

ΕΝΗΜΕΡΩΣΗ ΓΙΑ ΤΟΥΣ ΚΙΝΔΥΝΟΥΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

1. Παραβίαση προσωπικών δεδομένων (GDPR)

Για τη διασφάλιση των προσωπικών δεδομένων στις 27 Απριλίου 2016 ψηφίστηκε ο Κανονισμός 2016/679 της Ευρωπαϊκής Ένωσης, ευρύτερα γνωστός ως Γενικός Κανονισμός για την Προστασία Δεδομένων - ΓΚΠΔ (και στα αγγλικά General Data Protection Regulation - GDPR), και τέθηκε σε υποχρεωτική εφαρμογή για όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης στις 25 Μαΐου 2018. Όταν το παραπάνω νομικό πλαίσιο δεν εφαρμόζεται γίνεται Παραβίαση προσωπικών δεδομένων.

Παραβίαση προσωπικών δεδομένων λοιπόν είναι η παραβίαση της ασφάλειας που οδηγεί σε τυχαιά και παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.



Προσοχή όμως:

Η παραβίαση είναι ένα είδος περιστατικού ασφάλειας. Δεν είναι όλα τα περιστατικά ασφάλειας παραβιάσεις προσωπικών δεδομένων.

Συνέπεια μιας παραβίασης είναι ότι ο Υπεύθυνος Επεξεργασίας δεν είναι σε θέση να διασφαλίσει τη συμμόρφωση με τις αρχές που αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι οποίες περιγράφονται συνοπτικά στο άρθρο 5 του GDPR, ιδίως της ακεραιότητας και της εμπιστευτικότητας.

Πηγές:

https://www.lawspot.gr/gdpr/faq?lspt_context=gdpr

https://www.sev.org.gr/Uploads/Documents/51324/4_diaxeirisi_peristatikon_paraviasis_desomenon.pdf

Video:

<https://www.youtube.com/watch?v=cAHO8-qQ0nM>

2. Cyberbullying – Διαδικτυακός Εκφοβισμός

Διαδικτυακός εκφοβισμός συμβαίνει όταν κάποιος κακόβουλος παρενοχλεί ένα άτομο με τη χρήση της τεχνολογίας. Η παρενόχληση αυτή μπορεί να γίνεται σε τακτικά ή άτακτα χρονικά διαστήματα μέσω οποιασδήποτε πράξης εκφοβισμού, επιθετικότητας, τρομοκρατικής ή αυταρχικής συμπεριφοράς.

Ο διαδικτυακός εκφοβισμός περιλαμβάνει καταστάσεις όπως:

- η αποστολή ανήθικων μηνυμάτων,
- ο αποκλεισμός ατόμων από εφαρμογές συνομιλιών,
- το hacking ενός ξένου λογαριασμού,
- η δημοσίευση ενοχλητικών φωτογραφιών,
- διάδοση προσβλητικών φημών κ.α.

Ένα θύμα διαδικτυακού εκφοβισμού μπορεί να βιώσει μία πολύ αγχώδη κατάσταση, καθώς τα μηνύματα μπορούν να σταλούν ανώνυμα και επομένως είναι δύσκολο να γνωρίζει ποιος είναι ο θύτης. Επιπλέον, ο διαδικτυακός εκφοβισμός μπορεί να συμβεί οποιαδήποτε στιγμή της ημέρας από οποιοδήποτε μέρος. Όταν τα μηνύματα ή οι φωτογραφίες δημοσιευθούν στο διαδίκτυο προβάλλονται άμεσα σε πολλούς χρήστες και αυτό αναστατώνει τα θύματα που βλέπουν πόσο γρήγορα μία φωτογραφία ή μια φήμη διαδίδεται στο διαδίκτυο. Ο εκφοβισμός μέσω του διαδικτύου μπορεί να είναι άμεσος ή έμμεσος εμπλέκοντας και άλλα άτομα που ενδεχομένως να μην γνωρίζουν προσωπικά το θύμα.



