Βιωματική Διάλεξη με θέμα

«Εκφοβισμός και Διαδίκτυο»

ΟΧΙ στον εκφοβισμό,

ΝΑΙ στην αγάπη και στον σεβασμό!

ΔΗΜΟΤΙΚΟ ΣΧΟΛΕΙΟ ΠΕΡΑ

ΧΩΡΙΟΥ ΝΗΣΟΥ Α΄

ΤΕΤΑΡΤΗ 20 ΔΕΚΕΜΒΡΙΟΥ 2023

Ερωτήσεις που πρέπει να υποβάλλετε ΠΡΙΝ αγοράσετε κινητό στο παιδί σας

1. Πρόσβαση στο διαδίκτυο

• Έχει αυτή η συσκευή πρόσβαση στο διαδίκτυο; Ποιες είναι ακριβώς οι δυνατότητες που παρέχει;

• Υπάρχει δυνατότητα να ενεργοποιηθούν φίλτρα έτσι ώστε να αποκλείεται η πρόσβαση σε περιεχόμενο που θεωρείτε ακατάλληλο;

• Υπάρχει η δυνατότητα απενεργοποίησης του browser έτσι ώστε το παιδί να μην μπορεί να μπει στον ιστό;

• Αν το παιδί εισέρχεται στο διαδίκτυο από το Wi-Fi του σπιτιού ισχύουν οι ρυθμίσεις ασφαλείας που είναι ήδη ενεργοποιημένες;

• Πώς μπορεί από το κινητό να έχει πρόσβαση σε τηλεοπτικά προγράμματα και προγράμματα μουσικής;. Υπάρχει τρόπος να οριστεί η πρόσβαση σε περιεχόμενο με βάση την επιτρεπόμενη ηλικία;

2. Επικοινωνία

• Με ποιους τρόπους μπορεί η συγκεκριμένη συσκευή να παρέχει επικοινωνία;

• Υπάρχουν ρυθμίσεις που αν εφαρμοστούν να μην επιτρέπεται στο παιδί να κάνει βιντεοκλήσεις;

• Υπάρχουν ρυθμίσεις που αν εφαρμοστούν να μην επιτρέπουν σε πολλούς χρήστες να παίζουν ένα παιχνίδι;

•Με ποιο τρόπο γίνεται αναφορά για ανεπιθύμητα ή ενοχλητικά μηνύματα ή κλήσεις;

3. Εφαρμογές

• Υπάρχει τρόπος να μην επιτρέπεται στο παιδί να κατεβάζει εφαρμογές που δεν είναι κατάλληλες για την ηλικία του;

• Με ποιο τρόπο γίνεται αναφορά για μια εφαρμογή;

• Υπάρχουν κάποιες εφαρμογές που μπορούν να με βοηθήσουν να προστατέψω το παιδί μου;

4. Προστασία προσωπικών δεδομένων

• Πώς ενεργοποιείται ο κωδικός για κλείδωμα της οθόνης του τηλεφώνου όταν δεν είναι σε χρήση;

• Αυτή η συσκευή περιέχει υπηρεσίες τοποθεσίας; Υπάρχουν ρυθμίσεις που αν εφαρμοστούν να μην εμφανίζεται η τοποθεσία που βρίσκεται το παιδί ;

5. Κόστος

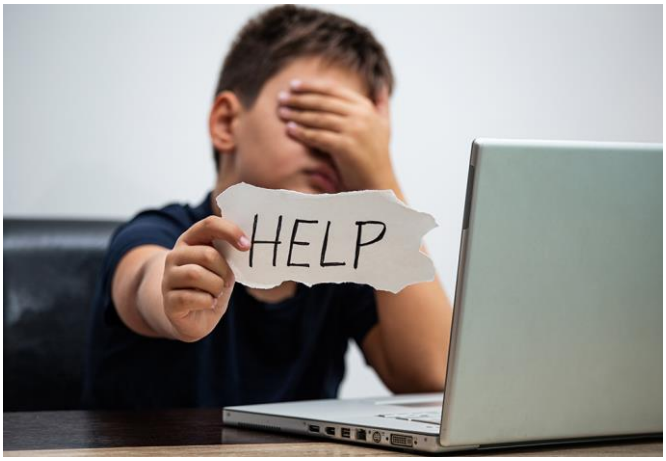
• Με ποιους τρόπους το παιδί μπορεί να «φουσκώσει» το λογαριασμό χρησιμοποιώντας το κινητό;

• Υπάρχουν ρυθμίσεις ασφαλείας για αυτό το θέμα που μπορούν να ενεργοποιηθούν;

• Πώς μπορεί το παιδί να ξοδέψει χρήματα σε εφαρμογές ή σε άλλο περιεχόμενο; Υπάρχουν γονικές ρυθμίσεις ή τρόποι να αποτραπούν τέτοιες δαπάνες;

Πληροφορίες για ασφαλή και υπεύθυνη χρήση του Διαδικτύου μπορείτε να βρείτε:

- Κυπριακό Κέντρο Ασφαλούς Διαδικτύου – CYberSafety, https://internetsafety.pi.ac.cy/
- Στην ιστοσελίδα της Αστυνομίας Κύπρου, Τμήμα Καταπολέμησης Ηλεκτρονικού Εγκλήματος, https://www.police.gov.cy/police/police.nsf/All/3F95673F057221ECC2258522005E3712?OpenDocument
- στην ιστοσελίδα του Κέντρου Ασφαλούς Διαδικτύου – CYberSafety, https://cybersafety.cy/



ΚΙΝΔΥΝΟΙ ΔΙΑΔΙΚΤΥΟΥ

Ακατάλληλο Περιεχόμενο

Περιγραφή:

Ο όρος ακατάλληλο περιεχόμενο είναι υποκειμενικός σε σχέση με την ηλικία ή και την ψυχική κατάσταση του κάθε ατόμου. Για παράδειγμα ένα περιεχόμενο μπορεί να θεωρηθεί μη αποδεκτό για ένα μικρό παιδί εάν αυτό περιέχει ακατάλληλο υλικό, το οποίο μπορεί να προκαλέσει ψυχικές διαταραχές, να σοκάρει ή ακόμα να προωθήσει λάθος συμπεριφορές. Το ίδιο περιεχόμενο μπορεί όμως να θεωρηθεί κατάλληλο για ένα μεγαλύτερο σε ηλικία άτομο.

Συνήθως με τον όρο ακατάλληλο περιεχόμενο, αναφερόμαστε σε περιεχόμενο, το οποίο μπορεί να περιλαμβάνει ρατσιστικό ή ξενοφοβικό περιεχόμενο, προώθηση επιβλαβών συμπεριφορών, προώθηση τυχερών παιχνιδιών, παρουσίαση πορνογραφικού υλικού, προώθηση βίας κ.λ.π.

Πού μπορεί να συμβεί: ιστοσελίδες αμφίβολου προέλευσης, μέσα από τα διαδικτυακά παιχνίδια (online games), μέσω του ηλεκτρονικού ταχυδρομείου, μέσω του κινητού τηλεφώνου

Αντιμετώπιση

- Καταγγέλλουμε ιστοσελίδες με ακατάλληλο περιεχόμενο στη Γραμμή Βοήθειας και Καταγγελιών 1480 https://internetsafety.pi.ac.cy/1480
- Αυτά που διαβάζουμε ή βλέπουμε στο Διαδίκτυο δεν είναι πάντοτε ορθά. Ρωτάμε άτομα που εμπιστευόμαστε, εάν έχουμε αμφιβολίες
- Αξιολογούμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο και ελέγχουμε το συγγραφέα, την προέλευση της σελίδας, τη βιβλιογραφία της πληροφορίας
- Χρησιμοποιούμε πολλαπλές πηγές πληροφοριών και διασταυρώνουμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο
- Εγκαθιστούμε λογισμικό φιλτραρίσματος πληροφοριών σε υπολογιστές που χρησιμοποιούνται από παιδιά (π.χ. “Safe Internet” της Αρχής Τηλεπικοινωνιών Κύπρου)
- Εάν κάτι μας κάνει να νιώθουμε άβολα ή αμήχανα, κλείνουμε το browser μας και το αναφέρουμε αμέσως σε κάποιο ενήλικα
- Χρησιμοποιούμε τη δυνατότητα του browser μας που ονομάζεται “Αγαπημένα” για να τοποθετήσουμε τις ιστοσελίδες που είναι ασφαλείς και επισκεπτόμαστε συχνά

Ανεπιθύμητα Μηνύματα

Περιγραφή:

Ανεπιθύμητα Μηνύματα θεωρούνται τα μηνύματα εκείνα που υπό κανονικές συνθήκες οι χρήστες δεν θα επέλεγαν να δουν και τα οποία διανέμονται σε μεγάλο αριθμό παραληπτών. Παραδείγματα ανεπιθύμητων μηνυμάτων είναι μηνύματα που περιέχουν διαφημιστικά για αμφίβολα προϊόντα, μηνύματα με περιεχόμενο που συσχετίζεται με ψευδοτυχερά παιχνίδια, ψευδονομικές υπηρεσίες, πορνογραφικό υλικό κτλ. Πολύ συχνό φαινόμενο είναι και η λήψη αλυσιδωτών μηνυμάτων (chain e-mails). Τα μηνύματα αυτά είναι, συνήθως, ανεπιθύμητα και ο αποστολέας ζητά από τον παραλήπτη να προωθήσει το μήνυμα σε άλλα άτομα, τα οποία γνωρίζει. Ο κίνδυνος εδώ, είναι ότι κάθε φορά που προωθούμε ένα μήνυμα, αν δεν είμαστε προσεχτικοί, μαζί με αυτό εμφανίζεται και η ηλεκτρονική διεύθυνση όλων των προηγούμενων ατόμων που προώθησαν το ίδιο μήνυμα. Έτσι δεν γνωρίζουμε ποιος θα παραλάβει το μήνυμα και τι θα κάνει με τις ηλεκτρονικές διευθύνσεις, οι οποίες θα εμφανίζονται σε αυτό.

