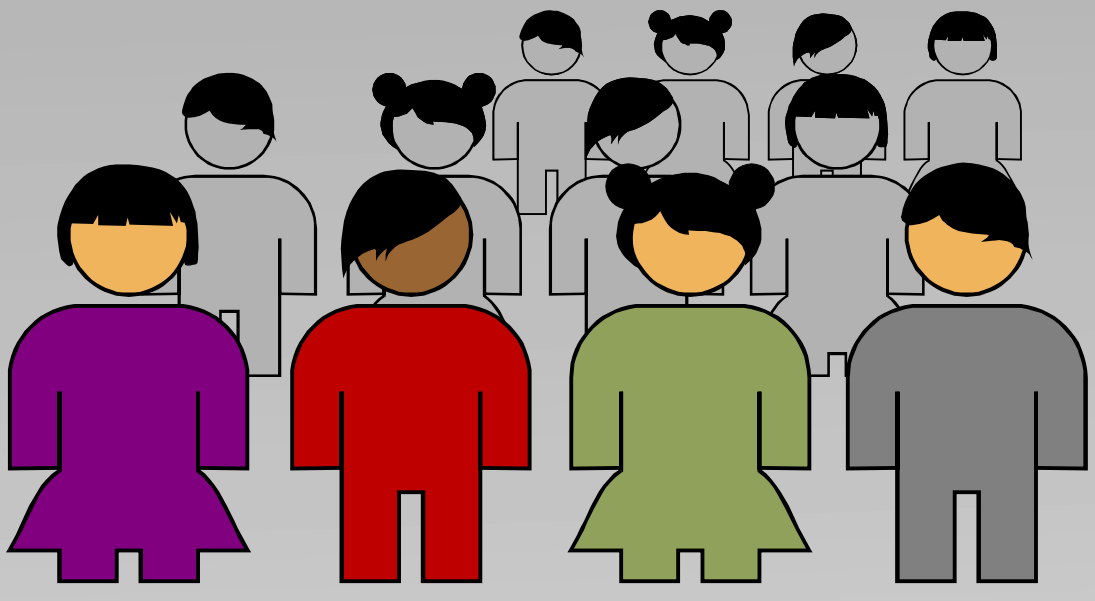
Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

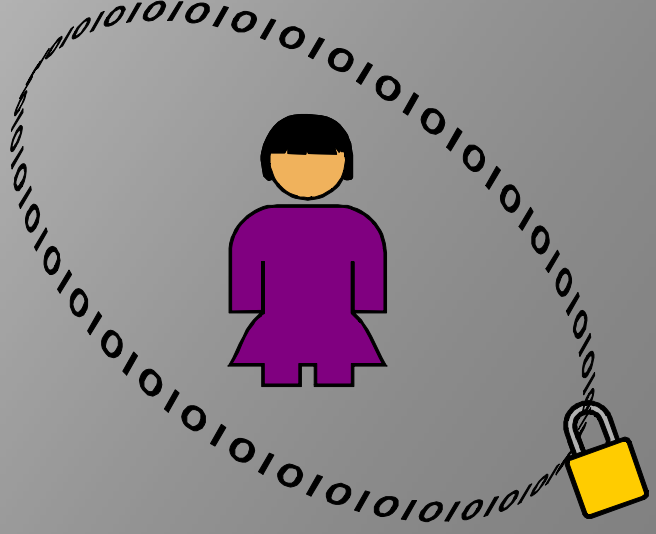
Μην παίρνεις τίποτα ως δεδομένο...

Σκέψου πιο... προσωπικά!

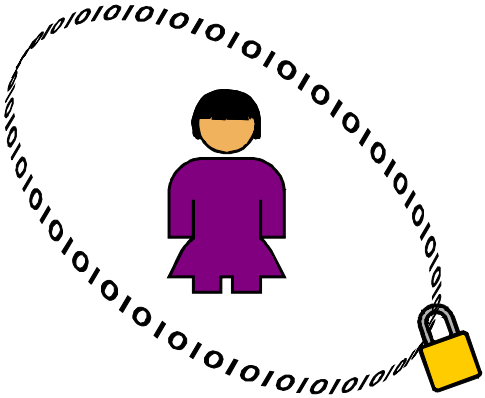


Προσωπικά Δεδομένα και Διαδίκτυο

Μαθαίνω για τα προσωπικά μου δεδομένα



Ιδιωτικότητα, παρακαλώ!



Η ιδιωτική σου ζωή είναι πολύτιμη.

Για όλους μας υπάρχουν πράγματα που δε θα θέλαμε να μοιραστούμε με άλλους ανθρώπους. Όχι απαραίτητα επειδή πρέπει να τα κρατήσουμε κρυφά, αλλά επειδή αποτελούν αποκλειστικά προσωπική μας υπόθεση.

Υπάρχουν φορές που μπορεί να θες να παραμείνεις εντελώς «ανώνυμος». Και να νιώθεις ασφαλής ότι δεν υπάρχει κάποιος που ξέρει τα πάντα για τη ζωή σου ή είναι σε θέση να παρακολουθεί όλες σου τις δραστηριότητες.

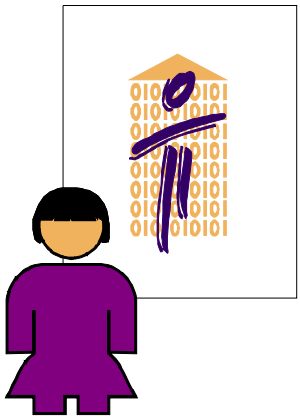
Γι' αυτό πρέπει να μπορείς να επιλέγεις ποιες πληροφορίες δίνεις στους άλλους και ποιες κρατάς μόνο για τον εαυτό σου.

Τα προσωπικά σου δεδομένα είναι όλες οι πληροφορίες που αναφέρονται σε σένα. Είναι το όνομά σου, η διεύθυνσή σου, ο αριθμός του κινητού σου, το σχολείο στο οποίο πηγαίνεις, τα μέρη όπου ταξιδεύεις, τα αντικείμενα που αγοράζεις, το προφίλ σου στο **facebook**, οι φωτογραφίες σου από πέρυσι το καλοκαίρι, το βίντεο της παρέας σου από τη χθεσινή γιορτή...

Διατηρώντας τον έλεγχο των προσωπικών σου δεδομένων, διατηρείς και τον έλεγχο της ιδιωτικής σου ζωής.

Μπορεί να εκπλαγείς αν σκεφτείς πόσες αποφάσεις παίρνεις για τα προσωπικά σου δεδομένα και την ιδιωτικότητά σου κάθε μέρα... και πόσο σημαντικές μπορεί να είναι αυτές...

Λίγα λόγια για τα προσωπικά δεδομένα



Παρακάτω θα βρεις χρήσιμες πληροφορίες για τα προσωπικά σου δεδομένα και τα δικαιώματά σου. Αν θες να μάθεις περισσότερα συμβουλεύσου τον διαδικτυακό τόπο της Αρχής **http://www.dpa.gr** ή διάβασε το ενημερωτικό φυλλάδιό μας που βρίσκεται στο διαδικτυακό τόπο **http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/NEWSMAIN/PUBLICATIONS/ENTYPO_GENERAL_FINAL_LOW_PAGES_0.PDF**

Διάβασε και μάθε με τις παρακάτω ερωτήσεις/απαντήσεις:

Τι είναι τα προσωπικά δεδομένα;

Προσωπικά δεδομένα είναι κάθε πληροφορία που σε χαρακτηρίζει, όπως για παράδειγμα το όνομά σου, η διεύθυνσή σου, το τηλέφωνό σου, τα ενδιαφέροντά σου, οι επιδόσεις σου στο σχολείο, οι φωτογραφίες σου, οι απόψεις σου, κ.α.

Μερικές φορές τα προσωπικά σου δεδομένα αφορούν ιδιαίτερα ευαίσθητα στοιχεία της ιδιωτικής σου ζωής, όπως στο θρήσκευμά σου, στις πολιτικές σου πεποιθήσεις, στην κατάσταση της υγείας σου ή στην ερωτική σου ζωή.

Πώς χρησιμοποιούνται τα προσωπικά μου δεδομένα;

Πολλές από τις καθημερινές σου δραστηριότητες βασίζονται στην επεξεργασία των προσωπικών σου δεδομένων:

- Η φόρμα που συμπληρώνεις για συμμετοχή στο διαγωνισμό της εταιρείας ηλεκτρονικών παιχνιδιών περιέχει προσωπικά σου στοιχεία, όπως όνομα, τηλέφωνο, διεύθυνση και ηλικία.
- Το ίδιο συμβαίνει και κατά την εγγραφή σου σε ένα διαδικτυακό **(on-line)** κατάστημα βιβλίων.
- Το σχολείο σου τηρεί δεδομένα για τους βαθμούς και τις επιδόσεις σου.
- Ο γιατρός που επισκέφτηκες τηρεί τις ιατρικές σου εξετάσεις και άλλα σχετικά στοιχεία για την υγεία σου.
- Ο αθλητικός σύλλογος στον οποίο είσαι μέλος τηρεί τα στοιχεία που έδωσες κατά την εγγραφή σου, καθώς και ιατρικά πιστοποιητικά.
- Το προφίλ σου στο **Facebook** περιέχει πληροφορίες για τους φίλους σου, τα ενδιαφέροντά σου, αλλά και άλμπουμ με φωτογραφίες σου.
- Το ηλεκτρονικό φόρουμ για μουσική που παρακολουθείς περιέχει στοιχεία για τις μουσικές προτιμήσεις σου και τους καλλιτέχνες που σε ενδιαφέρουν.

