

Ερευνητική Εργασία Α' Λυκείου

«Πλοήγηση στο διαδίκτυο: ΜΚΔ και υπερβολική
ενασχόληση, Άγνωστοι και cyber bullying,προσωπικά
δεδομένα και ασφαλείς κωδικοί, Ασφαλής
συμπεριφορά»



3ο ΓΕΛ Θήβας

Τμήμα Α1

Υπεύθυνη Καθηγήτρια: Μαρία Βασιλείου

Σχολικό Έτος 2017-2018

Α' Τετράμηνο

Πίνακας περιεχομένων

ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΚΑΙ ΣΥΜΠΕΡΙΦΟΡΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.....	3
Πρόλογος	3
Κίνδυνοι στο διαδίκτυο	4
Spam	4
Παραπλήροφορηση.....	5
Cookies	5
Κανόνες ασφαλούς πλοήγησης	6
Συμβουλές για τους εκπαιδευτικούς	7
Συμβουλές για τον χρήστη.....	8
Safe Line.....	9
ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ-ΥΠΕΡΒΟΛΙΚΗ ΕΝΑΣΧΟΛΗΣΗ	11
Πρόλογος	11
Κανόνες Ορθής Χρήσης Των ΜΚΔ.....	11
Δημοσίευση-Ανάρτηση-Διαγραφή Πληροφορίας	11
Ευαίσθητες προσωπικές πληροφορίες.....	12
Ρυθμίσεις Ασφάλειας της πλατφόρμας-Κοινωνικού Δικτύου (social	13
network).....	13
Κακόβουλο Υλικό-πληροφορία η οποία βρίσκεται εντός του	13
κοινωνικού δικτύου (Social Network).....	13
Δικαιώματα Πνευματικής Ιδιοκτησίας.....	13
Υπερβολική ενασχόληση.....	14
Τρόποι περιορισμού της χρήσης του διαδικτύου:	14
Κοινωνική Απομόνωση (Social isolation).....	15
ΑΓΝΩΣΤΟΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ & CYBER BULLYING	16
Συμβουλές αντιμετώπισης του Cyberbullying.....	18
ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ	20
Τρόποι επεξεργασίας.....	20
Συλλογή και επεξεργασία προσωπικών δεδομένων	20
Τρόποι παραβίασης.....	21
Άλλοι τρόποι παραβίασης προσωπικών δεδομένων είναι οι εξής:	21
Τρόποι προστασίας	22
ΠΗΓΕΣ.....	24

ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΚΑΙ ΣΥΜΠΕΡΙΦΟΡΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ



<http://www.newsbomb.gr/media-agb/story/366810/megali-tileoptiki-kampania-enimerosis-gia-tin-asfaleia-sto-diadiktyo>

Πρόλογος

Η έννοια του κινδύνου δεν είναι απολύτως προσδιορισμένη με έναν διεθνώς αποδεκτό τρόπο. Οι διαδικτυακοί κίνδυνοι μπορούν να πάρουν πολλές μορφές. Ωστόσο, υπάρχουν μέθοδοι για την αντιμετώπιση αυτού του φαινομένου.

Σχεδόν οποιαδήποτε καθημερινή δραστηριότητα στο διαδίκτυο συνεπάγεται επεξεργασία των προσωπικών μας δεδομένων. 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 Πολιτική Προστασίας Απορρήτου ενημερώνει για τις πολιτικές και πρακτικές συλλογής, διατήρησης, αποθήκευσης, επεξεργασίας και χρήσης των προσωπικών δεδομένων των χρηστών/επισκεπτών μιας ιστοσελίδας, καθώς και το εάν και με ποιο τρόπο θα κοινοποιηθούν σε τρίτους. Θα πρέπει να περιέχει τη σχετική νομοθεσία που διέπει τον κλάδο και είναι εφαρμοστέα στη χώρα που δραστηριοποιείται η εταιρεία.

Η γνωστοποίηση σε τρίτους μηνυμάτων ή φωτογραφιών προκλητικού περιεχομένου που αφορούν ανήλικους είναι μια πολύ σοβαρή συμπεριφορά που μπορεί, κατά περίπτωση, να υπαχθεί στη νομοθεσία που απαγορεύει τη συλλογή και επεξεργασία ευαίσθητων προσωπικών δεδομένων (Ν. 2472/1997) ή ακόμη και να συνιστά αδίκημα σχετικό με παιδική κακοποίηση (άρθρο 348 Α Π.Κ.).

Θυμάμαι ότι οτιδήποτε μοιράζομαι στο διαδίκτυο ή μέσω κινητών τηλεφώνων φεύγει από το δικό μου έλεγχο και δεν ξέρω ποτέ πού μπορεί να καταλήξει.

Οι φωτογραφίες ή τα μηνύματα μπορεί να διανεμηθούν σε πολύ μικρό χρονικό διάστημα σε πλήθος ατόμων ή/και να δημοσιευτούν σε διάφορους ιστόχους. Ακόμα, ενδέχεται κάποιος ηθελημένα να μοιραστεί τις φωτογραφίες μας.

Είναι μάλλον αδύνατο να εξαφανίσει κανείς εντελώς τα ψηφιακά του «ίχνη», τουλάχιστον όσον αφορά τις υπηρεσίες κοινωνικής δικτύωσης. Η πιο ριζική λύση θα ήταν η οριστική διαγραφή του προφίλ, χωρίς δυνατότητα επαναφοράς. Για όσους, πάντως, θέλουν να συνεχίσουν να χρησιμοποιούν τον λογαριασμό τους, τα περισσότερα social media προσφέρουν τρόπους ώστε να αποσύρουν από την «κοινή θέα» τις αναρτήσεις για τις οποίες οι χρήστες μετάνιωσαν στην πορεία.

Κίνδυνοι στο διαδίκτυο



Οι διαδικτυακοί κίνδυνοι είναι κίνδυνοι που σχετίζονται με το να είναι κάποιος χρήστης του διαδικτύου. Οι κίνδυνοι αυτοί μπορεί επίσης να αφορούν στην πρόσβαση σε ανεπιθύμητες πληροφορίες. Υπάρχει μεγάλη ποικιλία διαδικτυακών από θέματα ασφάλειας ως διάφορα είδη θυματοποίησης.

