SaferInternet4Kids.gr
ΓΙΑ ΕΝΑ ΑΣΦΑΛΕΣΤΕΡΟ ΔΙΑΔΙΚΤΥΟ

ΟΚΤΩΒΡΙΟΣ ΤΕΥΧΟΣ 1ο 2022

DIGIZENS

Ένα περιοδικό από το Πάνελ Νέων του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου

Το διαδίκτυο είναι ένα υπέροχο μέρος που όμως περιέχει πολλούς κινδύνους. Εμείς είμαστε εδώ για να σας βοηθήσουμε να πλοηγήστε με ασφάλεια!

Για πληροφορίες και εκπαιδευτικό υλικό επισκεφθείτε τη σελίδα **Saferinternet4kids.gr**.

Για υποστήριξη από ειδικούς αν κάτι σας ανησυχήσει στο διαδίκτυο καλέστε την **Help-line** στο 2106007686.

Και αν συναντήσετε παράνομο περιεχόμενο κάντε καταγγελία στη **Safeline.gr**.

SaferInternet4Kids.gr

help line saferinternet

safeLine.gr

EDITORIAL

Η ιδέα δημιουργίας ενός περιοδικού, στο οποίο θα καταγράφονται οι απόψεις των νέων για τον κόσμο του διαδικτύου μας φάνηκε ιδιαίτερα ελκυστική.

Τα μέλη του πάνελ νέων του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου συνεργάστηκαν με μεράκι και μέσα από τα δικά τους μάτια ανέλυσαν θέματα που τους απασχολούν όσον αφορά στην ενασχόλησή τους με το διαδίκτυο.

Δημιουργήσαμε σαν ομάδα ένα περιοδικό από νέους για νέους και ελπίζουμε να το απολαύσετε.

DIGIZENS λοιπόν! Σε καλωσορίζουμε και σε παραδίδουμε ελεύθερο στο αναγνωστικό κοινό, να μοιράσεις απλόχερα τη γνώση και τις βάσεις για ένα καλύτερο και ασφαλέστερο διαδίκτυο!

3 τρόποι για να εντοπίσετε ένα **γατόψαρο**

της Φωτεινής Αλεξίου

Στην γλώσσα του internet, γατόψαρο ή αλλιώς catfish ονομάζεται η διαδικασία στην οποία ένας άνθρωπος δημιουργεί ένα προφίλ στα social media, χρησιμοποιώντας ψεύτικα στοιχεία (άλλο όνομα, φωτογραφίες που δεν του ανήκουν κλπ). Οι περισσότεροι άνθρωποι, που πέφτουν θύματα catfish, χρειάζονται αρκετό καιρό ή ακόμη και χρόνια για να αντιληφθούν τα ψέμματα. Γι' αυτό και υπάρχουν κάποιοι βασικοί τρόποι να καταλάβετε πότε ένας άνθρωπος, που γνωρίζετε από τα social media, σας λέει ψέμματα.

1. Το προφίλ του φαίνεται ψεύτικο.

Όταν γνωρίζετε έναν άνθρωπο μόνο από τα social media, καλό θα ήταν να προσέξετε πολύ κάποια συγκεκριμένα πράγματα στο προφίλ του. Ένας πολύ καλός τρόπος είναι να κοιτάξετε την λίστα των φίλων του. Αν έχει μια αρκετά αληθοφανή λίστα φίλων ή ακόμη καλύτερα αν έχετε κοινούς φίλους, είναι πολύ πιθανό ότι πρόκειται για ένα αληθινό προφίλ.

2. Δεν σας μιλάει στο τηλέφωνο.