Πού μπορεί να συμβεί: στο ηλεκτρονικό ταχυδρομείο, λίστες ομάδων πληροφόρησης, στο κινητό τηλέφωνο, ακατάλληλα παιχνίδια, ηλεκτρονικός τζόγος, ακατάλληλο/παράνομο περιεχόμενο, υποκλοπή προσωπικών δεδομένων (Phishing)

Αντιμετώπιση

- Είμαστε προσεχτικοί όταν δίνουμε την ηλεκτρονική μας διεύθυνση
- Ρυθμίζουμε την υπηρεσία φιλτραρίσματος του ηλεκτρονικού μας ταχυδρομείου, ώστε να σταματά ανεπιθύμητα μηνύματα.
- Όταν το μήνυμα είναι από άγνωστο αποστολέα να μην παραπλανόμαστε ώστε να κάνουμε κλικ σε συνδέσμους παρόμοιους με «Κάνε κλικ εδώ, εάν δεν θέλεις να παίρνεις τέτοια μηνύματα», γιατί αυτό επιβεβαιώνει στον αποστολέα ότι η ηλεκτρονική διεύθυνσή μας είναι σωστή. Έτσι, ο αποστολέας θα συνεχίσει να την χρησιμοποιεί ή θα μπορέσει πιο εύκολα να την πουλήσει σε άλλους
- Είμαστε προσεχτικοί όταν δίνουμε τον αριθμό του κινητού μας τηλεφώνου. Ανεπιθύμητα μηνύματα μπορούμε να πάρουμε και στο κινητό (sms spam)
- Χρησιμοποιούμε την κρυφή κοινοποίηση(Bcc) στο ηλεκτρονικό ταχυδρομείο, εάν θέλουμε να προωθήσουμε κάποιο μήνυμα σε πολλούς παραλήπτες, ούτως ώστε να προστατεύσουμε τις ηλεκτρονικές διευθύνσεις των παραληπτών
- Όταν δεχόμαστε ανεπιθύμητα μηνύματα, τα διαγράφουμε χωρίς να τα διαβάζουμε
- Είναι καλό να χρησιμοποιούμε δύο διευθύνσεις: μια για να επικοινωνούμε με φίλους, συγγενείς,

συναδέλφους και μια άλλη για εγγραφές σε υπηρεσίες στο Διαδίκτυο, συμμετοχή σε forum κ.ά. Έτσι, αν παίρνουμε πολλά ανεπιθύμητα μηνύματα στη δεύτερη διεύθυνση μπορούμε εύκολα να τη διαγράψουμε και να δημιουργήσουμε μια καινούρια

- Μπορούμε να κρύψουμε την ηλεκτρονική μας διεύθυνση από προγράμματα ανίχνευσης ηλεκτρονικών διευθύνσεων. Αυτό μπορούμε να το κάνουμε , δηλώνοντάς την μέσα σε αρχείο εικόνας ή περιγράφοντας την με κείμενο αντί πληκτρολογώντας την ως έχει (π.χ. αντί για dog@home.cy πληκτρολογούμε dog at home telia cy)

Αποξένωση από τον Πραγματικό Κόσμο

Περιγραφή:

Η αλόγιστη και πολύωρη χρήση του Διαδικτύου, δημιουργεί συναισθηματική απόσταση και αλλοιώνει την ποιότητα επικοινωνίας ανάμεσα στους ανθρώπους, κάτι το οποίο πολλές φορές οδηγεί στην Αποξένωσή τους από τον Πραγματικό Κόσμο.
Αρκετοί είναι αυτοί οι οποίοι ξοδεύουν άπειρες ώρες μπροστά στον υπολογιστή παίζοντας διαδικτυακά παιχνίδια, σερφάροντας στο Διαδίκτυο ή ακόμα και επικοινωνώντας με φίλους τους μέσω του Διαδικτύου. Η πολύωρη ενασχόληση με τα πιο πάνω, οδηγεί πολλές φορές στην Αποξένωση από τον Πραγματικό Κόσμο εφόσον επιτρέπει στους ανθρώπους να ψυχαγωγούνται ή να επικοινωνούν χωρίς τα πλεονεκτήματα και τα μειονεκτήματα της προσωπικής επαφής. Αρκετοί είναι αυτοί για παράδειγμα οι οποίοι αναπτύσσουν Διαδικτυακές (on-line) σχέσεις χωρίς να εγκαταλείπουν τα σπίτια τους.
Όλα αυτά γίνονται σε βάρος του χρόνου που διαφορετικά μπορούν να έχουν διαθέσιμο για τη συμμετοχή σε άλλες δραστηριότητες με φίλους, γείτονες ή ομάδες ανθρώπων με κοινά εν- διαφέροντα. Ως αποτέλεσμα, κάποιοι άνθρωποι δεν μπορούν να ταυτιστούν με τους άλλους νιώθοντας αποκλεισμένοι στην εντός του Διαδικτύου κοινωνική τους ζωή.

Πού μπορεί να συμβεί: Γενικά στο Διαδίκτυο (π.χ. διαδικτυακά παιχνίδια, κοινωνικά δίκτυα, δωμάτια συνομιλίας)

Αντιμετώπιση

- Χρησιμοποιούμε το Διαδίκτυο με μέτρο, συμπεριλαμβάνοντας στο πρόγραμμά μας εναλλακτικές δραστηριότητες που περιλαμβάνουν ενασχόληση με ομαδικά αθλήματα, χορωδίες, χορό και άλλες.

Εκφοβισμός (Cyberbullying)

Περιγραφή:

Εκφοβισμός είναι δυνατό να συμβεί μέσω του Διαδικτύου και περιλαμβάνει εσκεμμένη, επαναλαμβανόμενη και εχθρική συμπεριφορά απέναντι σε άτομο ή ομάδα ατόμων με σκοπό την πρόκληση συναισθηματικής και ψυχολογικής βλάβης.
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. Η σύγχρονη έρευνα έχει δείξει ότι το σχολείο, όταν υπάρχει πληροφόρηση και ενημέρωση του προσωπικού, μπορεί να αντιμετωπίσει το πρόβλημα (Bhat, 2008).

Πού μπορεί να συμβεί: μέσω ηλεκτρονικού ταχυδρομείου (e-mail), στα δωμάτια συναντήσεων (chat rooms), σε σελίδες διαμοιρασμού και προβολής βίντεο, σε ιστολόγια (blogs) ή άλλες ιστοσελίδες που στοχεύουν να βλάψουν άτομα

Αντιμετώπιση:

- Εάν πέσουμε θύμα εκφοβισμού, σταματάμε αμέσως την επικοινωνία με το θύτη
- Εμπιστευόμαστε στους γονείς μας ή σε κάποιο ενήλικα τον εκφοβισμό που έχουμε δεχθεί
- Δεν προωθούμε εκφοβιστικά μηνύματα
- Αν γνωρίζουμε κάποιο φίλο που είναι θύτης τον συμβουλεύουμε να σταματήσει
- Φιλτράρουμε ηλεκτρονικά μηνύματα από άτομα που μάς παρενοχλούν και μπλοκάρουμε την πρόσβασή τους στο ιστολόγιό μας
- Επικοινωνούμε με τη Γραμμή Βοήθειας και Καταγγελιών 1480 https://internetsafety.pi.ac.cy/1480

Αποπλάνηση

Περιγραφή:

Αποπλάνηση συμβαίνει όταν άγνωστοι κακόβουλα εκμεταλλεύονται το στοιχείο της ανωνυμίας στο Διαδίκτυο για να προσεγγίσουν ανήλικα παιδιά με στόχο τη σεξουαλική παρενόχληση.

Στο Διαδίκτυο ποτέ δεν μπορούμε να είμαστε σίγουροι

ποιος είναι ο συνομιλητής μας στις ηλεκτρονικές μας επικοινωνίες, ακόμα και αν βλέπουμε τη φωτογραφία του ή αν χρησιμοποιούμε κάμερα. Έτσι, πολλοί επιτήδειοι εκμεταλλεύονται το γεγονός αυτό, δίνουν ψεύτικα στοιχεία (κυρίως για την ηλικία τους) και ξεκινούν συζητήσεις με τα πιθανά θύματά τους με στόχο να αναπτύξουν φιλική με αυτά σχέση και να αποσπάσουν όσο το δυνατό περισσότερες πληροφορίες (π.χ. τόπο διαμονής, τα ενδιαφέροντά τους, τα χόμπι τους, τις σεξουαλικές τους εμπειρίες κ.λ.π.).

Τα δωμάτια επικοινωνίας (chat rooms) είναι ένας δημοφιλής τρόπος επικοινωνίας μεταξύ των νέων αλλά και δημοφιλές μέσο αποπλάνησης (Shannon, 2008). Αυτά είναι εικονικά μέρη όπου άνθρωποι από όλο τον κόσμο μπορούν να «συναντηθούν» και να «συνομιλήσουν» μέσω μηνυμάτων. Πρέπει να γνωρίζουμε όμως ότι οποιοσδήποτε μπορεί, χρησιμοποιώντας απλά ένα ψευδώνυμο, να παρακολουθεί ή να συμμετέχει σε συζητήσεις μας.