Είναι δυνατό τα προσωπικά μου δεδομένα να χρησιμοποιηθούν... εναντίον μου;

Αν δεν προσέξεις πώς και πού τα δημοσιοποιείς ή αν πέσουν σε λάθος χέρια, τα προσωπικά σου δεδομένα μπορούν να χρησιμοποιηθούν από κάποιους για να σε δυσφημίσουν ή να σε φέρουν σε δύσκολη θέση, αποκαλύπτοντας ιδιωτικές σου στιγμές... Οι πληροφορίες αυτές είναι δυνατόν να δυσκολέψουν τη ζωή σου στο μέλλον, π.χ. όταν θα ψάχνεις για δουλειά ή θα θες να σπουδάσεις στο πανεπιστήμιο ή να πάρεις δάνειο από μία τράπεζα. Σε ακραίες περιπτώσεις μπορεί να πέσεις ακόμα και θύμα υποκλοπής ταυτότητας **(**δηλαδή κάποιος που έχει τα δεδομένα σου μπορεί να προσποιείται ότι είσαι εσύ**)** ή θύμα παρενόχλησης και εξαπάτησης.

Πότε επιτρέπεται κάποιος να χρησιμοποιεί τα προσωπικά μου δεδομένα;

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 Αρχή Προστασίας Δεδομένων είναι ο αρμόδιος φορέας για την εφαρμογή αυτής της νομοθεσίας **(**νόμοι **2472/1997** και **3471/2006)**.

Ως βασικός κανόνας ισχύει ότι για να χρησιμοποιήσει κάποιος τα προσωπικά σου δεδομένα για έναν συγκεκριμένο σκοπό πρέπει να έχει εξασφαλίσει την συγκατάθεσή σου και, σε αρκετές περιπτώσεις, τη συναίνεση των γονιών σου. Με αυτό εννοούμε ότι, αφού προηγουμένως έχεις ενημερωθεί ακριβώς για το ποιος είναι αυτός που θέλει να χρησιμοποιήσει τα δεδομένα σου, για ποιον λόγο θέλει να τα χρησιμοποιήσει, ποια στοιχεία σου θέλει να πάρει και με ποιους θα τα μοιραστεί, τότε έχεις δεχθεί και έχεις πει με σαφή τρόπο ότι συμφωνείς.

Η συγκατάθεση είναι ο γενικός κανόνας, αλλά υπάρχουν και εξαιρέσεις. Για παράδειγμα κάποιοι οργανισμοί, όπως π.χ. ο δήμος ή το σχολείο σου, μπορούν να επεξεργάζονται συγκεκριμένα προσωπικά δεδομένα χωρίς τη συγκατάθεσή σου. Αυτό συμβαίνει γιατί τα δεδομένα σου είναι απαραίτητα για να εκτελέσουν το έργο τους και αυτό συνήθως ορίζεται σε κάποιο νόμο.

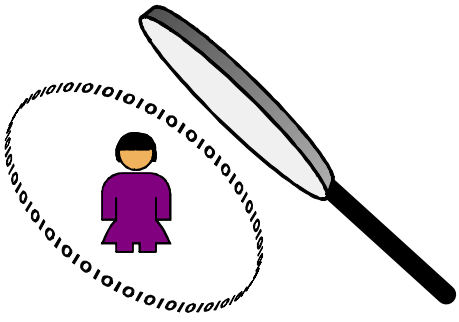
Ποια είναι τα δικαιώματα μου σε σχέση με τα προσωπικά μου δεδομένα;

- Όταν κάποιος σου ζητά να του δώσεις προσωπικά σου δεδομένα, έχεις το δικαίωμα να γνωρίζεις ακριβώς την ταυτότητά του, τον σκοπό για τον οποίο χρειάζεται τα δεδομένα σου, σε ποιους θα τα στείλει, καθώς και ποιοι θα έχουν πρόσβαση σε αυτά.

- Έχεις το δικαίωμα να γνωρίζεις ποια δεδομένα τηρούν οι άλλοι **(**οργανισμοί ή άτομα**)** για σένα και μπορείς να τους ζητάς να σε ενημερώνουν για αυτό.

- Έχεις το δικαίωμα να ζητάς τη διαγραφή ή τη διόρθωση των προσωπικών σου δεδομένων, όταν θεωρείς ότι η πληροφορία αυτή σε θίγει ή είναι λανθασμένη ή όταν διαφωνείς με την επεξεργασία αυτών των δεδομένων.

Με «παρακολουθεί» κανείς;



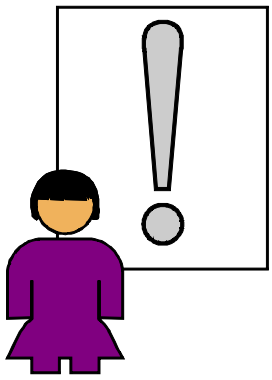
Έχεις καταλάβει πόσο συχνά τα προσωπικά σου δεδομένα αποτελούν αντικείμενο επεξεργασίας;

Σκέψου μια μέρα στη ζωή σου...

Είναι καλό να γνωρίζεις πόσο συχνά αφήνεις «ίχνη» γύρω σου... Ίσως κάποιες φορές να μην το θέλεις...

7:15	**Διαβάζεις το e-mail σου –** ο πάροχος ηλεκτρονικών επικοινωνιών καταγράφει την ώρα που μπήκες στο λογαριασμό σου, τον αποστολέα του μηνύματός σου, καθώς και την ώρα που σου έστειλε το μήνυμα.
7:30	**«Κατεβάζεις» ένα τραγούδι στο iPod –** η εταιρεία που σου πουλάει το τραγούδι καταγράφει το **e-mail** σου και τις μουσικές σου προτιμήσεις.
7:50	**Η μητέρα σου σε πάει με το αυτοκίνητο στο σχολείο –** το αυτοκίνητο διαθέτει συσκευή **GPS** που καταγράφει τη διαδρομή σας από το σπίτι στο σχολείο. Σε κάποια σημεία της διαδρομής υπάρχουν κάμερες ρύθμισης της κυκλοφορίας και ελέγχου παραβιάσεων του Κώδικα Οδικής Κυκλοφορίας.
10:10	**Μπαίνεις στην τάξη –** στο απουσιολόγιο του τμήματός σου καταγράφονται οι απόντες για κάθε διδακτική ώρα. Ο σχολικός σου φάκελος περιλαμβάνει τους βαθμούς και τις αξιολογήσεις που σε αφορούν.
12:00	**Ο κολλητός σου σε τραβάει μια φωτογραφία με το κινητό –** η φωτογραφία είναι αστεία και λέει πως μπορεί αργότερα να την ανεβάσει στο **facebook**.
15:00	**Σερφάρεις στο διαδίκτυο από το σπίτι –** ο **browser** που χρησιμοποιείς καταγράφει τις σελίδες που επισκέπτεσαι. Κάποιες σελίδες εγκαθιστούν στον υπολογιστή σου μικρά αρχεία **(cookies)** ώστε να μπορούν να σε αναγνωρίζουν όταν θα τις ξαναεπισκεπτείς.Μάθε περισσότερα.
15:15	**Κλικάρεις μια διαφήμιση που έχει ενδιαφέρον –** η διαφημιστική εταιρεία καταγράφει τις προτιμήσεις σου ώστε να μπορεί να σου στέλνει προσφορές για προϊόντα που σε ενδιαφέρουν.
15:30	**Στέλνεις μια ηλεκτρονική κάρτα σε έναν φίλο που έχει γενέθλια –** για την αποστολή της κάρτας πρέπει να συμπληρώσεις μια φόρμα με διάφορα προσωπικά σου στοιχεία και το **email** σου.
16:00	**Ψάχνεις στοιχεία για την έκθεση που πρέπει να παραδώσεις αύριο –** στο **google** καταγράφονται όλες οι αναζητήσεις που πραγματοποιείς, μαζί με την χρονική στιγμή της αναζήτησης και τη διεύθυνση δικτύου **(IP)** με την οποία ο υπολογιστής σου συνδέεται, μέσω του Παρόχου, στο διαδίκτυο.
18:00	**Πηγαίνεις στο γυμναστήριο –** στην είσοδο υπάρχει κάμερα που καταγράφει όσους μπαίνουν και βγαίνουν. Στην υποδοχή «περνάς» την κάρτα μέλους σου από το ειδικό μηχάνημα που την σκανάρει και εμφανίζει τα στοιχεία σου στην οθόνη.
19:00	**Ακούς τα φωνητικά σου μηνύματα στο κινητό –** το τηλέφωνο σου καταγράφει όλους όσους σε κάλεσαν, τους αριθμούς τηλεφώνου τους και τις ώρες κλήσης.
22:00	**Μπαίνεις στο Facebook –** διαβάζεις τι έκαναν σήμερα οι φίλοι σου και γράφεις τα δικά σου νέα. Βλέπεις ότι έχεις γίνει **tagged** στην σημερινή φωτογραφία που ήδη ανέβασε ο κολλητός σου και κάποιοι έχουν ήδη βάλει σχόλια. Αποδέχεσαι τα **friend requests** για δύο νέους φίλους, παρόλο που τον έναν δεν το ξέρεις πολύ καλά.

Συμβουλές



Προσπάθησε να διατηρείς τον έλεγχο των προσωπικών σου δεδομένων:

- **Ρώτα γιατί είναι απαραίτητα τα δεδομένα σου –** Σκέψου ποιος είναι αυτός που τα ζητάει. Είναι κάποιος που εμπιστεύεσαι; Πώς πρόκειται να τα χρησιμοποιήσει; Θα τα αποστείλει σε άλλους και, αν ναι, σε ποιους; Αν δεν είσαι σίγουρος για κάτι από όλα αυτά, ρώτα και μάθε πριν διαθέσεις πληροφορίες που σε αφορούν.

- **Σκέψου πριν αποκαλύψεις δεδομένα –** Αν λαμβάνεις γράμματα, **e-mails,** μηνύματα στο κινητό ή στο **Facebook** που σου ζητούν πληροφορίες, μην απαντήσεις αν δεν είσαι σίγουρος από ποιον προέρχονται.

- **Διάβαζε προσεκτικά τα «ψιλά γράμματα» -** Κάποιες εταιρείες μπορεί να γράφουν εκεί όρους για την χρησιμοποίηση των δεδομένων σου, π.χ. για διαφημιστικούς σκοπούς. Θυμήσου ότι πρέπει πάντα να δίνεις τη συγκατάθεσή σου γι' αυτό.

