



CYBERBULLYING

Ο **διαδικτυακός εκφοβισμός** είναι οποιαδήποτε πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς που πραγματοποιείται μέσω του Διαδικτύου και των κινητών τηλεφώνων, η οποία επαναλαμβάνεται και στόχος του επιτιθέμενου είναι να προκαλέσει ζημιά ή να βλάψει το θύμα του.

Για να χαρακτηρίσουμε μια πράξη ως εκφοβισμό θα πρέπει:

- να γίνεται συστηματικά
- να υπάρχει πρόθεση
- να γίνεται με στόχο να πληγώσει κάποιον
- να υπάρχει ανισορροπία δυνάμεων των ατόμων που εμπλέκονται (αυτός που εκφοβίζει να είναι πιο δυνατός σωματικά ή ψυχολογικά από αυτόν που εκφοβίζεται, με αποτέλεσμα ο τελευταίος να είναι αβοήθητος έναντι εκείνου που τον παρενοχλεί)
- το θύμα να μην μπορεί να υπερασπιστεί τον εαυτό του.

ΣΥΜΒΟΥΛΕΣ:

Μπορεί να συμβεί σε όλους!

- Ό,τι κάνουμε στο Διαδίκτυο έχει συνέπειες και στην πραγματική ζωή...
- Ο ρόλος του παρατηρητή είναι κρίσιμος. Μη μένουμε απλοί θεατές! Οι πράξεις μας μπορούν να κάνουν τη διαφορά! Σπάσε τον κύκλο του εκφοβισμού και μίλα!
- Θυμόμαστε ότι και αυτός/ή που υφίσταται αλλά και αυτός/αυτή που κάνει το cyberbullying χρειάζονται βοήθεια, καθώς και οι δύο διαχειρίζονται με διαφορετικό τρόπο τα συναισθήματά τους.

Προτεινόμενες ενέργειες σε ένα περιστατικό cyberbullying:

- Δίνουμε στον συνομιλητή μας την ευκαιρία να συζητήσει μαζί μας οτιδήποτε του συμβαίνει χωρίς να υποτιμήσουμε τα παράπονά του ή να χάσουμε την ψυχραιμία μας. Δίνουμε χρόνο να αποτυπώσει τα γεγονότα ακριβώς όπως τα αισθάνεται ενθαρρύνοντάς τον.
- Για τους ανηλίκους, η επικοινωνία με το παιδί είναι το κλειδί! Είναι σημαντικό να ακούσουμε προσεκτικά τι λέει το παιδί για τις online εμπειρίες του και να επισκεφτούμε μαζί τις ιστοσελίδες που επισκέπτεται.
- Κρατάμε όλα τα αποδεικτικά στοιχεία και δεν τα διαγράφουμε σε περίπτωση που απαιτηθεί διερεύνηση του περιστατικού.

- Συχνά, αυτός που κάνει cyberbullying είναι κάποιος γνωστός αυτού που το υφίσταται. Σε αυτήν την περίπτωση είναι σημαντική η συνεργασία όλων των εμπλεκόμενων (γονέων, σχολείου, κοινότητας).
- Σε περιπτώσεις όπου η παρενόχληση επιμένει και προέρχεται από άγνωστο αποστολέα, μπορούμε να καταγγείλουμε το περιστατικό σε οποιαδήποτε Αστυνομική ή Δικαστική Αρχή.
- Ζητάμε τη βοήθεια ενός ειδικού ψυχικής υγείας σε τέτοιου είδους θέματα.