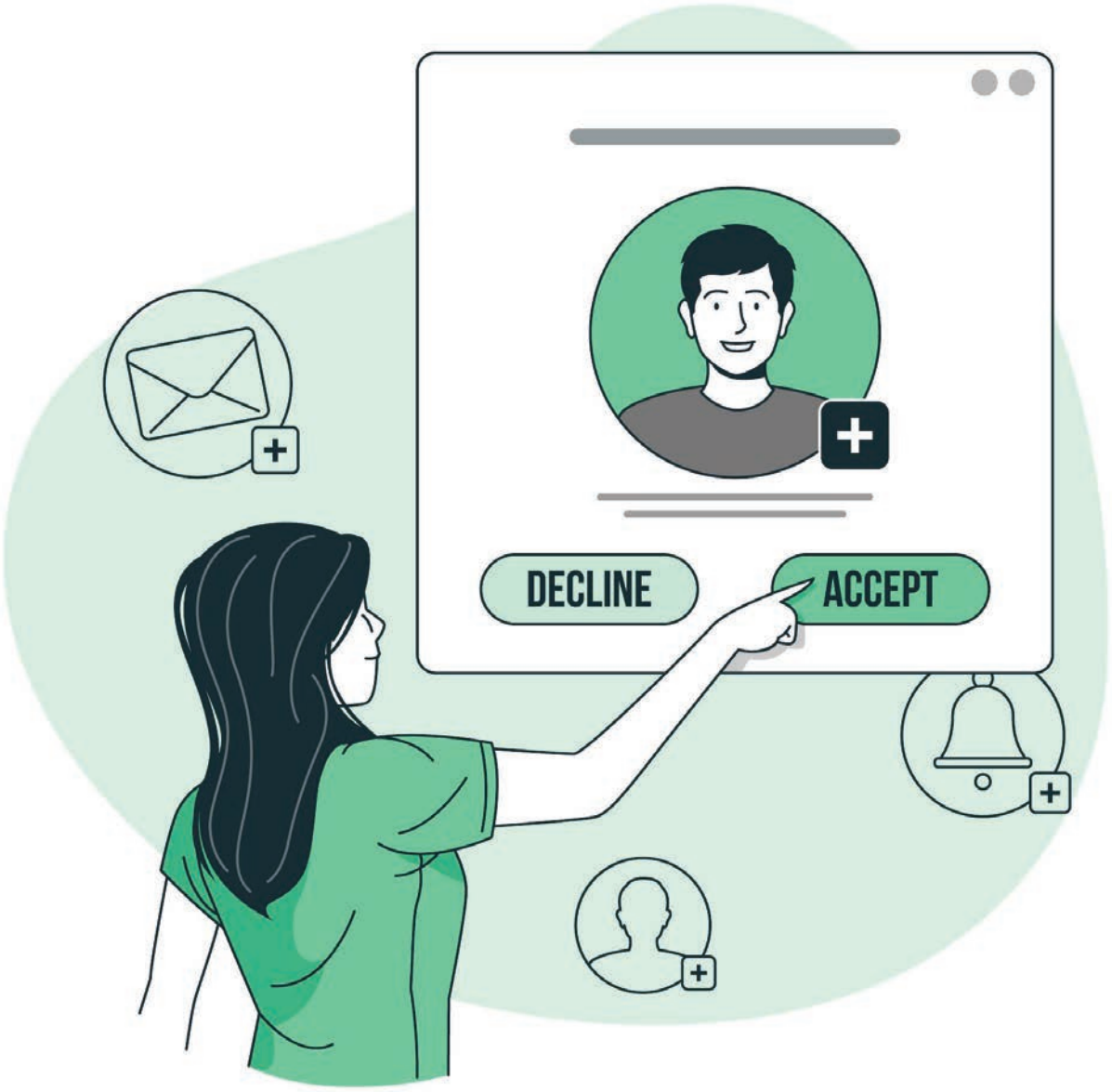
Ένας τέτοιος άνθρωπος θα βρίσκει πάντα μια δικαιολογία για να αποφύγει αυτόν τον τρόπο επικοινωνίας. Θα αποφεύγει πάντα την απάντηση σε αυτήν την ερώτηση. Το καλύτερο που μπορείτε να

κάνετε είναι να επιμένετε να μιλήσετε μαζί του, είτε μέσω τηλεφώνου ή ακόμη καλύτερα και με βιντεοκλήση. Αν αυτός ο άνθρωπος δεν έχει κάτι να κρύψει, δεν θα έχει πρόβλημα να μιλήσει μαζί σας.

3. Διαθέτει ψεύτικες φωτογραφίες.

Φυσικά, ένας άνθρωπος που κάνει catfish σε άτομα δεν πρόκειται να χρησιμοποιεί δικές του φωτογραφίες στο προφίλ του. Μια καλή αναζήτηση, των φωτογραφιών που σας έχει δώσει, στο ίντερνετ θα δώσει κάποιες απαντήσεις στις υποψίες σας. Επιπλέον μπορείτε να του ζητάτε να σας στέλνει κάποιες ιδιαίτερες φωτογραφίες (για παράδειγμα μπορείτε να του ζητήσετε μια φωτογραφία, στην οποία κρατάει ένα χαρτί που γράφει το όνομά σας ή γενικά μια φράση που σας αρέσει).

Ελπίζω αυτοί οι τρόποι να σας βοηθήσουν να αποφύγετε τέτοιου είδους, συναισθηματικές κυρίως απάτες ή αν βρίσκεστε σε μια τέτοια κατάσταση να καταλάβατε με τι είδους άτομα μιλάτε.



Η έμφυλη βία στο διαδίκτυο

της Μαρίνας Κοπιδάκη

Η έμφυλη βία είναι, δυστυχώς, ένα πανανθρώπινο και καθημερινό φαινόμενο το οποίο χαρακτηρίζεται από τη διενέργεια οποιαδήποτε επιβλαβούς πράξης εναντίον ενός ατόμου με γνώμονα το φύλο του. Τέτοιες πράξεις είναι αναγκαίο να καταγγέλλονται και να διώκονται καθώς αποτελούν ζήτημα παραβίασης της ιδιωτικής ζωής και σοβαρής απειλής στην ψυχοσωματική υγεία των ανθρώπων. Με το ίντερνετ όμως να κάνει ολοένα εντονότερη την παρουσία του στην ζωή μας η ανάπτυξη ενός νέου είδους έμφυλης βίας έγινε πλέον αναπόφευκτη. Αυτή είναι η διαδικτυακή έμφυλη βία.