- **Διάβαζε την πολιτική ιδιωτικότητας στις ιστοσελίδες που επισκέπτεσαι –** μάθε πώς χρησιμοποιούν τα δεδομένα σου, π.χ. αν εγκαθιστούν αρχεία **cookies** και αν προωθούν τις πληροφορίες που σε αφορούν σε διαφημιστικές εταιρείες.

- **Εμπιστεύσου το ένστικτό σου –** Αν δεν είσαι σίγουρος για την ασφάλεια μιας ιστοσελίδας ή δεν νιώθεις άνετα με τον τρόπο που πρόκειται να χρησιμοποιηθούν τα προσωπικά σου δεδομένα, προτίμησε κάποια άλλη.

- **Δυσκόλεψε τους... «κακούς» –** Χρησιμοποίησε διαφορετικά συνθηματικά στους λογαριασμούς σου **(**π.χ. **e-mail, Facebook, Twitter).** Διάλεξε συνθηματικά που είναι εύκολο για σένα να θυμάσαι, αλλά δύσκολο για τους άλλους να μαντέψουν.

- **Σκέψου ποιος μπορεί να βλέπει τα δεδομένα σου –** Μην επισκέπτεσαι ιστοσελίδες που δεν θα ήθελες οι άλλοι να γνωρίζουν όταν μοιράζεσαι τον υπολογιστή σου με άλλους.

- **Σκέψου πριν αγοράσεις στο διαδίκτυο –** Χρησιμοποίησε ασφαλείς ιστοσελίδες, στις οποίες φαίνονται καθαρά τα στοιχεία επικοινωνίας της εταιρείας και οι οποίες διαθέτουν πολιτική ιδιωτικότητας. Έλεγχε αν είναι ασφαλές το κανάλι επικοινωνίας **(**π.χ. θα πρέπει η διεύθυνση της σελίδας να ξεκινάει με **https** και στο πρόγραμμα πλοήγησης στο διαδίκτυο να εμφανίζεται ένα λουκέτο ως εικονίδιο**).**

- **Θυμήσου να αποσυνδέεσαι από τις ιστοσελίδες,** στις οποίες έχεις εισέλθει**/**συνδεθεί με χρήση συνθηματικών **(**π.χ. όταν κάνεις αγορές από το διαδίκτυο ή την ιστοσελίδα κοινωνικής δικτύωσης**).**

- **Κράτα τον υπολογιστή σου ασφαλή –** Χρησιμοποίησε προγράμματα τείχους ασφαλείας **(firewall)** και προστασίας από ιούς **(antivirus).** Φρόντισε τα προγράμματα αυτά να είναι ενημερωμένα.

Πώς μπορεί να σε βοηθήσει η Αρχή

Αν ανακαλύψεις ότι κάποιος παραβιάζει τα προσωπικά σου δεδομένα, όπως π.χ. ότι τα συλλέγει ή τα δημοσιοποιεί (π.χ. «ανεβάζει» φωτογραφίες σου στο διαδίκτυο) χωρίς τη συγκατάθεσή σου, ενημέρωσε αμέσως τους γονείς σου και απευθύνσου στην Αρχή Προστασίας Δεδομένων για να σε βοηθήσει.

Στοιχεία επικοινωνίας με την Αρχή:

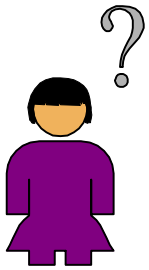
Ταχυδρομική Διεύθυνση:

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Γραφεία: Κηφισίας **1-3**, Τ.Κ. **115 23**, Αθήνα

Τηλεφωνικό Κέντρο: +30 210 6475600

Ηλεκτρονικό Ταχυδρομείο: contact@dpa.gr

Πόση πληροφορία αποκαλύπτεις για τον εαυτό σου;



Αφιέρωσε λίγο χρόνο για να κάνεις το επόμενο **quiz** και δες αν είσαι αρκετά προσεκτικός με τα προσωπικά σου δεδομένα στη καθημερινότητά σου**!** Απάντησε σε πέντε σύντομες ερωτήσεις**,** επιλέγοντας αυτό που σου ταιριάζει καλύτερα**.**

1. Ενημερώνεις το προφίλ σου στο Facebook, το MySpace, το Twitter ή κάποια άλλη σελίδα κοινωνικής δικτύωσης που χρησιμοποιείς. Τι κάνεις;

α**)** Ανεβάζεις ό, τι πληροφορία θέλεις**. (**Έτσι κι αλλιώς είναι απλά μόνο οι φίλοι σου μπορούν τα δουν**...).**

β**)** Προσπαθείς να είσαι επιλεκτικός στην πληροφορία που ανεβάζεις για εσένα και για τους άλλους**. (**Δεν θα ανέβαζες κάτι που θα ντρεπόσουν να δουν οι γονείς σου**).**

γ**)** Προσπαθείς να ανεβάζεις μόνο πληροφορία που δεν περιέχει προσωπικά δεδομένα **(**αφήνοντας έξω τα στοιχεία επικοινωνίας σου**,** την ημερομηνία γέννησής σου**,** φωτογραφίες σου**, ..).**

2. Είσαι σε κάποιο Internet Café και θέλεις να διαβάσεις τα μηνύματα στο λογαριασμό ηλεκτρονικού ταχυδρομείου σου. Τι κάνεις;

α**)** Τα διαβάζεις κανονικά **(**Δεν θεωρείς ότι υπάρχει κάποιο πρόβλημα ασφάλειας**.** Και άλλωστε**...** ποιον ενδιαφέρει να δει το **email** σου**;)**

β**)** Τα διαβάζεις αφού έχεις βεβαιωθεί ότι δεν βλέπει κανείς την οθόνη σου **(**Λίγη προσοχή δεν βλάπτει**...).**

γ**)** Τα διαβάζεις αφού έχεις βεβαιωθεί ότι δεν βλέπει κανείς την οθόνη σου**,** ενώ πριν φύγεις φροντίζεις να αποσυνδεθείς από την ιστοσελίδα του **email** και να διαγράψεις το **«**ιστορικό**» (history)** του προγράμματος πλοήγησης **(**Θέλεις να είσαι απόλυτα ασφαλής όταν χρησιμοποιείς κοινόχρηστους υπολογιστές**).**

3.Σε καλούν να λάβεις μέρος σε ένα διαγωνισμό για να κερδίσεις ένα ταξίδι στην Καραϊβική. Τι κάνεις:

α) Μπαίνεις στο διαγωνισμό και παρέχεις όλα τα προσωπικά στοιχεία που σου ζητάνε στη φόρμα συμμετοχής. (Σκέφτεσαι ότι κάτι πρέπει να δώσεις κι εσύ για να κερδίσεις ένα δωρεάν ταξίδι)

β) Ρίχνεις μια ματιά στις πληροφορίες για την επεξεργασία των προσωπικών δεδομένων που έχει η φόρμα και αν είναι εντάξει μπαίνεις στο διαγωνισμό. (Ξέρεις πως πάντα πρέπει να προσέχεις για την προστασία της ιδιωτικότητάς σου).

γ) Διαβάζεις με λεπτομέρεια τις πληροφορίες για την επεξεργασία των προσωπικών δεδομένων στη φόρμα και μόνο αν τις βρεις ικανοποιητικές συμπληρώνεις τη φόρμα, παρέχοντας όσο το δυνατόν λιγότερο προσωπικά δεδομένα. (Ποτέ δεν πρέπει να έχεις απόλυτη εμπιστοσύνη όταν πρόκειται για την ιδιωτική σου ζωή).

4.Ο φίλος σου δεν έχει πιστωτική κάρτα και θέλει να δανειστεί τη δική σου για να αγοράσει κάτι από το Ίντερνετ. Θα του έστελνες με email τα στοιχεία της πιστωτικής σου κάρτας;

α) Ναι. (Ποιος νοιάζεται για την «υποκλοπή ταυτότητας»; Καλή τύχη σε όσους θεωρούν ότι μπορούν να γίνουν εκατομμυριούχοι με τα στοιχεία της άδειας κάρτας σου...)

β) Ίσως. (Γενικά προσπαθείς να κρυπτογραφείς τα **emails** με σημαντική πληροφορία ή να δίνεις απόρρητα στοιχεία μέσω τηλεφώνου, αλλά καμιά φορά μπορεί αυτό να μην είναι δυνατό).

γ) Ποτέ. (Δεν εμπιστεύεσαι το **email**, καθώς ξέρεις πως δεν είναι τόσο δύσκολο για τους **hackers** να το υποκλέψουν).

5. Πόσο συχνά διαβάζεις την πολιτική ιδιωτικότητας μιας εταιρείας στο Ίντερνετ ή ρωτάς τι σκοπεύει να κάνει η εταιρεία με τα προσωπικά σου δεδομένα πριν τα αποκαλύψεις;

α) Ποτέ. (Ας μην υπερβάλλουμε. Οι εταιρείες προστατεύουν τα προσωπικά δεδομένων των πελατών τους, όπως λέει ο νόμος).

β) Μερικές φορές. (Μόνο όταν η εταιρεία σου φανεί πολύ «περίεργη»).

γ) Πάντα. (Πρέπει πάντα να προφυλάσσεις τα προσωπικά σου δεδομένα).

ΑΠΟΤΕΛΕΣΜΑΤΑ

Περισσότερα «α»: Τυχερός αλλά... ριψοκίνδυνος!

Χρησιμοποιείς υπολογιστή από τα πέντε σου, αλλά ποτέ δεν σου έχει συμβεί κάτι κακό. Οπότε σκέφτεσαι: «Γιατί να αρχίσω τώρα να ανησυχώ για τα προσωπικά μου δεδομένα;» Σωστά; Λάθος! Ο τρόπος που χειρίζεσαι τα δεδομένα που σε αφορούν μπορούν να σε βάλει σε κίνδυνο, το ίδιο και τους φίλους σου. Είναι καιρός να αρχίσεις να ελέγχεις τις πληροφορίες που αποκαλύπτεις και να μην βάζεις σε ρίσκο την προσωπική σου ζωή. Η αξία της ιδιωτικότητας σου φαίνεται μόνο όταν είναι πια πολύ αργά. Άλλαξε στάση και προστάτευσε τον εαυτό σου!