ΔΙΑΔΙΚΤΥΑΚΑ ΠΑΙΧΝΙΔΙΑ

Τα **διαδικτυακά παιχνίδια** είναι δισδιάστατα ή τρισδιάστατα παιχνίδια που παίζονται στον ηλεκτρονικό υπολογιστή ή στις παιχνιδομηχανές και, μέσω του Διαδικτύου, ο χρήστης μπορεί να παίξει και να αλληλεπιδρά σε έναν ενιαίο, εικονικό κόσμο

ΠΡΟΣΕΧΟΥΜΕ ΤΑ ΑΚΟΛΟΥΘΑ:

- Ο κόσμος που περιγράφουν δεν σταματά ποτέ και υφίσταται ακόμα και όταν ο παίκτης δεν είναι συνδεδεμένος.
- Προσφέρουν ένα ισχυρότατο σύστημα συνεχών ανταμοιβών μέσα από πίστες και ανταμοιβές, μέσα σε έναν κόσμο που συνεχώς εξελίσσεται και εμπλουτίζεται.
- Επιτρέπουν την ταυτόχρονη επικοινωνία χιλιάδων παικτών, από διαφορετικές χώρες και πολιτισμικό υπόβαθρο, και την αλληλεπίδραση τους, ενώ το διαδικτυακό προφίλ των παικτών μπορεί να μην ταυτίζεται με τα πραγματικά τους στοιχεία.
- Τα διαδικτυακά παιχνίδια κρατάνε τους παίκτες σε εγρήγορση και είναι σχεδιασμένα από ειδικούς προκειμένου να προσελκύουν μεγάλο αριθμό παικτών.

ΣΥΜΒΟΥΛΕΣ:

- Παίζουμε με όρια και κανόνες!
- Ο εθισμός στα διαδικτυακά παιχνίδια αφορά παιδιά αλλά και ενήλικες.
- Στην περίπτωση ανηλικών διαθέτουμε τον απαραίτητο χρόνο για να πλοηγηθούμε μαζί με το παιδί. Ο σκοπός μας είναι να βοηθήσουμε τα παιδιά μας να αναπτύξουν τα ίδια τον απαραίτητο αυτοέλεγχο και αυτοπειθαρχία αναφορικά με τη χρήση του Διαδικτύου.



Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ



Για περισσότερες πληροφορίες:

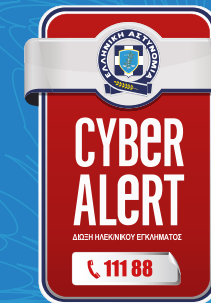


ΕΠΙΚΟΙΝΩΝΙΑ

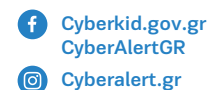
Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος – Cyber Crime Division
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11522
e-mail: ccu@cybercrimeunit.gov.gr, Τηλ.: **11188**

Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδας
Μοναστηρίου 326, Θεσσαλονίκη, Τ.Κ. 54121
e-mail: ydheve@cybercrimeunit.gov.gr, Τηλ.: **11188**

Ενημερωθείτε για θέματα ασφαλούς πλοήγησης στο Διαδίκτυο στο cyberkid.gov.gr και στο www.cyberalert.gr



#ασφάλεια_στον_κυβερνοχώρο
πλοηγούμεστε με ασφάλεια στο Διαδίκτυο



Cyberkid.gov.gr
CyberAlertGR

Cyberalert.gr



Cyber Alert



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Προστασίας του Πολίτη



ΕΛΑΣ
Επόμενο
Βήμα



Αρχηγείο
Ελληνικής Αστυνομίας



Το Διαδίκτυο είναι πλέον μέρος της καθημερινότητας δισεκατομμυρίων χρηστών και απαραίτητο εργαλείο για το μέλλον.

Κάθε χρήστης του Διαδικτύου (Internet), αφήνει κατά την πλοήγησή του σε αυτό ηλεκτρονικά ίχνη τα οποία αποτελούν την (ηλεκτρονική) ταυτότητά του και η οποία είναι μοναδική στην παγκόσμια διαδικτυακή κοινότητα.