Η έμφυλη βία μέσω του ίντερνετ εκδηλώνεται με πράξεις κακοποιητικές οι οποίες πραγματοποιούνται με την χρήση των νέων μέσων της τεχνολογίας. Τα πιο συνήθη θύματα, σύμφωνα πάντα με έρευνες, αποτελούν οι γυναίκες, τα κορίτσια μικρής ηλικίας ή τα μέλη της κοινότητας LGBTQ+. Κακόβουλες ενέργειες σαν κι αυτές μπορεί να είναι η σεξουαλική εκμετάλλευση, η ρητορική μίσους ή και η παρακολούθηση μέσω εφαρμογών GPS. Φυσικά η επίδραση τους στην ψυχοσύνθεση των θυμάτων μπορεί να αποδειχθεί καταστροφική πράγμα που καθιστά την αντιμετώπισή τους όχι απλώς κρίσιμη άλλα αναγκαία.

Οι κύριοι στόχοι για την καταστολή του φαινομένου δεν αφορούν ωστόσο μονάχα την αντιμετώπιση της ήδη υπάρχουσας κατάστασης αλλά περιλαμβάνουν την πρόληψη και άμβλυνση παρόμοιων συμπεριφορών στο μέλλον. Έτσι η αποστολή αυτή καθίσταται ακόμα πιο απαιτητική με κύριους στόχους την διασφάλιση ότι όλα τα θύματα της έμφυλης βίας έχουν επαρκή και έγκαιρη πρόσβαση σε ποιοτικές υπηρεσίες που θα ανταποκριθούν στο κάλεσμά τους καθώς και την μείωση του κινδύνου εμφάνισης έμφυλης βίας στο διαδίκτυο. Για να επιτευχθεί φυσικά αυτό απαιτείται όχι μόνο η δραστηριοποίηση των ίδιων των θυμάτων αλλά και η ορθή συμπεριφορά κάθε χρήστη του διαδικτύου που γίνεται «μάρτυρας» σε μια τέτοια κατάσταση.

Η αντιμετώπιση του διαδικτυακού μίσους από τον ίδιο τον δέκτη είναι σημαντικό να γίνεται με την καταγγελία του φαινομένου και όχι κρύβοντάς το εξαιτίας του αισθήματος του φόβου. Αρχικά σημαντικό είναι το θύμα να απευθυνθεί σε κάποιον που εμπιστεύεται, πράγμα που θα έχει ως αποτέλεσμα την ανακούφιση από το άγχος και την συναισθηματική σύγχυση που συνήθως προκαλεί η εμπειρία της διαδικτυακής παρενόχλησης. Έπειτα, σημαντικό είναι σε περίπτωση που οποιοσδήποτε αισθανθεί ανασφαλής κατά την πλοήγηση του στο διαδίκτυο εξαιτίας της δραστηριότητας κάποιου άλλου χρήστη, να κάνει άμεσα αναφορά σε εκείνον έχοντας διατηρήσει φυσικά κάποιο μόνιμο αρχείο ως αποδεικτικό στοιχείο του πιθανώς κακοποιητικού φαινομένου ώστε αν η κατάσταση επιδεινωθεί να υπάρξει η δυνατότητα να στροφής στις αρχές και δίωξης του κακόβουλου χρήστη.

Επιπλέον, εξίσου σημαντικός είναι ο ρόλος των υπόλοιπων χρηστών που γίνονται «θεατές» σε τέτοιου είδους κακοποιητικά φαινόμενα. Σε περίπτωση που πέσει στην αντίληψη κάποιου χρήστη μια πιθανή βίαια συμπεριφορά είναι απαραίτητη η παρέμβαση με στόχο την καταστολή του φαινομένου. Υπάρχει η δυνατότητα ένας «θεατής» να έρθει σε επικοινωνία με το θύμα μέσω προσωπικού μηνύματος ώστε να μάθει αν είναι καλά και αν χρειάζεται βοήθεια ή ακόμα να καταγγείλει ο ίδιος την παρενόχληση με σκοπό να αποκλείσει τους κακόβουλους χρήστες. Τέλος, είναι κρίσιμο η παρουσία της έμφυλης βίας στον κυβερνοχώρο να μην αποκρύπτεται και να γίνεται συζήτηση για αυτό καθώς και να μοιράζονται πληροφορίες με στόχο την ενημέρωση και αποτελεσματικότερη αποφυγή της.