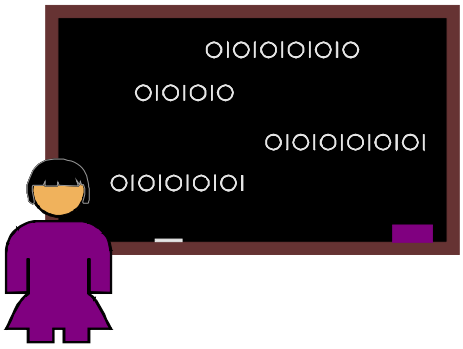
Περισσότερα «β»: Προσεκτικός αλλά... χαλαρός.

Ξέρεις ότι τα προσωπικά σου δεδομένα είναι σημαντικά και γενικά φροντίζεις για την προστασία τους. Συχνά διαβάζεις τις πολιτικές ιδιωτικότητας στις ιστοσελίδες που επισκέπτεσαι και σκέφτεσαι πριν ανεβάσεις στο **facebook** αστείες φωτογραφίες σου από πάρτυ. Αλλά πόσο συχνά εμπιστεύεσαι το ένστικτό σου; Ίσως όχι πολύ συχνά. Αν η ιστοσελίδα ενός διαγωνισμού φαίνεται παράξενη, μην εγγραφείς. Αν πρέπει να στείλεις απόρρητες πληροφορίες μέσω **email**, χρησιμοποιείσαι οπωσδήποτε κρυπτογράφηση, αλλιώς βρες άλλο τρόπο να το κάνεις. Καλό είναι να είσαι χαλαρός στο θέμα των προσωπικών σου δεδομένων, αλλά μπορείς να είναι πιο ασφαλής με λίγη ακόμα προσπάθεια!

Περισσότερα «γ»: Ασφαλής και... σίγουρος.

Η προστασία των προσωπικών σου δεδομένων είναι πολύ σημαντική για εσένα. Δεν είσαι διατεθειμένος να αφήσεις κανέναν να ανακατεύεται στα προσωπικά σου θέματα. Δεν θες να υπερβάλλεις. Αλλά προτιμάς να ξέρεις ότι το πρόγραμμα προστασίας από τους ιούς είναι ενημερωμένο, τα συνθηματικά σου ασφαλή (και δεν τα σημειώνεις σε χαρτί μπροστά στην οθόνη σου) και ότι η προσωπική σου πληροφορία είναι διαθέσιμη μόνο σε εκείνους που πραγματικά εμπιστεύεσαι. Μπράβο, είσαι στη σωστή κατεύθυνση!

Εκπαιδευτικό Υλικό



Το υλικό που προτείνουμε μπορεί να βοηθήσει στην ενημέρωση των μαθητών για την προστασία των προσωπικών τους δεδομένων με συγκεκριμένα θέματα συζήτησης και προβληματισμού στην τάξη, καθώς και με χρήση διαδραστικών εργαλείων όπως **quiz** και βίντεο.

Εκπαιδευτική ενότητα: «Μαθαίνω για τα προσωπικά μου δεδομένα»

Γενική περιγραφή

Σκοπός της ενότητας αυτής είναι:

Α) να κατανοήσουν οι μαθητές την έννοια των προσωπικών δεδομένων και τον τρόπο που αυτή η έννοια συνδέεται με την ιδιωτική τους ζωή σε καθημερινή βάση

Β) να ενημερωθούν για τα δικαιώματά τους στην προστασία των προσωπικών τους δεδομένων, και

Γ) να μάθουν με κάποιες απλές πρακτικές συμβουλές πώς μπορούν οι ίδιοι/ίδιες να προφυλάσσουν τον εαυτό τους από την κακόβουλη ή/και παράνομη χρήση των στοιχείων τους.

Ιδιαίτερη έμφαση πρέπει να δοθεί στην αποκάλυψη προσωπικών δεδομένων στο διαδίκτυο, κυρίως μέσω ιστοσελίδων διαδικτυακών αγορών, φόρουμ, ιστολογίων **(blogs)**, καθώς και σελίδων κοινωνικής δικτύωσης όπως το **Facebook**.

Προτεινόμενη δομή ενημέρωσης

1. Τι είναι προσωπικά δεδομένα **(**από τη σελίδα **«**Λίγα λόγια για τα προσωπικά δεδομένα**»)**

2. Παραδείγματα χρήσης προσωπικών δεδομένων **(**από τις σελίδες **«**Λίγα λόγια για τα προσωπικά δεδομένα**»** και **«**Με παρακολουθεί κανείς;**»)**

3. Ποιοι είναι οι κίνδυνοι από την παραβίαση ή χωρίς λόγο αποκάλυψη προσωπικών δεδομένων **(**από τις σελίδες **«**Λίγα λόγια για τα προσωπικά δεδομένα**»** και **«**Βίντεο**»)**

4. Πρακτικές συμβουλές **(**από τις σελίδες **«**Συμβουλές**»** και **«**Πως μπορεί να σε βοηθήσει η Αρχή**»).**

Προτάσεις για συζήτηση/ανταλλαγή απόψεων

Ζητήστε από τους μαθητές

1. Να σκεφτούν σε ποιες καθημερινές τους συνήθειες αποκαλύπτονται ή χρησιμοποιούνται προσωπικά τους δεδομένα**.**

2. Να περιγράψουν την αντίληψη τους περί προστασίας προσωπικών δεδομένων και ιδιωτικότητας**.** Τι θεωρούμε σήμερα ιδιωτική ζωή και πώς έχει αλλάξει η αντίληψη μας για αυτή από την εποχή των γονιών μας**;**

3. Να αναφέρουν κάποια περίπτωση που παραβιάστηκαν προσωπικά δεδομένα δικά τους ή κάποιου άλλου **(**μπορεί να το έχουν διαβάσει ή ακούσει**).** Να αναζητήσουν τέτοιες περιπτώσεις στο διαδίκτυο**.**

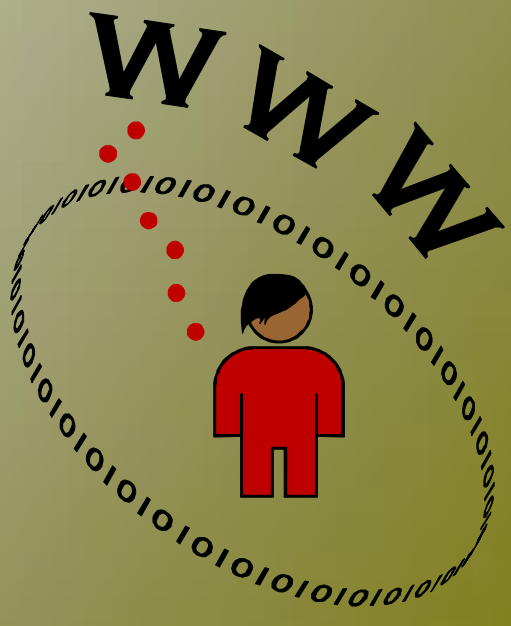
4. Να σκεφτούν πόσο ανώνυμοι θεωρούν πως είναι στο διαδίκτυο**.** Υπάρχουν φορές που νιώθουν ότι μπορεί κάποιος να τους παρακολουθεί ή ότι κάποια από τα στοιχεία που δημοσιοποιούν μπορεί να τους προκαλέσουν προβλήματα στο μέλλον**;**

5. Να σκεφτούν αν ακολουθούν κάποια από τις πρακτικές συμβουλές για την προστασία των προσωπικών τους δεδομένων**.**

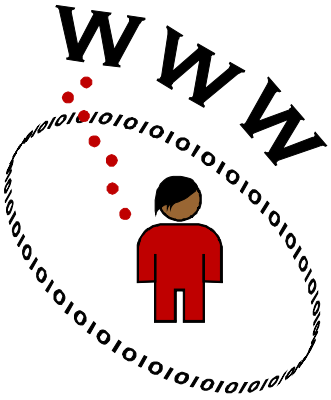
Εργαλεία

- Τυπώστε και κάντε μαζί με τους μαθητές το σύντομο **quiz** για την αποκάλυψη δεδομένων**.**
- Δείξτε τους το εύκολο **online** τεστ της Αρχής για την κλοπή ταυτότητας **(Identity theft).** Κάντε όλοι μαζί το τεστ στην τάξη**.**
- Χρησιμοποιείστε τα προτεινόμενα βίντεο για να δώσετε περισσότερη έμφαση στους κινδύνους από την αποκάλυψη προσωπικών δεδομένων**.**
- Επισκεφτείτε την ιστοσελίδα **http://browserspy.dk** , όπου μπορεί κανείς να δει τι πληροφορίες μεταδίδει το πρόγραμμα πλοήγησης απλά και μόνο όταν επισκεπτόμαστε μία ιστοσελίδα **(**δώστε ιδιαίτερη έμφαση στις επιλογές **«IP Address»** και **«Geolocation»)**

Σκέφτομαι πριν δημοσιεύσω



Τα γραπτά μένουν



Το διαδίκτυο σου παρέχει τη δυνατότητα να δημοσιοποιήσεις προσωπικά σου δεδομένα με όποιο τρόπο εσύ επιθυμείς.

Συνήθως σκέφτεσαι: «αφού δεν είναι κάτι για το οποίο ντρέπομαι, ούτε κάτι που θέλω να κρύψω, γιατί όχι;»

Και όμως, έχεις ποτέ σκεφτεί ότι όσα δημοσιεύεις μπορεί να χρησιμοποιηθούν από άτομα που δεν θέλεις ή δεν γνωρίζεις και με τρόπο ενοχλητικό ή προσβλητικό για εσένα; Όπως ότι κάποιος μπορεί να αναρτήσει φωτογραφίες σου σε ιστοσελίδες με τις οποίες είσαι ιδεολογικά αντίθετος/η ή να υποκλέψει δεδομένα σου για να σε εξαπατήσει ή ακόμα και να σου κάνει κακό...