Spam

Spam ονομάζεται η μαζική αποστολή ηλεκτρονικών μηνυμάτων σε μια προσπάθεια προώθησης προϊόντων ή ιδεών. Τα μηνύματα αυτά στέλνονται στο ηλεκτρονικό ταχυδρομείο ή στο κινητό τηλέφωνο του χρήστη. Λόγω του χαμηλού κόστους, η

αποστολή μπορεί να γίνει σε πολύ μεγάλο αριθμό αποδεκτών. Τα μηνύματα αυτά σχετίζονται συχνά με διαφημίσεις προϊόντων ή υπηρεσιών, την προώθηση τυχερών παιχνιδιών (καλυμμένων ενίοτε ως κερδών σε μία κλήρωση στην οποία ο χρήστης ποτέ δεν συμμετείχε), με πορνογραφικό υλικό. Μερικές φορές με πρόσχημα μία ιστορία στην οποία (υποτίθεται ότι) υπάρχουν αδιάθετα κάποια σημαντικά χρηματικά ποσά, ο χρήστης καλείται να συμμετάσχει προσφέροντας υπηρεσίες για τις οποίες (υποτίθεται ότι) θα αμειφθεί πλουσιοπάροχα. Τα μηνύματα αυτά πολλές φορές αποστέλλονται μαζικά σε μεγάλους αριθμούς και μεταφράζονται από γλώσσα σε γλώσσα με αυτόματους, μεταφραστές στις περιπτώσεις αυτές οι ίδιες οι μεταφράσεις παράγουν κείμενα ακατανόητα ή με χονδροειδή γλωσσικά ή επικοινωνιακά λάθη καθιστώντας πολύ εύκολη τη διαπίστωση ότι πρόκειται για ψευδή μηνύματα.

Παραπλήροφρηση

Το διαδίκτυο παρέχει αναρίθμητους πόρους και ευκαιρίες μάθησης, από την άλλη δε διαθέτει τις απαραίτητες δικλίδες ασφάλειας για τον έλεγχο της εγκυρότητας των πληροφοριών που δημοσιεύονται, με αποτέλεσμα, σε κάποιες περιπτώσεις με την δημοσίευση αναληθών, τροποποιημένων ή ελλιπών πληροφοριών, μπορεί ο χρήστης να οδηγηθεί σε λανθασμένα, ανακριβή και αναξιόπιστα συμπεράσματα .

Χαρακτηριστικό παράδειγμα της παραπληροφόρησης είναι οι αστικοί μύθοι οι οποίοι λόγω του διαδικτύου διαδίδονται με μεγαλύτερη ευκολία, σε περισσότερο πληθυσμό. Η κακόβουλη πρόθεση, ο εμπλουτισμός με τεχνολογία υψηλότερης ποιότητας και με γνωρίσματα που παρέχουν φαινομενική αυθεντικότητα, κάνουν τους σημερινούς διαδικτυακούς αστικούς μύθους πιο αληθοφανείς και ενδεχομένως πιο επιβλαβείς.

Κατά συνέπεια, κρίνεται αναγκαία η ανάπτυξη κριτικής σκέψης από το χρήστη του διαδικτύου, προκειμένου να κρίνει την ακρίβεια των πληροφοριών αυτών και να ξεχωρίσει τη μη έγκυρη πληροφορία. Όπως είναι φυσικό ο κίνδυνος της παραπληροφόρησης είναι ιδιαίτερα αυξημένος με απρόβλεπτα αποτελέσματα σε νεαρά άτομα τα οποία λόγω ηλικίας δεν έχουν οξυμένη την κριτική τους σκέψη και ικανότητα.

Cookies

Τα cookies είναι μικρά αρχεία που αποθηκεύονται από τον περιηγητή σας στον υπολογιστή, στο tablet, το κινητό τηλέφωνο και γενικά στη συσκευή με την οποία περιηγείστε σε κάποια ιστοσελίδα. Κάθε cookie περιέχει πληροφορίες όπως συνήθως το όνομα του ιστότοπου από τον οποίο προέρχεται. Επιτρέπουν στους ιστότοπους να αποθηκεύουν διάφορες ανώνυμες πληροφορίες όπως για παράδειγμα τις προτιμήσεις του επισκέπτη ή αν έχει επισκεφθεί ξανά τον ιστότοπο. Ένα «cookie» μπορεί να εγκατασταθεί μόνο εφόσον έχει εξασφαλιστεί η συγκατάθεση του συνδρομητή ή χρήστη.



<http://www.elpidazois.gr/el/static/asfaleia-sto-diadiktyo-sta-plaisia-project-sto-1o-gymnasio-argous.aspx>

Κανόνες ασφαλούς πλοήγησης

- Η κοινοποίηση ενός προσωπικού δεδομένου στο οποίο εικονίζεται ένα άλλο άτομο **ΠΡΕΠΕΙ** να γίνεται με τη σύμφωνη συγκατάθεσή του.
- Προσβλητικό περιεχόμενο στο διαδίκτυο **ΠΡΕΠΕΙ να καταγγέλλεται άμεσα** έτσι ώστε να γίνονται οι απαραίτητες ενέργειες προκειμένου να αποσυρθεί από τον ιστό.
- Κατά τη σύνδεση στο διαδίκτυο από δίκτυα δημόσιας χρήσης **ΠΡΕΠΕΙ** να αποφεύγεται η μετάδοση προσωπικών στοιχείων.
- Για την ασφαλή πλοήγηση στο διαδίκτυο είναι σημαντικό να μην κατεβάζουμε μουσική και παιχνίδια από site τα οποία δεν είναι έμπιστα έτσι ώστε να μην κολλήσουμε κάποιον ιό.
- Κατά την πλοήγηση στο διαδίκτυο, εάν ληφθεί κάποιο email που φαινομενικά είναι έμπιστο, **ΠΡΕΠΕΙ** να κρίνουμε την προέλευσή του γιατί μπορεί να είναι πλαστό.
- Αν κάποιος έχει δημιουργήσει λογαριασμό με τον οποίο σας παριστάνει θα πρέπει να κάνετε αναφορά και να ζητήσετε από το διαχειριστή να κλείσει το ψεύτικο προφίλ.

Συμβουλές για τους εκπαιδευτικούς



<http://www.ert.gr/perifereiakoi-stathmoi/ioanina/asfalisi-ploigisi-sto-diadiktyo-apo-tin-ya-igoumenitsas/>

Μιλήστε στα παιδιά σας για τον διαδικτυακό εκφοβισμό όπως θα το κάνατε για άλλα είδη εκφοβισμού και προτρέψτε τα να έρθουν σε εσάς αν ποτέ οποιοσδήποτε τους προκαλέσει αναστάτωση στο διαδίκτυο, στο κινητό τους ή άλλες συσκευές. Ρωτήστε το παιδί πράγματα όπως :

- Αν έλαβε ποτέ κάποιο email ή γραπτό μήνυμα που το αναστάτωσε.
- Αν συμμετείχε στον εκφοβισμό κάποιου άλλου στο διαδίκτυο ή μέσω του κινητού του.

