά τον εκφοβισμό, την απειλή, την ταπείνωση ή την παρενόχληση παιδιών, προεφήβων και εφήβων που δέχονται μέσω της χρήσης του Διαδικτιου, κινητών τηλεφώνων είτε άλλων ψηφιακών τεχνολογιών από ομηλίκους τους.

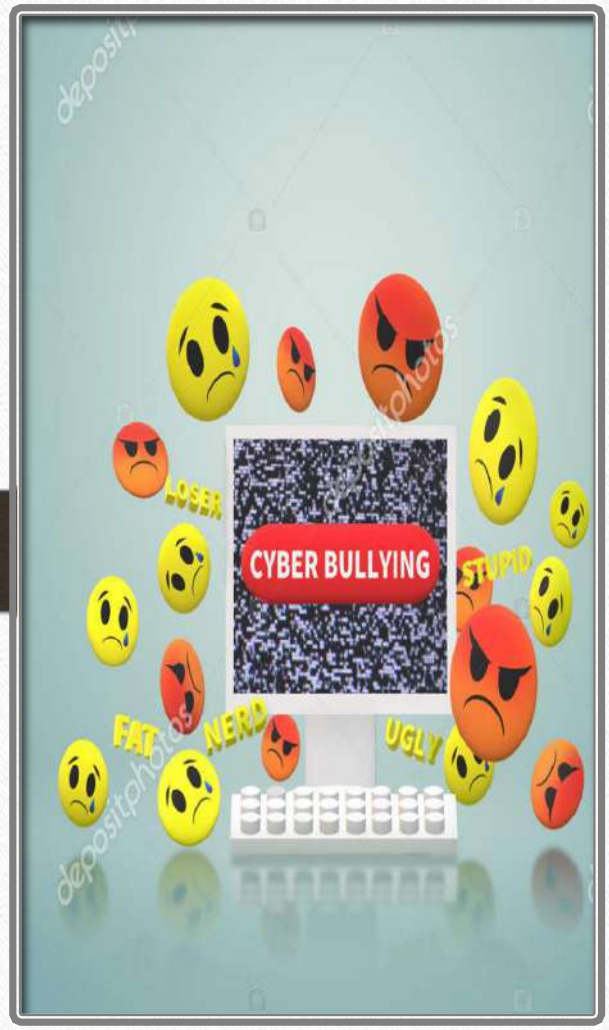
ΤΙ ΠΡΟΚΑΛΕΙ Ο ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ

Το φαινόμενο του Διαδικτυακού εκφοβισμού προκαλει 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. 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.

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 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





Η συχνότητα των απειλών

1. Η επικοινωνία πραγματοποιείται μόνο μια φορά
2. Η επικοινωνία επαναλαμβάνεται με ίδιο ή διαφορετικό τρόπο
3. Η επικοινωνιακή δραστηριότητα αυξάνεται
4. Τρίτα άτομα εμπλέκονται στην επικοινωνία με αποτέλεσμα το άτομο να λαμβάνει μηνύματα από διαφορετικούς παραλήπτες

[εβαλα αυτό γιατι δεν μπορουσα να βαλω γνωστοι διαδικτυακοι εκφοβισμοι]

Τροποι Αντιμετωπισης

- 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 ασ είτε σε κάποια αρμόδια υπηρεσία Δίωξης Ηλεκτρονικού εγκλήματος
- Αναφορά της περίστασης στον γονέα ή τον κηδεμόνα του ατόμου.

ΟΙ ΠΗΓΕΣ

- Διαδικτυακός εκφοβισμός - Βικιπαίδεια (wikipedia.org)

Διαδικτυακός εκφοβισμός

- ΒΑΣΙΛΗΣ Σ.

ΕΙΣΑΓΩΓΗ

- Ένα μεγάλο μέρος του νέου πληθυσμού έχει πέσει θύμα του διαδικτυακού εκφοβισμού. Είναι ένα φαινόμενο που όλο και αυξάνεται, για αυτό πρέπει να προσέχουμε και να δώσουμε πιο πολύ σημασία.

ΤΙ ΣΗΜΑΙΝΕΙ ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ

- Αλλά τι σημαίνει διαδικτυακός εκφοβισμός; Ο όρος αναφέρεται στον εκφοβισμό, την απειλή, την ταπείνωση ή την παρενόχληση παιδιών, προεφήβων και εφήβων που δέχονται μέσω της χρήσης του Διαδικτύου, κινητών τηλεφώνων είτε άλλων ψηφιακών τεχνολογιών από συνομηλίκους τους.
- Στον Διαδικτυακό εκφοβισμό παρατηρείται η συμμετοχή συνομηλίκων και από τις δύο πλευρές, ή τουλάχιστον η συμμετοχή ενός ενήλικα υποκινούμενη από κάποιον ανήλικο εναντίον άλλου ανηλίκου.

ΑΙΤΙΑ

- 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 στοχεύοντας στην εκδήλωση ποικίλων αντιδράσεων και στην ικανοποίηση αναγκών που σχετίζονται με την επιβολή εξουσίας και ελέγχου. Σπανιότερα, η αποστολή μηνυμάτων σε λάθος παραλήπτες μπορεί να αποτελέσει αιτία του φαινομένου

Τρόποι αντιμετώπισης

- Για να αντιμετωπίσουμε το cyber-bullying [διαδικτυακό εκφοβισμό], θέλει πρώτα Θάρρος.
- Και δεύτερο, να απευθυνθούμε στους σωστούς φορείς.
- Η καλύτερη προστασία είναι να γνωρίζουμε τους τρόπους αντιμετώπισης εκ των προτέρων. Καθώς αυτοί μπορούν να μας βοηθήσουν να διατηρήσουμε την περιήγηση μας με ασφαλεια στον κυβερνοχώρο.

- Παρακάτω θα σας αναφέρουμε μερικούς **τρόπους αντιμετώπισης** :
-
- 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 περίστασης στον γονέα ή τον κηδεμόνα του ατόμου.
- Μπορεί επίσης να ζητήσει βοήθεια μέσω της συμβουλευτικής γραμμής Βοήθειας Help-line (διαθέσιμη τηλεφωνικά στο 210-6007686 και μέσω του ιστοχώρου www.help-line.gr.
- Επίσης μέσω της ιστοσελίδας του, SaferInternet4Kids.gr μπορείς να ενημερωθείς και να αντλήσεις υλικό σχετικό με την ασφαλή χρήση του Ίντερνετ. Και της χρήσης των κοινωνικών δικτύων. Το ενημερωτικό αυτό portal απευθύνεται τόσο σε γονείς και εκπαιδευτικούς, όσο και σε εφήβους και παιδιά. Και περιλαμβάνει κατάλληλο υλικό
- πολυμέσων, το οποίο είναι εγκεκριμένο από το Υπουργείο Παιδείας και Θρησκευμάτων.
-

Παραβίαση προσωπικών δεδομένων

Αλέξης Κ.

ΕΙΣΑΓΩΓΗ

- Η αλματώδης ανάπτυξη του Ίντερνετ έχει αλλάξει ριζικά τη ζωή μας μιας και κανείς δεν μπορεί να αμφισβητήσει την επανάσταση που έχει φέρει στον τρόπο ζωής του σύγχρονου ανθρώπου.

- Παραβίαση δεδομένων έχουμε όταν τα δεδομένα για τα οποία είναι υπεύθυνη μία εταιρεία ή ένας οργανισμός προσβάλλονται από συμβάν ασφαλείας που έχει ως αποτέλεσμα παραβίαση της εμπιστευτικότητας, της διαθεσιμότητας ή της ακεραιότητας. Αν συμβεί αυτό και είναι πιθανό η παραβίαση να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες ενός ατόμου, η εταιρεία/οργανισμός πρέπει να ειδοποιήσει την εποπτική αρχή χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός 72 ωρών από τη στιγμή που έχει λάβει γνώση της παραβίασης. Εάν η εταιρεία ή ο οργανισμός σας είναι επεξεργαστής δεδομένων, πρέπει να ειδοποιήσει τον υπεύθυνο επεξεργασίας δεδομένων για την παραβίαση δεδομένων.

ΜΟΡΦΕΣ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

Υποκλοπή Προσωπικών Δεδομένων στο Διαδίκτυο

- Υποκλοπή Προσωπικών Δεδομένων στο Διαδίκτυο είναι η πράξη της εξαπάτησης ενός χρήστη κάνοντας τον να δώσει προσωπικές πληροφορίες σε μια «πλαστή ιστοσελίδα» στο Διαδίκτυο (π.χ. διεύθυνση, αριθμό ταυτότητας, αριθμό διαβατηρίου, αριθμούς τραπεζικών λογαριασμών, πιστωτικών καρτών κ.λπ.). Μια τέτοιου είδους δραστηριότητα επιτρέπει σε έναν απατεώνα (cracker) να κλέψει ή να πλαστογραφήσει τα στοιχεία του θύματος ή/και να κερδίσει παράνομη πρόσβαση στα δεδομένα του, όπως προσωπικούς λογαριασμούς, συνδρομές, e-mail, κωδικούς, κ.λπ.