Υπάρχει ωστόσο και η δυνατότητα «ιδιωτικής συνομιλίας», όπου κάποιοι από τα μέλη της ομάδας αποφασίζουν να απομονωθούν από τους άλλους σε ένα ιδιαίτερο «δωμάτιο» και να επικοινωνούν μόνο μεταξύ τους. Υπάρχουν συχνά καταγγελίες παιδιών ότι, κατά τη διάρκεια τέτοιου είδους συνομιλίας, έχουν δεχτεί προτροπές από αγνώστους για συνάντηση σε πραγματικό χώρο. Σε χώρες του εξωτερικού έχουν παρουσιασθεί έως τώρα δεκάδες περιπτώσεις παιδιών που εξαφανίσθηκαν, έπεσαν θύματα παιδοφίλων ή κυκλωμάτων παιδικής πορνογραφίας, ή παρασύρθηκαν από κακόβουλους αγνώστους, τους οποίους «συνάντησαν» σε δωμάτια επικοινωνίας (Craven, et al, 2006).

Πού μπορεί να συμβεί: δωμάτια συνομιλίας (chat rooms), σελίδες κοινωνικών δικτύων

Αντιμετώπιση:

- Δεν δίνουμε τα προσωπικά μας στοιχεία σε ένα δωμάτιο συνομιλίας. Ποτέ δεν μπορούμε να είμαστε σίγουροι για την ταυτότητα του συνομιλητή μας
- Δεν συναντούμε κάποιο ξένο, τον οποίο γνωρίσαμε σε ένα δωμάτιο συνομιλίας. Αν μάς ζητηθεί κάτι τέτοιο το συζητάμε αμέσως με κάποιο ενήλικα
- Μπορούμε να αποθηκεύουμε τις ηλεκτρονικές μας συνομιλίες. Αν μια συνομιλία μας έκανε να νιώσουμε άβολα ή μας έφερε σε δύσκολη θέση, κρατάμε αντίγραφο. Αυτό θα μας βοηθήσει να καταγγείλουμε τον επιτήδειο που προσπάθησε να μας παραπλανήσει
- Διαβάζουμε τους όρους χρήσης, τον κώδικα επικοινωνίας και τη δήλωση απορρήτου στη διαδικτυακή τοποθεσία συνομιλίας, προτού αρχίσουμε τη συνομιλία

Βίαια Παιχνίδια

Περιγραφή:

Σύμφωνα με έρευνες, εκατομμύρια άτομα αφιερώνουν χρόνο σε καθημερινή βάση σε ηλεκτρονικά παιχνίδια (http://www.appdata.com). Όπως στην αγορά έτσι και στο Διαδίκτυο υπάρχουν διάφορες κατηγορίες παιχνιδιών. Η πιο δημοφιλής κατηγορία παιχνιδιών είναι η κατηγορία παιχνιδιών δράσης η οποία χωρίζεται σε άλλες υποκατηγορίες, όπως παιχνίδια πολεμικών τεχνών (Beat'em up), λαβυρίνθων (maze), πλατφόρμας (platform), βολών (shooters) κ.ά.

Η κατηγορία βολών θεωρείται η πλέον βίαια κατηγορία παιχνιδιών και έχει κατακριθεί ιδιαίτερα για τα κακά πρότυπα και τις αρνητικές επιδράσεις που πιθανότατα να έχει, ειδικά σε νεαρά άτομα . Όπως λέει και το όνομα, σκοπός είναι να χρησιμοποιήσουμε όπλα, ώστε να εξοντώσουμε τους αντιπάλους και να ολοκληρώσουμε τις αποστολές του παιχνιδιού.

Βία όμως που εκφράζουμε στα παιχνίδια μπορεί να την εμφανίσουμε και στην κανονική μας ζωή. Ανησυχητικά είναι τα συμπεράσματα που προκύπτουν από τις έρευνες των Πανεπιστημίων της Καλιφόρνια και του Σαν Φρανσίσκο στις ΗΠΑ. Οι μελετητές βρήκαν ότι η βία στα ηλεκτρονικά παιχνίδια προκαλεί αντικοινωνική και πολεμοχαρή συμπεριφορά στην καθημερινότητα των παιδιών ηλικίας 18 έως 21 (Ferguson, 2007).

Αυτό το ενισχύει και ο οργανισμός ISFE (Interactive Software Federation of Europe), όπου σύμφωνα με έρευνές του, υψηλά επίπεδα έκθεσης σε βίαια ηλεκτρονικά παιχνίδια σχετίζονται έντονα με αυξανόμενη επιθετική συμπεριφορά στο σχολείο και στο ελεύθερο παιχνίδι και οδηγούν στην εγκληματικότητα.

Εδώ υπάρχει το ζήτημα του ενδεχομένως ακατάλληλου για την ηλικία του παιδιού περιεχόμενο. Για το σκοπό αυτό η βιομηχανία παιχνιδιών εφαρμόζει κώδικες σήμανσης των παιχνιδιών όπως π.χ. Πανευρωπαϊκού Συστήματος Πληροφόρησης για τα Ηλεκτρονικά Παιχνίδια (Pan European Game Information – PEGI). Στη σήμανσή του, το PEGI αναφέρει τόσο την ηλικιακή ομάδα στην οποία απευθύνεται ο κάθε τίτλος, καθώς και τα στοιχεία που περιλαμβάνει (π.χ. βία, ρατσιστικά στοιχεία, κ.ά.).

Πού μπορεί να συμβεί: Διαδικτυακά παιχνίδια, Αυτόνομα παιχνίδια τα οποία μπορούμε να παίξουμε με άλλους παίκτες μέσω δικτύου, παιχνίδια κονσόλας

Αντιμετώπιση

- Ενημερωνόμαστε για τον τρόπο αξιολόγησης του Πανευρωπαϊκού Συστήματος Πληροφόρησης για τα Ηλεκτρονικά Παιχνίδια (Pan European Game Information – PEGI). Κοιτάζοντας τη σήμανση PEGI στο κουτί του παιχνιδιού ή στην ιστοσελίδα από την οποία αυτό είναι διαθέσιμο, μπορούμε να προσδιορίσουμε αν ένα παιχνίδι είναι κατάλληλο για μας.

Επιβλαβείς Συμπεριφορές

Περιγραφή:

Το γεγονός ότι το Διαδίκτυο δεν είναι υπό τη δικαιοδοσία οποιουδήποτε καθιστά αδύνατο τον έλεγχο του περιεχομένου του. Ιστοσελίδες για βουλιμία, ανορεξία, αυτοκτονία, σατανισμό και τυχερά παιχνίδια υπάρχουν πολλές και παρακινούν σε επιβλαβείς συμπεριφορές. Για παράδειγμα, σύμφωνα με το Eating Disorders Review (2003), άρχισαν να εμφανίζονται ιστοσελίδες υπέρ των διατροφικών διαταραχών και, παρά τις προσπάθειες που κατέβαλαν ομάδες εναντίον της ανορεξίας και της βουλιμίας, αυτές οι ιστοσελίδες παραμένουν προσβάσιμες.

Σύμφωνα με έρευνα από την British Medical Journal, οι άνθρωποι που ψάχνουν πληροφορίες για τρόπους αυτοκτονίας είναι πιθανότερο να βρουν σελίδες που την ενθαρρύνουν παρά σελίδες που προσφέρουν βοήθεια και στήριξη. Από 240 ιστοσελίδες που βρέθηκαν το 2008 να αναφέρουν την αυτοκτονία οι 45 περίπου την ενθάρρυναν, την προωθούσαν ή την διευκόλυναν.

Πού μπορεί να συμβεί: Κατά την πλοήγηση μας σε οποιαδήποτε ιστοσελίδα του Διαδικτύου

Αντιμετώπιση

- Χρησιμοποιούμε τη δυνατότητα του φυλλομετρητή μας που ονομάζεται “Αγαπημένα” (My Favourites) για να τοποθετήσουμε τις ιστοσελίδες που είναι ασφαλείς και επισκεπτόμαστε συχνά
- Αυτά που διαβάζουμε ή βλέπουμε στο Διαδίκτυο δεν είναι πάντοτε ορθά. Αν συναντήσουμε ιστοσελίδες με περιεχόμενο που μας σοκάρει, τότε το αναφέρουμε σε κάποιον ενήλικα
- Καταγγέλλουμε ιστοσελίδες με ακατάλληλο περιεχόμενο στη Γραμμή Βοήθειας και Καταγγελιών 1480 https://internetsafety.pi.ac.cy/1480

Εθισμός

Περιγραφή:

Εθισμός στο Διαδίκτυο μπορεί να προκύψει με την πολύωρη ενασχόληση ατόμων σε διαδικτυακές δραστηριότητες όπως είναι τα παιχνίδια, δωμάτια συζητήσεων, ηλεκτρονικός τζόγος και άλλα.