Αν το παιδί σας, σας πει ότι έχει πέσει θύμα διαδικτυακού εκφοβισμού, προσφέρετέ του και πρακτική και συναισθηματική υποστήριξη:

- Εξηγήστε του ότι δεν πρέπει να απαντά στον εκφοβισμό, καθώς αυτό θα μπορούσε να χειροτερέψει τα πράγματα.
- Εκμεταλλευθείτε στο μέγιστο τα ενσωματωμένα εργαλεία στις υπηρεσίες διαδικτύου ή κινητής τηλεφωνίας του παιδιού σας, ώστε να αποτρέψετε περαιτέρω εκφοβισμό.
- Αν το παιδί σας πιστεύει πως αυτός που διέπραξε τον εκφοβισμό είναι συμμαθητής του, μιλήστε στο δάσκαλό του.

Αν πιστεύετε ότι το παιδί σας θα μπορούσε να χρησιμοποιεί νέες τεχνολογίες για να εκφοβίσει κάποιον άλλον:

- Μιλήστε του σχετικά με τον διαδικτυακό εκφοβισμό και εξηγήστε γιατί αυτό είναι απαράδεκτο και πρέπει να σταματήσει.
- Αν δεν είχε συνειδητοποιήσει πως αυτό που έκανε ήταν εκφοβισμός, εξηγήστε του ότι ο εκφοβισμός δεν είναι απλώς σωματικός. Το να χρησιμοποιείς την τεχνολογία για να πειράξεις, να εξευτελίζεις και να διαβάλλεις είναι επίσης εκφοβιστική συμπεριφορά.

- Προτρέψτε το να μιλήσει σε εσάς ή σε έναν δάσκαλο, για οποιοδήποτε εκφοβισμό στον οποίο είναι μάρτυρας, συμπεριλαμβανομένων των περιστατικών διαδικτυακού εκφοβισμού.

Συμβουλές για τον χρήστη



<http://allanea.gr/02/2015/%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%AE%CF%82-%CF%80%CE%B5%CF%81%CE%B9%CE%AE%CE%B3%CE%B7%CF%83%CE%B7-%CF%83%CF%84%CE%BF-%CE%B4%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF/>

- Μια καλή επιλογή είναι η Ανοιχτή Γραμμή για το παράνομο περιεχόμενο στο διαδίκτυο SafeLine (www.safeline.gr) η οποία συνεργάζεται τόσο με την Ελληνική Αστυνομία όσο και με τη Europol και στην οποία μπορούμε να κάνουμε την καταγγελία μας είτε επώνυμα είτε ανώνυμα.
- Αποφύγετε να επισκέπτεστε σελίδες στις οποίες πρέπει να δώσετε προσωπικούς σας μυστικούς κωδικούς (passwords), ιδιαίτερα αν η ανταλλαγή πληροφορίας δεν πραγματοποιείται κρυπτογραφημένα (π.χ. <https://>). Είναι πιθανό τα δίκτυα αυτά να μην είναι ασφαλή και να υποκλαπούν προσωπικά σας δεδομένα.
- Επιβεβαιώστε ότι χρησιμοποιείτε ασφαλή σύνδεση όταν στέλνετε ευαίσθητες προσωπικές πληροφορίες μέσω του παγκόσμιου ιστού (Web). Αυτό φαίνεται από το εικονίδιο του κλειδωμένου λουκέτου το πεδίο διευθύνσεων, ενώ η διεύθυνση στην οποία συνδέεστε πρέπει να αρχίζει με <https://> αντί του <http://>.
- Δε δελεαζόμαστε ποτέ από χρήματα ή δώρα για να κάνουμε κάτι ακατάλληλο. Ζητάμε τη συμβουλή και την υποστήριξη κάποιου ενήλικα που εμπιστευόμαστε. Είναι σημαντικό να θυμόμαστε ότι η σωματική και η ψυχική μας ακεραιότητα είναι προτεραιότητα και οφείλουμε τόσο εμείς όσο και οι γονείς μας να την προστατεύουμε.

- Δεν πρέπει ποτέ να απαντάμε, να σχολιάζουμε ή να κοινοποιούμε περιεχόμενο όταν είμαστε θυμωμένοι. Είναι πολύ πιθανό να πούμε πράγματα για τα οποία θα μετανιώσουμε αργότερα αλλά δε θα μπορούμε να τα πάρουμε πίσω. Περισσότερες πληροφορίες για την προστασία των προσωπικών δεδομένων μπορεί να αναζητήσει κανείς στο διαδικτυακό τόπο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα <http://www.dpa.gr>

Safe Line



Η SafeLine ξεκίνησε τη λειτουργία της στις 14 Απριλίου 2003. Είναι η μοναδική ανοικτή γραμμή καταγγελιών παράνομου περιεχομένου στο Διαδίκτυο και επίσημο μέλος του INHOPE (Διεθνής Σύνδεσμος Ανοικτών Γραμμών Διαδικτύου) από τις 18 Οκτωβρίου 2005.

Βασικά μέριμνα της SafeLine είναι η εξάλειψη φωτογραφιών και βίντεο που απεικονίζουν κακοποίηση ανηλίκων, καθώς και η προάσπιση του δικαιώματος της ασφαλούς πλοήγησης του παιδιού στο Διαδίκτυο. Στα παραπάνω προστίθεται και η αντιμετώπιση της παρενόχλησής του μέσω του κυβερνοχώρου ή του κινητού τηλεφώνου αλλά και η αντιμετώπιση περιεχομένου που αφορά τη βία, το ρατσισμό, την ξενοφοβία και γενικά καθετί το οποίο αντιβαίνει στην Ελληνική Νομοθεσία.

Το 2008, η SafeLine ένωσε τις δυνάμεις της με την Δράση Ενημέρωσης και Επαγρύπνησης και παράλληλα, δημιουργήθηκε η Γραμμή Βοηθείας Help-line.gr. Οι τρεις δράσεις δημιούργησαν τον Ελληνικό Κέντρο Ασφαλούς Διαδικτύου με στόχο μια πιο πολύπλευρη και οργανωμένη προσπάθεια που ενσωματώνει την ενημέρωση & αφύπνιση του κοινού, την καταγγελία, καθώς και την πρόληψη & βοήθεια κάτω από το ίδιο κοινό έργο.

Η Safe Line λειτουργεί από το 2003 με την στήριξη της Ευρωπαϊκής Επιτροπής. Από 1/7/2016 συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση, διευκόλυνση "Συνδέοντας την Ευρώπη" στο πλαίσιο του έργου "The Hellenic Safer Internet Centre – Making a Better and Safer Internet for Kids and the Society (EL-SIC)" και υλοποιείται από το Ινστιτούτο Πληροφορικής του Ιδρύματος Τεχνολογίας και Έρευνας.

Η δημιουργία ενός ασφαλέστερου και ποιοτικότερου διαδικτύου είναι υπόθεση όλων μας!