- Τα προσωπικά σου δεδομένα είναι όλες οι πληροφορίες που αναφέρονται σε σένα. Είναι το όνομά σου, η διεύθυνσή σου, ο αριθμός του κινητού σου, το σχολείο στο οποίο πηγαίνεις, τα μέρη όπου συχνάζεις. Μερικές φορές τα προσωπικά σου δεδομένα αφορούν ιδιαίτερα ευαίσθητα στοιχεία της ιδιωτικής σου ζωής, όπως στο θρήσκευμά σου, στις πολιτικές σου πεποιθήσεις ή στην κατάσταση της υγείας σου και άλλα. Πολλές φορές, ιδιαίτερα στα κοινωνικά δίκτυα, δημοσιεύεις δεδομένα σου που μπορούν να χρησιμοποιηθούν από άτομα που δε γνωρίζεις με κακόβουλο σκοπό. Προσεκτικός πρέπει να είσαι όχι μόνο όταν δημοσιεύεις πληροφορίες για σένα τον ίδιο αλλά και πληροφορίες που αφορούν άλλα άτομα. Για να το κάνεις αυτό θα πρέπει να έχεις ΠΑΝΤΑ τη συγκατάθεσή τους. Διατηρώντας τον έλεγχο των προσωπικών μας δεδομένων ουσιαστικά διατηρούμε τον έλεγχο της ιδιωτικής μας ζωής.

ΠΕΡΙΓΡΑΦΗ

Συμβουλές για να παραμείνεις ασφαλής

- Προσέχουμε πάντα τα προσωπικά μας δεδομένα στο διαδίκτυο, συμπεριλαμβανομένου των φωτογραφιών και των βίντεο που δημοσιοποιούμε.
- Δε δημοσιεύουμε προσωπικά στοιχεία στο διαδίκτυο, όπως όνομα, τηλέφωνο, διεύθυνση, σε ποιο σχολείο πηγαίνουμε, ή πληροφορίες για την οικογένειά μας.
- Όταν μπαίνουμε σε ιστοχώρους που ζητούν προσωπικά στοιχεία, συμβουλευόμαστε πάντα κάποιον ενήλικα και διαβάζουμε τους «όρους χρήσης» του κάθε ιστοχώρου.
- Δε δίνουμε ποτέ τους κωδικούς μας σε κανέναν.
- Επιλέγουμε «δυνατούς» κωδικούς, αποτελούμενους από 8 τουλάχιστον χαρακτήρες.
- Χρησιμοποιώντας ψευδώνυμα σε ιστολόγια μπορούμε να προστατέψουμε την ταυτότητά μας.

- Θυμόμαστε ότι δεν είμαστε ποτέ αόρατοι στο διαδίκτυο. Όλοι οι χρήστες του διαδικτύου αφήνουν «ηλεκτρονικά αποτυπώματα».
- Δημιουργούμε ασφαλή προφίλ στις σελίδες κοινωνικής δικτύωσης. Ρυθμίζουμε το προφίλ μας, ώστε να μην είναι ορατό σε αγνώστους, και προσέχουμε να μη δεχόμαστε για διαδικτυακούς φίλους άτομα που δε γνωρίζουμε στον πραγματικό κόσμο.
- Θυμόμαστε ότι οτιδήποτε ανεβάζουμε στο Διαδίκτυο μπορεί να μείνει εκεί για πάντα! Αισθανόμαστε άνετα αν τις πληροφορίες ή φωτογραφίες που ανεβάζουμε στο διαδίκτυο τις δει ο δάσκαλός μας, ο μελλοντικός μας φίλος, ο μελλοντικός μας εργοδότης; Εάν η απάντηση είναι «όχι», τότε δε θα πρέπει να τις ανεβάζουμε.
- Σεβόμαστε και δεν δημοσιοποιούμε προσωπικά δεδομένα άλλων ατόμων χωρίς τη συγκατάθεσή τους.

Συμβουλές για να παραμείνεις ασφαλής

Παραβίαση προσωπικών δεδομένων

https://cybersafety.cy/

Ναταλία Τ.

Ορισμόςhttps://el.wikipedia.org/wiki/

- **Παραβίαση δεδομένων** είναι η σκόπιμη ή ακούσια διαρροή ασφαλών ή ιδιωτικών / εμπιστευτικών πληροφοριών σε μη αξιόπιστο περιβάλλον. Άλλοι όροι για αυτό το φαινόμενο περιλαμβάνουν **ακούσια αποκάλυψη πληροφοριών**, **διαρροή δεδομένων** και **διαρροή πληροφοριών**. Τα περιστατικά παραβίασης κυμαίνονται από εναρμονισμένες επιθέσεις από μαύρα καπέλα, ή άτομα που χακάρουν για προσωπικό κέρδος, που σχετίζονται με το οργανωμένο έγκλημα, τον πολιτικό ακτιβισμό ή τις εθνικές κυβερνήσεις έως την απρόσεκτη απόρριψη μεταχειρισμένου εξοπλισμού υπολογιστών ή μέσων αποθήκευσης δεδομένων.

Τι κινδύνους έχει? https://cybersafety.cy/

- Η παραβίαση προσωπικών δεδομένων έχει ως αποτέλεσμα τη δημόσια έκθεση της προσωπικής μας ζωής, χωρίς να έχουμε την δυνατότητα να ελέγξουμε από ποιον και πως αυτές οι πληροφορίες θα χρησιμοποιηθούν(π.χ. κλοπή ταυτότητάς μας , χρήση των πληροφοριών αυτών για προσβολή

Κοινωνικά δίκτυαhttps://cybersafety.cy/

- Από την ηλικία των 14 ετών, μπορεί ένα παιδί να αναλάβει υπεύθυνα την εγγραφή του σε υπηρεσίες κοινωνικής πληροφόρησης (π.χ

  Facebook,Twitter,Tiktok,Instagram).
- Πριν από την ηλικία των 14 ετών, είναι απαραίτητη η συγκατάθεση των γονέων ή κηδεμόνων, εφόσον αυτό επιτρέπεται ηλικιακά, από τις υπηρεσίες κοινωνικής πληροφορίας.

Συμβουλές για την προστασίαhttps://cybersafety.cy/

- Προσέχω, όταν δημοσιεύω προσωπικά στοιχεία στο Διαδίκτυο, όπως τηλέφωνο, διεύθυνση, σε ποιο σχολείο πηγαίνω ή *πληροφορίες για την οικογένειά μου.*
- Δεν επικοινωνώ ή δίνω προσωπικές πληροφορίες σε άγνωστα πρόσωπα. Πίσω από ένα άγνωστο διαδικτυακό προφίλ, δεν μπορώ να είμαι βέβαιος για την ταυτότητα του ατόμου με το οποίο επικοινωνώ.

Ευχαριστω για την παρακολουθηση Ναταλια Τ. Στ1

- ΣΜΑΡΑΓΔΑ Μ.

ΠΑΡΑΒΊΑΣΗ ΠΡΟΣΩΠΙΚΏΝ ΔΕΔΟΜΈΝΩΝ

ΕΙΣΑΓΩΓΉ

- Ορισμός της παραβίασης προσωπικών δεδομένων: Μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη ή απώλεια ευαίσθητων προσωπικών πληροφοριών.
- Σημασία της ασφάλειας δεδομένων: κρίσιμης σημασίας για τη διαφύλαξη της ιδιωτικής ζωής των ατόμων και την πρόληψη της κακής χρήσης.
- Στατιστικά στοιχεία για την άνοδο των παραβιάσεων δεδομένων: Παρουσιάστε τις πρόσφατες τάσεις για να τονίσετε τον επείγοντα χαρακτήρα του ζητήματος.

ΠΏς ΧΡΗΣΙΜΟΠΟΙΟΎΝΤΑΙ ΤΑ ΠΡΟΣΩΠΙΚΆ ΜΟΥ ΔΕΔΟΜΈΝΑ

- Πολλές από τις καθημερινές σου δραστηριότητες βασίζονται στην επεξεργασία των προσωπικών σου δεδομένων:
- Η φόρμα που συμπληρώνεις για συμμετοχή στον διαγωνισμό της εταιρείας ηλεκτρονικών παιχνιδιών περιέχει προσωπικά σου στοιχεία, όπως όνομα, τηλέφωνο, διεύθυνση και ηλικία.
- 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.
- Ο γιατρός που επισκέφτηκες τηρεί τις ιατρικές σου εξετάσεις και άλλα σχετικά στοιχεία για την υγεία σου.
- Ο αθλητικός σύλλογος στον οποίο είσαι μέλος τηρεί τα στοιχεία που έδωσες κατά την εγγραφή σου, καθώς και ιατρικά πιστοποιητικά.
- 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.
- Η εφαρμογή που «κατέβασες» στο «έξυπνο» κινητό σου αποκτά πρόσβαση σε πολλά προσωπικά σου δεδομένα.

ΕΊΝΑΙ ΔΥΝΑΤΌΝ ΤΑ ΠΡΟΣΩΠΙΚΆ ΜΟΥ ΔΕΔΟΜΈΝΑ ΝΑ ΧΡΗΣΙΜΟΠΟΙΗΘΟΎΝ… ΕΝΑΝΤΊΟΝ ΜΟΥ

- Αν δεν προσέξεις πώς και πού τα δημοσιοποιείς 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 θα θέλεις να σπουδάσεις στο πανεπιστήμιο ή να πάρεις δάνειο από μια τράπεζα. Σε ακραίες περιπτώσεις μπορεί να πέσεις ακόμα και θύμα υποκλοπής ταυτότητας (δηλαδή κάποιος που έχει τα δεδομένα σου μπορεί να προσποιείται ότι είσαι εσύ) ή θύμα παρενόχλησης και εξαπάτησης.