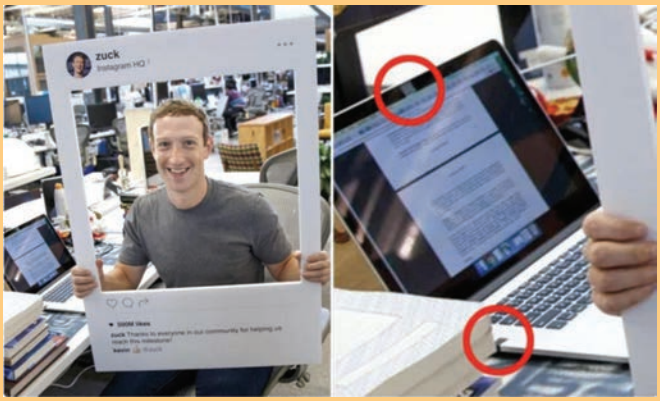
Για την επίτευξη λοιπόν όλων των παραπάνω στόχων εμείς, στο saferinternet4kids, δουλεύουμε καθημερινά ώστε να εξαλείψουμε αυτά τα φαινόμενα λειτουργώντας όχι μόνο ως φορέας υποστήριξης και καταγγελίας αλλά και ως φορέας ενημέρωσης και εκπαίδευσης όσο αναφορά κάθε είδους νοσηρό φαινόμενο και επιβλαβές περιεχόμενο σε αυτόν τον νέο και δυνητικά υπέροχο χώρο του διαδικτύου μας!

Να κεράσουμε ένα **Cookie;**

της Ηλέκτρας Χατζηδημητρίου

Στα δεξιά, βλέπετε μια φωτογραφία του Μάρκ Ζούκερμπεργκ από το 2016, ιδιοκτήτη και ιδρυτή πολλών κοινωνικών δικτύων όπως το Facebook, Instagram και Whattsapp να γιορτάζει 500 δισεκατομμύρια χρήστες του Instagram. Αυτό που ο κόσμος αμέσως παρατήρησε είναι ότι ο CEO της Meta και συνιδρυτής της Facebook έχει καλύψει με προστατευτική ταινία την κάμερα και το μικρόφωνό του. Μήπως ξέρει κάτι που δεν ξέρουμε; Η φωτογραφία έκανε τον κύκλο του Διαδικτύου, δίνοντας αφετηρία σε μεγάλες συζητήσεις τόσο για την ασφάλειά μας κατά την χρήση του Διαδικτύου όσο και για το ποιός μπορεί να προσπαθήσει να υποκλέψει συζητήσεις ή βίντεό μας όσο εμείς σερφάρουμε στο Ίντερνετ. Και οι περισσότεροι από εμάς ακολουθούμε μέχρι και σήμερα το παράδειγμα του Ζούκερμπεργκ έχοντας συνεχώς καλυμμένη την κάμερα του λάπτοπ. Από ποιόν όμως προστατευόμαστε; Τι είναι αυτό που θέτουμε σε κίνδυνο όταν κρατάμε την κάμερα και το μικρόφωνο ακάλυπτα; Γιατί να προσπαθήσει κάποιος να μας βιντεοσκοπήσει ή να μας μαγνητοφωνήσει χωρίς την θέλησή μας;

Ένας από τους μεγαλύτερους κινδύνους



σήμερα στο διαδίκτυο και ίσως η σημαντικότερη πηγή πλούτου για τις μεγάλες εταιρίες όπως τη Meta, την Amazon και την Google είναι η κλοπή προσωπικών δεδομένων. Δηλαδή, η συλλογή ιδιωτικών πληροφοριών (όπως τα γενέθλιά μας, την χώρα στην οποία μένουμε, το αγαπημένο μας τραγούδι ή το αγαπημένο μας χόμπι) που έπειτα αναπαράγονται και διακινούνται, χρησιμοποιούνται σε έρευνες και αποθηκεύονται ώστε να αποκτήσουν οι εταιρείες τα απαραίτητα εφόδια για να μας χειραγωγήσουν και για να μας πουλήσουν τα προϊόντα τους. Στη συλλογή αυτή μπορεί να συναινέσουμε (όταν, για παράδειγμα, συμπληρώνουμε τα στοιχεία μας για να δημιουργήσουμε έναν λογαριασμό στο Facebook ή όταν αποδεχόμαστε τα cookies σε έναν ιστότοπο) ή τα δεδομένα μας συλλέγονται