Σκέψου σωστά και έξυπνα στο διαδίκτυο

ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ-ΥΠΕΡΒΟΛΙΚΗ ΕΝΑΣΧΟΛΗΣΗ

Πρόλογος

Όταν αναφερόμαστε στα Μέσα Κοινωνικής Δικτύωσης εννοούμε τους Διαδικτυακούς τόπους που παρέχουν ως υπηρεσία την παραγωγή και δημοσίευση περιεχομένου από τους ίδιους τους χρήστες του Διαδικτύου και όχι από κάποια εταιρία. Οι περισσότερες υπηρεσίες αυτής της μορφής ενθαρρύνουν τη συζήτηση, τα σχόλια, την αλληλεπίδραση και το διαμοιρασμό οποιασδήποτε πληροφορίας μεταξύ των χρηστών. Οι χρήστες κάνουν ψηφιακούς φίλους με τους οποίους επικοινωνούν, ανταλλάσσουν απόψεις και ψηφιακό περιεχόμενο κάθε μορφής (εικόνες ,κείμενα, συνδέσμους,videοκ.λπ.)Τα δημοφιλέστερα Μέσα Κοινωνικής Δικτύωσης είναι: facebook, instagram, YouTube, twitter, tumblr, skype, Wikipedia κ.α .



Κανόνες Ορθής Χρήσης Των ΜΚΔ

Η δραστηριοποίηση στα Μέσα Κοινωνικής Δικτύωσης-ΜΚΔ προϋποθέτει την ύπαρξη και υιοθέτηση κανόνων οι οποίοι θα διευκολύνουν την χρήση των “Μέσων Κοινωνικής Δικτύωσης-ΜΚΔ” και παράλληλα θα ελαχιστοποιήσουν τη διαρροή ευαίσθητων πληροφοριών μέσα από αυτά. **Οι βασικότεροι κανόνες ορθής χρήσης των “Μέσων Κοινωνικής Δικτύωσης- ΜΚΔ” αναφέρονται παρακάτω:**

Δημοσίευση-Ανάρτηση-Διαγραφή Πληροφορίας

- ✦ Η Δημοσίευση-Ανάρτηση Πληροφορίας είναι ψηφιακή, μόνιμη, διαδίδεται ταχύτατα, είναι μη αναστρέψιμη και είστε ο αποκλειστικός υπεύθυνος γι' αυτή. Η διαγραφή της πληροφορίας ουσιαστικά δεν είναι διαγραφή.
- ✦ Τα προφίλ και τα στοιχεία που δημιουργούνται σε ΜΚΔ μπορούν να αντιγραφούν και να αποθηκευτούν από τρίτους, δημιουργώντας ένα ψηφιακό φάκελο των προσωπικών σας δεδομένων.
- ✦ Από τη στιγμή που θα αναρτηθεί-δημοσιευθεί στα Κοινωνικά Δίκτυα-ΚΔ (social networks) οποιαδήποτε πληροφορία, δεν είναι δυνατή η “ανάκληση” της.
- ✦ Ακόμη και μετά την εντολή για διαγραφή της, δεν σημαίνει ότι πραγματικά η πληροφορία έχει διαγραφεί. Πιθανώς αυτή να έχει αρχειοθετηθεί από την εταιρεία στην οποία ανήκει το “Κοινωνικό Δίκτυο”, ή από άτομα τα οποία παρακολουθούν τις αναρτήσεις σας. Ακόμη και αν ένα προφίλ διαγραφεί, είναι πολύ πιθανό ότι, τα στοιχεία του θα παραμείνουν αποθηκευμένα σε μια βάση δεδομένων στο διαδίκτυο.
- ✦ Οι χρήστες που επιθυμούν να διαγράψουν λογαριασμούς από ΜΚΔ διαπιστώνουν ότι, είναι σχεδόν αδύνατο να αφαιρέσουν πληροφορίες δευτέρου βαθμού που συνδέονται με το προφίλ τους, όπως επί παραδείγματι τα δημόσια σχόλια σχετικά σε άλλα προφίλ.

- ⊕ Επίσης, θα πρέπει να γνωρίζετε ότι οποιοδήποτε υλικό (κείμενο, φωτογραφία, βίντεο) το οποίο αναρτάται-δημοσιεύεται μπορεί να μεταδοθεί ταχύτατα (viral) στον χώρο των “κοινωνικών δικτύων”, με τέτοιο τρόπο ώστε πολύ σύντομα να μην έχετε τον έλεγχο του.
- ⊕ Μη ξεχνάτε ότι είστε υπεύθυνοι για ό,τι αναρτάτε-δημοσιεύετε.

Ευαίσθητες προσωπικές πληροφορίες

- ⊕ Μην αποκαλύπτετε μέσω των δημοσιεύσεων-αναρτήσεων σας προσωπικές ευαίσθητες πληροφορίες.
- ⊕ Αποφύγετε τη δημοσίευση ή τουλάχιστον προσπαθήστε να ελάχιστο -ποιήσετε την αποκάλυψη μέσω των κοινωνικών δικτύων ευαίσθητων προσωπικών πληροφοριών για τον εαυτό σας και την οικογένειά σας οι οποίες μπορούν να χρησιμοποιηθούν από κακόβουλους χρήστες σε διάφορες επιθέσεις, ακόμη και προσπάθειες πλαστοπροσωπίας (id-theft).
- ⊕ Μια καλή προσέγγιση είναι να λειτουργείτε πάντα με την παραδοχή ότι, οτιδήποτε δημοσιεύετε στο διαδίκτυο μπορεί να κλαπεί από έτερους κακόβουλους χρήστες, πιθανώς και εγκληματίες, ή τους αντιπάλους σας.
- ⊕ Το περιεχόμενο των κοινωνικών δικτύων που αφορά στο προσωπικό των ΕΔ και στις οικογένειές τους, αποτελεί σημαντικό στόχο για εκείνους που θέλουν να αποκτήσουν πρόσβαση σε αυτές τις πληροφορίες για πολλούς λόγους (κατασκοπεία, μίσηση, εκβιασμό, εκφοβισμό).
- ⊕ Αναρωτηθείτε: “Τι θα μπορούσε ένα κακόβουλο άτομο να κάνει με αυτές τις πληροφορίες; Θα μπορούσε να παραβιάσει την ασφάλεια τη δική μου, της οικογένειάς μου;
- ⊕ Η ανάρτηση μη διαβαθμισμένων ευαίσθητων πληροφοριών θα μπορούσαν να είναι εξίσου επικίνδυνη με την ανάρτηση διαβαθμισμένων πληροφοριών.
- ⊕ Εξετάστε την πιθανότητα να χρησιμοποιήσετε ένα ψευδώνυμο ως όνομα, για την προστασία των ιδιωτικών σας πληροφοριών.
- ⊕ Ιδιαίτερη προσοχή χρειάζεται, στο τι πληροφορίες δημοσιεύουν τα μέλη της οικογένειάς σας και κυρίως τα μικρά παιδιά στα κοινωνικά δίκτυα, γιατί αυτό μπορεί να τα εκθέσει σε διάφορους κινδύνους, τους οποίους αυτά δεν αντιλαμβάνονται.
- ⊕ Η Υπηρεσία Ηλεκτρονικού Εγκλήματος έχει πολλά στοιχεία για περιπτώσεις βιασμών, κακοποίησης, ή και δολοφονίας μικρών παιδιών από αγνώστους, που γνώρισαν μέσω κοινωνικών δικτύων. Σε περίπτωση ανάγκης, οι γονείς πρέπει να εγκαθιστούν ειδικά φίλτρα ασφαλείας, τα οποία να απαγορεύουν την πρόσβαση του παιδιού τους, σε κοινωνικά δίκτυα από τον υπολογιστή.
- ⊕ Προτιμότερο είναι πάντως, να συζητούν με το παιδί, τους σοβαρούς κινδύνους που πιθανό να αντιμετωπιστούν, καθώς η απαγόρευση χρήσης δεν λύνει πάντα το πρόβλημα, αφού τα παιδιά μπορούν να χρησιμοποιήσουν τον υπολογιστή ενός φίλου/μιας φίλης.