ΑΣΦΑΛΕΙΑ ΣΥΣΚΕΥΩΝ

- Αλλάζουμε τον εργοστασιακό κωδικό του Wi-Fi στο οικιακό router. Χρησιμοποιούμε ως κωδικό Wi-Fi έναν κωδικό με γράμματα, αριθμούς και σύμβολα. Η αλλαγή γίνεται μέσω app (ρυθμίσεις router - αλλαγή κωδικού Wi-Fi) σε λίγα δευτερόλεπτα.
- Δημιουργούμε guest λογαριασμούς στο Wi-Fi όταν μας επισκέπτονται φίλοι μας και επιθυμούμε να συνδεθούν σε αυτό.
- Διατηρούμε τις συσκευές μας ασφαλείς ενημερώνοντας το λογισμικό, το antivirus και κατεβάζοντας εφαρμογές μόνο από τα επίσημα καταστήματα εφαρμογών (App Store, Play Store).
- Κλειδώνουμε τις συσκευές μας χρησιμοποιώντας ισχυρό κωδικό ή μοτίβο κλειδώματος, Face ID, Touch ID, βιομετρικά δεδομένα. Αξιοποιούμε τις ενσωματωμένες κλειδοθήκες στο κινητό.
- Εγκαθιστούμε λογισμικό εύρεσης συσκευής, ώστε να διαγράψουμε το περιεχόμενό της απομακρυσμένα αν την απωλέσουμε, και εφόσον ξανασυνδεθεί στο Διαδίκτυο.
- Ενεργοποιούμε στα e-mails και στους λογαριασμούς στα μέσα κοινωνικής δικτύωσης τον έλεγχο ταυτότητας δύο παραγόντων (2fa).



ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν **δεδομένα προσωπικού χαρακτήρα** όπως ονοματεπώνυμο, τηλέφωνο επικοινωνίας, διεύθυνση κατοικίας ή εργασίας κ.ά..

ΣΥΜΒΟΥΛΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ:

- Πριν αναρτήσουμε μια φωτογραφία ή ένα video εξετάζουμε προσεκτικά τις πληροφορίες που δίνουμε μέσα από αυτά π.χ. περιβάλλον στο οποίο κινούμαστε, σημαντικές ημερομηνίες για εμάς, βιοτικό επίπεδο, τοποθεσία στην οποία βρισκόμαστε κ.α..
- Δεν αναρτούμε και δεν αποστέλλουμε σε ιδιωτικές συνομιλίες, φωτογραφίες ή βίντεο που δεν θα δείναμε σε ανθρώπους στον «πραγματικό κόσμο» ή που μπορούν να μας φέρουν σε δύσκολη θέση τώρα ή στο μέλλον. Θυμόμαστε ότι ακόμα και οι γνωστοί μπορεί να αποδειχθούν άγνωστοι!
- Κατά την πλοήγησή μας χρησιμοποιούμε ψευδώνυμο το οποίο όμως δεν παραπέμπει στην ηλικία ή το φύλο μας.



- Η αίσθηση ανωνυμίας στο Διαδίκτυο και η δυνατότητα δημιουργίας ψεύτικων προφίλ, οδηγεί στο να μην ξέρουμε πραγματικά με ποιον επικοινωνούμε. Άντρες χρησιμοποιούν προφίλ με γυναικεία χαρακτηριστικά και το αντίστροφο, προσπαθώντας να αποσπάσουν τα προσωπικά στοιχεία χρηστών και να τους παρασύρουν.
- Σε περίπτωση που επιμένουμε να συναντηθούμε στην πραγματική ζωή με κάποιον που γνωρίσαμε στο διαδίκτυο, φροντίζουμε η συνάντηση να γίνει σε δημόσιο χώρο παρουσία οικείων μας.
- Προστατεύουμε τη διαδικτυακή μας φήμη επανεξετάζοντας τις αναρτήσεις μας από τότε που δημιουργήσαμε τους λογαριασμούς μας στα μέσα κοινωνικής δικτύωσης.
- Κρατάμε τους λογαριασμούς μας ιδιωτικούς.