ΠΌΤΕ ΕΠΙΤΡΈΠΕΤΑΙ ΚΆΠΟΙΟς ΝΑ ΧΡΗΣΙΜΟΠΟΙΕΊ ΤΑ ΠΡΟΣΩΠΙΚΆ ΜΟΥ ΔΕΔΟΜΈΝΑ;

- Στην Ελλάδα, όπως και στις υπόλοιπες χώρες της Ευρωπαϊκής Ένωσης, υπάρχει ειδική νομοθεσία που προστατεύει τα άτομα από την ανεξέλεγκτη χρήση των προσωπικών τους δεδομένων. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι ο αρμόδιος φορέας για την εφαρμογή αυτής της νομοθεσίας (Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) & ν. 4624/2019).
- Ως βασικός κανόνας ισχύει ότι για να χρησιμοποιήσει κάποιος τα προσωπικά σου δεδομένα για έναν συγκεκριμένο σκοπό πρέπει να έχει εξασφαλίσει τη συγκατάθεσή σου και, σε αρκετές περιπτώσεις, τη συναίνεση των γονιών σου(βλ. στη συνέχεια). Με αυτό εννοούμε ότι, αφού προηγουμένως έχεις ενημερωθεί ακριβώς για το ποιος είναι αυτός που θέλει να χρησιμοποιήσει τα δεδομένα σου, για ποιον λόγο θέλει να τα χρησιμοποιήσει, ποια στοιχεία σου θέλει να πάρει και με ποιους θα τα μοιραστεί, έχεις δεχθεί και έχεις πει με σαφή τρόπο ότι συμφωνείς.

- **Προσοχή**: Σε τυπικές υπηρεσίες διαδικτύου (κοινωνικά δίκτυα, διαδικτυακά παιχνίδια, κ.λπ.) ελλοχεύουν σημαντικοί κίνδυνοι για τα προσωπικά δεδομένα, αφού ενδεχομένως να υπάρχουν «κρυφοί» σκοποί σχετικά με δημιουργία προφίλ προσωπικότητάς σου, εμπορίας προσωπικών σου δεδομένων κ.ά. Γι΄ αυτόν το λόγο, όχι μόνο απαιτείται η ρητή συγκατάθεσή σου κατόπιν πλήρους ενημέρωσης για το τι ακριβώς επεξεργασία πρόκειται να συμβεί στα δεδομένα σου, αλλά επιπλέον θα πρέπει να είσαι τουλάχιστον 15 ετών: διαφορετικά, απαιτείται –για αυτές τις υπηρεσίες– **συγκατάθεση του γονέα σου**.
- Η συγκατάθεση είναι ο γενικός κανόνας για όλες τις περιπτώσεις, αλλά υπάρχουν και εξαιρέσεις. Για παράδειγμα κάποιοι οργανισμοί, όπως π.χ. ο δήμος ή το σχολείο σου, μπορούν να επεξεργάζονται συγκεκριμένα προσωπικά δεδομένα χωρίς τη συγκατάθεσή σου. Αυτό συμβαίνει γιατί τα δεδομένα σου είναι απαραίτητα για να εκτελέσουν το έργο τους και αυτό συνήθως ορίζεται σε κάποιο νόμο. Επίσης, σε κάποιες περιπτώσεις τα προσωπικά σου δεδομένα είναι απαραίτητα για να λάβεις ένα προϊόν ή μια υπηρεσία, όπως όταν παραγγέλνεις μια συσκευή μέσω διαδικτύου και την παραλαμβάνεις στο σπίτι σου.

ΠΟΙΑ ΕΊΝΑΙ ΤΑ ΔΙΚΑΙΏΜΑΤΑ ΜΟΥ ΣΕ ΣΧΈΣΗ ΜΕ ΤΑ ΠΡΟΣΩΠΙΚΆ ΜΟΥ ΔΕΔΟΜΈΝΑ;

- Όταν κάποιος σου ζητά να του δώσεις προσωπικά σου δεδομένα, έχεις το δικαίωμα να γνωρίζεις ακριβώς την ταυτότητά του, τον σκοπό για τον οποίο χρειάζεται τα δεδομένα σου, σε ποιους θα τα στείλει, καθώς και ποιοι θα έχουν πρόσβαση σε αυτά.Σε διαδικτυακή υπηρεσία, απαιτείται η συναίνεση του γονέα σου σε κάθε περίπτωση **αν είσαι κάτω των 15 ετών**.
- Έχεις το δικαίωμα να γνωρίζεις ποια δεδομένα τηρούν οι άλλοι (οργανισμοί ή άτομα) για σένα και μπορείς να τους ζητάς να σε ενημερώνουν γι' αυτό.
- Έχεις το δικαίωμα να ζητάς τη διαγραφή ή τη διόρθωση των προσωπικών σου δεδομένων, όταν θεωρείς ότι η πληροφορία αυτή σε θίγει ή είναι λανθασμένη ή όταν διαφωνείς με την επεξεργασία αυτών των δεδομένων.

ΠΗΓΕΣ

- https://www.dpa.gr/el/foreis/asfaleia_dedomenwn/gnwstopoiisi_paraviasis
- https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_el
- https://www.nb.org/blog/post/ypdik-parabiasi-eyais8htwn-prosopikon-dedomenon-stoixeia-ths-antikeimenikis-ipostasis
- https://www.aon.com/greece/articles/data-breach.jsp
- https://www.lawspot.gr/nomika-nea/paraviasi-prosopikon-dedomenon-nees-kateythyntiries-grammes-gia-tis-gnostopoiiseis-apo

ΑΠΑΤΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Παναγιώτης Μ.

ΤΙ ΕΙΝΑΙ Η ΑΠΑΤΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Ως **απάτη στο διαδίκτυο** αναφέρεται η εγκληματική δραστηριότητα μέσω κακόβουλου λογισμικού που στοχεύει κάποια συσκευή (υπολογιστή, κινητό τηλέφωνο, δίκτυο υπολογιστών), και ως κύριο στόχο έχει την απόσπαση χρημάτων από το θύμα.

Μερικά παραδείγματα είναι:

HACKING

Μέσω του hacking, οι κυβερνοεγκληματίες (Hackers) αποκτούν πρόσβαση στους λογαριασμούς ηλεκτρονικού ταχυδρομείου και κοινωνικών δικτύων των χρηστών. Έτσι μπορούν είτε να αποσπάσουν ευαίσθητα προσωπικά δεδομένα ή χρήματα αλλά και να στείλουν κακόβουλα μηνύματα εκ μέρους του χρήστη, ψάχνοντας κι άλλα θύματα.

PHISHING

Η πρακτική αυτή είναι γνωστή και ως ηλεκτρονικό ψάρεμα και περιγράφει την διαδικτυακή απάτη που σκοπό έχει να αποσπάσει κωδικούς ασφαλείας και μυστικούς κωδικούς για διαδικτυακές συναλλαγές. Το Phishing μπορεί να περιλαμβάνει από ηλεκτρονικά μηνύματα και sms (το λεγόμενο smishing) έως πλαστές ιστοσελίδες, μια πολύ κοινή πρακτική που συνεχώς εξελίσσεται για να γίνεται πιο πειστική.

SIM SWAPPING

Η πρακτική αυτή αποτελεί επίσης μία διαδικτυακή απάτη και σχετίζεται με το Phishing και συμβαίνει όταν ένας εγκληματίας αποκτά αντίγραφο της κάρτας SIM ενός χρήστη και προχωρά σε πλαστοπροσωπία, αποκτώντας έλεγχο στον αριθμό τηλεφώνου του θύματος. Η πρακτική αυτη είναι ιδιαίτερα επικίνδυνη καθώς ο εγκληματίας αποκτά πρόσβαση σε όλες τις πληροφορίες και τα δεδομένα του θύματος, με αποτέλεσμα την πρόσβαση σε τραπεζικούς λογαριασμούς, καθώς με τον έλεγχο του κινητού τηλεφώνου μπορεί να χρησιμοποιήσει κωδικούς επαλήθευσης.

RANSOMWARE

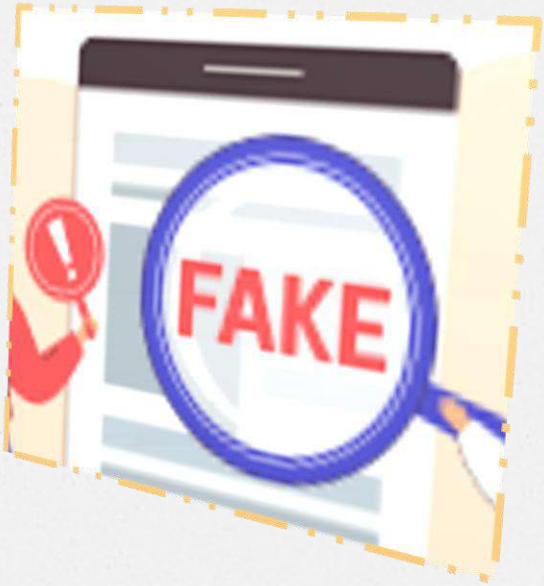
Με αυτή την πρακτική οι κυβερνοεγκληματίες ζητούν εκβιαστικά χρήματα μετά από μια κυβερνοεπίθεση για να απελευθερώσουν κλειδωμένα συστήματα ή αρχεία, ή για να μην δημοσιεύσουν ιδιωτικό υλικό. Μπορεί να συμβεί τόσο σε ιδιώτες όσο και σε μεγάλους οργανισμούς και εταιρείες.

ΤΕΛΟΣ

Άλλες απειλές περιλαμβάνουν την παράνομη παρακολούθηση ή υποκλοπή δεδομένων, την παραβίαση πνευματικών δικαιωμάτων και άλλα.

Για την αντιμετώπιση των παραπάνω από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος του Αρχηγείου Ελληνικής Αστυνομίας, τέθηκε σε λειτουργία το τηλεφωνικό κέντρο Cyberalert, μέσω του πανελλαδικού αριθμού κλήσης 111 88.

Απάτες στο διαδίκτυο



Μαρία-Εφραιμία Β.

Εισαγωγή…

Όπως συμβαίνει στον πραγματικό κόσμο έτσι και στο διαδίκτυο υπάρχουν απατεώνες που προσπαθούν να παραβιάσουν τα προσωπικά δεδομένα (διεύθυνση, τηλέφωνο, επίθετο κ.α.) ή και να παραβιάσουν τον αριθμό μιας κάρτας για να πάρουν τα χρήματα πολλών ανθρώπων.