Έχεις αναλογιστεί τι συνέπειες μπορεί να έχουν σε **12 -15** χρόνια από σήμερα οι δημοσιεύσεις που κάνεις τώρα;

Για παράδειγμα, ότι ο μελλοντικός σου εργοδότης μπορεί να χρησιμοποιήσει όποια πληροφορία βρει για σένα και το παρελθόν σου στο διαδίκτυο... Το ίδιο και ο μελλοντικός σου σύντροφος, φίλος αλλά και τα ίδια σου τα παιδιά ή τα εγγόνια...

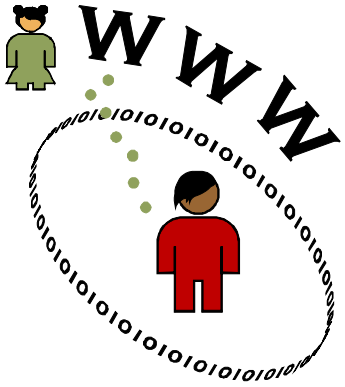
Είσαι σίγουρος ότι οι απόψεις σου θα παραμείνουν πάντα οι ίδιες;

Καταστάσεις, παρέες, γνώμες για τις οποίες «περηφανεύεσαι» σήμερα, και στις οποίες έδωσες δημοσιότητα μέσω του διαδικτύου, μπορεί να σε φέρουν σε δύσκολη θέση αύριο...

Το δικαίωμα στη «λήθη», όσον αφορά τις πληροφορίες στο διαδίκτυο, είναι το να μπορούμε να «διαγράφουμε» μέρος του παρελθόντος μας από το διαδίκτυο... Κι όμως, δεν είναι πάντα δυνατό κάποιος να σβήσει πληροφορίες και φωτογραφίες που έχουν αναρτηθεί σε κάποια ιστοσελίδα. Γιατί μπορεί τα δεδομένα αυτά να έχουν περιληφθεί ήδη και σε πολλές άλλες ιστοσελίδες, αλλά και να είναι διαθέσιμα μέσω μηχανών αναζήτησης, όπως το **Google**...

...για αυτό **...«**πριν δημοσιεύσεις, σκέψου**»!**

Τα δεδομένα των άλλων…



Κάποιες φορές μπορεί να αναρτάς πληροφορίες για άλλα άτομα στο διαδίκτυο **(**π.χ. σε κάποια ιστοσελίδα, ιστολόγιο **- blog,** υπηρεσία κοινωνικής δικτύωσης**),** όπως φωτογραφίες των φίλων σου από εκδρομές και πάρτυ ή βίντεο που τράβηξες με το κινητό σου**.**

Θυμήσου ότι για να το κάνεις αυτό πρέπει οπωσδήποτε να έχεις πάρει προηγουμένως την έγκριση **(**ή αλλιώς τη συγκατάθεση**)** των ατόμων αυτών**!**

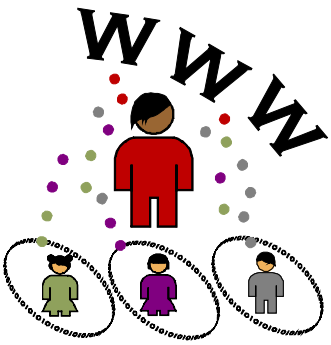
Για παράδειγμα για να προχωρήσεις στην ανάρτηση φωτογραφιών ή βίντεο στο προφίλ σου στο **Facebook** πρέπει να έχεις τη συγκατάθεση αυτών που απεικονίζονται**!**

Δεν έχει σημασία το αν αναφέρεις και το όνομά τους με τη δημοσίευση των φωτογραφιών ή όχι: πρέπει πάντα να έχεις πάρει την έγκρισή τους**.**

Πρόσεξε ότι ακόμα και αν έχεις πάρει έγκριση τη στιγμή της δημοσίευσης είσαι υποχρεωμένος να διαγράψεις κάθε φωτογραφία**/**βίντεο**/**πληροφορία για κάποιον όταν αλλάξει γνώμη και στο ζητήσει**.**

Ας μην είμαστε όμως και υπερβολικοί**…** όταν έχεις κάποια φωτογραφία με την οποία απαθανάτισες ένα γεγονός, π.χ συναυλία, παρέλαση, αθλητική δραστηριότητα, και στην οποία εμφανίζονται πρόσωπα στο **«**φόντο**»** που δεν **«**φαίνονται**»** καθαρά, τότε μπορείς να την αναρτήσεις, προσέχοντας πάντα το πού και το πώς**…**

Εσύ, ως … αρχισυντάκτης

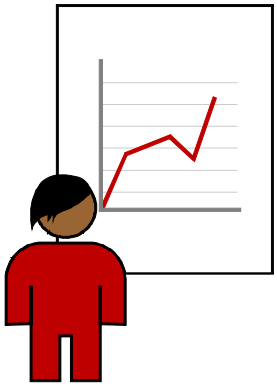


Κάποιες φορές μπορεί εσύ ο ίδιος**/**η ίδια να συντονίζεις τις πληροφορίες που **«**ανεβάζουν**»** άλλοι στο διαδίκτυο, π.χ. ως διαχειριστής περιεχομένου κάποιας ιστοσελίδας ή ενός ιστολογίου **(blog)** ή ενός ηλεκτρονικού φόρουμ **(forum).**

Μπορείς να φανταστείς το ρόλο σου ως τον αντίστοιχο του **«**αρχισυντάκτη**»** ενός εντύπου**.**

Σκέψου καλά τι επιτρέπεις να δημοσιευτεί: χωρίς να **«**λογοκρίνεις**»** αυθαίρετα το περιεχόμενο των όσων γράφονται θα πρέπει να ορίσεις το **«**ύφος**»,** το περιεχόμενο και να ενημερώσεις τους υπόλοιπους**…** **«**συντάκτες**»** κατάλληλα για τους όρους και τις προϋποθέσεις χρήσης της ιστοσελίδας, ιστολογίου, φόρουμ, κλπ. Για παράδειγμα μπορείς να ζητάς από όσους συμμετέχουν στις συζητήσεις να μη χρησιμοποιούν υβριστική γλώσσα, να μην αποστέλλουν πληροφορίες ρατσιστικού ή ξενοφοβικού περιεχομένου και να μην αποκαλύπτουν προσωπικά δεδομένα άλλων προσώπων χωρίς αυτά τα πρόσωπα να έχουν δώσει τη συγκατάθεσή τους**.**

Οι αριθμοί μιλούν…



Στην Ευρώπη, το **9%** των παιδιών ηλικίας **11-16** ετών έπεσαν θύματα παράνομης χρήσης των προσωπικών τους δεδομένων στο διαδίκτυο.

*Πηγή: Έρευνα του Δικτύου **«EU Kids Online»***

Στη Νορβηγία, το **23%** των νέων μεταξύ **8** και **18** έτυχε να δουν φωτογραφίες και άλλα προσωπικά τους δεδομένα στο διαδίκτυο χωρίς την έγκρισή τους. Το **41%** αυτών ήταν μεταξύ **17** και **18** ετών. Το **25%** των νέων της ίδιας κατηγορίας **(17 – 18** ετών**)** παραδέχεται ότι έχει δημοσιοποιήσει φωτογραφίες και βίντεο στα οποία εμφανίζονται άλλα πρόσωπα, χωρίς την έγκρισή τους.

Σε άλλη έρευνα μεταξύ νέων, το **2007** περισσότεροι από ένας στους οκτώ βρήκαν **«**κακή**»** πληροφορία για αυτούς στο διαδίκτυο.

Πηγή: Νορβηγική Αρχή Προστασίας Δεδομένων

Έχει συμβεί…

«Ανακάλυψε την εικόνα της σε ιστοσελίδα ναζιστικού περιεχομένου»

Ένα κορίτσι δημοσίευσε φωτογραφίες της σε μία ιστοσελίδα μέσω της οποίας γνώριζε συχνά φίλους με χόμπυ τη φωτογραφία. Λίγους μήνες αργότερα βρήκε τη φωτογραφία της σε μία ρατσιστική ιστοσελίδα, με τίτλο **«**Νορβηγικές ομορφιές**»** όπου υπήρχαν φωτογραφίες από **122** κορίτσια και το κείμενο έγραφε **«**εικόνες για όσους αγαπούν την νορβηγική φυλή**… ».** Πολλές από αυτές τις φωτογραφίες τις είχαν πάρει από την ιστοσελίδα τη σχετική με τη φωτογραφία… καμία από τις κοπέλες δεν ήξερε κάτι για αυτό**…**

«Πόζες στο… YouTube»

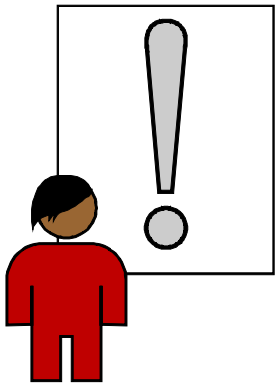
Μια **14-**χρονη κοπέλα πόζαρε για τον φίλο της μπροστά από μία διαδικτυακή κάμερα **(webcam).** Δύο εβδομάδες αργότερα, όλοι μπορούσαν να τη δουν στο **YouTube.** Αυτό που ξεκίνησε σαν αθώα πλάκα είχε μετατραπεί σε εφιάλτη για το κορίτσι. Σε **19** ώρες, το βιντεάκι είχαν δει **600** άνθρωποι**!**

«Το blog δεν ξεχνάει»