GROOMING - SEXTING - SEXTORTION

- Τα συχνότερα περιστατικά που εντοπίζει η Υπηρεσία μας τα τελευταία έτη είναι η πορνογραφία ανηλίκων, η προσβολή γενετήσιας αξιοπρέπειας ανηλίκων, ο διαδικτυακός εκβιασμός και εξαναγκασμός ανηλίκων και ενηλίκων (sextortion) αλλά και η ανταλλαγή μηνυμάτων ερωτικού περιεχομένου και προκλητικών φωτογραφιών μεταξύ γνωστών ή αγνώστων (sexting).
- Τόσο οι ενήλικοι όσο και οι ανήλικοι, μπορεί να συνομιλούν διαδικτυακά με άτομα που δε γνωρίζουν, νομίζοντας ότι μιλάνε με κάποιο γνωστό ή κάποιο άτομο της ηλικίας τους. Αφού δημιουργηθεί κλίμα οικειότητας και εμπιστοσύνης, επέρχεται άρση αναστολών και πείθονται να αποστείλουν τα προσωπικά τους στοιχεία, όπως ονοματεπώνυμο, διευθύνσεις, τηλεφωνικούς αριθμούς, να ανεβάσουν (upload) ή να αποστείλουν (send) φωτογραφίες τους, κάποιες φορές με προκλητικό περιεχόμενο ή πείθονται να συναντηθούν με τα άτομα αυτά.



ΠΡΟΕΙΔΟΠΟΙΗΤΙΚΑ ΣΗΜΑΔΙΑ:

- Πάρα πολύ καλό για να είναι αληθινό; - Μας κολακεύει και μας δίνει πολλή προσοχή; - Επαινεί τις φωτογραφίες του προφίλ μας; - Μοιράζεται όλα τα ενδιαφέροντά μας;
- Κάνει ό,τι μπορεί για να κερδίσει την εμπιστοσύνη μας κάνοντάς μας να αισθανόμαστε ξεχωριστοί;
- Λέει ότι είναι πολύ γοητευμένος/η πολύ σύντομα και επιδιώκει προσωπικές συζητήσεις;
- Ζητάει να μεταφέρουμε τη συνομιλία μας σε ιδιωτικό δωμάτιο συνομιλίας;
- Το μικρό μας μυστικό! Ζητάει να κρατήσουμε τη συνομιλία μας μυστική ή λέει ότι θα έχουμε πρόβλημα αν το μάθει κάποιος άλλος;
- Ζητάει να ανταλλάξουμε προσωπικές φωτογραφίες και video ενώ κάνει εκείνος/η πάντα την αρχή;
- Ισχυρίζεται ότι η webcam έχει χαλάσει;

Στόχος των δραστών είναι:

- Η παραγωγή πρωτότυπου υλικού πορνογραφίας.
- Ο εκβιασμός και εξαναγκασμός με οικονομικό ή σεξουαλικό όφελος.
- Η δια ζώσης συνάντηση.

Σε περίπτωση που κάποιος πολίτης πέσει θύμα διαδικτυακού εκφοβισμού και εξαναγκασμού, δεν πρέπει να πληρώσει ή να συναντηθεί με τον δράστη ή να στείλει επιπλέον υλικό με προσωπικό περιεχόμενο υποκύπτοντας στον εκβιασμό.

Ενημερωτική εκστρατεία

«#Say NO»

της Europol



Αν μας συμβεί ακολουθούμε τα παρακάτω βήματα:

- Δεν υποκύπτουμε στους εκβιασμούς και δεν πληρώνουμε.
- Μιλάμε σε κάποιον/α που εμπιστευόμαστε και αν είμαστε ανήλικοι στους γονείς/κηδεμόνες μας.
- Για να βοηθήσουμε κάποιον που έχει εμπλακεί σε αντίστοιχη υπόθεση παραμένουμε ψύχραιμοι και ακούμε όλη την ιστορία χωρίς να διακόψουμε.
- Συλλέγουμε τις αποδείξεις (screenshots) στις οποίες φαίνεται το link ή ο αποστολέας και κάνουμε αποθήκευση (save) ή εκτύπωση (print).
- Σταματάμε την επικοινωνία και μπλοκάρουμε τον χρήστη.
- Επικοινωνούμε με τις οικείες Αστυνομικές - Εισαγγελικές Αρχές.
- Κρατάμε τους λογαριασμούς μας ιδιωτικούς.