Συμβουλές για να παραμείνεις ασφαλής:

- Δεν απαντάμε στα εκφοβιστικά μηνύματα.
- Μπλοκάρουμε την πρόσβαση του αποστολέα.
- Κρατάμε και αποθηκεύουμε τα μηνύματα ή τις συνομιλίες. Αυτό θα μας είναι χρήσιμο, εάν χρειαστεί ή εάν θελήσουμε να το καταγγείλουμε.
- Δεν προωθούμε μηνύματα ή εικόνες και φωτογραφίες που θα μπορούσαν να πληγώσουν τα συναισθήματα κάποιου. Έχουμε στο μυαλό μας ότι, εάν κάποιος μας στείλει ένα μήνυμα και το προωθήσουμε ή γελάσουμε με αυτό, στην ουσία γινόμαστε και εμείς μέρος του εκφοβισμού.
- Αναφέρουμε το πρόβλημά μας στους γονείς μας ή σε άλλους ενήλικους που εμπιστευόμαστε. Σε κάθε περίπτωση μπορούμε να απευθυνθούμε και στη γραμμή βοήθειας [help-line](https://saferinternet4kids.gr/hot-topics-ef/cyberbullying-ef/) όπου εξειδικευμένοι γιατροί και ψυχολόγοι με μεγάλη εμπειρία σε προβληματικές συμπεριφορές στο διαδίκτυο μπορούν να μας παρέχουν συμβουλές και υποστήριξη.

Πηγές:

<https://saferinternet4kids.gr/hot-topics-ef/cyberbullying-ef/>

Video:

<https://www.youtube.com/watch?v=SbMVvUcMFZ0>

3. Catfishing – Διαδικτυακό ψάρεμα

Το Catfishing είναι μια παραπλανητική δραστηριότητα όπου ένα άτομο δημιουργεί ένα φανταστικό πρόσωπο ή ψεύτικη ταυτότητα σε μια υπηρεσία κοινωνικής δικτύωσης, στοχεύοντας συνήθως ένα συγκεκριμένο θύμα.

Τα social media έχουν κατακλύσει τη ζωή μας και όλα τα κάνουμε από εκεί πλέον. Ενημέρωση, dating, ακόμη και συνταγές, τα βρίσκουμε όλα στα social media. Υπάρχουν θετικά και αρνητικά, αλλά το βασικότερο όλων είναι να έχουμε μέτρο.

Ένα φαινόμενο που παρατηρείται έντονα στα social media, είναι το λεγόμενο «catfishing». Η κυριολεκτική έννοια της λέξης είναι «ψάρεμα γατόψαρου», αλλά μεταφορικά σημαίνει δόλωμα και εξαπάτηση.

Στον κόσμο των social σημαίνει εξαπάτηση. Δηλαδή, μπορεί να μιλάς με κάποιον άνθρωπο για αρκετό καιρό και να σου παρουσιάζει μια άλλη εικόνα από αυτή που έχει στην πραγματικότητα. Συζητάτε και σου λέει πράγματα τα οποία δεν ισχύουν και όλα τα σχετικά. Όταν εσύ ζητάς να βρεθείτε, αρνείται, και πάει λέγοντας.

Το φαινόμενο αυτό είναι αρκετά μυστήριο και πολλές φορές μπορεί να είναι και επικίνδυνο γιατί δεν γνωρίζεις την πραγματική ταυτότητα κάποιου. Μάλιστα, στην Αμερική υπάρχουν ολόκληρες εκπομπές αφιερωμένες σε αυτό και προσπαθούν να βρουν ποιος κρύβεται πίσω από το προφίλ που μιλάει με άλλους.



Πηγές:

<https://en.wikipedia.org/wiki/Catfishing>

<https://www.neolaia.gr/2018/11/19/esi-xereis-ti-einai-to-catfishing/>

Video:

<https://www.youtube.com/watch?v=Y6ajaAuwFBY>

4. Fake News – Ψευδή Νέα

Ότι αναφέρετε στο διαδίκτυο δεν είναι πάντα αλήθεια. Τα ψευδονέα ή ψευδείς ειδήσεις ή πλαστές ειδήσεις (γνωστά και ως fake news), είναι ένα είδος κίτρινου τύπου ή προπαγάνδα που γίνεται με σκόπιμη παραπληροφόρηση ή με φάρσες που διαδίδονται με παραδοσιακά μέσα μαζικής ενημέρωσης ή με τα μέσα κοινωνικής δικτύωσης. Η διασπορά ψευδών ειδήσεων προκαλείται συχνά από δημοσιογράφους που πληρώνουν πηγές πληροφοριών, μια αμφιλεγόμενη πρακτική που ονομάζεται πληρωμένη δημοσιογραφία. Οι ειδήσεις τελικά συχνά αναστέλλονται ως παραπληροφόρηση, αλλά περιστασιακά καταφέρνουν να φθάσουν μέχρι τα παραδοσιακά μέσα μαζικής ενημέρωσης. Τα ψευδονέα γράφονται και δημοσιεύονται συνήθως με σκοπό να παραπλανήσουν, προκειμένου να βλάψουν έναν οργανισμό, ένα νομικό ή φυσικό πρόσωπο, ή και για οικονομικά ή πολιτικά οφέλη συχνά χρησιμοποιώντας τίτλους με εντυπωσιασμό, ή εξ ολοκλήρου κατασκευασμένους για την αύξηση της αναγνωσιμότητας.