χωρίς εμείς να το καταλαβαίνουμε ή να το θελουμε (όταν καταγράφεται κάτι από το μικρόφωνό μας αν και την έχουμε κλειστή). Αυτή η δραστηριότητα αποτελεί μια χυδαία, ατέρμονη παραβίαση της ιδιωτικότητας του ανθρώπου που προσβάλει τόσο την ιδέα της ιδιωτικότητας στο σύγχρονο κόσμο, όσο και την κυριότητα κάθε ανθρώπου σε πληροφορίες που αφορούν τον ίδιο και την ζωή του. Ένα πολύ απλό παράδειγμα είναι η υποκλοπή του ιστορικού αναζήτησής μας στο Google. Αυτό είναι αδιαμφισβήτητα μία από τις σημαντικότερες ιδιωτικές μας πληροφορίες, αφού μαρτυρά τα ενδιαφέροντά μας, τις ευαισθησίες μας και την προσωπικότητά μας. Με αυτές τις πληροφορίες μια εταιρία κατέχει κάθε στοιχείο που χρειάζεται για να μας αποπλανήσει και να μας κάνει πελάτες της. Αν σήμερα αναζητήσει κανείς στο Google ζευγάρια αθλητικά παπούτσια, και μάλιστα κοιτάξει εκατό φωτογραφίες αθλητικών παπουτσιών χρώματος μωβ, των οποίων η τιμή είναι μεταξύ 50 και 100 ευρώ, η Google θα συλλέξει αυτά τα στατιστικά και θα τα πουλήσει σε εταιρίες όπως την Nike και την Intersport. Την επόμενη φορά που ο ίδιος χρήστης θα συνδεθεί στο διαδίκτυο, οι ιστοσελίδες θα γεμίσουν με διαφημίσεις Nike και Intersport μωβ αθλητικών παπουτσιών που δεν κοστίζουν πάνω από 100 ευρώ. Η παραβίαση, όμως, της ιδιωτικότητας έχει πια λάβει ακόμη μεγαλύτερες διαστάσεις πέρα από τις στοχευμένες διαφημίσεις (targeted/relevant ads). Τα προσωπικά δεδομένα πλέον μπορούν κυριολεκτικά να ανεβάζουν κυβερνήσεις. Στην τελευταία φάση του προεκλογικού αγώνα για τις εκλογές του 2016 στην Αμερική, το Facebook (σήμερα ονόματι Meta) πούλησε στην Cambridge Analytica τα προσωπικά δεδομένα (σχετικά με τις πολιτικές πεποιθήσεις) όσων αμερικανών ψηφοφόρων είχαν λογαριασμό Facebook (περίπου 10 εκατομμυρίων). Στα δεδομένα αυτά η εταιρία απέκτησε πρόσβαση παρακολουθώντας τις πολιτικές προτιμήσεις κάθε Αμερικανού πολίτη καταγράφοντας τα like και τα post κάθε χρήστη, τους ακολούθους και τα σχόλια που κάθε χρήστης έκανε σε πολιτικοποιημένα άρθρα και συζητήσεις. Παράλληλα, σε έντονα δραστήριους σε πολιτικές συζητήσεις χρήστες, η πλατφόρμα έστελνε quiz προσωπικότητας,

κατασκευασμένα από τον Αμερικανό ερευνητή του Cambridge Aleksandr Kogan, που αν και έμοιαζαν με ασήμαντα παιχνίδια, στην πραγματικότητα κατέγραφαν πολύτιμες πληροφορίες σχετικά με τα ενδιαφέροντα και τις προτιμήσεις κάθε χρήστη. Τα δεδομένα αυτά, συλλεγμένα και παραχωρημένα χωρίς να το ξέρουν οι χρήστες, χρησιμοποιήθηκαν από την Cambridge Analytica για την δημιουργία στοχευμένων πολιτικών διαφημίσεων που υποστηρίζουν τον Donald Trump (που, με λίγα λόγια, έλεγαν στους ψηφοφόρους αυτό που ήθελαν να ακούσουν). Σύμφωνα με εκτενείς στατιστικές έρευνες, οι διαφημίσεις αυτές έπαιξαν καθοριστικό ρόλο στην εκλογή του Τραμπ. Πέρα, λοιπόν από την ιδιωτικότητα, η κλοπή των δεδομένων αυτών παραβιάζει πλέον πολύτιμους, πανανθρώπινους θεσμούς όπως την δημοκρατία, την ελευθερία του λόγου και της έκφρασης, το δικαίωμα εκλέγειν-εκλέγεσθαι.

Έχοντας, λοιπόν, στο μυαλό, την τεράστια σημασία της υποκλοπής προσωπικών δεδομένων, είναι σημαντικό να αρχίσουμε να παλεύουμε ενάντια στην παραβίαση των δικαιωμάτων μας για το χρηματικό όφελος εταιριών. Πολλοί επιστήμονες προτείνουν ότι είναι ιδιαίτερα σημαντικό να παλέψουμε ώστε να αποζημιωθούμε χρηματικά για τις παραβιάσεις αυτές, με χρηματικά ποσά ανάλογα του κέρδους κάθε εταιρείας που χρησιμοποιεί τα δεδομένα μας. Άλλοι θεωρούν ότι υπάρχει κάποιο όφελος στο να χρησιμοποιούνται τα δεδομένα μας αρκεί αυτό να γίνεται ελεγμένα με την συναίνεση του χρήστη. Οποια, όμως, και να είναι η στάση μας σε αυτό το debate, δεδομένης της έκτασης αυτού του προβλήματος πρέπει αδιαμφισβήτητα να κινητοποιηθούμε. Πρώτο βήμα είναι η ενημέρωση. Σίγουρα θα έχετε ακούσει αμέτρητες θεωρίες συνομωσίας (όπως τα τσιπάκια του Bill Gates στο εμβόλιο κατά του Covid) που προσπαθούν (αλλά αποτυχαίνουν) να ερμηνεύσουν ή να καταλάβουν πως οι εταιρείες κλέβουν τα δεδομένα μας. Η άγνοιά μας σε αυτό το κομμάτι και γενικότερα στην λειτουργία των αλγορίθμων των κοινωνικών δικτύων και του Ίντερνετ είναι το μεγάλο προβάδισμα όσων προσπαθούν να μας παραπλανήσουν στο να μοιραστούμε προσωπικές πληροφορίες.