Ένα άτομο είναι εθισμένο όταν χαρακτηρίζεται από τουλάχιστο τρία από τα πιο κάτω:

- Χρήση του Διαδικτύου για μεγαλύτερο χρονικό διάστημα από το προτιθέμενο
- Κατανάλωση υπερβολικού χρόνου ή/και χρήματος σε δραστηριότητες σχετικές με το Διαδίκτυο
- Συμπτώματα Συνδρόμου Απόσυρσης, όπως για παράδειγμα άγχος, έμμονη σκέψη για το Διαδίκτυο, όνειρα για το Διαδίκτυο
- Χρήση Διαδικτύου προκειμένου να αποφευχθούν συμπτώματα απόσυρσης
- Μείωση λειτουργικότητας του ατόμου. Συνήθως παραμελούν την προσωπική τους υγεία, γευματίζουν ανθυγιεινά, σταματούν τα αγαπημένα τους ενδιαφέροντα, εγκαταλείπουν το σχολείο, συγκρούονται έντονα στο σπίτι με τους γονείς τους, έχουν μεγάλη ένταση και θυμό που οδηγεί ακόμα και στη βία (Chakraborty, 2010)
- Συνέχιση χρήσης του Διαδικτύου παρά τη γνώση της παραπάνω δυσλειτουργίας

Σύμφωνα με στατιστικά στοιχεία της Μονάδας Εφηβικής Υγείας (Μ.Ε.Υ.) στην Ελλάδα, το φαινόμενο είναι συχνότερο σε αγόρια, σε δυσλειτουργικές οικογένειες και σε παιδιά με καταθλιπτικά συναισθήματα ή σύνδρομο υπερκινητικότητας.

Πού μπορεί να συμβεί: Συνήθως οι έφηβοι εθίζονται παίζοντας διαδικτυακά παιχνίδια ή/και τζόγο, Σε ιστοσελίδες κοινωνικής δικτύωσης

Αντιμετώπιση:

- Ευαισθητοποιούμαστε και ενημερωνόμαστε για το φαινόμενο του εθισμού
- Χρησιμοποιούμε το Διαδίκτυο με μέτρο, συμπεριλαμβάνοντας στο πρόγραμμά μας εναλλακτικές δραστηριότητες που περιλαμβάνουν ενασχόληση με ομαδικά αθλήματα, χορωδίες, χορό και άλλες
- Καλλιεργούμε ορθές στάσεις αξιοποίησης του Διαδικτύου από μικρές ηλικίες
- Καλλιεργούμε ορθές στάσεις αξιοποίησης του Διαδικτύου από μικρές ηλικίες. Εάν παρατηρήσουμε υπερβολική χρήση ή/και συμπεριφορές εθισμού αναζητούμε βοήθεια στη Γραμμή Βοήθειας και Καταγγελιών 1480 https://internetsafety.pi.ac.cy/1480

Παραπληροφόρηση

Περιγραφή:

Παραπληροφόρηση στο Διαδίκτυο είναι δυνατό να συμβεί με την παρουσίαση διάφορων ψευδών ή αναληθών ή τροποποιημένων πληροφοριών σε ιστοσελίδες, με πιθανό σκοπό την παραπλάνησή μας. Παραπληροφόρηση συμβαίνει και όταν οι πληροφορίες είναι ελλιπείς με αποτέλεσμα να οδηγήσουν σε λανθασμένα συμπεράσματα.

Πού μπορεί να συμβεί: Σε οποιαδήποτε σελίδα του Διαδικτύου που προσφέρει πληροφορίες

Αντιμετώπιση:

- Αξιολογούμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο και ελέγχουμε το συγγραφέα, την προέλευση της σελίδας, τη βιβλιογραφία της πληροφορίας
- Χρησιμοποιούμε πολλαπλές πηγές πληροφοριών και διασταυρώνουμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο
- Επισκεπτόμαστε βιβλιοθήκες, όχι απλώς το Διαδίκτυο, και χρησιμοποιούμε ποικιλία πηγών, όπως εφημερίδες, περιοδικά και βιβλία
- Χρησιμοποιούμε διάφορες μηχανές αναζήτησης και όχι μόνο μία για να βελτιωθεί σημαντικά η ικανότητά μας να βρίσκουμε ποιοτικές πληροφορίες
- Μαθαίνουμε πώς λειτουργεί το Διαδίκτυο και γνωρίζουμε πως ο καθένας μπορεί να δημιουργήσει μια διαδικτυακή τοποθεσία, χωρίς να τον ελέγχει κανείς. Γι' αυτό το λόγο απαιτείται να χρησιμοποιούμε πηγές που γενικά θεωρούνται έγκυρες
- Μαθαίνουμε πώς να διακρίνουμε ένα γεγονός από μια άποψη και να αναγνωρίζουμε την προκατάληψη, την προπαγάνδα και τις τοποθεσίες που χρησιμοποιούν ιδεολογικά στερεότυπα
- Εγκαθιστούμε φίλτρα λογισμικού που μπορούν να αποκλείσουν πηγές που περιέχουν μίσος, ρατσισμό και άλλου είδους προπαγάνδα

Ηλεκτρονικός Τζόγος

Περιγραφή:

Με τον όρο Ηλεκτρονικός Τζόγος εννοούμε τη δραστηριότητα κατά την οποία δύο ή περισσότερα άτομα συναντώνται διαδικτυακά με σκοπό την ανταλλαγή στοιχημάτων. Μια τέτοια δραστηριότητα περιλαμβάνει το ρίσκο της πραγματικής οικονομικής απώλειας ή του κέρδους.

Ένα από τα βασικότερα προβλήματα του τζόγου είναι η απώλεια χρημάτων. Κάποιος μπορεί να χάσει τις οικονομίες του, το σπίτι του, την περιουσία του ακόμη και το/τη σύζυγό της/του. Πολλοί είναι αυτοί που εθίζονται και δεν μπορούν να σταματήσουν πιστεύοντας πως στον επόμενο γύρο θα πάρουν τα λεφτά τους πίσω. Έτσι εκτός από την σπατάλη πολλών χρημάτων οδηγούνται παράλληλα στη σπατάλη πολλού χρόνου, παραμέληση των υποχρεώσεών τους με όλες τις επακόλουθες συνέπειες του εθισμού. Είναι γνωστό ότι ακόμα και η ενασχόληση με περιβάλλοντα τζόγου, στα όπου δεν γίνεται χρήση πραγματικών χρημάτων, μπορεί να προκαλέσει τον εθισμό (Hyder et al, 2008).

Η ευκολία πρόσβασης σε ιστοσελίδες ηλεκτρονικού τζόγου αυξάνει τους κινδύνους εμπλοκής παιδιών και εφήβων σε τέτοιες δραστηριότητες.

(Βίντεο από Συμβούλιο Μέσων Ενημέρωσης για Παιδιά και Νέους -Δανία)

Πού μπορεί να συμβεί: Σε ιστοσελίδες ειδικά κατασκευασμένες για ηλεκτρονικό τζόγο, Μέσα από ανεπιθύμητα μηνύματα που προσκαλούν τους χρήστες να παίξουν σε ηλεκτρονικά καζίνα, να ασχοληθούν με αθλητικά στοιχήματα και άλλα

Αντιμετώπιση:

- σελίδες που αφορούν ηλεκτρονικό τζόγο
- Αγνοούμε ανεπιθύμητα μηνύματα τα οποία μας προσκαλούν να παίξουμε σε ηλεκτρονικά καζίνα, να ασχοληθούμε με στοιχήματα και άλλα

Ιοί (Virus)

Περιγραφή:

Ιός είναι κακόβουλο πρόγραμμα, το οποίο εγκαθίσταται στον υπολογιστή, συνήθως εν αγνοία του χρήστη, και ενεργοποιείται είτε κάποια προκαθορισμένη χρονική στιγμή είτε ύστερα από κάποια συγκεκριμένη ενέργεια. Η ενεργοποίηση ενός ιού μπορεί να έχει ως αποτέλεσμα διάφορες συνέπειες, επικίνδυνες ή μη. Συγκεκριμένα, μπορεί να έχει ως αποτέλεσμα το συνεχές άνοιγμα διαφόρων παραθύρων στην οθόνη, μπορεί όμως και να προκαλέσει την καταστροφή δεδομένων σε αρχεία ή άλλες βλάβες. Ένας ιός ενσωματώνεται σε ηλεκτρονικά μηνύματα και προγράμματα, έτσι ώστε όταν ανοίξουμε τα μηνύματα αυτά ή εκτελέσουμε τα προγράμματα, ενεργοποιούμε άθελά μας και τον ιό.

Πού μπορεί να συμβεί

- Μέσω του ηλεκτρονικού ταχυδρομείου όπου λαμβάνουμε μολυσμένα συνημμένα αρχεία (attachments) ηλεκτρονικών μηνυμάτων (e-mail), τα οποία όταν τα ανοίξουμε ενεργοποιούμε άθελά μας τους ιούς
- Κατά την εγκατάσταση μολυσμένων προγραμμάτων (κάποιες φορές εκτελούμε εν αγνοία μας μολυσμένα προγράμματα με αποτέλεσμα να ενεργοποιούμε τους ιούς)
- Κατά την πλοήγηση μας σε μολυσμένες σελίδες (ιστοσελίδες που έχουν δημιουργηθεί με τέτοιο τρόπο ώστε να μεταδίδουν ιούς στον υπολογιστή μας, όταν τις επισκεφτούμε ή όταν κατεβάσουμε ένα αρχείο).
- Κατά την ανταλλαγή αρχείων (εν αγνοία μας παίρνουμε/ανοίγουμε αρχεία, τα οποία είναι μολυσμένα).