Τι είναι οι Διαδικτυακές απάτες;

Η **διαδικτυακή απάτη** είναι τύπος απάτης ή εξαπάτησης του ηλεκτρονικού εγκλήματος που χρησιμοποιεί το Διαδίκτυο και μπορεί να περιλαμβάνει απόκρυψη πληροφοριών ή παροχή εσφαλμένων πληροφοριών με σκοπό την εξαπάτηση των θυμάτων για την απόσπαση χρημάτων, περιουσίας και κληρονομιάς.

Είδη από απάτες

- Spamming
- Διαδικτυακή απάτη που υπόσχεται δωρεάν αεροπορικά εισιτήρια.
- Phishing προσωπικών δεδομένων.
- Απάτες με αγορές
- Απάτες με διαγωνισμούς
- Τηλεφωνικές απάτες

Τρόποι αντιμετώπισης

- Επιλέξτε κωδικούς πρόσβασης και PIN που θα ήταν δύσκολο να μαντέψουν οι άλλοι και αλλάζετέ τα τακτικά. Μην τα αποθηκεύετε στο τηλέφωνο ή τον υπολογιστή σας.
- Αν λάβετε κάποιο ύποπτο email κάντε μια αναζήτηση στο Διαδίκτυο χρησιμοποιώντας τα ονόματα ή την ακριβή διατύπωση του email ή του μηνύματος για να ελέγξετε για τυχόν αναφορές σε απάτη – πολλές απάτες μπορούν να εντοπιστούν με αυτόν τον τρόπο.

Τρόποι αντιμετώπισης

- Μην ανοίγετε συνημμένα και μην κάνετε κλικ σε συνδέσμους σε μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα κοινωνικής δικτύωσης που έχετε λάβει από αγνώστους – απλώς πατήστε διαγραφή.
- Χρησιμοποιήστε το λογισμικό ασφαλείας σας για να εκτελέσετε έλεγχο κακόβουλου λογισμικού εάν πιστεύετε ότι η ασφάλεια του υπολογιστή σας έχει παραβιαστεί.

Πηγές

- https://cyberalert.gr/apates-meso-diadiktiou/
- https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%B9%CE%BA%CF%84%CF%85%CE%B1%CE%BA%CE%AE_%CE%B1%CF%80%CE%AC%CF%84%CE%B7
- https://www.kathimerini.gr/life/technology/561813544/se-exarsi-oi-apates-meso-diadiktyoy-stin-ellada-ta-10-vimata-gia-na-prostateytoyme/

ΤΕΛΟΣ

ΑΠΑΤΕΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Απο τον Αλεξ

HACKERS

Οι χάκερ είναι άτομα που χρησιμοποιούν τις δεξιότητές τους στον προγραμματισμό και στον υπολογιστή για να αποκτήσουν μη επιτρεπομενα πρόσβαση σε συστήματα ή δίκτυα. Υπάρχουν διάφοροι τύποι χάκερ...
Είναι ένας τεράστιος και πολύπλοκος κόσμος και τα κίνητρα πίσω από το hacking μπορεί να διαφέρουν πολύ. Τα μέτρα κυβερνοασφάλειας είναι ζωτικής σημασίας για την προστασία από μη εξουσιοδοτημένη πρόσβαση και παραβιάσεις δεδομένων.

Black Hat Hackers: Αυτοί είναι οι «κακοί» που χακάρουν με κακόβουλη πρόθεση, όπως η κλοπή δεδομένων, η διάδοση κακόβουλου λογισμικού ή η πρόκληση διαταραχών.

White Hat Hackers: Τα «καλά παιδιά» που χρησιμοποιούν τις δεξιότητές τους για να βοηθήσουν τους οργανισμούς να ενισχύσουν την ασφάλειά τους. Συχνά εργάζονται στον τομέα της κυβερνοασφάλειας και του ηθικού hacking.

- Gray Hat Hackers: Κάπου στο ενδιάμεσο, αυτοί οι χάκερ μπορεί να μην έχουν κακόβουλη πρόθεση, αλλά εξακολουθούν να εισβάλλουν σε συστήματα χωρίς την κατάλληλη εξουσιοδότηση.

- Script Kiddies: Αυτά είναι συνήθως άτομα με μικρότερη εξειδίκευση που χρησιμοποιούν προκαθορισμένο λογισμικό ή σενάρια για να χακάρουν. Συχνά δεν καταλαβαίνουν την τεχνολογία, αλλά χρησιμοποιούν εργαλεία που έχουν δημιουργηθεί από άλλους.
- Χακτιβιστές: Αυτοί οι χάκερ υποκινούνται από κοινωνικούς ή πολιτικούς λόγους. Χρησιμοποιούν τις δεξιότητές τους για να προωθήσουν την ατζέντα τους ή για να διαμαρτυρηθούν

SCAMMERS

Οι scammers είναι άτομα ή ομάδες που εξαπατούν άλλους για να κερδίσουν κάτι, συχνά χρήματα ή προσωπικές πληροφορίες. Ακολουθούν ορισμένοι συνήθεις τύποι απάτης... Είναι απαραίτητο να είστε σε εγρήγορση, να επαληθεύετε την ταυτότητα άγνωστων επαφών και να χρησιμοποιείτε ασφαλή κανάλια για ευαίσθητες πληροφορίες για να αποφύγετε να πέσετε θύματα απάτης. Αν κάτι φαίνεται πολύ καλό για να είναι αληθινό, μάλλον είναι!

Ψάρεμα: Οι απατεώνες στέλνουν πλαστά email, μηνύματα ή ιστότοπους που φαίνονται νόμιμοι

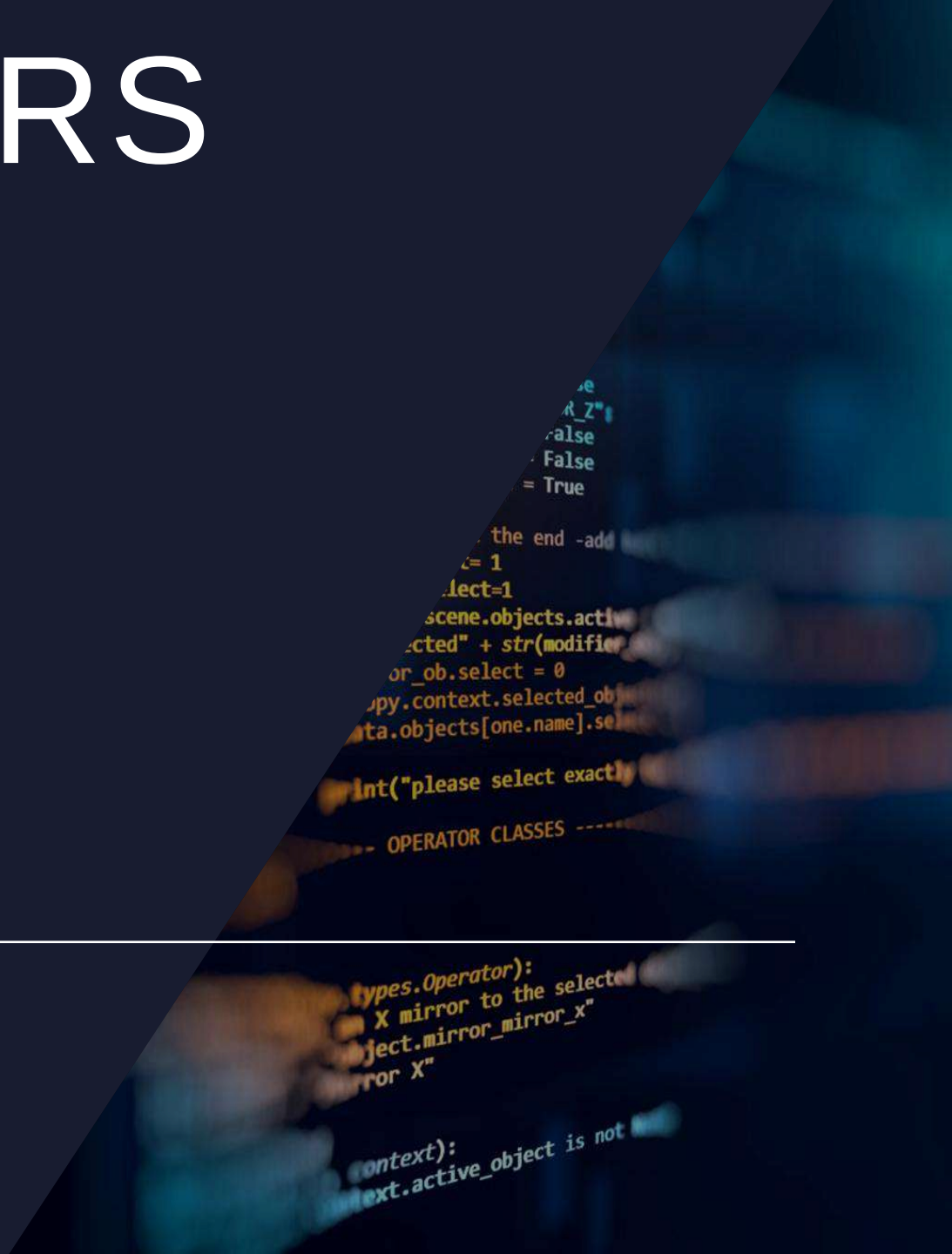
όπως κωδικούς πρόσβασης ή στοιχεία πιστωτικών καρτών.

Απομίμηση: Οι απατεώνες μπορεί να παρουσιάζονται ως κάποιος άλλος, όπως κυβερνητικός αξιωματούχος, τεχνική υποστήριξη ή μέλος της οικογένειας, για να χειραγωγήσουν τα θύματα ώστε να στείλουν χρήματα ή να αποκαλύψουν προσωπικές πληροφορίες.

- **Απάτες διαδικτυακών αγορών:**
- **Τα ψεύτικα ηλεκτρονικά καταστήματα μπορεί να προσφέρουν δελεαστικές προσφορές για προϊόντα, αλλά ποτέ να μην παραδίδουν τα αγαθά ή να παρέχουν προϊόντα κατώτερης ποιότητας.**
- Απάτες με λαχεία ή έπαθλα: Τα θύματα ενημερώνονται ότι έχουν κερδίσει μια λαχειοφόρο αγορά ή ένα έπαθλο, αλλά πρέπει να πληρώσουν τέλη ή να παράσχουν προσωπικές πληροφορίες για να το διεκδικήσουν - δεν υπάρχει πραγματικό βραβείο.

SPAMMERS

Οι Spammers είναι οι πιο καλοί απο τους τρείς επειδή
το μονο κακό που κάνουν είναι να σε ενοχλούν



ΤΕΛΟΣ

Ευχαριστώ που το είδατε

ΙΟΙ

ΕΝΑΣ ΚΙΝΔΥΝΟΣ
ΤΟΥ ΔΙΑΔΥΚΤΙΟΥ

ΤΙ ΕΙΝΑΙ ΕΝΑΣ ΙΟΣ;

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. 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. 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).

ΤΡΟΠΟΙ ΔΙΑΔΟΣΗΣ ΕΝΟΣ ΙΟΥ

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.

ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΕΝΟΣ ΙΟΥ

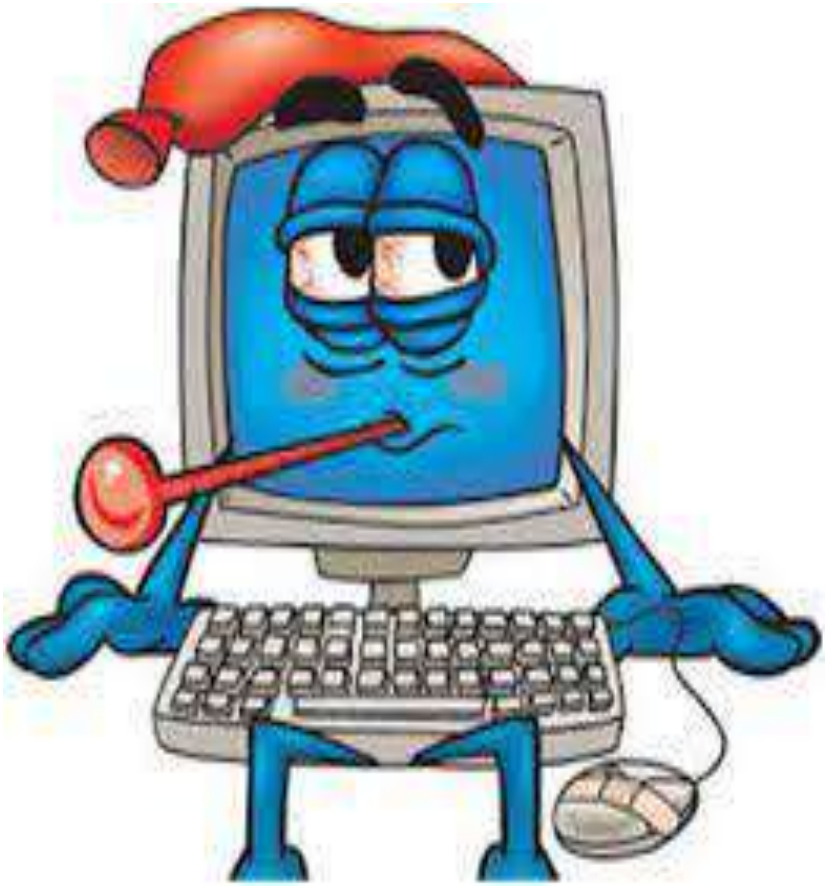
Οι ιοί αποτέλεσαν και αποτελούν έναν από τους πλέον διαδεδομένους τύπους κακόβουλου λογισμικού. Η ανίχνευση τους από τον απλό χρήστη είναι από δύσκολη έως αδύνατη, ορισμένοι μάλιστα ιοί είναι τόσο προσεκτικά δημιουργημένοι που ακόμη και ο πλέον ειδικευμένος χρήστης αδυνατεί να τους εντοπίσει χωρίς να 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. Οι δημιουργοί ιών λαμβάνουν υπόψη τις μεθόδους εντοπισμού και προσπαθούν να τις εξουδετερώσουν ακόμη και με απενεργοποίηση του αντιϊκού. Αυτό σημαίνει ότι ο χρήστης θα πρέπει να ενημερώνει συχνά το λογισμικό του αλλά και να δημιουργεί τις ειδικές δισκέτες, που τα περισσότερα αντιβιοτικά προγράμματα προτείνουν τη δημιουργία τους, ώστε να είναι δυνατή η εκκαθάριση και η επαναφορά του συστήματος μετά από τυχόν μόλυνσή τους. Βέβαια σε περίπτωση που το antivirus που έχουμε εγκαταστήσει στον υπολογιστή μας δεν μπορεί να αντιμετωπίσει τον ιό, μπορούμε να κάνουμε Format, δηλαδή να κάνουμε διαγραφή όλων των δεδομένων του υπολογιστή, είτε από μόνοι μας είτε να τον πάμε σε κάποιο ειδικό κατάστημα για να μας το κάνουν.

Ιοί υπολογιστών

Εργασία στο μάθημα της Πληροφορικής

του μαθητή του τμήματος ΣΤ1

Νικόλαου Λ.



Τι είναι ιός υπολογιστή

- 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.
- Οι ιοί δεν πρέπει να συγχέονται με τα «σκουλήκια» υπολογιστών (worms) και τους δούρειους ίππους (trojan horses).
- Οι ιοί μπορούν να εκμεταλλευθούν τις υπηρεσίες του Διαδικτύου, όπως το World Wide Web, το ηλεκτρονικό ταχυδρομείο και την υπηρεσία συνομιλιών (Internet Relay Chat, IRC).

Προβλήματα που δημιουργούν οι ιοί στους υπολογιστές

- Κάποιοι ιοί προξενούν 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 ζημία, αλλά απλά γνωστοποιούν την παρουσία τους με την εμφάνιση στην οθόνη κειμένου, βίντεο, ή ηχητικών μηνυμάτων, μερικές φορές αρκετά χιουμοριστικών.
- Τέλος, ένα μεγάλο ποσοστό των ιών δεν έχει σκοπό την καταστροφή των δεδομένων του χρήστη ή την παρενόχλησή του, αλλά την κλοπή προσωπικών του δεδομένων ή την εισαγωγή του υπολογιστή-στόχου σε κάποιο παράνομο δίκτυο (botnet) χωρίς τη συγκατάθεση του χρήστη.

Ιστορική αναδρομή

- Ιός ανιχνεύθηκε για πρώτη φορά στο ARPANET, τον πρόδρομο του Διαδικτύου στις αρχές της δεκαετίας του 1970. Εμφάνιζε το μήνυμα "I'M THE CREEPER! CATCH ME IF YOU CAN". Σε σύντομο χρονικό διάστημα, ωστόσο, εμφανίστηκε ένα πρόγραμμα, το οποίο αποκαλούσε εαυτόν "Reaper", ανώνυμου δημιουργού, το οποίο ανίχνευε τον CREEPER στους υπολογιστές που είχε μολύνει και τον διέγραφε.

- 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 (Richard Skrenta) για υπολογιστές Apple II με λειτουργικό σύστημα το Apple DOS 3.3. Τον αποθήκευσε σε μια δισκέτα και την έδωσε σε φίλους και γνωστούς του. Οι περισσότεροι υπολογιστές, εκείνη την εποχή, δε διέθεταν σκληρό δίσκο κι έτσι οι ανταλλαγές δισκετών ήταν πολύ συχνές. Όταν ο υπολογιστής εκκινούσε από τη μολυσμένη δισκέτα αντιγραφόταν μόνος του σε όποια άλλη δισκέτα είχε εκείνη τη στιγμή πρόσβαση ο υπολογιστής.

- Ο πρώτος ιός που εμφανίστηκε στους προσωπικούς υπολογιστές ήταν ο ιός Brain (γνωστός και ως Ashar, (C)Brain, Clone, Nipper, Pakistani, Lahore, Pakistani flu, Pakistani Brain). Δημιουργήθηκε στο Πακιστάν το 1986 από τους αδελφούς Basit και Amjad Farooq Alvi. Προσέβαλε τον τομέα εκκίνησης (boot sector) του σκληρού δίσκου.