Ορίστε, λοιπόν, 2 μύθοι (και οι αλήθειες) γύρω από την κλοπή προσωπικών δεδομένων στο διαδίκτυο:

Μύθος: Το μικρόφωνο και η κάμερα καταγράφουν τι λέω και τι κάνω.

Αλήθεια: Αυτό θα ήταν πρακτικά ανέφικτο, αφού το να είμαστε συνέχεια σε απευθείας σύνδεση με τον Ζούκερμπεργκ απαιτεί πολύ αποθηκευτικό χώρο, εξαιρετικά γρήγορες ταχύτητες Ίντερνετ (σίγουρα θα έχετε παρατηρήσει ότι αν προσπαθήσετε να σερφάρετε στο διαδίκτυο ενώ μιλάτε σε κάποιον στο τηλέφωνο το κινητό κολλάει/ αργεί να φορτώσει), και δεν χρησιμεύει σε τίποτα αφού πολύ μικρό ποσοστό αυτών που κάνουμε και λέμε είναι χρήσιμο. Στην πραγματικότητα, καταγράφονται λέξεις ή φράσεις σε πολύ μικρές γραμμές κώδικα που μεταφράζονται από υπολογιστές σε στατιστικά, χωρίς να παρεμβαίνει απαραίτητα κάποιος άνθρωπος. Οι φράσεις αυτές είναι πολύ εξειδικευμένες και πρέπει να τις πούμε πολλές φορές. Για παράδειγμα, αν σε μια συζήτησή μας αναφερθεί η λέξη «ποδόσφαιρο», ο υπολογιστής δεν καταγράφει γιατί οποιοσδήποτε θα μπορούσε να κάνει συζήτηση για το συγκεκριμένο άθλημα. Αν, βέβαια, πούμε το όνομα κάποιου παίκτη ή κάποιου προπονητή, και μάλιστα 2 ή περισσότερες φορές, ο υπολογιστής πιάνει τις λέξεις και τις καταγράφει, γιατί θεωρεί ότι είμαστε φαν αφού έχουμε εξειδικευμένες γνώσεις.

Μύθος: με καλούς κωδικούς και πολλή προσοχή μπορώ να είμαι απολύτως προστατευμένος/η από κλοπή προσωπικών δεδομένων.

Αλήθεια: Ακόμη και αν είναι όλα προστατευμένα, στην πραγματικότητα δεν υπάρχει κανένας γνωστός τρόπος να αφαιρέσουμε τελείως το ηλεκτρονικό μας αποτύπωμα, μόνο να το ελαχιστοποιήσουμε. Μόνο και μόνο το να κάνουμε λάικ σε ένα ποστ για την καινούργια ταινία της Μάρβελ είναι αρκετά δεδομένα ώστε το Facebook και η Disney να συνεργαστούν και να μας στείλουν διαφημίσεις σχετικές με αυτό, να βελτιώσουν τα προϊόντα τους και να συνεχίσουν να ανεβάζουν σχετικές αναρτήσεις. Πρέπει, παρά την προσοχή στην δραστηριότητά μας, να είμαστε πάντα σε εγρήγορση και να γνωρίζουμε ότι πολλά δεδομένα μας συλλέγονται παρά την θέλησή μας.

Επόμενο βήμα είναι μερικές εύκολες ενέργειες που μπορεί να μας προστατεύσουν αρκετά. Ορίστε, τέλος, μερικά βήματα για καλύτερη προστασία των προσωπικών δεδομένων:

- Μην φοβηθείς να πατήσεις όχι σε pop-ups για cookies. Στην ουσία χρειάζεται απλώς λίγα παραπάνω δευτερόλεπτα για να αρνηθείς.
- Πήγαινε στις ρυθμίσεις της συσκευής σου και ρύθμισε ποιές εφαρμογές και πως θα συλλέγουν τα προσωπικά σου δεδομένα. Τα περισσότερα τηλέφωνα έχουν τρόπο να σε προστατεύσουν από εφαρμογές.
- Κάνε έλεγχο των διαδικτυακών αναζητήσεων. Μην βάζεις διευθύνσεις ή γενέθλια σε ιστοσελίδες που δεν γνωρίζεις, πρόσεχε πότε και πώς υπογραμμίζεις τις προτιμήσεις σου.
- Φτιάξε δύσκολους κωδικούς, διαφορετικούς, και κράτα τους σε χειρόγραφη σημείωση, μην αποθηκεύεις. Σε πολλές ιστοσελίδες όπως το Instagram ή το BeReal, μοιραζόμαστε με φίλους πληροφορίες όπως την τοποθεσία μας, τις προτιμήσεις μας. Προστάτεψέ τα με καλούς κωδικούς.