Αντιμετώπιση:

- Δεν ανοίγουμε ηλεκτρονικά μηνύματα που έχουν σταλεί από άγνωστους αποστολείς
- Αποφεύγουμε ύποπτες ιστοσελίδες και, αν μπούμε κατά λάθος σε κάποια, την εγκαταλείπουμε αμέσως. Αν εμφανιστούν παράθυρα που ζητούν να συμφωνήσουμε σε οτιδήποτε τα κλείνουμε αμέσως και δεν πατούμε τυχόν κουμπιά μέσα σε αυτά
- Έχουμε στον υπολογιστή μας εγκατεστημένο και ενημερωμένο πρόγραμμα εναντίον των ιών (antivirus software)
- Επιτρέπουμε έλεγχο του υπολογιστή μας για ιούς δια μέσου του Διαδικτύου, μόνο εάν εμείς το έχουμε ζητήσει από έμπιστη ιστοσελίδα
- Χρησιμοποιούμε firewall, λογισμικό που αποτρέπει μη εξουσιοδοτημένα άτομα να αποκτήσουν πρόσβαση στον υπολογιστή μας
- Δημιουργούμε εφεδρικά αρχεία ασφαλείας, τα οποία αποθηκεύουμε σε μονάδα αποθήκευσης εκτός του ηλεκτρονικού υπολογιστή ή ακόμα και σε άλλο φυσικό χώρο από αυτόν που βρίσκεται ο υπολογιστής μας
- Αποφεύγουμε την εγκατάσταση εκτελέσιμων αρχείων, αρχείων με κατάληξη .exe, εκτός και αν γνωρίζουμε και εμπιστευόμαστε την προέλευσή τους

Παιδική Πορνογραφία

Περιγραφή:

Παιδική πορνογραφία ορίζεται ως οι αναπαραστάσεις ανηλίκων που συμμετέχουν σε σεξουαλικές πράξεις ή καταστάσεις που υποδηλώνουν σεξουαλικές δραστηριότητες. Μερικές φορές ο ορισμός περιλαμβάνει εικόνες που έχουν υποστεί επεξεργασία από ηλεκτρονικό υπολογιστή. Η παιδική πορνογραφία θεωρείται έγκλημα και υπόκειται σε ποινικές κυρώσεις.

Η παιδική πορνογραφία ορίζεται διαφορετικά από τη νομοθεσία της κάθε χώρας. Σύμφωνα με τη Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης, η παιδική πορνογραφία έχει τις εξής μορφές:

- Ένας ανήλικος που συμμετέχει σε σεξουαλική δραστηριότητα.
- Ένα άτομο που συμμετέχει σε σεξουαλική δραστηριότητα προσποιούμενο ότι είναι ανήλικο.
- Ρεαλιστικές εικόνες που αναπαριστούν ένα ανήλικο να συμμετέχει σε σεξουαλικές δραστηριότητες.

Σύμφωνα με ανακοίνωση στην ιστοσελίδα του φορέα για την ασφάλεια του Διαδικτύου στην Κύπρο (www.cyberethics.info) τον Αύγουστο του 2009, η 14η ιστοσελίδα προτίμησης των Κυπρίων είναι πορνογραφικού περιεχομένου. Η 14η θέση είναι η ψηλότερη θέση προτίμησης για πορνογραφική ιστοσελίδα ανάμεσα σε ευρωπαϊκές χώρες. Αυτές οι πληροφορίες είναι ανησυχητικές, γιατί σύμφωνα με ειδικούς κλινικούς σεξολόγους, οι άνθρωποι που εθίζονται στην πορνογραφία τείνουν να έχουν διαταραγμένη αντίληψη για τις ανθρώπινες σχέσεις, κάτι που μπορεί να τους αποξενώσει από τους συντρόφους τους. Επίσης, επισημαίνουν ότι οι ανήλικοι είναι πιο επιρρεπείς σε αυτό γιατί τους λείπει η συναισθηματική ωριμότητα.

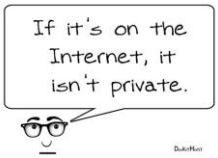
Η εξάπλωση των κυκλωμάτων παιδοφιλίας είναι ανησυχητική. Τα κυκλώματα αυτά είναι ομάδες ατόμων, τα οποία εργάζονται μαζί μέσω του Διαδικτύου με στόχο τη συλλογή και διανομή πορνογραφικού υλικού για τη δική τους ικανοποίηση. Τέτοιες ενέργειες αποτελούν έγκλημα και υπόκεινται στο νόμο.

Πού μπορεί να συμβεί: Σε ιστοσελίδες τις οποίες χειρίζονται κυκλώματα παιδοφιλίας, Σε ηλεκτρονικά μηνύματα με φωτογραφίες παιδικής πορνογραφίας

Αντιμετώπιση

- Αν γνωρίζουμε κάποιον που ασχολείται με την παιδική πορνογραφία, τον καταγγέλλουμε στη Γραμμή Βοήθειας και Καταγγελιών 1480 https://internetsafety.pi.ac.cy/1480 ή/και στην αστυνομία στο Γραφείο Καταπολέμησης Ηλεκτρονικού Εγκλήματος 22808200
- Αποφεύγουμε διαδικτυακές συζητήσεις με αγνώστους και κυρίως δεν συμφωνούμε ποτέ να συναντήσουμε κάποιο «φίλο» που, μόλις γνωρίσαμε διαδικτυακά
- Αν κάποια διαδικτυακή συζήτηση μάς κάνει να νιώσουμε άβολα την σταματάμε αμέσως και αναφέρουμε το γεγονός σε κάποιο ενήλικα.
- Δεν στέλνουμε φωτογραφίες που είναι δυνατό να μας εκθέσουν μέσω του ηλεκτρονικού ταχυδρομείου
- Δεν ανεβάζουμε σε ιστοσελίδες κοινωνικού δικτύου π.χ. στο Facebook ή Hi5 φωτογραφίες μας, οι οποίες είναι προκλητικές
- Δεν δίνουμε προσωπικά στοιχεία σε ιστοσελίδες αμφιβόλου προελεύσεως και περιεχομένου.
- Έχουμε πρόγραμμα προστασίας από κακόβουλο λογισμικό (antivirus, antispyware, firewall)

Παραβίαση Ιδιωτικής Ζωής



Περιγραφή:

Σε κάθε βήμα της περιδιάβασής μας στο Διαδίκτυο "προσφέρουμε" προσωπικές πληροφορίες. Αυτές οι πληροφορίες είναι σαν ένα γρίφος που πρέπει να συμπληρωθεί για να αποκαλυφθεί η εικόνα μας. Η περιήγηση μας στο Διαδίκτυο έχει πολλά κοινά με τη ζωή

μας στο φυσικό κόσμο. Έτσι τίθενται κάποια πολύ σοβαρά ζητήματα: της προστασίας των προσωπικών μας δεδομένων, της ορθής και ηθικής επικοινωνίας με τη βοήθεια της τεχνολογίας και το γεγονός πως ό,τι και αν κάνουμε στο Διαδίκτυο αφήνει ίχνη.

Όταν στέλνουμε ηλεκτρονικά μηνύματα σίγουρα δίνουμε πληροφορίες στο άτομο με το οποίο επικοινωνούμε. Εάν δεν είμαστε προσεχτικοί, μπορεί επίσης να δώσουμε πληροφορίες σε ένα μεγάλο αριθμό ατόμων, συμπεριλαμβανομένου του εργοδότη μας, της κυβέρνησης, του παροχέα ηλεκτρονικού ταχυδρομείου και οποιουδήποτε βρίσκεται στη διαδρομή του μηνύματός μας προς τον παραλήπτη.

Προσεχτικοί πρέπει να είμαστε και όταν συμμετέχουμε σε ομάδες συζητήσεων (groups ή listserves) του Διαδικτύου όπου είμαστε μέλη και δίνουμε προσωπικές πληροφορίες σε όλα τα μέλη της ομάδας (π.χ. διεύθυνση του ηλεκτρονικού μας ταχυδρομείου). Δεν απαγορεύεται σε μέλος να πάρει και να διανέμει τη διεύθυνσή μας.

Σημαντικό είναι να γνωρίζουμε ότι κατά την πλοήγησή μας στο Διαδίκτυο με χρήση οποιουδήποτε browser αφήνουμε ίχνη. Όταν απλά κοιτάζουμε πληροφορίες στο Διαδίκτυο πολύ πιθανόν ο browser μας να δίνει τον αριθμό του υπολογιστή και τις σελίδες που επισκεφθήκαμε στον παροχέα Διαδικτύου. Αν το browser χειρίζεται και το ηλεκτρονικό μας ταχυδρομείο, τότε πολύ πιθανόν να παρέχει την ηλεκτρονική διεύθυνση και το τηλέφωνό μας.

Επίσης πολλές από τις ιστοσελίδες που επισκεπτόμαστε, φυλάνε στον υπολογιστή μας δεδομένα για την επίσκεψη μας, τα λεγόμενα “Cookies”. Τα Cookies είναι μικρά κομμάτια από πληροφορίες όπως το όνομα χρήστη, πληροφορίες της εγγραφής μας σε μια σελίδα, προτιμήσεις, διαδικτυακά «καλάθια με ψώνια» και λοιπά. Οι νόμιμες εταιρείες χρησιμοποιούν τα Cookies για να κάνουν προσφορές σε χρήστες που τους επισκέπτονται ξανά. Παράνομες εταιρείες χρησιμοποιούν Cookies για να πάρουν πληροφορίες για τους χρήστες και να τις πουλήσουν σε εταιρείες Marketing.

Προσεχτικοί πρέπει να είμαστε και όταν στέλνουμε Μηνύματα της Στιγμής (Instant Messages) π.χ. με Google Talk ή με Microsoft Live Messenger. Πρέπει να γνωρίζουμε ότι πολλές από αυτές τις εταιρείες αυτόματα αποθηκεύουν τα μηνύματά μας, εκτός και εάν έχουμε κάνει τις ανάλογες ρυθμίσεις.

Κοινωνικά Δίκτυα όπως το Facebook και MySpace επιτρέπουν την αποστολή φωτογραφιών και την αποθήκευση προσωπικών σημειώσεων. Προσωπικές πληροφορίες που ανταλλάσσονται σε τέτοια δίκτυα μπορεί να προκαλέσουν προβλήματα του χρήστη με το σχολείο, τον εργοδότη του και όχι μόνο. Τέτοιες ιστοσελίδες δέχονται συχνά και με ευκολία επισκέψεις από παιδοφίλους που ενδιαφέρονται είτε να παραπλανήσουν ανήλικους σε πραγματικές συναντήσεις ή να κλέψουν φωτογραφίες και πληροφορίες που ανταλλάσσονται από άτομα που χρησιμοποιούν αυτά τα δίκτυα.

Ίχνη στο Διαδίκτυο είναι δυνατό να αφήσουμε και κατά τη χρήση ιστολογίων (Blog). Πολλοί νεαροί που χρησιμοποιούν το Διαδίκτυο, έχουν δημιουργήσει το δικό τους ιστολόγιο (Blog), κάτι σαν ενημερωτικό φυλλάδιο ή εφημερίδα, το οποίο ανανεώνεται συχνά και είναι για ελεύθερη πρόσβαση. Οι χρήστες των ιστολογίων μπορούν να καταθέσουν σχόλια. Σε κάποια από τα ιστολόγια χρειάζεται να κάνει κάποιος εγγραφή για να μπορεί να σχολιάσει, δίνοντας έτσι πληροφορίες όπως ηλεκτρονική διεύθυνση, όνομα κ.λπ.

Πού μπορεί να συμβεί: Μέσω ηλεκτρονικού ταχυδρομείου, Σε ομάδες συζητήσεων (groups ή list-serves) του Διαδικτύου, Κατά την πλοήγηση μας στο Διαδίκτυο με οποιοδήποτε browser, Όταν στέλνουμε μηνύματα της στιγμής (Instant Messages), Σε κοινωνικά δίκτυα, όπως το Facebook και MySpace, Σε ιστολόγια του Διαδικτύου (blogs)

Αντιμετώπιση

- Διαβάζουμε τους κανονισμούς του παροχέα Διαδικτύου για ιδιωτικότητα και τους εμπεδώνουμε. Αν δεν συμφωνούμε, δεν προχωράμε στη δημιουργία λογαριασμού για την υπηρεσία που προσφέρει
- Ανανεώνουμε τα browsers μας με αναβαθμίσεις ασφαλείας (security updates), ώστε οι τρόποι προστασίας μας να γίνονται συστηματικά καλύτεροι
- Αλλάζουμε τις ρυθμίσεις του browser μας ώστε να έχει υψηλή ιδιωτικότητα και να απαγορεύει τα cookies. Πρέπει να γνωρίζουμε όμως ότι, εάν επιλέξουμε ψηλή ιδιωτικότητα, τότε μπορεί να μην μπορέσουμε να δουλέψουμε πάνω στους τραπεζικούς μας λογαριασμούς ή να ψωνίσουμε χρησιμοποιώντας το Διαδίκτυο, χωρίς αλλαγή αυτών των ρυθμίσεων
- Διαγράφουμε cookies που αποθηκεύονται στον υπολογιστή μας
- Προσπαθούμε να χρησιμοποιούμε διάφορες μηχανές αναζήτησης κάθε φορά. Με αυτόν τον τρόπο μειώνουμε το μέγεθος της πληροφορίας που κατακρατείται από μια ιστοσελίδα. Για παράδειγμα μπορούμε να χρησιμοποιούμε Yahoo για το ηλεκτρονικό ταχυδρομείο και Google για αναζητήσεις
- Θυμόμαστε ότι μπορεί είτε ο αποστολέας είτε ο παραλήπτης, να αποδεχθεί να αποκαλυφθεί η ηλεκτρονική μας διεύθυνση (e-mail) όταν συμμετέχουμε σε διαδικτυακές συζητήσεις, που κάποτε ονομάζονται list-servers. Επίσης, θυμόμαστε ότι με τη συμμετοχή μας σε τέτοιες συζητήσεις διαθέτουμε

την ηλεκτρονική μας διεύθυνση σε ένα, μεγάλο πολλές φορές, αριθμό ατόμων

- Εγκαθιστούμε αντικατασκοπικό πρόγραμμα (anti-spyware) για αποτροπή της παράνομης παρακολούθησης της διαδικτυακής μας δραστηριότητας
- Προστατεύουμε την ιδιωτική μας ζωή, αποφεύγοντας τη δημοσιοποίηση προσωπικών δεδομένων ή δεδομένων που αφορούν φίλους και οικογένεια. Το ίδιο ισχύει και για προσωπικές φωτογραφίες και βίντεό μας
- Οι υπηρεσίες ιστολογίων συνήθως μας επιτρέπουν κάποιο έλεγχο ως προς το τι μπορούμε να μοιραζόμαστε δημόσια, π.χ. τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή ακόμα και τα σχόλιά μας. Διαβάζουμε τις σχετικές συμφωνίες και δηλώσεις απορρήτου προσεκτικά και γνωρίζουμε τι απαιτείται και τι αποκαλύπτεται
- Τα πιο πολλά ιστολόγια επιτρέπουν σχόλια στους αναγνώστες. Πολλά από αυτά επιτρέπουν ανώνυμα σχόλια αλλά κάποια απαιτούν εγγραφή και τουλάχιστον μια ηλεκτρονική διεύθυνση. Σκεφτόμαστε προσεκτικά πόσες πληροφορίες θέλουμε να δώσουμε και εάν θέλουμε προσωπικά δεδομένα να συνδεθούν με τα σχόλιά μας
- Αποφασίζουμε ποιο θέλουμε να είναι το ακροατήριο ενός ιστολογίου. Εάν γράφουμε μόνο για φίλους και την οικογένεια μπορούμε να κάνουμε το ιστολόγιο προσβάσιμο, επιβάλλοντας χρήση κωδικού
- Χρησιμοποιώντας ψευδώνυμα σε ιστολόγια μπορούμε να προστατέψουμε την ταυτότητά μας.
- Θυμόμαστε οτι έχουμε την επιλογή να ρυθμίσουμε τις μηχανές αναζήτησης έτσι ώστε να μην παρουσιάζουν το ιστολόγιο μας στα αποτελέσματά τους.
- Χρησιμοποιούμε κωδικούς ασφαλείας από συνδυασμό γραμμάτων και αριθμών που είναι δύσκολο να μαντέψει ή να ανακαλύψει κάποιος διασταυρώνοντας πληροφορίες. Αποφεύγουμε, επίσης, κωδικούς ασφαλείας που είναι αποφθέγματα ή λέξεις από λεξικά
- Δεν μοιραζόμαστε τους κωδικούς πρόσβασης που έχουμε με άλλα άτομα
- Επικοινωνούμε με τα άτομα που δημοσιεύουν προσωπικά μας στοιχεία σε ιστολόγιο και ζητούμε να τα αφαιρέσουν – σε ιστολόγια συνήθως βρίσκονται τα στοιχεία επικοινωνίας όπως η ηλεκτρονική μας διεύθυνση (e-mail) όσων συμμετέχουν – ή επικοινωνούμε με τους υπευθύνους του ιστολογίου
- Αντιλαμβανόμαστε ότι κατά την πλοήγησή μας στο Διαδίκτυο αφήνουμε ίχνη, επομένως πρέπει να είμαστε προσεκτικοί
- Σεβόμαστε και δεν δημοσιοποιούμε προσωπικά δεδομένα άλλων ατόμων χωρίς τη συγκατάθεσή τους.

Παραποίηση Γλώσσας

Περιγραφή:

Η ανάγκη για γρήγορη και εύκολη επικοινωνία, μια συνήθεια που την αποκτήσαμε με την είσοδο της κινητής τηλεφωνίας και του Διαδικτύου στη ζωή μας, άρχισε να οδηγεί στην Παραποίηση της Γλώσσας μας. Αντί ελληνικά, δηλαδή, χρησιμοποιούνται τα “greeklish”, ελληνικά γραμμένα με λατινικούς χαρακτήρες, στα οποία ο τονισμός και η ορθογραφία δεν είναι σημαντικά. Για παράδειγμα η φράση «θα σε δω σε λίγο» αποδίδεται εσφαλμένα «tha se do se ligo».

Αυτό ξεκίνησε, επειδή η χρήση του ελληνικού αλφαβήτου στην τεχνολογία ήταν είτε αδύνατη είτε δύσκολη. Παρόλο που τα τελευταία χρόνια πολλοί υπολογιστές και προγράμματα χρησιμοποιούν την ελληνική γλώσσα, πάρα πολλοί δεν επικοινωνούν στα ελληνικά αλλά σε greeklish όταν στέλνουν μηνύματα στο κινητό ή όταν χρησιμοποιούν το Διαδίκτυο. Υπάρχουν επίσης ιστοσελίδες όπου η γλώσσα που χρησιμοποιείται δεν είναι τα Ελληνικά αλλά τα greeklish και σε σελίδες του Διαδικτύου διατίθενται greeklish converters, προγράμματα που μετατρέπουν greeklish σε Ελληνικά και το αντίστροφο. Όλα αυτά μπορούν να οδηγήσουν όχι μόνο στη παραποίηση της γλώσσας μας αλλά, όπως κάποιοι υποστηρίζουν και στην αλλοίωση της ταυτότητας των Ελλήνων.