Ρυθμίσεις Ασφάλειας της πλατφόρμας-Κοινωνικού Δικτύου (social network)

- ⊕ Εξετάστε και τροποποιείτε προσεκτικά τις ρυθμίσεις ασφαλείας της κοινωνικής πλατφόρμας (social network) που δραστηριοποιείστε.
- ⊕ Εξοικειωθείτε με τους όρους υπηρεσίας του κάθε ιστότοπου κοινωνικής δικτύωσης και να τους ακολουθείτε.
- ⊕ Εξετάστε προσεκτικά τους όρους χρήσης που αφορούν στην εμπιστευτικότητα και στην προστασία των δεδομένων και όλες τις ρυθμίσεις ασφαλείας και προστασίας των προσωπικών δεδομένων (privacy settings) της πλατφόρμας (social network) στην οποία δραστηριοποιήστε και κάντε τις κατάλληλες ρυθμίσεις.
Για παράδειγμα:
 - ✚ Αλλάζετε τακτικά τους Κωδικούς Ασφαλείας (password) του λογαριασμού σας. Επίσης, να είστε προσεκτικοί σε ποιους επιτρέπετε να έχουν πρόσβαση στους λογαριασμούς των κοινωνικών μέσων σας.
 - ✚ Χρησιμοποιήστε τις επιλογές ασφαλείας (security settings) που υπάρχουν στο προφίλ σας (profile).
 - ✚ Ρυθμίστε τις επιλογές ασφαλείας που θα επιτρέπουν την προβολή του προφίλ σας, αλλά και των δημοσιεύσεων-αναρτήσεων σας σε συγκεκριμένο κοινό (για παράδειγμα μόνο στους φίλους σας).
 - ✚ Μην αποδέχεσθε εύκολα συνδέσεις (connection establishment) με πρόσωπα που δεν γνωρίζετε προσωπικά
 - ✚ Απενεργοποιήστε τις υπηρεσίες εντοπισμού θέσης (location based services-Geotagging7) που διαθέτουν τα “κοινωνικά δίκτυα”, κυρίως από τις κινητές σας συσκευές, αν δεν τις χρειάζεσθε. Καλό θα είναι να μην γνωστοποιείτε, αν δεν είναι απαραίτητο, τη θέση σας στο ευρύτερο κοινό σας για διάφορους λόγους (π.χ. πιθανότητα κλοπής).

Κακόβουλο Υλικό-πληροφορία η οποία βρίσκεται εντός του

κοινωνικού δικτύου (Social Network)

- ⊕ Δώστε την κατάλληλη προσοχή στο υλικό (φωτογραφίες, βίντεο, αρχεία) το οποίο κυκλοφορεί εντός του κοινωνικού δικτύου.
- ⊕ Το υλικό (φωτογραφίες, βίντεο, αρχεία) το οποίο κυκλοφορεί στα κοινωνικά δίκτυα μπορεί εύκολα και γρήγορα να γίνει ιογενές.
- ⊕ Επανεξετάστε προσεκτικά το υλικό (φωτογραφίες, βίντεο, αρχεία) που αναρτάτε πριν τη δημοσίευσή του
- ⊕ Επίσης δώστε την κατάλληλη προσοχή στο υλικό το οποίο προέρχεται από άλλους χρήστες, το οποίο μπορεί με τη σειρά του να είναι μολυσμένο και να δημιουργήσει πρόβλημα στο δικό σας λογισμικό.

Δικαιώματα Πνευματικής Ιδιοκτησίας

- ⊕ Σεβαστείτε τα πνευματικά δικαιώματα.
- ⊕ Σεβαστείτε την πνευματική ιδιοκτησία και μη παραβιάζετε τα δικαιώματα πνευματικής ιδιοκτησίας

- ⊕ Μην δημοσιεύσετε οποιαδήποτε πληροφορία ή άλλο υλικό που προστατεύεται από Πνευματικά Δικαιώματα, χωρίς την άδεια του κατόχου αυτών.
- **Ιδιωτική Ζωή**
- ⊕ Μην παραβιάζετε την ιδιωτική ζωή άλλων.
- ⊕ Μην δημοσιεύσετε οποιαδήποτε πληροφορία που παραβιάζει την προστασία της ιδιωτικής ζωής, ή τα προσωπικά δεδομένα και δικαιώματα των άλλων.

Υπερβολική ενασχόληση

Ενδείξεις υπερβολικής χρήσης του διαδικτύου:

- η απομάκρυνση από την οικογένεια και τους φίλους για χάρη του διαδικτύου



- παραμέληση της διατροφής και του ύπνου λόγω της ενασχόλησης με το διαδίκτυο

- διαρκής σκέψη για το πότε θα ξανασυνδεθείς σε αυτό

- η αδυναμία του ατόμου να συνεχίσει τις δραστηριότητες του

- οι ανεπιτυχείς

προσπάθειες να μειώσει ή να ελέγξει το χρόνο ενασχόλησης με το διαδίκτυο

- η επιθυμία να περνά ολόένα και περισσότερο χρόνο στο διαδίκτυο και περισσότερο από αυτό που είχε αρχικά προγραμματίσει
- η παραμέληση ή και απομόνωση από την οικογένεια και τους φίλους
- το συναισθηματικό κενό, η ανία, η ανησυχία, η άσχημη διάθεση και η επιθετικότητα

Τρόποι περιορισμού της χρήσης του διαδικτύου:

- ✓ η επέκταση του δικτύου των φίλων
- ✓ η εύρεση νέων ενδιαφερόντων
- ✓ η θέσπιση ορίων σχετικά με τις ώρες που δαπανά κανείς στο διαδίκτυο
- ✓ η ώθηση σε κοινωνικές και αθλητικές δραστηριότητες
- ✓ η καθιέρωση οικογενειακών δραστηριοτήτων που δεν εμπεριέχουν τη χρήση υπολογιστή και διαδικτύου
- ✓ η τοποθέτηση του υπολογιστή σε δωμάτιο κοινής χρήσης από την οικογένεια και όχι στο δωμάτιο των παιδιών
- ✓ η εγκατάσταση και η χρησιμοποίηση προγραμμάτων που ελέγχουν την πρόσβαση σε συγκεκριμένες ιστοσελίδες αλλά και τον χρόνο παραμονής στον ιστόχωρο

Ωστόσο, επιτρέψτε την πρόσβαση στο διαδίκτυο διότι συχνά ο αποκλεισμός οδηγεί στη μυθοποίηση ενώ μας ενδιαφέρει ο σωστός έλεγχος και όχι η απόρριψη του διαδικτύου

Κοινωνική Απομόνωση (Social isolation)

Η υπερβολική ενασχόληση των Μέσων Κοινωνικής Δικτύωσης έχει ως αποτέλεσμα την αποξένωση των χρηστών από τον πραγματικό κόσμο (Social isolation). Στη σημερινή εποχή ένα μεγάλο ποσοστό των νεαρών ατόμων ασχολούνται όλο και περισσότερο με ψηφιακά παιχνίδια, με την άμεση online συνομιλία (chat rooms), με σελίδες, κοινωνικής δικτύωσης κι έτσι αποξενώνονται από το φυσικό τους περιβάλλον. Ο χρόνος που αφιερώνουν στις ενασχολήσεις αυτές είναι πολύ μεγάλος και έχει ως αποτέλεσμα να αποκλείει άλλου είδους δραστηριότητες και σε ακραίες περιπτώσεις την ατομική περιποίηση του εαυτού του. Οι σχέσεις με τους γύρω του, τους φίλους, τους συγγενείς και τους γονείς γίνονται προβληματικές. Έτσι δημιουργείται (εκτός των άλλων) μια γενικότερη αποξένωση των χρηστών από το περίγυρό τους. Έτσι η online ζωή γίνεται για τους εθισμένους χρήστες πολύ πιο σημαντική από την πραγματική. Το συγκεκριμένο φαινόμενο έχει αναγνωριστεί ως ένα είδος πάθησης που χρειάζεται θεραπείας



ΑΓΝΩΣΤΟΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ & CYBER BULLYING

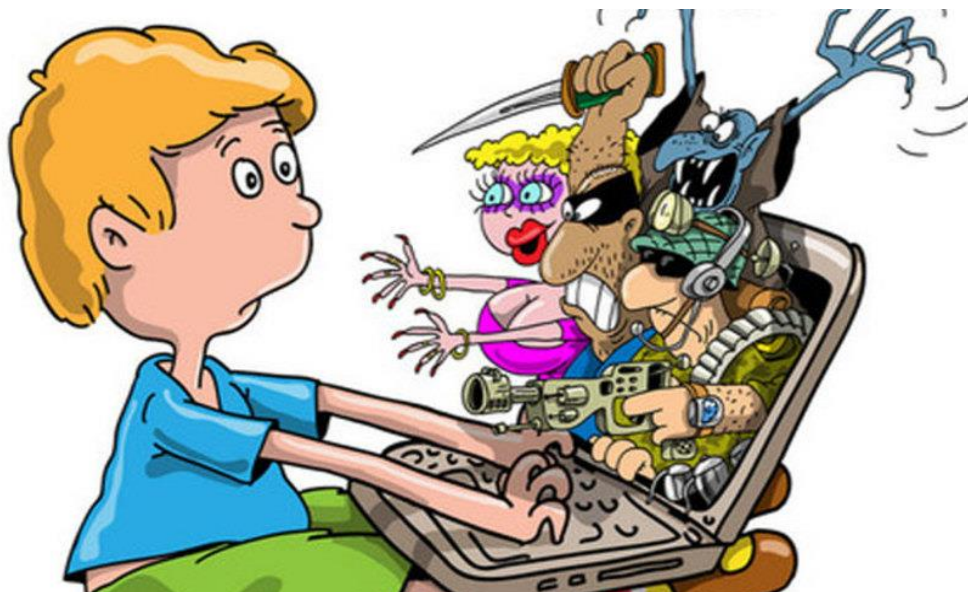
Ο Διαδικτυακός Εκφοβισμός ορίζεται ως «μια επιθετική, σκόπιμη και επαναλαμβανόμενη πράξη η οποία πραγματοποιείται από ένα άτομο ή μια ομάδα ατόμων, μέσω της χρήσης ηλεκτρονικών μορφών επικοινωνίας, εναντίον ενός ατόμου που δεν μπορεί να υπερασπιστεί τον εαυτό του» **πηγή: internet-φυλλάδιο**



Η αυξανόμενη χρήση των ηλεκτρονικών συσκευών και του διαδικτύου τον καθιστά ως την μορφή εκφοβισμού με το μεγαλύτερο ρυθμό αύξησης. Πραγματοποιείται μέσα από το ηλεκτρονικό τα δωμάτια συζητήσεων, τους ιστότοπους κοινωνικής δικτύωσης, τις ιστοσελίδες, τα ιστολόγια, τα Διαδικτυακά παιχνίδια και κινητά τηλέφωνα.

Οι μορφές που μπορεί να έχει είναι:

- ❖ Ο εξευτελισμός του θύματος
- ❖ Η αποστολή προσβλητικών και άσεμνων μηνυμάτων μέσω Διαδικτυακών εφαρμογών
- ❖ Η αποστολή απειλητικών μηνυμάτων
- ❖ Το άσεμνο περιεχόμενο κατά την διάρκεια συνομιλιών
- ❖ Η δημοσιοποίηση προσωπικών βίντεο ή φωτογραφιών χωρίς την άδεια του ιδιοκτήτη
- ❖ Ο εξευτελισμός ενός νεαρού ατόμου με την δημιουργία ενός προφίλ το οποίο περιλαμβάνει λανθασμένα στοιχεία



Η ιδιαιτερότητα του διαδικτυακού εκφοβισμού έγκειται στο γεγονός πως επεμβαίνει στον προσωπικό χώρο του θύματος, ενώ είναι δύσκολος ο περιορισμός του εξαιτίας της αδυναμίας ελέγχου του αριθμού και του περιεχόμενου των μηνυμάτων που μπορεί να λάβει ένας χρήστης του διαδικτύου.

Ο **κυβερνοεκφοβισμός** είναι ο εκφοβισμός που ασκείται μέσω των ψηφιακών μέσων. Σύμφωνα με τον ιστοχώρο αυτοί που προκαλούν το cyberbullying χρησιμοποιούν τις νέες τεχνολογίες για να κάνουν κακό σε διάφορους νέους, σε μερικές όμως περιπτώσεις μπορεί να υποδυθούν εσένα και να σου κλέψουν την ταυτότητά σου. Μερικές από τις πιο κοινές μεθόδους είναι οι εξής:

- Εκφοβισμός με γραπτό μήνυμα : να λαμβάνει ένα παιδί προσβλητικό ή απειλητικό μήνυμα
- Παρενόχληση/κλήσεις-φάρσα : να καλεί ένας ξένος ένα παιδί πολλές φορές λέγοντας του διάφορα προσβλητικά πράγματα
- Δημοσίευση και κοινοποίηση εικόνων χωρίς την άδεια του παιδιού : διάφορες φωτογραφίες που απεικονίζουν το παιδί θα μπορούσαν να αναρτηθούν στο διαδίκτυο με το όνομα του παιδιού σε μια ετικέτα
- Happy slapping : ένας άγνωστος θα μπορούσε με το κινητό του να βιντεοσκοπήσει το παιδί καθώς το κακοποιεί σωματικά.
- Εκφοβισμός μέσω υπολογιστή ή μηνυμάτων : ένα οποιοδήποτε παιδί θα μπορούσε να λάβει ενοχλητικά μηνύματα από έναν άγνωστο.
- Εκφοβισμός σε chatroom : ένα άλλος χρήστης θα μπορούσε να πει αγενή πράγματα για εσάς ή το παιδί σας.
- Εκφοβισμός μέσω κοινωνικού δικτύου : ένας άγνωστος θα μπορούσε να ανεβάσει προσβλητικά πράγματα για το παιδί σας στο facebook ή να φτιάξει ένα ψεύτικο προφίλ του παιδιού σας

- Εκφοβισμός κατά την διάρκεια ενός διαδικτυακού παιχνιδιού : αν το παιδί σας παίζει διαδικτυακά παιχνίδια με πολλούς παίκτες ένας από αυτούς ίσως να προσπαθήσει να το αποκλείσει. Μερικές έρευνες τέτοιου είδους μας δείχνουν τον διαδικτυακό εξοστρακισμό που έχει ως συνέπεια την χαμηλή αυτοεκτίμηση του παιδιού.



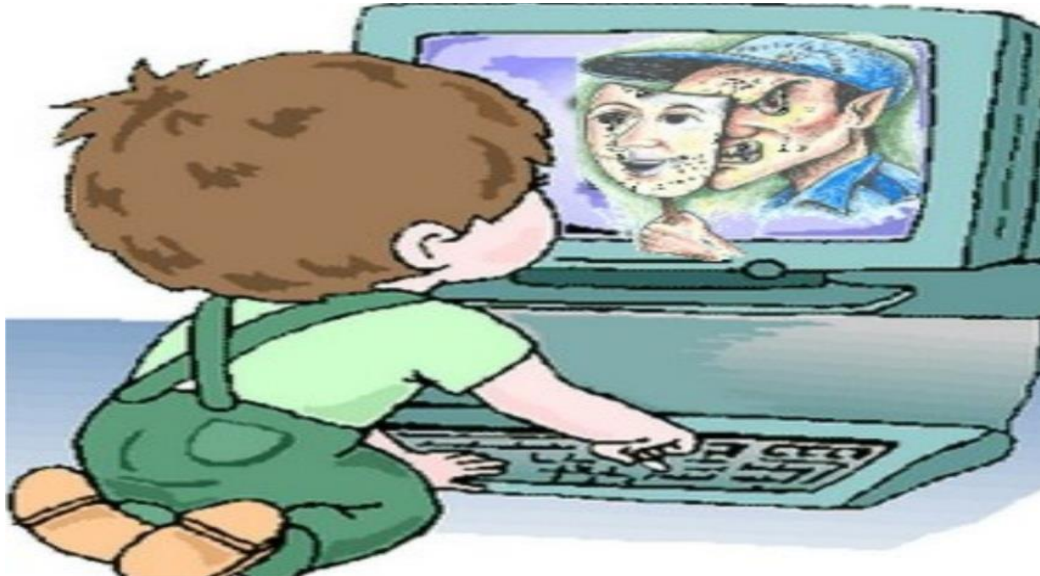
Συμβουλές αντιμετώπισης του Cyberbullying

Στο διαδίκτυο, όπως όλοι γνωρίζουμε, υπάρχουν διάφορες μορφές κινδύνων. Οι παρακάτω συμβουλές μας δείχνουν τους κυριότερους τρόπους αντιμετώπισης τους:

- Αν μετά από μία διαφωνία μερικά παιδιά σου στείλουν απειλητικά μηνύματα στο διαδίκτυο, εσύ αυτό που πρέπει να κάνεις είναι να τους μπλοκάρεις και έπειτα να το πεις στους γονείς σου.
- Σε περίπτωση που κάποιος σε παρενοχλήσει μέσω συνομιλίας διάγραψε τον και ενημέρωσε κάποιον ενήλικα. Αντιθέτως αν μόνο σε προσεγγίσει κάνε ακριβώς το ίδιο. Αν κάποιος δημιουργήσει ψεύτικο προφίλ με το όνομά σου και το χρησιμοποιεί για να στέλνει εκφοβιστικά μηνύματα να τον καταγγείλεις στον διαχειριστή της ιστοσελίδας ώστε να του διαγράψει το προφίλ. Επίσης αν πέσεις θύμα διαδικτυακού εκβιασμού αναφέρσου στην ελληνική ανοιχτή γραμμή www.safeline.gr. Και τέλος αν κάποιος κοινοποιήσει μια φωτογραφία σου χωρίς να το ξέρεις ενημέρωσε κάποιον μεγαλύτερο ώστε να τον αναφέρει στον διαχειριστή του site.



Πηγή:safer internet 4kids.



ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Τι είναι τα προσωπικά δεδομένα;

Τα προσωπικά δεδομένα χωρίζονται σε δύο ειδών κατηγορίες. Αυτές είναι οι εξής:

A) Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων.

B) Ευαίσθητα χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Τα ευαίσθητα δεδομένα προστατεύονται από τον Νόμο με αυστηρότερες ρυθμίσεις από ότι τα απλά προσωπικά δεδομένα.