Πηγές:
https://www.dailymail.co.uk/news/article-3653442/Paranoid-little-Mark-Zuckerberg-covers-Macbook-s-camera-audio-jack-pieces-tape.html
https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/
https://www.politico.eu/article/cambridge-analytica-facebook-data-brittney-kaiser-privacy/
https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy
https://www.forbes.com/sites/ashleystahl/2021/06/04/what-you-need-to-know-to-protect-your-data-online/
https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

Είμαι **παιδί**... Ποιος θα μου μάθει τι πρέπει να **προσέχω** στο **διαδίκτυο**;

της Μαριάννας Κυριακάκη

Ακούμε γύρω μας ότι σήμερα τα παιδιά από πολύ μικρή ηλικία, πριν ακόμα πάνε στο νηπιαγωγείο, χρησιμοποιούν το διαδίκτυο. Και αναρωτιέμαι ποιος θα μάθει σε αυτά τα παιδιά πως να πλοηγούνται με ασφάλεια; Προσπαθώ να θυμηθώ ποιος μου έμαθε εμένα. Λίγο η μαμά και ο μπαμπάς, λίγο στο δημοτικό, λίγο η μεγάλη μου αδερφή, λίγο η φίλοι μου... Όλοι από λίγο τελικά... Και έμαθα; Τι έμαθα;

Φέτος πάω Τρίτη Γυμνασίου. Στο σχολείο προσθέσανε επιτέλους στην διδακτική μας ύλη το μάθημα του ασφαλούς διαδικτύου. Ένα βήμα που προσωπικά θεωρώ είναι πολύ μεγάλο και θα βοηθούσε πολύ προς την κατεύθυνση επιμόρφωσης των παιδιών αν οι συνθήκες ήταν καταλληλότερες. Δυστυχώς οι διδακτικές ώρες του μαθήματος είναι περιορισμένες και επουδενί αρκετές με αποτέλεσμα οι μαθητές να μην μπορούν να κατανοήσουν και να αφομοιώσουν το μάθημα όπως πρέπει. Αν και η διδακτέα ύλη είναι αρκετή και αξιόλογη ο εκπαιδευτικός δεν έχει τον απαραίτητο χρόνο, με συνέπεια εν τάχει να προσπαθεί να μάθει στους μαθητές του τις βασικές αρχές ψηφιακής ασφάλειας. Όποτε όσο σημαντικό και αν είναι το γεγονός ότι τα παιδιά έχουν την ευκαιρία να διδαχτούν το πως να προστατεύσουν τον εαυτό τους online, η έλλειψη διδακτικού χρόνου στην ουσία ακυρώνει κάθε προσπάθεια. Η αύξηση των διδακτικών ωρών των μαθήματος είναι αναγκαία αν θέλουμε να έχουμε επιμορφωμένους και ασφαλείς νέους στο διαδίκτυο. Ας παραδεχτούμε το γεγονός ότι οι νέοι σήμερα περνάνε το μέγιστο του χρόνου τους στις οθόνες. Αν λοιπόν αυτοί οι νέοι δεν έχουν την απαραίτητη εκπαίδευση και τα εφόδια θα είναι εκτεθειμένοι σε μεγάλο κίνδυνο.

Η Αθηνά, ο Ερμής και η Άρτεμη μαθαίνουν στη γιαγιά της Αθηνάς πώς να πλοηγείται με ασφάλεια στο διαδίκτυο. Της μιλούν για την υπερβολική ενασχόληση, τους κινδύνους που υπάρχουν στα κοινωνικά δίκτυα, στα διαδικτυακά παιχνίδια καθώς και πως να αποφεύγει τις διαδικτυακές απάτες...

Της δίνουν και μια κορυφαία συμβουλή:

Αν κάτι μας αναστατώσει στο διαδίκτυο το λέμε αμέσως σε έναν ενήλικα που εμπιστευόμαστε.

Ένα σπουδαίο εργαλείο

του Φίλιππου Γιαμαλή

Το διαδίκτυο έχει μπει πλέον στην καθημερινότητα των περισσότερων ανθρώπων, λόγω των πλεονεκτημάτων του που διευκολύνουν τη ζωή του κάθε χρήστη. Έτσι λοιπόν, θετικά του διαδικτύου μπορούμε να χαρακτηρίσουμε την άμεση πρόσβαση σε πληροφορίες, με αποτέλεσμα την απόκτηση γνώσεων τόσο από παιδιά όσο και από ενήλικες, την παροχή ψυχαγωγίας μέσω παιχνιδιών, βίντεο και μουσικής. Επίσης, το διαδίκτυο καταφέρνει να καταργήσει τα σύνορα και τις αποστάσεις, παρέχοντας μας τη δυνατότητα να στείλουμε μηνύματα, φωτογραφίες, και βίντεο σε χρήστες από όλο τον κόσμο, καθώς και να ενημερωνόμαστε άμεσα για διεθνή γεγονότα.