Επίσης είναι πολύ συχνό φαινόμενο οι νεαροί να χρησιμοποιούν εικόνες ή διάφορα άλλα ακρώνυμα για να επικοινωνήσουν γρήγορα και άμεσα. Αυτά συμπεριλαμβάνουν τα εικονίδια συναισθημάτων (emotions) και τα ακρώνυμα. Τα Emotions είναι εικονίδια τα οποία στόχο έχουν να εκφράσουν κάποια συναισθήματα. Μπορούμε να δημιουργήσουμε ένα emotion πληκτρολογώντας τον κατάλληλο συνδυασμό

χαρακτήρων (π.χ. ο συνδυασμός σημαίνει «χαμόγελο»). Τα Ακρώνυμα είναι συνδυασμοί πλήκτρων για συντομογραφία λέξεων ή ακόμα και προτάσεων (π.χ. ο συνδυασμός POS σημαίνει «Parent Over Shoulder»).

Πού μπορεί να συμβεί: Όταν στέλνουμε μηνύματα μέσω κινητού τηλεφώνου (sms), Όταν γράφουμε ηλεκτρονικά μηνύματα στο ηλεκτρονικό ταχυδρομείο (e-mail), Σε κάθε δραστηριότητα του Διαδικτύου που χρησιμοποιεί το γραπτό λόγο ως μέσο επικοινωνίας

Αντιμετώπιση

- Χρησιμοποιούμε την ελληνική γλώσσα, όπου αυτό είναι δυνατό

Φυσικές Παθήσεις

Περιγραφή:

Με την εισαγωγή του Διαδικτύου στη ζωή μας, οι ώρες χρήσης του υπολογιστή έχουν αυξηθεί κατακόρυφα. Η πολύωρη χρήση του Διαδικτύου είτε είναι για έρευνα είτε για παιχνίδι είτε για κοινωνικοποίηση εγκυμονεί κινδύνους για την υγεία μας. Πέρα από τις διαταραχές στην όραση και τις υποψίες για ενδεχόμενα προβλήματα εξαιτίας της έκθεσης σε ακτινοβολία, κυρίως από τις οθόνες, εκείνοι που ασχολούνται για ώρες μπροστά στον υπολογιστή χωρίς διάλειμμα ή εναλλαγή δραστηριοτήτων κάνοντας μεγάλο αριθμό επαναλαμβανόμενων κινήσεων μπορεί να προσβληθούν από διάφορες μυοσκελετικές παθήσεις. Κακώσεις όπως ο ευθειασμός του αυχένα, ο πόνος του αγκώνα (tennis elbow), τενοντίτιδα, πηχαιοκαρπική άρθρωση και άλλες παθήσεις έχουν συνδέσει το όνομά τους με την υπερβολική χρήση του υπολογιστή.

Μια φυσική πάθηση μπορεί να συμβεί ανεξάρτητα με το είδος της δραστηριότητας στο Διαδίκτυο όταν:

- Η χρήση του υπολογιστή είναι πολύωρη και χωρίς διαλείμματα
- Η απόσταση των ματιών μας από τον υπολογιστή είναι λανθασμένη και η οθόνη βρίσκεται σε λανθασμένο ύψος από το επίπεδο των ματιών μας
- Δεν καθόμαστε σε ορθή θέση μπροστά από τον υπολογιστή
- Το δωμάτιο στο οποίο βρίσκεται ο υπολογιστής δεν φωτίζεται ομοιόμορφα
- Οι προδιαγραφές του εξοπλισμού του υπολογιστή δεν είναι τουλάχιστον εργονομικές

Αντιμετώπιση:

- Βεβαιωνόμαστε ότι ο εξοπλισμός του υπολογιστή ακολουθεί τις διεθνείς προδιαγραφές εργονομίας για την ασφάλεια του χρήστη από φυσικές παθήσεις
- Βεβαιωνόμαστε ότι η απόσταση της οθόνης από τα μάτια μας είναι μεταξύ 50 και 70 εκατοστών
- Βεβαιωνόμαστε ότι το κέντρο της οθόνης βρίσκεται περίπου 15° από το επίπεδο των ματιών μας. Αντιμετώπιση Κλείνουμε σε τακτά διαστήματα τα μάτια μας για λίγα λεπτά
- Εστιάζουμε κάθε 10 λεπτά περίπου σε κάποιο μακρινό σημείο, εκτός οθόνης
- Βεβαιωνόμαστε ότι το δωμάτιο του υπολογιστή φωτίζεται ομοιόμορφα και δεν υπάρχει πηγή φωτός στο πλάι της οθόνης
- Βεβαιωνόμαστε ότι κατά την πληκτρολόγηση η παλάμη και ο καρπός είναι σε ευθεία παράλληλη με το επίπεδο του δαπέδου
- Βεβαιωνόμαστε ότι πιάνουμε το ποντίκι χρησιμοποιώντας όλη την παλάμη μας και το μετακινούμε κινώντας όλο το βραχίονά μας
- Γενικά, βεβαιωνόμαστε ότι το σώμα μας έχει άνετη στάση όταν δουλεύουμε με τον υπολογιστή
- Σηκωνόμαστε και περπατάμε μετά από μία ώρα εντατικής ενασχόλησης με τον υπολογιστή
- Εναλλάσσουμε εργασίες που γίνονται με υπολογιστή με εργασίες στις οποίες δεν απαιτείται η χρήση υπολογιστή

Υποκλοπή Προσωπικών Δεδομένων (Phishing)

Περιγραφή:

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,ης 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/της, όπως προσωπικούς λογαριασμούς, συνδρομές, e-mail, κωδικούς, κ.λπ.

Κάποιοι θεωρούν τις Απάτες (Scams) ως ένα είδος υποκλοπής, μόνο που οι Απάτες συνήθως δεν ενδιαφέρονται για τις προσωπικές μας πληροφορίες, αλλά προσπαθούν να προκαλέσουν τον οίκτο μας για τον ανθρώπινο πόνο ώστε να προσφέρουμε λεφτά για να βοηθήσουμε ένα δήθεν καλό σκοπό. Για παράδειγμα, σχεδόν κάθε μεγάλη καταστροφή (σεισμός, πλημμύρες, πείνα, πόλεμος) έχει προκαλέσει πολυάριθμες ηλεκτρονικές απάτες, μηνύματα σε ιστοσελίδες που ζητούν από τους χρήστες να προσφέρουν λεφτά για να βοηθήσουν για κάποιο καλό σκοπό. Πολλοί άνθρωποι έχουν χάσει πολλά λεφτά για τέτοιους “καλούς” σκοπούς. Κάποιοι έχουν χάσει ακόμα και τη ζωή τους, καθώς έχουν ταξιδέψει σε άλλες χώρες για να γνωρίσουν αυτούς που επωφελούνταν των προσφορών τους.

Πού μπορεί να συμβεί:

- Μέσω ηλεκτρονικών μηνυμάτων (e-mail) που ξεγελούν το χρήστη ώστε να οδηγηθεί σε πλαστές ιστοσελίδες
- Κατά το φυλλομέτρημα οποιασδήποτε σοβαρής ιστοσελίδας, η οποία έχει μολυνθεί απο ιο
- Κατά τη περιήγηση σε ιστοσελίδες με αναληθή προϊόντα και πληροφορίες
- Κατά τη χρήση οποιουδήποτε φυλλομετρητή Διαδικτύου, ο οποίος έχει μολυνθεί με πρόγραμμα που καταγράφει προσωπικές και οικονομικές πληροφορίες,

τις οποίες χρησιμοποίησε ο χρήστης σε επισκέψεις του σε σελίδες που του τις ζητούν

Αντιμετώπιση:

- Ελέγχουμε πάντοτε τον αποστολέα ενός μηνύματος και διερευνούμε την υπόστασή του
- Γνωρίζουμε ότι νόμιμοι φιλανθρωπικοί οργανισμοί συνήθως στέλνουν ηλεκτρονικές εκκλήσεις για βοήθεια μόνο σε ανθρώπους που το έχουν ζητήσει. Άλλες παρόμοιες εκκλήσεις, που σχεδόν πάντα ακολουθούν ένα μεγάλο καταστροφικό γεγονός, είναι συνήθως ψευδείς. Επισκεπτόμαστε την επίσημη ιστοσελίδα του οργανισμού για να επιβεβαιώσουμε την αξιοπιστία της έκκλησης
- Ελέγχουμε πάντα τη νομιμότητα φιλανθρωπικών ιδρυμάτων, αναζητώντας σχετικές επίσημες ιστοσελίδες (π.χ. http://www.charitynavigator.org)
- Τηλεφωνούμε ή πηγαίνουμε απευθείας στην ιστοσελίδα ενός φιλανθρωπικού οργανισμού και βρίσκουμε τρόπους να προσφέρουμε μέσω αυτής, αντί να απαντούμε και να κατευθυνόμαστε από εκκλήσεις-μηνύματα που παραλαμβάνουμε
- Δεν ενεργοποιούμε απερίσκεπτα συνδέσμους από μηνύματα αμφιβόλου προελεύσεως και περιεχομένου γιατί αυτά μπορούν να μας οδηγήσουν σε παράνομες ή επιβλαβείς ιστοσελίδες που μπορεί να μοιάζουν νόμιμες
- Αποφεύγουμε να δίνουμε προσωπικές πληροφορίες μέσω του Διαδικτύου. Είναι απίθανο μια τράπεζα ή ένας φιλανθρωπικός οργανισμός να ζητά τέτοιες πληροφορίες με αυτόν τον τρόπο
- Γνωρίζουμε ότι σοβαρές τράπεζες και επενδυτικοί οργανισμοί χρησιμοποιούν το πρωτόκολλο επικοινωνίας https αντί για http για ασφάλεια των προσωπικών δεδομένων των πελατών τους. Το “S” σημαίνει ασφαλές πρωτόκολλο. Η ασφάλεια αυτή διακρίνεται στη γραμμή διεύθυνσης μιας ιστοσελίδας (https://……)
- Όταν μας ζητηθεί να πληκτρολογήσουμε ένα ψευδώνυμο συνομιλίας, διαλέγουμε ένα όνομα που δεν προδίδει τα προσωπικά μας στοιχεία όπως το όνομα, το επίθετο, την ημερομηνία γέννησής μας, τον χώρο διαμονής κ.λ.π.