Στο προσωπικό της **blog** μια έφηβη κοπέλα δημοσίευε τακτικά τις σκέψεις της και τα συναισθήματά της σχετικά με προβλήματα εφηβείας, π.χ το σοβαρό για εκείνη τότε πρόβλημα ακμής. Χρόνια αργότερα, κάνει μία σοβαρή σχέση… επιλέγει να είναι **«**φειδωλή**»** στις περιγραφές που κάνει για τα εφηβικά της χρόνια**…** μέχρι που ο σύντροφός της ανακαλύπτει στο διαδίκτυο τις παλιές της αναρτήσεις σχετικά με τα θέματα που είχε ως έφηβη**…** Εκείνη έρχεται σε αμηχανία, ντρέπεται**…**

Πηγή: Νορβηγική Αρχή Προστασίας Δεδομένων

Συμβουλές



- Όταν δημοσιεύεις πληροφορίες που σε αφορούν στο διαδίκτυο προσπάθησε να προστατεύεις τα προσωπικά σου δεδομένα και να μην ανακοινώνεις σε όλο τον κόσμο αυτά που δεν θα έλεγες σε κάποιον αν τον είχες πρόσωπο με πρόσωπο! Να θέτεις στον εαυτό σου τις ίδιες ερωτήσεις όπως αυτές που θέτεις στον «πραγματικό κόσμο»: θα ήθελες αυτές τις πληροφορίες να τις μάθουν όλοι οι φίλοι σου, οι καθηγητές σου, οι γονείς σου;

- Να συνειδητοποιήσεις ότι δεν είσαι ο κυρίαρχος των πληροφοριών που δημοσιεύεις στο διαδίκτυο. Οπότε ο καλύτερος τρόπος να προστατευτείς είναι να προσέχεις τι δημοσιεύεις.

- Να διαβάζεις προσεχτικά τους «όρους χρήσης» πριν εγγραφείς ή πριν «ανεβάσεις» πληροφορίες σε ιστοσελίδες, ηλεκτρονικά φόρα, ιστολόγια, ή υπηρεσίες κοινωνικής δικτύωσης. Μπορεί να σου φαίνεται «βαρετό», αλλά είναι πολύ σημαντικό!

- Να «μετράς τα λόγια σου» σε ιστολόγια, ηλεκτρονικά φόρα, κοινωνικά δίκτυα, κτλ. Φρόντισε να διατυπώνεις τα μηνύματά σου με τρόπο που να γίνονται κατανοητά και εκτός του πλαισίου συζήτησης (π.χ αν αστειεύεσαι για κάτι, να το λες καθαρά!). Προσπάθησε να διατηρείς ένα σωστό επίπεδο στη γλώσσα που χρησιμοποιείς χωρίς υβριστικά σχόλια για τους υπόλοιπους χρήστες. Αν είσαι διαχειριστής μιας τέτοιας ιστοσελίδας, ενημέρωσε σχετικά τους «συντάκτες» σου.

- Να αποφεύγεις να δημοσιεύεις φωτογραφίες σου ή βίντεο που θα μπορούσαν να γίνουν «ενοχλητικά».

- Να μην δημοσιεύεις περιεχόμενα που μπορεί να ενοχλήσουν κάποιον, ούτε φωτογραφίες και βίντεο χωρίς έγκριση. Σε περίπτωση αμφιβολίας, προσπάθησε να μπεις στη θέση αυτού του προσώπου και να φανταστείς τις συνέπειες... Σκέψου πόσο εύκολο είναι να γίνεις από «θύτης» «θύμα»...

- Να επαληθεύεις τακτικά τι είναι δημοσιευμένο στο διαδίκτυο σχετικά με εσένα (π.χ. βάλε το ονοματεπώνυμο σου σε μια μηχανή αναζήτησης για να δεις τι πληροφορίες θα «φέρει» για εσένα).

- Να χρησιμοποιείς εάν είναι δυνατόν ένα ψευδώνυμο κατά την εγγραφή σου σε ιστοσελίδες και ηλεκτρονικά φόρα που θα το επικοινωνείς μόνο σε κοντινούς σου ανθρώπους.

Πώς μπορεί να σε βοηθήσει η Αρχή

Σε περίπτωση που θέλεις να σβηστεί κάποια πληροφορία για σένα από το διαδίκτυο, πρώτα προσπάθησε να απευθυνθείς στο πρόσωπο που δημοσίευσε την πληροφορία.

Αν δεν ικανοποιηθείς, τότε προσπάθησε να απευθυνθείς στον πάροχο της υπηρεσίας μέσω της οποίας έγινε η δημοσίευση (δηλ. σε αυτόν που διαχειρίζεται την ιστοσελίδα).

Αν και πάλι δεν γίνει δεκτό το αίτημά σου τότε επικοινώνησε με την Αρχή Προστασίας Δεδομένων για να σε συμβουλέψουμε σχετικά.

Στοιχεία επικοινωνίας με την Αρχή:

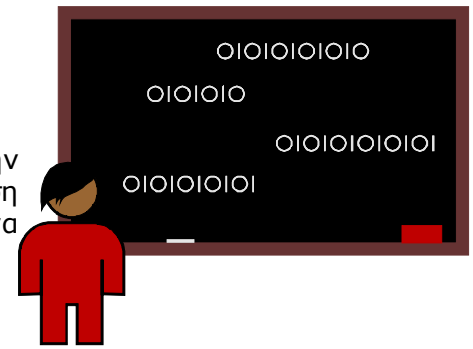
Ταχυδρομική Διεύθυνση:

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Γραφεία: Κηφισίας **1-3**, Τ.Κ. **115 23**, Αθήνα

Τηλεφωνικό Κέντρο: +30 210 6475600

Ηλεκτρονικό Ταχυδρομείο: contact@dpa.gr

Εκπαιδευτικό υλικό



Το υλικό που προτείνουμε παρακάτω μπορεί να βοηθήσει στην ευαισθητοποίηση των μαθητών σχετικά με τη δημοσίευση προσωπικών τους δεδομένων στο διαδίκτυο με συγκεκριμένα θέματα συζήτησης και προβληματισμού στην τάξη.

Εκπαιδευτική ενότητα: «Σκέφτομαι πριν δημοσιεύσω»

Γενική περιγραφή

Σκοπός της ενότητας αυτής είναι:

Α) να κατανοήσουν οι μαθητές ότι θα πρέπει να είναι προσεκτικοί και ιδιαίτερα επιλεκτικοί στο τι και πώς δημοσιεύουν στο διαδίκτυο για τον εαυτό τους και για τους άλλους.

Β) να κατανοήσουν τις δυνατότητες του διαδικτύου ως προς την αθέμιτη έκθεση προσωπικών δεδομένων και να μπορούν να ελέγχουν τη δημοσίευση των προσωπικών τους δεδομένων.

Γ) να μάθουν κάποιες απλές πρακτικές συμβουλές που αν ακολουθήσουν μπορούν να περιορίσουν τους κινδύνους αυτούς.

Προτεινόμενη δομή ενημέρωσης

1. Ενημέρωση για τη δυσκολία διαγραφής των δεδομένων που δημοσιεύονται στο διαδίκτυο σε αντιδιαστολή με την ευκολία αθέμιτης χρήσης τώρα ή στο μέλλον **(**από τη σελίδα **«**Τα γραπτά μένουν**»)**

2. Ενημέρωση για θέματα ευθύνης κατά τη δημοσίευση στο διαδίκτυο: ανάρτηση πληροφοριών για άλλα άτομα μόνο με τη συγκατάθεση των ατόμων αυτών με ιδιαίτερη έμφαση στις φωτογραφίες και τα βίντεο – ευθύνες των διαχειριστών ιστοσελίδων, ηλεκτρονικών φόρα. **(**από τις σελίδες **«**Τα δεδομένα των άλλων**»**, **«**Εσύ, ως… αρχισυντάκτης**»)**

3. Παραδείγματα **(**από τις σελίδες **«**Οι αριθμοί μιλούν**»** και **«**Έχει συμβεί**»)**

4. Πρακτικές συμβουλές **(**από τη σελίδα **«**Συμβουλές**»** και **«**Πώς μπορεί να σε βοηθήσει η Αρχή**»)**

Προτάσεις για συζήτηση / ανταλλαγή απόψεων

Μπορείτε να θέσετε τις παρακάτω ερωτήσεις στην τάξη και να ζητήσετε τις απόψεις – εμπειρίες των μαθητών:

- Έχετε ποτέ δημοσιεύσει την φωτογραφία κάποιου χωρίς να ζητήσετε την άδειά του πρώτα; Έχετε σκεφτεί πώς θα αντιδρούσε αν μάθαινε ότι το έχετε κάνει;
- Έχετε ποτέ δημοσιεύσει κάποια φωτογραφία δική σας ή φίλου σας που δεν θα θέλατε να τη δουν οι γονείς σας; Είσαστε σίγουροι ότι την είδαν μόνο όσοι πραγματικά θέλατε;
- Έχετε ποτέ αντιληφθεί να έχει δημοσιεύσει κάποιος δική σας φωτογραφία χωρίς να ζητήσει την άδειά σας πρώτα; Πώς νιώσατε; Πώς αντιδράσατε;
- Πιστεύετε ότι μπορεί κάτι που δημοσιεύετε σήμερα να σας δημιουργήσει πρόβλημα αύριο ή σε κάποια χρόνια; Π.χ σε σχέση με τον μελλοντικό εργοδότη σας, τον/την μελλοντική σας αγαπημένο/νη, τα παιδιά σας;

Θέματα για ομαδική δραστηριότητα

Θέμα 1

Φτιάξτε οδηγίες για το πότε επιτρέπεται να δημοσιεύει κανείς φωτογραφίες για άλλους στο διαδίκτυο.

- Τι ισχύει για φωτογραφίες από την παραλία, από πάρτυ ή από αγώνα ποδοσφαίρου;

Μπορείτε να σκεφτείτε περιπτώσεις που κάποιος μπορεί να έχει λόγους να μην θέλει να δημοσιεύονται φωτογραφίες του ή άλλη πληροφορία σχετικά με αυτόν στο διαδίκτυο;

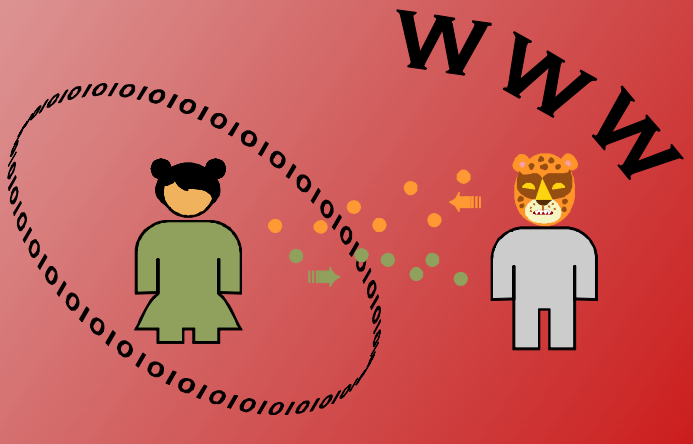
Θέμα 2

Βάλτε τα ονοματεπώνυμά σας σε μια μηχανή αναζήτησης για να δείτε τι πληροφορίες θα «φέρει» για εσάς.

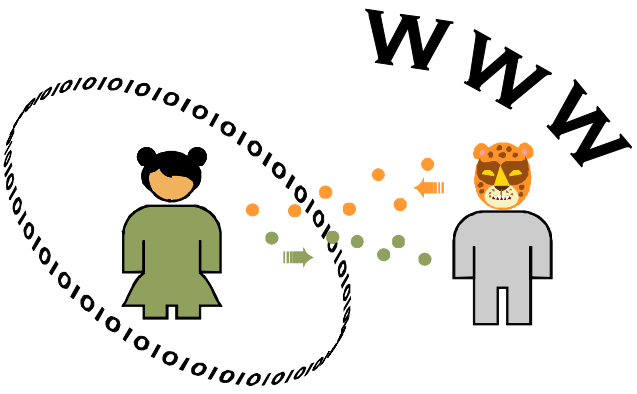
- Αισθάνεστε ότι τα αποτελέσματα δίνουν μια ακριβή εικόνα του ποιοι είστε;

- Γιατί ναι, γιατί όχι;

Γνωρίζω με ποιον μιλώ



Ποιός αλήθεια είναι;



Δεν είμαστε πάντα σίγουροι με ποι**ο**ν «μιλάμε» στο διαδίκτυο**!**

Όταν κάποιος φτιάχνει ένα προφίλ **(**π.χ. σε χώρους συζητήσεων**/**ηλεκτρονικά φόρα **- forum,** ιστολόγια **- blogs,** υπηρεσίες στιγμιαίων μηνυμάτων **- chat,** υπηρεσίες κοινωνικής δικτύωσης**)** αποφασίζει ο ίδιος εκείνη τη στιγμή για το **...** ποιος θέλει να είναι**.**

Αρκετοί μπορεί να χρησιμοποιούν την πραγματική τους ταυτότητα**.**

Και άλλοι μπορεί να πειραματίζονται με**...** διαφορετικές ταυτότητες**,** π.χ.**,** δηλώνοντας διαφορετικό φύλο ή ηλικία**,** και πιθανά χρησιμοποιώντας το διαδίκτυο για να **«**δοκιμάσουν**»** ή να **«**παίξουν**»** με διαφορετικές πτυχές της προσωπικότητάς τους**,** τις οποίες δεν νιώθουν άνετα να επιδεικνύουν στον πραγματικό κόσμο**.**

Υπάρχουν ακόμα και άτομα που δημιουργούν ψεύτικα προφίλ με σκοπό να εξαπατήσουν ή και να κάνουν κακό σε άλλους**.**

Ένα ακραίο αλλά χαρακτηριστικό παράδειγμα είναι ενήλικες **-** παιδεραστές που παρουσιάζονται ως παιδιά προσπαθώντας να έρθουν σε επαφή με υποψήφια θύματά τους μέσα από διαδικτυακά παιχνίδια ή σελίδες συζητήσεων**...** Στόχος τους είναι συχνά να κερδίσουν την εμπιστοσύνη ανηλίκων με σκοπό τη σεξουαλική κακοποίηση**...**

Πώς είμαστε λοιπόν σίγουροι με ποιον επικοινωνούμε στο χώρο συζήτησης**,** στο ηλεκτρονικό φόρουμ**,** στο ιστολόγιο**,** κ.ο.κ**;** Ποιος αλήθεια είναι στην **«**άλλη πλευρά**»** του καλωδίου**;**

Γνωριμίες στο διαδίκτυο

Το διαδίκτυο σου προσφέρει πολλές δυνατότητες για νέες γνωριμίες. Τι γίνεται όμως αν κάποιο από τα άτομα που γνωρίζεις **«**εκεί έξω**»** δεν είναι αυτό που πραγματικά λέει; Κι αν είναι κάποιος που θέλει να σε εξαπατήσει; Ή ακόμα και να σου κάνει κακό;

Είναι πολύ εύκολο να ξεγελαστείς.

Σκέψου το εξής σενάριο:

- Κάποιος σε προσκαλεί σε ιδιωτική συνομιλία **(invite)** σε μια υπηρεσία στιγμιαίων μηνυμάτων **(**π.χ. **Msn** ή **Icq)**. Από την περιγραφή του, σου κεντρίζει το ενδιαφέρον και σου φαίνεται συμπαθητικό άτομο.

- Έχοντας κερδίσει την εμπιστοσύνη σου, μπορεί πλέον να μάθει από εσένα προσωπικές πληροφορίες, όπως η διεύθυνσή σου, το τηλέφωνό σου, διάφορες καθημερινές σου συνήθειες, τον κοινωνικό σου κύκλο ή φωτογραφίες σου. Αν είσαι εντελώς απρόσεκτος μπορεί να σου αποσπάσει ακόμα και προσωπικούς κωδικούς, π.χ. στο προφίλ σου στο **Facebook** ή στο λογαριασμό ηλεκτρονικού ταχυδρομείου σου **(e-mail)**.

Κι αν τελικά το άτομο αυτό δεν είναι τόσο καλό όσο φαίνεται; Κι αν έχει κακόβουλες προθέσεις; Τι **«**κακό**»** μπορεί να κάνει με αυτή την πληροφορία που εσύ ο ίδιος του έδωσες;

- Να σε διαβάλλει **(**εκθέτοντας φωτογραφίες σου ή άλλα προσωπικά σου δεδομένα σε μέρη ή άτομα που δεν θα ήθελες**)**.

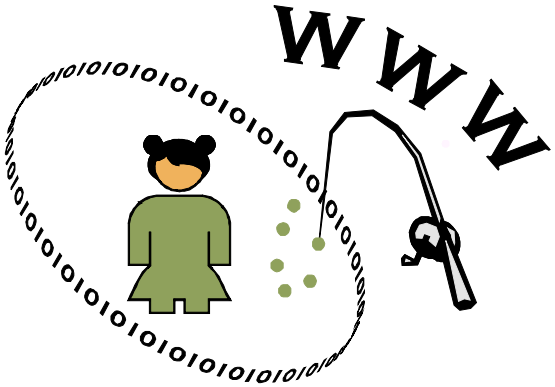
- Να προσπαθήσει να σε ξεγελάσει, π.χ. ζητώντας σου να τοποθετήσεις χρήματα σε κάποιο τραπεζικό λογαριασμό **(**επικαλούμενος κάποια έκτακτη ανάγκη**)**.

- Να **«**υποκλέψει**»** την ταυτότητά σου **(**π.χ. να αποστέλλει **e-mail** με τον δικό σου λογαριασμό ηλεκτρονικού ταχυδρομείου, να χρησιμοποιεί το προφίλ στο **Facebook** προσποιούμενος εσένα, κλπ**)**.

- Να παρενοχλεί εσένα ή τους φίλους σου.

- Να σε παρασύρει σε συνάντηση με σκοπό να σε εξαπατήσει ή να σου κάνει κακό**...**

«Ψάρεμα» στο διαδίκτυο



Phishing είναι η απόπειρα που μπορεί να κάνει κάποιος για να... «ψαρέψει» προσωπικά σου δεδομένα στο διαδίκτυο.

Σίγουρα κάποια στιγμή σου έχει συμβεί χωρίς ίσως να το έχεις καταλάβει.....

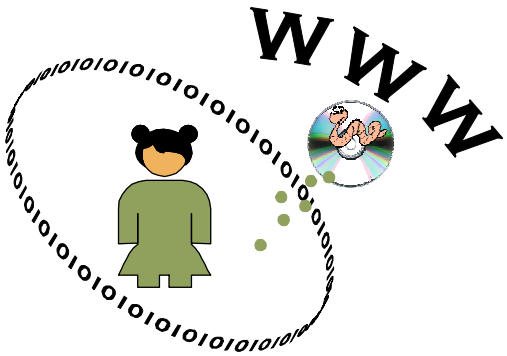
Το phishing γίνεται με τη αποστολή κάποιου ψεύτικου παραπλανητικού μηνύματος (συνήθως **e-mail**), πολλές φορές δελεαστικού, για να σε ξεγελάσει, του οποίου ο πραγματικός αποστολέας δεν είναι αυτός που φαίνεται. Το μήνυμα αυτό αποσκοπεί στο να σε πείσει να δώσεις προσωπικά σου δεδομένα ή να πατήσεις σε κάποιο σύνδεσμο (**link**), που στην πραγματικότητα δεν είναι «αθώος» (π.χ. είναι δυνατό «πατώντας» τον σύνδεσμο να εγκατασταθεί στον υπολογιστή σου κακόβουλο ή κατασκοπευτικό λογισμικό).

Για παράδειγμα, ένα τέτοιο μήνυμα μπορεί να ισχυρίζεται ότι απαιτείται να ενημερώσεις άμεσα κάποια προσωπικά σου στοιχεία σε μία ιστοσελίδα για λόγους ασφαλείας: στην πραγματικότητα όμως, δίνοντας τα στοιχεία σου, αυτά πηγαίνουν σε λάθος χέρια!