Τρόποι επεξεργασίας

Συλλογή και επεξεργασία προσωπικών δεδομένων

Σύμφωνα με τους κανόνες της ΕΕ για την προστασία των δεδομένων, τα προσωπικά σας δεδομένα μπορούν να αποτελέσουν αντικείμενο επεξεργασίας μόνο σε ορισμένες περιπτώσεις και υπό ορισμένους όρους, όπως:

- αν έχετε δώσει τη συγκατάθεσή σας (πρέπει να ενημερώνεστε για τη συλλογή των δεδομένων σας)
- αν η επεξεργασία των δεδομένων είναι αναγκαία για μια σύμβαση, αίτηση για θέση εργασίας ή αίτηση χορήγησης δανείου
- αν υπάρχει νομική υποχρέωση για επεξεργασία των δεδομένων σας

- αν η επεξεργασία είναι προς το «ζωτικό συμφέρον» σας, π.χ. αν ένας γιατρός χρειάζεται πρόσβαση στα ιατρικά σας δεδομένα σε περίπτωση που είχατε κάποιο ατύχημα
- αν η επεξεργασία είναι αναγκαία για την άσκηση καθηκόντων που εξυπηρετούν το δημόσιο συμφέρον ή για την άσκηση καθηκόντων από την κυβέρνηση, τις φορολογικές αρχές, την αστυνομία ή άλλους δημόσιους φορείς.

Προσωπικά δεδομένα σχετικά με τη φυλετική ή την εθνική καταγωγή σας, τον σεξουαλικό σας προσανατολισμό, τα πολιτικά σας φρονήματα, τις θρησκευτικές ή φιλοσοφικές σας πεποιθήσεις, τη συμμετοχή σας σε συνδικαλιστικές οργανώσεις ή την υγεία σας δεν μπορούν να αποτελέσουν αντικείμενο επεξεργασίας παρά μόνο σε συγκεκριμένες περιπτώσεις (π.χ. όταν έχετε δώσει τη ρητή συγκατάθεσή σας ή όταν η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή του εθνικού δικαίου). Οι κανόνες αυτοί ισχύουν τόσο για τους δημόσιους όσο και για τους ιδιωτικούς φορείς.



Τρόποι παραβίασης

Άλλοι τρόποι παραβίασης προσωπικών δεδομένων είναι οι εξής:

- Υποκλοπή προσωπικών δεδομένων των χρηστών μέσω «**Phishing**».

Οι απάτες phishing είναι από τις πιο διαδεδομένες και σχετικά εύκολες μορφές απατών στον κυβερνοχώρο. Παρόλο που οι απάτες phishing είναι ευρέως διαδεδομένες παγκοσμίως και επιχειρούνται καθημερινά από εκατοντάδες κακόβουλους χρήστες, είναι εφικτό να καταπολεμηθούν σε μεγάλο βαθμό. Ένας πολύ καλός τρόπος για την προστασία από απάτες phishing είναι η εγκατάσταση κάποιου αξιόπιστου λογισμικού ασφαλείας, αλλά η καλύτερη προστασία είναι η εκπαίδευση των χρηστών στο τι είναι το phishing και πώς να το διακρίνουν.

Τι είναι το phishing;

Το Phishing είναι μια ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο κακόβουλος χρήστης υποδύεται μία αξιόπιστη οντότητα βασιζόμενος στην άγνοια του

χρήστη (θύματος), με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων, όπως κωδικούς λογαριασμών, αριθμούς πιστωτικών καρτών κ.α. Στα ελληνικά το phishing μπορεί να αποδοθεί ως «Ηλεκτρονικό Ψάρεμα».

- Υποκλοπή προσωπικών δεδομένων των χρηστών μέσω **«Pharming»**.

Το pharming είναι μια πρόσφατη μορφή εγκλήματος που έχει και αυτή σαν στόχο την κλοπή προσωπικών δεδομένων των χρηστών. Αλλά έχει διαφορές στο πως επιτυγχάνεται σε σχέση με το phishing. Ένας hacker είναι αυτός που με κάποιους τρόπους καταφέρνει να ανακατευθύνει τους επισκέπτες ενός site σε ένα άλλο «ψεύτικο». Το pharming μπορεί να επιτευχθεί αλλάζοντας το hosts file στον υπολογιστή του θύματος. Το αρχείο αυτό είναι εγκατεστημένο στο σύστημα του Η/Υ και είναι υπεύθυνο για να συγκεντρώνει τις IP διευθύνσεις του χρήστη. Ένας ακόμη τρόπος επίθεσης είναι η εκμετάλλευση των τρωτών σημείων του λογισμικού ενός DNS server. Ένας τέτοιος server είναι υπεύθυνος στο να «μεταφράζει» τα ονόματα των διευθύνσεων του Internet σε IP addresses. Υπάρχουν όμως σημεία στο λογισμικό αυτών των servers που μπορούν να χαρακτηριστούν τρύπες ασφαλείας που συνήθως είναι εκμεταλλεύσιμες από τους hackers.

- Υποκλοπή προσωπικών δεδομένων των χρηστών μέσω ανάρτησης φωτογραφιών χωρίς την άδεια τους.
- Αποδοχή αιτημάτων φιλίας αγνώστων χρηστών με ψευδή στοιχεία ταυτότητας.
- Η αφετηρία συζήτησης με άτομα αγνώστων στοιχείων και προέλευσης.



Τρόποι προστασίας

- Η σωστή δημιουργία κωδικών πρόσβασης με ποικίλων ειδών χαρακτήρες (π.χ. f00@e1#) και η αποφυγή χρήσης ονομάτων, ημερομηνιών γεννήσεως και διευθύνσεων.
- Δεν πρέπει να μοιραζόμαστε τους κωδικούς πρόσβασης με φίλους, γνωστούς αλλά και με άλλους χρήστες.
- Για την παραμονή ασφαλών κωδικών δεν πρέπει να γίνεται η αποθήκευσή τους στους browsers.
- Όταν κάποιος εισέρθει στην περιοχή μας, πρέπει να αλλάξουμε κωδικό πρόσβασης, να επικοινωνήσουμε με τη Safe line, και να αναφέρουμε το πρόβλημα στο διαχειριστή του site.

Κίνδυνοι & ασφαλής πλοήγηση στο διαδίκτυο

- Αν λάβουμε κάποιο e-mail από ένα site για να δώσουμε τον κωδικό πρόσβασης μας για να γίνουν κάποιες τροποποιήσεις στον λογαριασμό σου, πρέπει να αγνοήσουμε το μήνυμα και το διαγράφουμε.



ΠΗΓΕΣ

[http://www.safeline.gr/poioi-eimaste/skopos-mas.](http://www.safeline.gr/poioi-eimaste/skopos-mas)

[http://www.iefimerida.gr/cookies.](http://www.iefimerida.gr/cookies)

[https://saferinternet4kids.gr/quiz-saferinternet4kids/.](https://saferinternet4kids.gr/quiz-saferinternet4kids/)

<https://www.dpa.gr>

<https://www.safeline.gr>