Κατηγορίες

Οι ιοί μπορούν να ταξινομηθούν σε δύο μεγάλες κατηγορίες:

- 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)

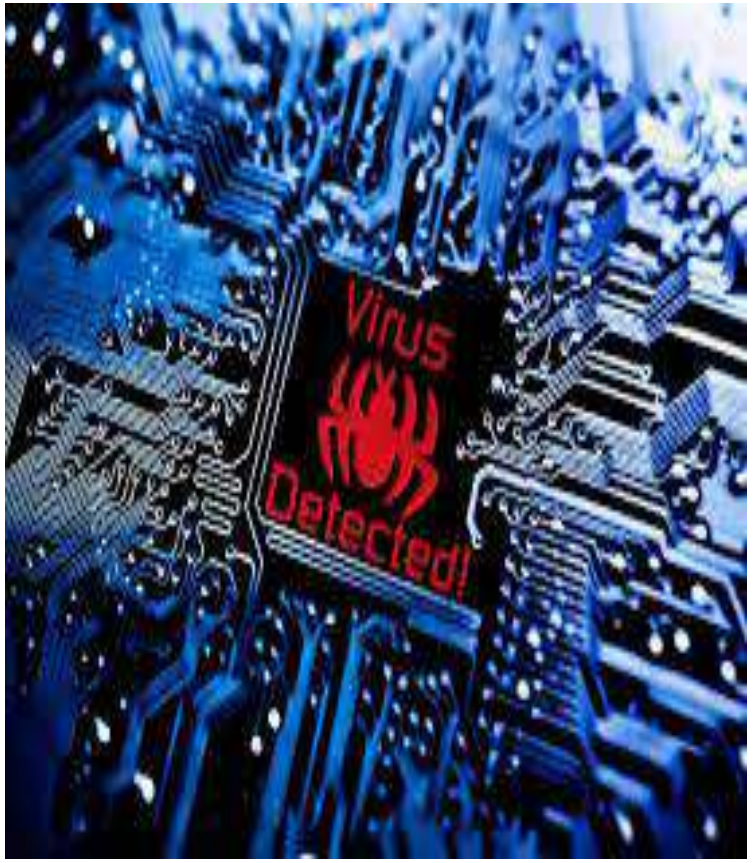
Πολυτμηματικοί ιοί (Multipartite Viruses)

Ιοί πλήρωσης κενών (Spacefiller Viruses)

Ιοί παραλλαγής (Camouflage Viruses) [5].

Προϋποθέσεις δράσης

- Πρέπει να μπορεί να εκτελέσει τον κώδικά του και να εξασφαλίσει πρόσβαση σε μέσα αποθήκευσης (κύρια στο σκληρό δίσκο, αλλά όχι μόνο).
- Πρέπει να μπορεί να προσκολλάτε σε εκτελέσιμα (executable) αρχεία είτε του λειτουργικού συστήματος είτε του κανονικού λογισμικού ενός συστήματος.
- Πρέπει να μπορεί να αναπαραχθεί και να εκτελεί τον κώδικά του.



Διάδοση ιών

Οι ιοί διαδίδονται από τον ένα υπολογιστή στον άλλο με δύο τρόπους:

- Είτε μέσω φορητού μέσου αποθήκευσης, είτε μέσω δικτύου.
- Είτε μέσω του Διαδικτύου. 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.

Τρόποι αντιμετώπισης

- Για την προστασία ενός συστήματος έχει δημιουργηθεί μια ειδική κατηγορία λογισμικού, γνωστή ως αντιϊκό (antivirus). 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.
- Βέβαια σε περίπτωση που το antivirus που έχουμε εγκαταστήσει στον υπολογιστή μας δεν μπορεί να αντιμετωπίσει τον ιό, μπορούμε να κάνουμε Format είτε από μόνοι μας είτε να πάμε τον υπολογιστή μας σε κάποιο ειδικό κατάστημα για να μας κάνουν Format.

Παιχνίδια στο διαδίκτυο

ΜΑΡΙΝΟΣ

ΕΙΣΑΓΩΓΗ

- Από τα παιχνίδια που σχετίζονται με τα σπορ, μέχρι τα παιχνίδια που έχουν συγκεκριμένες αποστολές που πρέπει να πετύχει ο χρήστης, τα διαδικτυακά παιχνίδια καλύπτουν ένα ευρύ φάσμα ενδιαφερόντων, ενώ επιτρέπουν τη συνεργασία των χρηστών μεταξύ τους

- . Τα διαδικτυακά παιχνίδια και οι εφαρμογές παρέχουν μία διασκεδαστική και κοινωνική μορφή διασκέδασης, ενθαρρύνοντας την ομαδικότητα και τη συνεργασία. Υπάρχουν πολλοί τρόποι για να παίξεις στο διαδίκτυο. Μερικοί από αυτούς είναι τα παιχνίδια που κυκλοφορούν δωρεάν στο ίντερνετ, τα παιχνίδια ή οι εφαρμογές στο κινητό και σε φορητές κονσόλες, καθώς επίσης τα παιχνίδια που αγοράζει κανείς για τον υπολογιστή και άλλες κονσόλες, όπως το PlayStation, το Nintendo ή το Xbox.
- Οι συμβουλές ασφάλειας για το ίντερνετ είναι άμεσα εφαρμόσιμες στο περιβάλλον των παιχνιδιών λόγω των κινδύνων που ενέχονται. Είναι σημαντικό τα παιδιά να γνωρίζουν για αυτούς τους κινδύνους και να αποκτήσουν τις ικανότητες και τις γνώσεις για τον περιορισμό τους.
- Όπως κάθε τι έτσι και τα ηλεκτρονικά παιχνίδια έχουν τα υπέρ και τα κατά τους. Πιο συγκεκριμένα υπάρχουν αρκετά οφέλη από την ενασχόληση των παιδιών με τα ηλεκτρονικά παιχνίδια.

Τι νέο υπάρχει στο online gaming;

Παιχνίδια εικονικής πραγματικότητας

Παιχνίδια όπως το Google Cardboard ή το Occulus Rift, προσθέτουν μία ακόμα διάσταση στο online gaming, καθώς επιτρέπουν στο χρήστη να βυθιστεί σε μία εμπειρία που μοιάζει αληθινή, διεγείροντας την ακοή ή την όρασή τους. Συνήθως, ο παίκτης θα πρέπει να φορά ένα ακουστικό για να βιώσει την εμπειρία των εικονικών παιχνιδιών πραγματικότητας.

Παιχνίδια επαυξημένης πραγματικότητας

Αυτό το είδος παιχνιδιών διαδίδονται όλο και περισσότερο, με παιχνίδια να οδηγούν τους χρήστες από το σπίτι στους δρόμους, ενώ παράλληλα παίζουν. Τα παιχνίδια επαυξημένης πραγματικότητας λειτουργούν με ηλεκτρονικές αναβαθμίσεις στην υπάρχουσα πραγματικότητα, επιτρέποντας στους παίκτες να αλληλεπιδρούν με αυτή. Οι παίκτες θα «δουν» πράγματα, τα οποία αντιλαμβάνονται ότι δεν είναι αληθινά, αλλά τους βοηθούν να συνεχίσουν το παιχνίδι.

Κίνδυνοι

ΕΘΙΣΜΟΣ

Τα διαδικτυακά παιχνίδια μπορούν συχνά να **εθίσουν** τα παιδιά. Απορροφούνται τόσο πολύ από τις κοινότητες των παιχνιδιών που χάνουν την επαφή με τους φίλους τους στο φυσικό κόσμο και διαθέτουν το χρόνο τους στους διαδικτυακούς τους φίλους. Πολλοί σπαταλούν πολλές ώρες τη νύχτα παίζοντας, ειδικά μετά που κοιμούνται οι γονείς τους. Για το λόγο αυτό συστήνεται ο υπολογιστής να τοποθετείται σε επιβλέψιμο χώρο

- . Έτσι οι γονείς θα μπορούν να ελέγχουν τα παιχνίδια που παίζουν τα παιδιά τους ώστε να σιγουρεύονται ότι αυτά είναι κατάλληλα για την ηλικία τους.

ΠΑΡΕΝΟΧΛΗΣΗ

Μερικά παιδιά που παίζουν διαδικτυακά παιχνίδια μπορούν να βασανίσουν άλλους παίχτες. Η εκάστοτε επιθετική συμπεριφορά εμφανίζει ποικιλομορφία. Μπορεί να είναι απλά δυσάρεστα σχόλια στο δωμάτιο συνομιλίας του παιχνιδιού μέχρι τη μόνιμη νίκη και την άρνηση γνώσεων στο πώς να προχωρήσει κάποιος στο επόμενο επίπεδο. Συνιστάται στα παιδιά να συμπεριφέρονται στους αντιπάλους τους στα διαδικτυακά παιχνίδια με τον ίδιο τρόπο που θα ήθελαν να τους συμπεριφέρονται.

ΕΠΙΚΙΝΔΥΝΗ ΣΥΜΠΕΡΙΦΟΡΑ

Υπάρχουν παιδιά που θέτουν τους εαυτούς τους σε κίνδυνο για να μπορέσουν να κλέψουν ή να ενημερωθούν για το πώς θα συνεχίσουν το παιχνίδι. Ενήλικες των οποίων οι σεξουαλικές τάσεις περιλαμβάνουν παιδιά, τα παροτρύνουν να εμπλακούν σε ακατάλληλες συμπεριφορές μέσω κάμερας ή συνομιλιών σεξουαλικού περιεχομένου ανταλλάσσοντας για τις συμπεριφορές αυτές ως επιβράβευση τις γνώσεις που έχουν. Τα παιδιά πρέπει να καταλάβουν ότι η συμπεριφορά τους στο Διαδίκτυο έχει συνέπειες και εκτός Διαδικτύου και ότι εάν κάποιος τα παροτρύνει να εμπλακούν σε σεξουαλικές δραστηριότητες θα πρέπει αμέσως να ενημερώσουν κάποιον ενήλικα που εμπιστεύονται.

Οφέλη

- Τα βιντεοπαιχνίδια είναι διασκεδαστικά και αναπτύσσουν τη δημιουργικότητα και τη φαντασία τους.
- Βοηθούν τα παιδιά να εξοικειωθούν με την τεχνολογία.
- Αυξάνουν την αυτοπεποίθησή τους, καθώς τους δίνουν τη δυνατότητα του ελέγχου.
- Μπορούν να αποτελέσουν χρήσιμα εκπαιδευτικά εργαλεία, αφού το παιδί μέσω κάποιων παιχνιδιών μπορεί να εμπεδώσει σχολικές γνώσεις και να εμπλουτίσει τις γενικές του γνώσεις.
- Συμβάλουν στην ανάπτυξη και στη βελτίωση κάποιων γνωστικών δεξιοτήτων όπως είναι η προσοχή, η παρατηρητικότητα, η απομνημόνευση, ο οπτικοκινητικός συντονισμός, η δεξιοτεχνία και η ικανότητα επίλυσης προβλημάτων.

• Μπορούν να αποτελέσουν μέσο κοινωνικοποίησης, αφού το παιδί καλεί τους φίλους του να παίξουν μαζί του, συζητάει τις επιδόσεις του με αυτούς και ανταλλάσσει πληροφορίες σχετικά με το παιχνίδι.

Τα ηλεκτρονικά παιχνίδια, παρά τους κινδύνους, είναι παιχνίδια και το παιδί δεν είναι κακό να παίζει αυτό που του αρέσει. Παρόλο αυτά, αυτό που χρειάζεται είναι οι γονείς να αναλάβουν την ευθύνη ότι τα παιδιά παίζουν ασφαλή ηλεκτρονικά παιχνίδια και έχουν σωστές ηλεκτρονικές συνήθειες.

ΠΑΙΧΝΙΔΙΑ ΣΤΟ ΔΙΑΔΥΚΤΙΟ

ΕΚΤΟΡΑΣ Δ.

ΕΙΣΑΓΩΓΗ

- Τα διαδικτυακά παιχνίδια και οι εφαρμογές παρέχουν μία διασκεδαστική και κοινωνική μορφή διασκέδασης, ενθαρρύνοντας την ομαδικότητα και τη συνεργασία. Υπάρχουν πολλοί τρόποι για να παίξεις στο διαδίκτυο. Μερικοί από αυτούς είναι τα παιχνίδια που κυκλοφορούν δωρεάν στο ίντερνετ, τα παιχνίδια ή οι εφαρμογές στο κινητό και σε φορητές κονσόλες, καθώς επίσης τα παιχνίδια που αγοράζει κανείς για τον υπολογιστή και άλλες κονσόλες, όπως το PlayStation, το Nintendo, το Wii ή το Xbox.
- Οι συμβουλές ασφάλειας για το ίντερνετ είναι άμεσα εφαρμόσιμες στο περιβάλλον των παιχνιδιών λόγω των κινδύνων που ενέχονται. Είναι σημαντικό τα παιδιά να γνωρίζουν για αυτούς τους κινδύνους και να αποκτήσουν τις ικανότητες και τις γνώσεις για τον περιορισμό τους.

ΔΙΑΔΙΚΤΥΑΚΑ ΠΑΙΧΝΙΔΙΑ

- Όπως και τα offline παιχνίδια, έτσι και τα διαδικτυακά παιχνίδια ή οι εφαρμογές μπορούν να έχουν εκπαιδευτικά παιχνίδια και να χρησιμοποιηθούν για να αναπτύξουν την ικανότητα επίλυσης προβλημάτων, την ομαδική εργασία και την κατανόηση.
- Παραδοσιακά τα παιχνίδια μπορούν να αγοραστούν από καταστήματα στη μορφή CD-ROM για τη χρήση σε υπολογιστή ή άλλη κονσόλα. Ωστόσο, τα τελευταία χρόνια αυξάνεται όλο και περισσότερο η αγορά μέσω διαδικτύου.
- Η διαδικτυακή σύνδεση που προσφέρει ένα παιχνίδι δίνει στο χρήστη μία νέα δυνατότητα, καθώς επιτρέπει την αλληλεπίδραση με άλλους παίκτες ανά τον κόσμο.
- Τα παιχνίδια πολλαπλών χρηστών επιτρέπουν τη συνομιλία μεταξύ αντιπάλων που στις περισσότερες περιπτώσεις δε γνωρίζονται μεταξύ τους. Αυτό έχει πολλά προτερήματα, αλλά μπορεί να δημιουργήσει διάφορα θέματα, όπως είναι η διαφορά ώρα στους χρήστες που προέρχονται από διαφορετικές χώρες, η οποία μπορεί να τους οδηγήσει στο να ξενυχτήσουν για να παίξουν με τον αντίπαλό τους. Επιπλέον, σε αυτές τις περιπτώσεις είναι σημαντικό να μην αποκαλύπτονται προσωπικές πληροφορίες και η συζήτηση να επικεντρώνεται μόνο στο παιχνίδι.

Τι νέο υπάρχει στο online gaming;

- Παιχνίδια όπως το Google Cardboard ή το Occulus Rift, προσθέτουν μία ακόμα διάσταση στο online gaming, καθώς επιτρέπουν στο χρήστη να βυθιστεί σε μία εμπειρία που μοιάζει αληθινή, διεγείροντας την ακοή ή την όρασή τους. Συνήθως, ο παίκτης θα πρέπει να φορά ένα ακουστικό για να βιώσει την εμπειρία των εικονικών παιχνιδιών πραγματικότητας.

Παιχνίδια επαυξημένης πραγματικότητας

- Αυτό το είδος παιχνιδιών διαδίδονται όλο και περισσότερο, με παιχνίδια να οδηγούν τους χρήστες από το σπίτι στους δρόμους, ενώ παράλληλα παίζουν. Τα παιχνίδια επαυξημένης πραγματικότητας λειτουργούν με ηλεκτρονικές αναβαθμίσεις στην υπάρχουσα πραγματικότητα, επιτρέποντας στους παίκτες να αλληλεπιδρούν με αυτή. Οι παίκτες θα «δουν» πράγματα, τα οποία αντιλαμβάνονται ότι δεν είναι αληθινά, αλλά τους βοηθούν να συνεχίσουν το παιχνίδι.

ΕΠΙΚΗΝΔΙΝΑ ΠΑΙΧΝΙΔΙΑ

- Το online gaming έχει μπει για τα καλά στη ζωή των παιδιών μας. Με γονική καθοδήγηση, μετριοπάθεια, κοινή λογική και ποικιλία, τα παιχνίδια μπορούν να αποτελέσουν πλεονέκτημα και όχι απειλή για την συναισθηματική, κοινωνική ακόμη και φυσική ανάπτυξη των παιδιών. Υπάρχουν όμως και αρκετοί κίνδυνοι που ξεκινούν μέσα από τη διαδικασία των παιχνιδιών για αυτό πρέπει να είμαστε πολύ προσεκτικοί και να έχουμε προνοήσει τα παιδιά να είναι ενημερωμένα και υποψιασμένα.
- Σημασία δεν έχει το όνομα του εκάστοτε παιχνιδιού αλλά το πόσο επικίνδυνο και παράτολμο μπορεί να γίνει. Υπάρχουν «παιχνίδια» που βάζουν το παιδί-θύμα σε διαδικασίες προκλήσεων που μπορεί να απειλήσουν τη σωματική του ακεραιότητα ή ακόμα και προτροπές για αυτοκτονία.
- Ο τρόπος λειτουργίας των συγκεκριμένων παιχνιδιών είναι πανομοιότυπος. Ο κακόβουλος ξεκινά να στέλνει μηνύματα ή να κάνει αιτήματα φιλίας σε ανήλικους χρήστες που φαίνεται από το προφίλ τους ότι αντιμετωπίζουν προβλήματα αυτοεκτίμησης ή νιώθουν μοναξιά. Αν το παιδί απαντήσει, ο κακόβουλος προσπαθεί να χτίσει ένα συναισθηματικό δέσιμο μαζί του με κύριο στόχο το παιδί να τον εμπιστευτεί και να κάνει ότι του πει.

Choking Game

- Τα πιο διάσημα είναι το
- **1.Choking Game**
- Κεντρική ιδέα του πρώτου είναι η διακοπή της τροφοδοσίας του εγκέφαλου με οξυγόνο, η οποία δημιουργεί ζαλάδα και μια αίσθηση ευφορίας και μερικές φορές καταλήγει στη λιποθυμία. Πρόκειται για μια πρόκληση (challenge) που καλούνται να εκπληρώσουν οι έφηβοι (συχνά υπό πίεση των συνομηλίκων τους), είτε μόνοι τους, με τη βοήθεια ενός σχοινιού ή μιας ζώνης, είτε με τη συμμετοχή ενός φίλου ή συμμαθητή.

Blue Whale Challenge.

- 2.Το Blue whale Challenge ή αλλιώς η «πρόκληση της μπλε φάλαινας» είναι μια σειρά δοκιμασιών που εξελίσσονται σε διάρκεια 50 ημερών και που σε ορισμένες περιπτώσεις την 51η μέρα κορυφώνονται με πράξεις οι οποίες οδηγούν στην αυτοχειρία. Μία από τις δοκιμασίες τις οποίες καλούνται να φέρουν εις πέρας οι έφηβοι είναι να χαράξουν λέξεις και σύμβολα στα χέρια τους, μεταξύ των οποίων και μια φάλαινα. Πρόσφατα δύο 15χρονα παιδιά στη Ρωσία αυτοκτόνησαν πέφτοντας από την οροφή της πολυκατοικίας.

MOMO

- Το παιχνίδι προκαλεί τους χρήστες να επικοινωνήσουν με ένα άγνωστο πρόσωπο, μέσω ενός αριθμού στο WhatsApp και να ολοκληρώσουν μια σειρά επικίνδυνων δοκιμασιών, που τελικά καταλήγουν σε αυτοτραυματισμό ή αυτοκτονία. Η αρχική «πρόκληση» θέλει τον/την παραλήπτη να επικοινωνεί με έναν άγνωστο αριθμό, που έχει ως avatar μία τρομακτική γυναικεία μορφή (εικόνα ενός αγάλματος της Gallery Vanilla στο Τόκιο / Ιαπωνία), και στη συνέχεια καλείται να ανταποκριθεί στις δοκιμασίες (μέσω κειμένων ή φωνητικών μηνυμάτων), κινηματογραφώντας τον εαυτό του/της, κατά την επίτευξη των προκλήσεων που του/της έχουν ανατεθεί. Σε περίπτωση που ο/η παραλήπτης δεν ανταποκριθεί ή δεν ολοκληρώσει τις δοκιμασίες, τότε δέχεται απειλές μέσω βίαιων εικόνων και εκβιασμών (π.χ., ο Momo γνωρίζει πού ζεις, ο Momo θα κάνει κακό στην οικογένειά σου).

ΤΙ ΝΑ ΚΑΝΕΤΕ

- Να κρατήσετε τα αποδεικτικά στοιχεία (μέσω στιγμιότυπων οθόνης – screen shots),
- Να αναφέρετε, μέσω εργαλείων αναφοράς καταγγελίας το περιστατικό και τα αποδεικτικά στοιχεία,
- Να μπλοκάρετε το άτομο ή τον αριθμό που σας παρενοχλεί,
- Να αναφέρετε, άμεσα, το γεγονός στους γονείς ή σε κάποιο ενήλικα που εμπιστεύεστε,
- Να καλέστε τη δωρεάν ανώνυμη Γραμμή Βοήθειας και Γραμμή Καταγγελιών στο 1480 ή τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.
- Σημειώνετε ότι, αν λάβετε ένα μήνυμα από έναν άγνωστο αριθμό στο WhatsApp, θα πρέπει να τον αποκλείσετε ή να τον αναφέρετε ως ανεπιθύμητο. Αν λάβετε ένα μήνυμα στο Instagram ή άλλη πλατφόρμα κοινωνικής δικτύωσης θα πρέπει να την αναφέρεται ως «βία ή απειλή βίας».
- Μην ανοίγετε ύποπτους συνδέσμους που σας αποστέλλονται στα Μέσα Κοινωνικής Δικτύωσης (π.χ., Facebook, Instagram).
- Αν πέσει στην αντίληψή σας ότι κάποιο άλλο παιδί ή έφηβος συμμετάσχει ή σχεδιάζει να συμμετάσχει στην πρόκληση “Momo” ή σε άλλες επικίνδυνες ενέργειες ενημερώστε άμεσα κάποιον/κάποια ενήλικα που εμπιστεύεστε ή καλέστε τη δωρεάν ανώνυμη Γραμμή Βοήθειας και Γραμμή Καταγγελιών στο 1480.
- Να θυμάστε πάντοτε ότι:
-
- Πρέπει να είστε υπερήφανοι για τον εαυτό σας,
- Πρέπει να κάνετε τις δικές σας προσωπικές επιλογές,

ΟΔΗΓΙΕΣ ΓΙΑ ΓΟΝΕΙΣ

- Χρειάζεται σωστή επικοινωνία με το παιδί. Το ενημερώνουμε για την πιθανότητα ενός τέτοιου ενδεχόμενου και αφήνουμε ανοιχτές τις γέφυρες επικοινωνίας έτσι ώστε να μην φοβηθεί να μας εμπιστευτεί αν κάτι συμβεί διαδικτυακά.
- Βάζουμε όρια όχι μόνο στο χρόνο χρήσης τους διαδικτύου αλλά και στον τρόπο χρήσης του. Για τα μικρότερα παιδιά ενεργοποιούμε τα εργαλεία γονικών ελέγχων σε όλες τις συσκευές και δεν τα αφήνουμε να πλοηγούνται ανεξέλεγκτα στο διαδίκτυο. Επιβλέπουμε με διακριτικότητα τα μεγαλύτερα παιδιά.
- Ενεργοποιούμε τις σωστές ρυθμίσεις ασφαλείας στα κοινωνικά δίκτυα που χρησιμοποιεί το παιδί. Προσέχουμε το προφίλ του να είναι ιδιωτικό έτσι ώστε να μην έχει πρόσβαση ο καθένας στο περιεχόμενο που κοινοποιείται.
- Συζητάμε με το παιδί τη σημασία της προστασίας των προσωπικών του πληροφοριών και πόσο σημαντικό είναι να μην αποδέχεται να έχει οποιαδήποτε επαφή με άτομα που δε γνωρίζει στον πραγματικό κόσμο.
- Εξηγούμε στο παιδί ότι ακόμα και αν κάτι κάνει λάθος εσείς ως γονείς θα είστε δίπλα του και όχι απέναντί του. Αρκεί να σας το εμπιστευτεί και μαζί να βρείτε τη λύση.

ΗΛΕΚΤΡΟΝΙΚΑ ΠΑΙΧΝΙΔΙΑ
(ΕΠΙΚΙΝΔΥΝΑ ΚΑΙ ΜΗ)

ΓΙΑΝΝΗΣ Μ.

- *Στ΄1*

ΕΙΣΑΓΩΓΗ

Στις μέρες μας παιδιά και ενήλικες στον ελεύθερο τους χρόνο

διαβάζουν βιβλία,

παρακολουθούν προγράμματα στην τηλεόραση και

παίζουν ηλεκτρονικά παιχνίδια.

Τα ηλεκτρονικά παιχνίδια διεκδικούν μεγάλο μερίδιο από το χρόνο των παιδιών, με τους γονείς να προβληματίζονται για αυτό το είδος διασκέδασης που πολλές φορές παίρνει τη μορφή εμμονικής ενασχόλησης.

Εμείς θα ασχοληθούμε με το θέμα των παιχνιδιών, τα οποία μπορεί να είναι ευεργετικά αλλά και όχι.

Πώς ελκύουν το κοινό και πώς διαδίδονται;

ΤΙ ΕΙΝΑΙ ΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΠΑΙΧΝΙΔΙΑ;

Ηλεκτρονικό παιχνίδι:

ένα παιχνίδι το οποίο χρησιμοποιεί ηλεκτρονικά στοιχεία για να δημιουργήσει ένα διαδραστικό σύστημα, μέσα στο οποίο μπορεί να παίξει ένας παίκτης.

Τα παιχνίδια στον υπολογιστή είναι προγράμματα, τα οποία φτιάχνονται από εξειδικευμένες εταιρίες με σκοπό να ελκύσουν τον κόσμο να παίξει και να αποφέρουν κέρδη.

Είδη παιχνιδιών:

- Πολεμικά
- δημιουργικά,
- αθλητικά
- χαλαρωτικά .

Παραδείγματα:

- Fortnite
- FC ή FIFA,
- Call of duty
- Roblox.

***Αρνητικές: ΕΘΙΣΜΟΣ (*:Εθισμός** είναι μια συμπεριφορά που χαρακτηρίζεται από εξάρτηση σε μια συγκεκριμένη δραστηριότητα αλλά και σε ουσίες.

Εθισμός: πιθανό να οδηγήσει σε

- διαταραχές ύπνου,
- πτώση σχολικής επίδοσης,
- επιθετικότητα,
- άγχος,
- κατάθλιψη,
- παραμέληση προσωπικής υγιεινής και φυσικής άσκησης,
- μείωση κοινωνικών συναναστροφών,
- περιορισμένη επικοινωνία με γονείς/φίλους κλπ.

Θετικές

- Βελτίωση της συγκέντρωσης, της μνήμης και της προσοχής
- Βελτίωση του οπτικοκινητικού συντονισμού
- Βελτίωση της παρατηρητικότητας
- Μπορούν να χρησιμεύσουν ως εκπαιδευτικά εργαλεία

ΕΠΙΔΡΑΣΕΙς

ΠΩΣ ΤΑ ΑΠΟΦΕΥΓΟΥΜΕ;

Οι γονείς που θα εντοπίσουν σημάδια εξάρτησης θα πρέπει καταρχάς να προσπαθήσουν να καταλάβουν τι συμβαίνει με το παιδί:

Η απόσυρση που παρατηρούν στο παιδί είναι αποτέλεσμα της ενασχόλησης με τον υπολογιστή ή η ενασχόληση αυτή κρύβει θέματα που αντιμετωπίζει το παιδί και επειδή δεν μπορεί να τα διαχειριστεί επιλέγει να αποσυρθεί στην οθόνη του υπολογιστή; Είναι σημαντικό να διατηρούν ανοιχτό το κανάλι επικοινωνίας με το παιδί

- Σε μια προσπάθεια να έρθουν πιο κοντά στο παιδί μπορούν **να ζητήσουν από το παιδί να τους μιλήσει για το παιχνίδι** πχ. να περιγράψει τους ήρωες , την πλοκή, να μιλήσει
- **Οι γονείς θα πρέπει να επενδύουν στον κοινό οικογενειακό χρόνο**, να σχεδιάζουν μαζί με το παιδί εξόδους , δραστηριότητες και μικρές εξορμήσεις στη φύση. Οι γονείς οφείλουν να είναι ενημερωμένοι για το περιεχόμενο των παιχνιδιών που προτιμά το παιδί τους και βέβαια να κάνουν την αγορά μαζί.
- **Τα σαφή και σταθερά όρια** βοηθούν το παιδί να γνωρίζει ποια συμπεριφορά είναι αποδεκτή και από ποιο σημείο και έπειτα η ενασχόληση με τα ηλεκτρονικά παιχνίδια βλάπτει την υγεία του.
- Ενισχύστε **ομαδικές** δραστηριότητες και προτρέψτε το παιδί να ασχοληθεί με τον **αθλητισμό.**

HTTPS://EL.WIKIPEDIA.ORG/WIKI/%CE%97%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C_%CF%80%CE%B1%CE%B9%CF%87%CE%BD%CE%AF%CE%B4%CE%B9

ΤΕΛΟΣ