Ωστόσο, η παρατεταμένη έκθεση μας στο διαδίκτυο προκαλεί πολλά προβλήματα, τα οποία αποτελούν τα αρνητικά του διαδικτύου και του υπολογιστή. Καταρχάς, υπάρχει κίνδυνος για τον υπολογιστή από ιούς ή άλλα κακόβουλα λογισμικά, αν δεν ληφθούν τα κατάλληλα μέτρα προστασίας. Το ηλεκτρονικό έγκλημα, καθώς και η υποκλοπή πνευματικών δικαιωμάτων και προσωπικών στοιχείων αποτελούν σημαντικούς παράγοντες λήψης πρόσθετων μέτρων για την προστασία μας. Παράλληλα, η προτίμηση πολλών ανθρώπων να μιλήσουν μέσω διαδικτύου παρά να βρεθούν από κοντά, αποδυναμώνει την αυθεντική επικοινωνία και οδηγεί τους ανθρώπους να απομακρύνονται μεταξύ τους. Τέλος, ο σημαντικότερος κίνδυνος για τους νέους είναι ο εθισμός στο διαδίκτυο, που συμβάλλει στην αποξένωση από τα αγαπημένα μας πρόσωπα και το περιβάλλον στο οποίο ζούμε.

Όλα αυτά μας δείχνουν ότι το διαδίκτυο είναι ένα πολύ σπουδαίο εργαλείο που έχουμε στα χέρια μας, το οποίο όμως μπορεί να μετατραπεί και σε επικίνδυνο όπλο.

Διαδικτυακή **εκμετάλλευση**

Ο εκφοβισμός έχει βρει στο χώρο του διαδικτύου ένα νέο ευρύ πεδίο δράσης. Άλλοτε ανώνυμα, άλλοτε με επώνυμες επιθέσεις πολλοί άνθρωποι γίνονται αποδέκτες κάθε λεκτικής ή μη λεκτικής συμπεριφοράς η οποία παίρνει τη μορφή πρότασης ή πρόσκλησης για τέλεση επικοινωνίας με σεξουαλικό περιεχόμενο.

Πρόκειται βέβαια, για μία εγκληματική πρακτική που οφείλει να κρατά σε εγρήγορση τους γονείς, προκειμένου να προφυλάξουν τα παιδιά τους από την επικοινωνία με τέτοια άτομα.

Οι διαδικτυακοί δράστες προσεγγίζουν τα θύματά τους, συνήθως, μέσω των κοινωνικών μέσων δικτύωσης παριστάνοντας συνομηλίκους του ίδιου ή του αντίθετου φύλου ή παίρνοντας την ταυτότητα ενός ελκυστικού άνδρα ή μιας ελκυστικής γυναίκας. Κατά τη διάρκεια της επικοινωνίας τους όταν καταφέρνουν να αποκτήσουν το «πολυπόθητο» υλικό, οι δράστες υπό την απειλή να δημοσιεύσουν το υλικό ή να το αποστείλουν στο οικείο περιβάλλον των θυμάτων, αποκαλύπτουν τους πραγματικούς τους σκοπούς, που είναι κυρίως σεξουαλικού ή οικονομικού ενδιαφέροντος.

Στο διαδίκτυο είναι πολύ εύκολο κάποιος να πει ψέματα για το ποιος πραγματικά είναι. Πρέπει να είμαστε πολύ προσεκτικοί και να τηρούμε κάποιους κανόνες για να είμαστε ασφαλείς στο διαδίκτυο. Προσαρμόζω τις ρυθμίσεις απορρήτου, έτσι ώστε να μην μπορούν όλοι να βλέπουν το προφίλ μας και τι ανεβάζουμε. Δεν ανοίγουμε ποτέ συνημμένα αρχεία και συνδέσμους από αγνώστους. Δεν κανονίζουμε ποτέ συναντήσεις με ανθρώπους που δεν γνωρίζουμε ακόμα και αν είναι «φίλοι μας» στο διαδίκτυο.

10th anniversary EUROPEAN CYBER SECURITY MONTH

ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ ΠΑΝΤΑ ΤΗΝ ΕΠΙΣΗΜΗ ΕΦΑΡΜΟΓΗ ΜΑΣ ΓΙΑ ΝΑ ΜΗΝ ΤΣΙΜΠΗΣΕΤΕ ΤΟ ΔΟΛΩΜΑ!

CHOOSE TO BE SAFE ONLINE

Περισσότερες πληροφορίες σχετικά με το ηλεκτρονικό ψάρεμα στον ιστότοπο: https://cybersecuritymonth.eu/

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

www

SaferInternet4Kids.gr
helpline saferinternet
safeLine.gr
ΙΤΕ ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ
INHOPE ins@fe
Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης