

PROJECT:ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ



ΟΜΑΔΑ 4: Πώς κάποιος μπορεί να μας παρενοχλήσει διαδικτυακά και τι μπορούμε να κάνουμε για το θέμα αυτό;

ΕΠΙΜΕΛΕΙΑ: ΚΑΜΠΟΥΡΑΚΗ ΖΑΧΑΡΟΥΛΑ

ΑΔΙΚΗΜΕΝΑΚΗ ΑΘΗΝΑ

ΒΕΙΣΑΚΗ ΑΘΗΝΑ

1. Τρόποι με τους οποίους μπορεί κάποιος να μας παρενοχλήσει διαδικτυακά

Μπορεί για παράδειγμα να:

- Κοροϊδέψουν ένα άτομο σε ένα chat-room.
- Να αποστείλουν αισχρά ή απειλητικά μηνύματα μέσω του διαδικτύου.
- Να στείλουν αισχρό υλικό κατά τις συνομιλίες.
- Να κοροϊδέψουν κάποιο με το να φτιάξουν ένα ψεύτικο προφίλ με εξευτελιστικές πληροφορίες.
- Να βάλουν προσωπικό υλικό κάποιου άλλου στο διαδίκτυο χωρίς την άδεια του.

2. Παγίδες διαδικτυακής παρενόχλησης

Πρώτη παγίδα: Κλοπή Προσωπικών δεδομένων ή Παραβίαση της Ιδιωτικής μας ζωής

Γνωρίζεται πως όταν δημιουργήσουμε ένα λογαριασμό στο Facebook εξ ορισμού όλοι οι χρήστες του Facebook έχουν πρόσβαση σε όλη τη πληροφορία, δεδομένα ανεβάσουμε πάνω στο λογαριασμό μας; Μήπως γνωρίζετε για ποιον αριθμό μιλάμε? ... οι χρήστες του Facebook ξεπερνούν τα 400 εκατομμύρια σε όλο τον κόσμο. Αυτό σημαίνει ότι αν εξαιρέσουμε τους φίλους σας περίπου 400 εκατομμύρια άσχετα άτομα με εσάς μπορούν να το θελήσουν να εισβάλουν στον λογαριασμό σας, να πάρουν τις φωτογραφίες σας και να τις χρησιμοποιήσουν όπως θέλουν αυτοί... Μπορούν επίσης να δουν πληροφορίες όπως για παράδειγμα το πού μένετε, πόσο χρονών είστε και τι κάνετε ανά πάσα στιγμή ... δεν σας τρομάζει αυτό?

Σκεφτείτε το διαφορετικά... Αν έρθει ένας άγνωστος στο δρόμο και σας ζητήσει να του δώσετε μια φωτογραφία σας ή σας ρωτήσει να του πείτε πού μένετε θα του πείτε? Με την ίδια λογική δεν τα το κάνατε ούτε στο Facebook.

Βεβαιωθείτε λοιπόν ότι στο εικονικό σας προφίλ έχουν πρόσβαση μόνο οι φίλοι σας!!! (Κάντε κλικ [εδώ](#) για οδηγίες).

Τώρα για να δούμε ποιους θεωρούμε ηλεκτρονικούς μας φίλους...

Κάντε λίγα μαθηματικά και σκεφτείτε πόσους φίλους έχετε στην πραγματική σας ζωή και πόσους φίλους έχετε στο Facebook! Σίγουρα ο αριθμός δεν είναι καθόλου ο ίδιος. Πολλής κόσμος έχει την τάση να κάνει add στο προφίλ του άτομα τα οποία αν τα συναντούσε στον δρόμο το πιο πιθανό ούτε γεια δεν θα τους έλεγε! Μην κάνετε φίλους σας οποιονδήποτε σας κάνει "add request". Από την στιγμή που τον κάνετε φίλο σας αυτόματα έχει πρόσβαση στο προφίλ σας. Οι σχέσεις μεταξύ των ατόμων δεν αλλάζουν επειδή αλλάζει ο τρόπος επικοινωνίας. Στην περίπτωση όμως που αποφασίσετε να προσθέσετε στην λίστα των φίλων σας όλο τον κόσμο που σας το ζητά, προσπαθήστε να μην ανεβάζετε πολύ προσωπικές φωτογραφίες και να μην γράφετε πολύ προσωπικά στοιχεία για σας. Πότε δεν ξέρετε αν κάποιος από τους «φίλους» σας, χρησιμοποιήσει κάποια φωτογραφία σας ή βίντεο, εναντίον σας με σκοπό να σας απομονώσει ή να σας βλάψει.

Δεύτερη παγίδα: Διαδικτυακός Εκφοβισμός (Cyberbullying)

Διαδικτυακός Εκφοβισμός είναι ο εκφοβισμός ο οποίος συμβαίνει μέσω του Διαδικτύου. Περιλαμβάνει εσκεμμένη, επαναλαμβανόμενη και εχθρική συμπεριφορά απέναντι σε κάποιο άτομο με σκοπό να το απομονώσει ή να το βλάψει. Ο Διαδικτυακός Εκφοβισμός συνήθως έχει τη μορφή ενός εκφοβιστικού, ρατσιστικού ή προσβλητικού ηλεκτρονικού μηνύματος, φωτογραφίας ή βίντεο.

Π.χ.

Αν κάποιος επανειλημμένα γράφει κάτι προσβλητικό για εσάς είναι εκφοβισμός.

Αν κάποιος έχει ανεβάσει ένα βίντεο ή μια φωτογραφία σας η οποία σας κάνει να νιώθετε άβολα και παρόλο που του το ζητήσατε δεν το κατεβάζει είναι εκφοβισμός

Αν δεχτείτε οποιονδήποτε είδος εκφοβισμού/παρενόχληση:

1. Εμπιστευτείτε το αμέσως σε κάποιον ενήλικα (γονιός, καθηγητής, φίλος)
2. Σταματήστε αμέσως την επικοινωνία με τον Θύτη. Έχετε την δυνατότητα να Φιλτράρετε ή να μπλοκάρετε τα μηνύματα από άτομα που σας παρενοχλούν
3. Αν χρειαστεί καταγγείλετε το περιστατικό στην Αστυνομία ή σε κάποια από τις Γραμμές Βοήθειας

Τρίτη Παγίδα: Αποπλάνηση

Αποπλάνηση συμβαίνει συνήθως όταν κάνουμε chat. Κακόβουλοι άγνωστοι προσπαθούν να μας αποπλανήσουν για να συναντηθούμε μαζί τους σε πραγματικό χώρο με στόχο τη σεξουαλική παρενόχληση.

Σύμφωνα με τη Στατιστική Υπηρεσία, στην Κύπρο, όσον αφορά τη σεξουαλική παρενόχληση ανηλίκων το 2004 είχαμε 11 υποθέσεις, το 2005 είχαμε 19 υποθέσεις και το 2006 22 υποθέσεις. Μάλιστα φαίνεται ότι τα αγόρια πιο εύκολα αποδέχονται τέτοιους είδους συναντήσεις.

Για τον λόγο αυτό:

- Μην ανεβάζετε πολύ προσωπικά σας στοιχεία στο facebook που να διευκολύνουν τον εντοπισμό: Τηλέφωνα, διευθύνσεις, φωτογραφίες που να φαίνετε το σπίτι μας, το σχολείο τα μέρη όπου συχνάζουμε.
- Μην δεχτείτε ποτέ να συναντήσετε κάποιο ξένο τον οποίον γνωρίσατε στο facebook. Δεν ξέρετε ποιος κρύβετε πίσω από την μάσκα του Διαδικτύου. Μπορεί να μην είναι αυτός που λέει.
- Σταματήστε αμέσως άβολες συζητήσεις και αποθηκεύουμε αντίγραφα της συνομιλίας
- Αν κάτι σας προκαλέσει ανησυχία, θα πρέπει αμέσως να αποθηκεύσουν αντίγραφα της συνομιλίας, να εγκαταλείψετε την συνομιλία και να το πείτε σε κάποιο ενήλικα.

Τέταρτη παγίδα: Μονιμότητα του Διαδικτύου

Προσπάθησε κανείς να διαγράψει τον λογαριασμό του από το Facebook; Δεν θα τα καταφέρει!

Ξέρετε ότι όταν κάποιος θέλει να εγκαταλείψει το Facebook δεν μπορεί να αποσύρει πλήρως το προφίλ του; Υπάρχει η δυνατότητα ΑΠΕΝΕΡΓΟΠΟΙΗΣΗΣ του προφίλ το οποίο σημαίνει ότι τα δεδομένα σας παρόλο που δεν είναι προσβάσιμα υπάρχουν όμως στους web servers του Facebook. Αυτό δεν είναι ίδιο με την διαγραφή. Αυτό σημαίνει ότι αυτά θα σας ακολουθούν για μια ζωή. Ποτέ δεν ξέρετε ποιος, πότε και πώς μπορεί κάποιος να χρησιμοποιήσει τα

προσωπικά σας δεδομένα.

Εάν θέλουμε λοιπόν να εγκαταλείψουμε το facebook:

1. Διαγράψτε όσα πιο πολλά στοιχεία
2. αντικαταστήστε τα υπόλοιπα με ψεύτικα.
3. Απενεργοποιήστε τα δεδομένα σας

3. Τι μπορούμε να κάνουμε για το θέμα αυτό

Τί πρέπει να προσέχεις στις ιστοσελίδες κοινωνικής δικτύωσης (π.χ. Facebook, My Space)

Νομίζω ότι δεν υπάρχει πρόβλημα να χρησιμοποιούμε το Facebook από τη στιγμή που ξέρουμε πώς να προστατευτούμε.