Η σημασία των ψεύτικων ειδήσεων έχει αυξηθεί στον σύγχρονο πολιτικό βίο. Για τα μέσα μαζικής ενημέρωσης, η δυνατότητα προσέλκυσης επισκεπτών στους ιστοτόπους τους είναι απαραίτητη για τη δημιουργία εσόδων από διαφημίσεις μέσω διαδικτύου. Εάν δημοσιεύσουν μια ιστορία με ψευδές περιεχόμενο θα προσελκύσουν χρήστες, προς όφελος των διαφημιζομένων και θα βελτιώσουν τις αξιολογήσεις. Η εύκολη πρόσβαση στα έσοδα από διαφημίσεις μέσω διαδικτύου, η αυξημένη δημοτικότητα των μέσων κοινωνικής δικτύωσης, κυρίως το Facebook News Feed, έχουν εμπλακεί στη διάδοση ψευδών ειδήσεων που ανταγωνίζονται με νόμιμες ειδήσεις. Εχθρικοί κρατικοί παράγοντες έχουν επίσης εμπλακεί στη δημιουργία και διάδοση ψευδονέων, ιδίως κατά τη διάρκεια των εκλογών. Τα ψευδονέα υπονομεύουν τη σοβαρή κάλυψη των μέσων ενημέρωσης και δυσκολεύουν τους δημοσιογράφους να καλύπτουν σημαντικές ειδήσεις.

Πηγές:

- <https://saferinternet4kids.gr/fake-news/>
- <https://saferinternet4kids.gr/video/fake-news-2/>

Video:

<https://www.youtube.com/watch?v=-ieqyITLdk>

5. Cyberstalking – Παρενόχληση Παρακολούθηση μέσω διαδικτύου

Η παρενόχληση στο διαδίκτυο, συχνά αναφερόμενη κι ως cyber harassment, αφορά την οποιαδήποτε ενόχληση μέσω email, προσωπικών μηνυμάτων, ή καταχωρήσεων σε ιστοσελίδα με ευθείες αναφορές (συνήθως προσβλητικές-υποτιμητικές) προς το άτομο. Προστάδιο της παρενόχλησης είναι η επίμονη, «φαινομενικά» αθώα, και πολλές φορές «κολακευτική» ενασχόληση με την δική σου διαδικτυακή δραστηριότητα, από συγκεκριμένο άτομο. Είναι ο άνθρωπος που θα σχολιάσει το οτιδήποτε κάνεις post πριν καν προλάβεις καλά καλά να το ανεβάσεις. Θα ποστάρει συνεχόμενα πράγματα στον δικό σου τοίχο,



αδιαφορώντας ότι αυτά τα βλέπουν και οι υπόλοιποι φίλοι σου. Κι αυτό θα συμβαίνει σε κάθε ώρα της κάθε μέρας, αφού συνήθως το άτομο αυτό δείχνει να είναι συνεχώς και αδιάκοπα παρών στην διαδικτυακή ζωή σου. Είναι επίσης ο άνθρωπος που θα συμμετέχει σε οποιαδήποτε συζήτηση σου με άλλους φίλους σου ακόμα κι αν δεν τον αφορά ή δεν έχει προσκληθεί σε αυτήν. Θα κάνει φίλους κάποιους φίλους σου, σίγουρα θα προσεγγίσει την οποιαδήποτε σχέση σου μόλις βρει την ευκαιρία, και πολύ συχνά θα φτάσει να κάνεις «φίλους» μέχρι και συγγενείς σου. Μέχρι στιγμής όλο αυτό δείχνει κολακευτικό. Πότε παύει να είναι κολακευτικό;

Όταν αρχίζεις να το αντιλαμβάνεσαι ως ενοχλητικό. Εδώ αξίζει να θυμάσαι πάντα ότι: Επικίνδυνο δεν γίνεται όταν το αντιληφθείς πλέον ως ενοχλητικό, επικίνδυνο ήταν ήδη εξαρχής...

Τι πρακτικές περιλαμβάνει συνήθως το cyberstalking:

- Προσπάθεια χειραγώγησης με συνεχή «παρουσία» στην διαδικτυακή σου ζωή
- Αποστολή ανώνυμων απειλητικών email από διαφορετικούς λογαριασμούς
- Χρησιμοποίηση της διαδικτυακής σου ταυτότητας σε άλλα κοινωνικά μέσα («κλέβει» την ζωή σου)
- Χρησιμοποίηση ψευδούς ταυτότητας, για να έρθει σε επαφή μαζί σου με κάθε τρόπο.
- Κλοπή προσωπικών σου στοιχείων, οικονομικών και άλλων πχ κωδικών, με σκοπό την πρόκληση άμεσης ζημιάς.
- Δημοσίευση προσωπικών σου στοιχείων σε δημόσιες ομάδες συζήτησης ή ακόμα και προσωπικών φωτογραφιών σου.

Το revenge porn είναι μια βασική υποκατηγορία του cyberstalking. Πρόκειται για την εκδίκηση προς το θύμα μέσω δημοσίευσης ερωτικών του φωτογραφιών χωρίς φυσικά την συναίνεσή του. Αν και η νομοθεσία παγκοσμίως γίνεται ολοένα και πιο αυστηρή με το συγκεκριμένο θέμα, εντούτοις η αμεσότητα και το αχανές του διαδικτύου καταστούν καθυστερημένη την όποια προστασία του θύματος μιας τέτοιας ενέργειας.

Τι άτομα είναι οι θύτες;

Πρόκειται για άτομα με εμφανή σημάδια ψυχοπαθολογίας που μπορεί να εκτείνεται από απλή έλλειψη αυτοπεποίθησης (κόμπλεξ κατωτερότητας), ως και σοβαρές Διαταραχές Προσωπικότητας. Αποζητούν μέσω αυτής της συμπεριφοράς τους:

- Την συναισθηματική «επαφή» μέσω απαιτητικής συμπεριφοράς
- Προσπάθεια διόρθωσης προηγούμενης απόρριψης που έχουν δεχθεί
- Εκδίκηση για προηγούμενη απόρριψη
- Φαντασιακή ή παραληρητική αίσθηση σχέσης με το θύμα
- Έκφραση του μίσους τους γενικά προς ομάδα ή φύλο

Πώς να προστατευτείς:

- Να επιλέγεις προσεκτικά τις διαδικτυακές επαφές σου
- Να μην δίνεις ποτέ προσωπικά σου στοιχεία σε άτομα που μόλις γνώρισες
- Απέφυγε οποιαδήποτε αποκάλυψη της προσωπικής σου ζωής δημοσίως στο διαδίκτυο
- Απέφυγε προσωπικές ομιλίες και συνδέσεις με ανθρώπους που ξέρεις μόνο διαδικτυακά και δεν έχεις γνωρίσει από κοντά.
- Και να θυμάσαι πάντα ότι η όλη επανάσταση με τα social media μετράει μόνο μια δεκαετία ζωής, οπότε σαν χώρος είναι ακόμα ανεξερεύνητος για όλους μας και προς τις δυνατότητές τους αλλά και προς τους κινδύνους του.

Πηγές:

<https://www.psychology.gr/blog/>

Video:

<https://www.youtube.com/watch?v=-iegqyITLdk>

6. Grooming - Αποπλάνηση μέσω διαδικτύου

Το διαδίκτυο αποτελεί ένα ιδανικό περιβάλλον για παιδιά και εφήβους να αναπτύξουν κοινωνικές επαφές, να ανακαλύψουν νέα πράγματα και να γίνουν δημιουργικοί. Ωστόσο οι διαδικτυακοί «φίλοι» μπορεί να μην είναι τελικά εκείνοι που υποστηρίζουν ότι είναι και αυτό είναι ένα σημείο που πρέπει να γίνει κατανοητό από όλους.

Το διαδικτυακό «grooming» συμβαίνει όταν ένας ενήλικας έρχεται σε επαφή μέσω του διαδικτύου με ένα παιδί ή έφηβο προκειμένου να το συναντήσει από κοντά και να το εκμεταλευτεί. Το διαδικτυακό grooming ή αλλιώς η «αποπλάνηση» μέσω διαδικτύου είναι ένα έγκλημα που τιμωρείται αυστηρά σε όλες τις χώρες της Ευρώπης. Μπορεί να συμβεί σε όλους τους ιστοχώρους που είναι πολύ δημοφιλείς στους εφήβους και στα παιδιά όπως στα διαδικτυακά παιχνίδια, στα κοινωνικά δίκτυα, στα δωμάτια συνομιλίας κλπ. Κάποιοι διαδικτυακοί groomers μπορεί να προσποιούνται ότι είναι συνομήλικοι σου χρησιμοποιώντας ψεύτικη φωτογραφία προφίλ και δηλώνοντας ψευδή ηλικία. Οι διαδικτυακοί groomers, συνήθως, έχουν γνώσεις στο να χειρίζονται ψυχολογικά και συναισθηματικά τους εφήβους (π.χ. γνωρίζουν την εφηβική γλώσσα και τον εφηβικό τρόπο σκέψης) και χρησιμοποιούν διάφορες τεχνικές προκειμένου να αποκτήσουν την εμπιστοσύνη σου.



Πού μπορείς να συμβεί :

- Δωμάτια συνομιλίας (chat rooms)
- Σελίδες κοινωνικών δικτύων

Συμβουλές για να παραμείνεις ασφαλής :

- Ας είμαστε προσεκτικοί ποιους αποδεχόμαστε να γίνουν “φίλοι” μας και με ποιους μιλάμε στο διαδίκτυο. Θυμόμαστε πάντα ότι είναι εύκολο να πει κάποιος ψέματα για το ποιος πραγματικά είναι.
- Έχουμε πάντα στο μυαλό μας ότι ακόμα και αν ο συνομιλητής μας στο Διαδίκτυο είναι πραγματικά αυτός που φαίνεται (π.χ. τον έχουμε δει σε web camera) υπάρχει η πιθανότητα να είναι μέλος ενός κυκλώματος που εκμεταλλεύεται παιδιά.
- Χρησιμοποιούμε τις ρυθμίσεις απορρήτου στους ιστοχώρους που επισκεπτόμαστε. Προσαρμόζουμε τις ρυθμίσεις, έτσι ώστε να μη βλέπουν όλοι το προφίλ μας ή τις φωτογραφίες μας.
- Δε βάζουμε προκλητικά ονόματα (username) στο προφίλ μας.
- Δεν κανονίζουμε ΠΟΤΕ συναντήσεις με ανθρώπους που στην ουσία δεν γνωρίζουμε, ακόμα και αν έχουμε γίνει “φίλοι” στο διαδίκτυο.
- Δεν ανταλλάσσουμε ευαίσθητες προσωπικές πληροφορίες ή ακατάλληλα βίντεο και φωτογραφίες. Μπορούν να μειώνουν για πάντα στο Διαδίκτυο και να διανεμηθούν στον οποιονδήποτε.
- Ακόμα και αν νιώθουμε άσχημα για κάτι που κάναμε στο διαδίκτυο, όπως ντροπή, φόβο ή και ενοχές, ζητάμε τη συμβουλή και την υποστήριξη κάποιου ενήλικα που ξέρουμε ότι μας αγαπάει και που εμπιστευόμαστε. Δεν ξεχνάμε ότι η σωματική μας και η ψυχική μας ακεραιότητα είναι προτεραιότητα και οφείλουμε να την προστατεύουμε.
- Σε κάθε περίπτωση δεν ενδίδουμε σε κανένα εκβιασμό. Δε δελεαζόμαστε από χρήματα και δώρα.
- Μαθαίνουμε τον τρόπο που μπορούμε να αποθηκεύσουμε μια ηλεκτρονική συνομιλία. Αυτό θα μας βοηθήσει να καταγγείλουμε αυτόν που μας έκανε να νιώσουμε άβολα ή μας έφερε σε δύσκολη θέση στο διαδίκτυο.

Πηγές:

<https://internetsafety.pi.ac.cy/kids/kids-danger/kids-seduction/>
<https://internetsafety.pi.ac.cy/kids/kids-danger/kids-seduction/>

Video:

<https://www.youtube.com/watch?v=ljC59oJASfE>