Sextortion

Περιγραφή:

Ο σεξουαλικός διαδικτυακός εξαναγκασμός και εκβιασμός σε άτομα, γνωστός και ως «sextortion», είναι μία μορφή σεξουαλικής εκμετάλλευσης, κατά την οποία, σεξουαλικές πληροφορίες (π.χ., βίντεο, εικόνες) χρησιμοποιούνται για σεξουαλική ή και οικονομική εκμετάλλευση των θυμάτων.

Πού και πώς μπορεί να συμβεί:

Οι διαδικτυακοί δράστες προσεγγίζουν τα θύματά τους, συνήθως, μέσω των μέσων κοινωνικής δικτύωσης (π.χ., Facebook, Twitter), παριστάνοντας συνομήλικους του ιδίου ή του αντιθέτου φύλου ή οικειοποιώντας την ταυτότητα ενός ελκυστικού άνδρα ή μίας ελκυστικής γυναίκας. Κατά τη διάρκεια της μεταξύ τους επικοινωνίας και των συνομιλιών που αναπτύσσουν, αφού αποκτήσουν την εμπιστοσύνη των θυμάτων και τα κάνουν να αισθανθούν όμορφα και οικεία, αξιώνουν υλικό ευαίσθητων προσωπικών δεδομένων (φωτογραφίες ή και βίντεο). Αφού παραλάβουν το σχετικό υλικό, στη συνέχεια, οι διαδικτυακοί δράστες, υπό την απειλή να δημοσιεύσουν το υλικό στο διαδίκτυο ή να το αποστείλουν στο οικείο περιβάλλον των θυμάτων, αποκαλύπτουν τους πραγματικούς τους σκοπούς, που είναι κυρίως σεξουαλικού ή και οικονομικού ενδιαφέροντος. Ειδικότερα, οι δράστες απαιτούν είτε την παραγωγή πρωτότυπου υλικού πορνογραφίας (φωτογραφίες ή και βίντεο με πορνογραφικό περιεχόμενο) είτε την κατ’ ιδίαν συνάντηση με τα θύματά τους είτε την καταβολή κάποιου σημαντικού χρηματικού ποσού.

Τι μπορείς να κάνεις αν πέσεις θύμα σεξουαλικού εξαναγκασμού και εκβιασμού;

Πολλά από τα περιστατικά σεξουαλικού διαδικτυακού εκβιασμού και εξαναγκασμού δεν καταγγέλλονται στις αρμόδιες Αρχές, είτε γιατί τα θύματα αισθάνονται ντροπή για το υλικό που κλήθηκαν να παράγουν είτε γιατί δε γνωρίζουν ότι έχει διαπραχθεί έγκλημα σε βάρος τους. Για τον λόγο αυτό, η πανευρωπαϊκή εκστρατεία ενημέρωσης «Say No!» απευθύνεται σε άτομα που στοχοποιούνται από επιτήδειους και συμβουλεύει: «Μην ενδώσετε, πληρώνοντας τον εκβιασμό και μην αισθάνεστε ντροπή να το καταγγείλετε στις αρμόδιες Αρχές επιβολής του νόμου (Αστυνομικές Αρχές)».

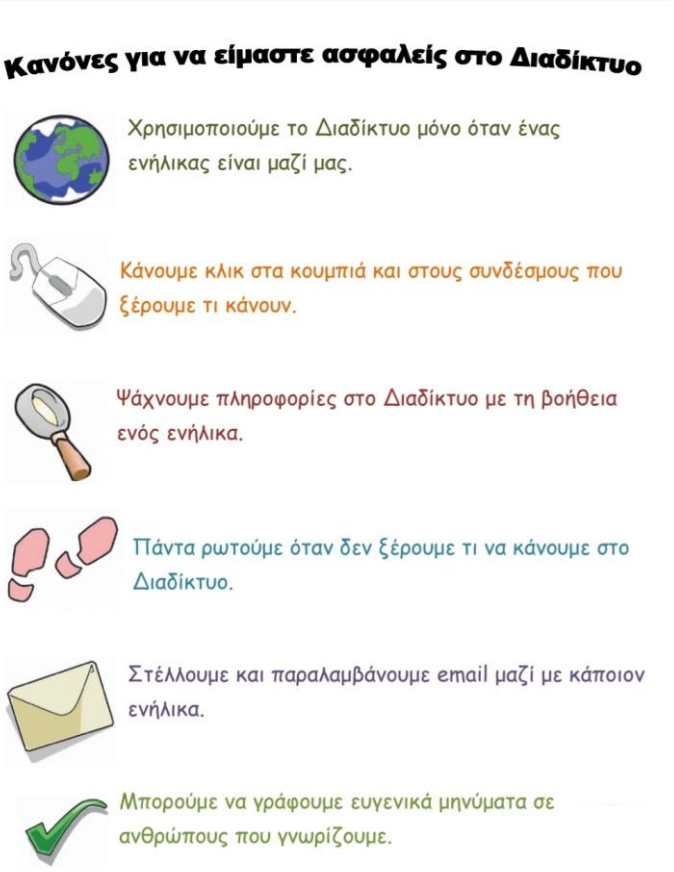
Σε περίπτωση που έχετε πέσει θύμα διαδικτυακού σεξουαλικού εξαναγκασμού και εκβιασμού, προτείνεται όπως ακολουθήσετε τα παρακάτω βήματα:

- Διατηρήστε τη ψυχραιμία σας
- Μην αποστείλετε άλλο υλικό ή καταβάλετε οποιοδήποτε χρηματικό ποσό και διακόψτε κάθε επικοινωνία με τον δράστη
- Μην διαγράψετε τα αποδεικτικά στοιχεία
- Κρατήσετε στιγμιότυπα οθόνης (screenshots) των αποδεικτικών στοιχείων (π.χ., συνομιλίες, e-mail)
- Χρησιμοποιήστε τα ενσωματωμένα εργαλεία αναφοράς και καταγγελιών του μέσου κοινωνικής δικτύωσης, στο οποίο έχετε πέσει θύμα
- «Μπλοκάρετε» το διαδικτυακό δράστη
- ΜΗΝ ΦΟΒΑΣΤΕ ΝΑ ΜΙΛΗΣΕΤΕ! Αναφέρετε το συμβάν στη Δίωξη Ηλεκτρονικού Εγκλήματος ή καλέστε για άμεση βοήθεια και καθοδήγηση, στη δωρεάν

ανώνυμη Γραμμή Βοήθειας (Helpline) και Καταγγελιών (Hotline) 1480.

Πώς να αποφύγετε να γίνετε θύμα διαδικτυακού σεξουαλικού εξαναγκασμού και εκβιασμού:

- Ενεργοποιήστε τις ρυθμίσεις απορρήτου στα μέσα κοινωνικής δικτύωσης στο Διαδίκτυο
- Αποφύγετε αιτήματα φιλίας από αγνώστους/ες και μην επικοινωνείτε με άτομα στο Διαδίκτυο, τα οποία δεν γνωρίζετε προσωπικά
- Μην μοιράζεστε/κοινοποιείτε προσωπικές πληροφορίες, φωτογραφικό υλικό ή άλλο περιεχόμενο σε άτομα εκτός του φιλικού σας πλαισίου
- Μην μοιράζεστε/στέλνετε υλικό (π.χ., εικόνες, βίντεο) ευαίσθητου περιεχομένου στο διαδίκτυο ή συμμετέχετε σε σεξουαλική συμπεριφορά μέσω web καμερών
- Μην ανοίγετε συνημμένα αρχεία και συνδέσμους από άτομα που δεν γνωρίζετε
- Απενεργοποιήστε τις ηλεκτρονικές σας συσκευές και τις web κάμερες, όταν δεν τις χρησιμοποιείτε
- Ενημερωθείτε για τους κινδύνους στο Διαδίκτυο και μάθετε πώς να τους αντιμετωπίσετε με ασφάλεια και υπευθυνότητα. Για την καλύτερη ενημέρωσή σας, μπορείτε να καλέσετε στη δωρεάν ανώνυμη Γραμμή Βοήθειας (Help Line) και Γραμμή Καταγγελιών (Hotline) 1480 ή και να επισκεφτείτε τη διαδικτυακή πύλη http://internetsafety.pi.ac.cy.



ΠΗΓΗ: Κυπριακό Κέντρο Ασφαλούς Διαδικτύου – CYberSafety, https://internetsafety.pi.ac.cy/