- Βεβαιώσου ότι το προφίλ σου είναι προσβάσιμο μόνο από τους φίλους σου
- Μη δίνεις σε κανέναν τον κωδικό πρόσβασης στο εικονικό προφίλ σου. Όποιος αποκτά πρόσβαση σε αυτό μπορεί να διαχειριστεί πλήρως τα δεδομένα που εμφανίζονται σε αυτό.
- Μην ανεβάζεις στο προφίλ σου φωτογραφίες όπου φαίνεται καθαρά η τοποθεσία στην οποία βρίσκεσαι, ειδικότερα αν πρόκειται για το σπίτι σου, το σχολείο ή μέρη που συχνάζεις. Έτσι θα μειώσεις τις πιθανότητες εντοπισμού σου στον φυσικό κόσμο.
- Να θυμάσαι ότι, ακόμα και όταν διαγράψεις το προφίλ σου, πολλές πληροφορίες δεν αφαιρούνται και ενδέχεται επίσης να τις συναντήσεις και αλλού στο Διαδίκτυο
- Να γνωρίζεις ότι, από τη στιγμή που θα προσθέσεις στη λίστα των φίλων σου κάποιο άτομο (αποδοχή «friend request»), αυτό αποκτά πρόσβαση στα προσωπικά δεδομένα που εμφανίζονται στο προφίλ σου, μεταξύ των οποίων οι φωτογραφίες και τα στοιχεία επικοινωνίας σου
- Αν δεχτείς οποιοδήποτε είδος εκφοβισμού σταμάτα αμέσως την επικοινωνία με το θύτη και ενημέρωσε αμέσως κάποιος ενήλικα. Αν χρειαστεί κατάγγειλε το περιστατικό στην Αστυνομία ή σε μια από τις Γραμμές Βοήθειας πιο κάτω.
- Μην δεχτείς να συναντήσεις κάποιο άτομο το οποίο γνώρισες από το Facebook

4. Πώς μπορεί η πρόληψη να βοηθήσει;

- Η πρόληψη λειτουργεί κυρίως πάνω σε μία πιο μακροπρόθεσμη βάση, αλλά είναι πολύ σημαντική για να αντιμετωπιστεί το πρόβλημα εις βάθος και αποτελεσματικά.
-

- Μέσω της εκπαίδευσης, η νεολαία αλλά και τα άτομα που ασχολούνται και εργάζονται για την νεολαία, έχουν την ευκαιρία να ενημερωθούν και να εκπαιδευτούν σωστά για τα ηλεκτρονικά προβλήματα και την σωστή χρήση της τεχνολογίας. Η ενημέρωση του κοινού, μπορεί να επιτευχθεί μέσω εκδηλώσεων, σεμιναρίων, εργαστήρια αλλά και γενικότερα μέσω ενεργειών που προωθούν την ενημέρωση για αυτά τα σημαντικά θέματα.
-
- Αυτός ακριβώς είναι ο ρόλος της Cyber Ethics στην Κύπρο. Μέσω της δράσης της που ονομάζεται κόμβος ευαισθητοποίησης και ενημέρωσης, προσπαθεί να συμβάλει στην δημιουργία ενός ασφαλούς διαδικτύου. Είναι πολύ σημαντικό να είσαι ενήμερος για αυτά τα προγράμματα στην χώρα σου, και να εκπαιδεύεσαι. Για να μην χρειαστεί να αντιμετωπίσεις ένα τέτοιο πρόβλημα, η πρόληψη είναι απαραίτητη.

5. Πώς να αντιμετωπίσεις το πρόβλημα;

- Σε όλες τις χώρες υπάρχουν διάφοροι οργανισμοί που μπορούν να σε βοηθήσουν να αντιμετωπίσεις ένα τέτοιο πρόβλημα. Στην Κύπρο, η **CyberEthics**, που είναι το Κυπριακό Κέντρο Ασφαλούς Διαδικτύου και λειτουργεί από το 2006, βασίζεται σε διάφορα ενημερωτικά εργαλεία για να αντιμετωπίσει το πρόβλημα αυτό, που αποτελούν τον κόμβο ευαισθητοποίησης όπως είναι ανοιχτή γραμμή επικοινωνίας καθώς και τηλεφωνική γραμμή βοήθειας.
- Μέσω αυτών των εργαλείων, έχεις την ευκαιρία να συζητήσεις και να αναφέρεις οποιαδήποτε μορφή ηλεκτρονικής βίας που έχεις βιώσει. Αφού αναφέρεις το πρόβλημά σου, το κέντρο θα σε ενημερώσει για τα βήματα που θα πρέπει να κάνεις για να αντιμετωπίσεις το πρόβλημα αποτελεσματικά, αλλά και το ίδιο το κέντρο θα αναλάβει δράση για σένα.
- Μην διστάσεις, και μην αφήσεις αυτό το πρόβλημα να σε βασανίζει. Αντιμετώπισέ το άμεσα!