Άλλο παράδειγμα είναι μήνυμα που μπορεί να λέει ότι κέρδισες σε κάποιο τυχερό παιχνίδι, π.χ. λοταρία, και να σε καλεί να δώσεις τα προσωπικά σου στοιχεία για να παραλάβεις το βραβείο. Σκέψου καλά: είναι δυνατόν να κερδίσεις σε ένα παιχνίδι χωρίς να παίξεις;

Το **phishing** είναι πλέον αρκετά εξελιγμένο: μπορεί ένα τέτοιο μήνυμα να σε παραπέμπει σε μία ψεύτικη ιστοσελίδα η οποία όμως να είναι πιστό αντίγραφο της αυθεντικής! (π.χ. της ιστοσελίδας κοινωνικής δικτύωσης που χρησιμοποιείς, όπου σου ζητείται να εισάγεις τα συνθηματικά σου).

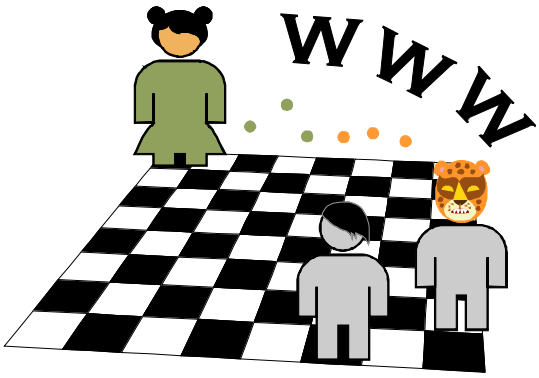
«Κακόβουλο» Λογισμικό



Υπάρχουν διάφορα προγράμματα/εφαρμογές, τα οποία μπορούν, αφού εγκατασταθούν στον υπολογιστή σου, να υποκλέψουν προσωπικά σου δεδομένα. Τα προγράμματα αυτά ανήκουν στην κατηγορία του ονομαζόμενου «κακόβουλου» λογισμικού. Η εγκατάστασή τους μπορεί να γίνει εύκολα αν ξεγελαστείς και «πατήσεις» κάποιο **link** σε μήνυμα **phishing** ή αν εγκαταστήσεις κάποιο πρόγραμμα που έχει κρυμμένο «κακόβουλο» λογισμικό.

Υπάρχουν διάφοροι τρόποι να προστατεύεσαι από τέτοιο «κακόβουλο» λογισμικό και ιούς. Διάβασε κάποιες χρήσιμες πληροφορίες από την ιστοσελίδα της Ομάδας Δράσης για την Ψηφιακή Ασφάλεια (**DART**):
http://kids.dart.gov.gr/KidsNewsInner.aspx?new_id=170&nwc_id=24

«Επικίνδυνα»... παιχνίδια;



Μπορεί να σου αρέσει να παίζεις παιχνίδια μέσω του διαδικτύου, όπως παιχνίδια στρατηγικής, δράσης, ρόλων ή εικονικών χαρακτήρων.

Έχεις όμως σκεφτεί ότι μπορεί να κινδυνεύσεις στην προσπάθειά σου απλά να ενημερωθείς για το πώς θα συνεχίσεις ένα... παιχνίδι;

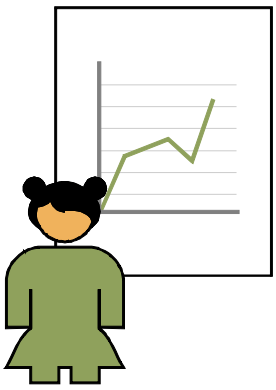
Ενήλικες με κακόβουλες προθέσεις μπορούν να σε παροτρύνουν να προβείς σε ακατάλληλες συμπεριφορές μέσω κάμερας ή συνομιλιών (ανταλλάσσοντας για τις συμπεριφορές αυτές τις γνώσεις που έχουν πάνω στο παιχνίδι).

Μπορούν επίσης να στείλουν κακόβουλο λογισμικό (π.χ. μέσω κάποιου **link**), προσποιούμενοι ότι είναι χρήσιμο υλικό για το παιχνίδι, ενώ ουσιαστικά με αυτόν τον τρόπο θέλουν να αποκτήσουν πρόσβαση στον υπολογιστή σου (και κατ' επέκταση, σε ό,τι προσωπικά δεδομένα τηρείς σε αυτόν).

Ορισμένοι συμπαίκτες σου (τους οποίους στην πραγματική ζωή δεν γνωρίζεις) μπορούν να προβούν σε παράνομη/προσβλητική συμπεριφορά εναντίον σου (μέσω επικοινωνίας στο πλαίσιο του παιχνιδιού) - ιδιαίτερα αν τους έχεις δώσει από μόνος σου προσωπικές πληροφορίες.

Επίσης, τυχόν κακή συμπεριφορά του χαρακτήρα που σε εκπροσωπεί στην «εικονική» σου ζωή (**avatar**) μέσω των διαδικτυακών παιχνιδιών, αν συσχετιστεί με την πραγματική σου ταυτότητα, θα μπορούσε να σε εκθέσει και στην πραγματική σου ζωή, στο παρόν ή και στο μέλλον...

Οι αριθμοί μιλούν...



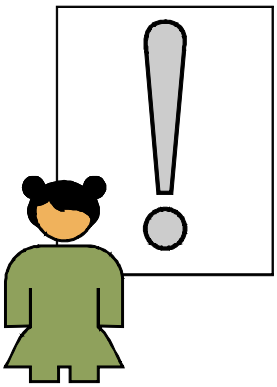
Το **29%** των παιδιών ηλικίας **9-16** που χρησιμοποιούν το διαδίκτυο στην Ευρώπη, έχουν στο παρελθόν επικοινωνήσει από κοντά με κάποιον που γνώρισαν στο διαδίκτυο.

Το **8%** των παιδιών έχουν συναντήσει από κοντά κάποιον που γνώρισαν στο διαδίκτυο κατά τη διάρκεια του προηγούμενου έτους. Το **1%** των παιδιών αυτών (ή **1** στα **7** από αυτά που είχαν τέτοια συνάντηση) ενοχλήθηκαν από αυτού του είδους την εμπειρία.

Το 9% των παιδιών ηλικίας 11-16 ετών έπεσαν θύματα παράνομης χρήσης των προσωπικών τους δεδομένων (7% παραβίαση κωδικών και 5% παραβίαση άλλων προσωπικών δεδομένων), ή θύματα οικονομικής απάτης (2%).

Πηγή: Έρευνα του Δικτύου EU Kids Online **(http://www.eukidsgreece.gr/)**

Συμβουλές



- **Προσπάθησε όσο είναι δυνατό να χρησιμοποιείς «ψευδώνυμα» -** όταν συμμετέχεις σε ιστολόγια και διαδικτυακούς χώρους συζητήσεων ή παιχνίδια. Διάλεγε ουδέτερα ψευδώνυμα... και μην αποκαλύπτεις σε κανένα ποια ψευδώνυμα χρησιμοποιείς.

- **Ποιός είναι πίσω από ένα ψευδώνυμο; -** Δεν μπορείς ποτέ να είσαι σίγουρος... Για αυτό πρέπει να μην γράφεις προσωπικά σου στοιχεία όταν είσαι **"on line"**, να μην κανονίζεις μόνος σου συναντήσεις με «εικονικούς» φίλους και να είσαι επιφυλακτικός με τις δηλώσεις και τις «αλήθειες» που γράφονται από άτομα που δεν γνωρίζεις.

- **Προστάτεψε με ζήλο τα αναγνωριστικά σου... -** Είναι πολύ δυσάρεστο να δεις να κυκλοφορούν μηνύματα που δεν θα έστελνες ποτέ με το δικό σου όνομα/ψευδώνυμο, γιατί κάποιος σου έκλεψε την ταυτότητά σου! Διάλεξε ένα μυστικό ψευδώνυμο και ένα πολύπλοκο συνθηματικό, που να περιλαμβάνει γράμματα, αριθμούς, ειδικούς χαρακτήρες, και προσπάθησε να το αλλάζεις τακτικά. Να αποφεύγεις να «θυμάται» ο Η/Υ σου συνθηματικά και πάντα να αποσυνδέεσαι στο τέλος της σύνδεσής σου **(session)**. Να μην αποκαλύπτεις τα συνθηματικά μέσω συνομιλίας σε πρόγραμμα **instant messaging** ή **e-mail**.

- **Προσοχή στην "εικονική" σου εικόνα... -** Στα διαδικτυακά παιχνίδια, ο εικονικός ήρωας που επιλέγουμε **(avatar)** δεν πρέπει να συνδέεται με πραγματικά μας στοιχεία, π.χ δική μας φωτογραφία, πραγματικό όνομα, διεύθυνση.

- **Μην "πατάς" ποτέ πάνω σε «ύποπτα» link... -** τα οποία αναγράφονται σε **e-mail** ή άλλα μηνύματα που λαμβάνεις, όσο δελεαστικά και αν δείχνουν **(**π.χ. σου λένε ότι κέρδισες σε λοταρία ή κληρονόμησες κάποιο μεγάλο ποσό ή έχεις σημαντική έκπτωση σε αγορά προϊόντος**)**. Ακόμα και αν το μήνυμα φαίνεται να προέρχεται από φίλο, πρέπει να είσαι απόλυτα σίγουρος ότι το έστειλε αυτός! Να αναλογίζεσαι πάντοτε αν το συγκεκριμένο μήνυμα θα είχε νόημα να το στείλει ο φίλος σου **(**συνέκρινε τον τρόπο γραφής του μηνύματος με τον τρόπο γραφής του φίλου σου, σκέψου αν έχει νόημα αυτό που ζητάει κτλ.**)** Ενημέρωσε τον φίλο σου για «ύποπτο» μήνυμα οποιουδήποτε τύπου δέχτηκες από αυτόν.

- **Χρησιμοποίησε περισσότερους από έναν λογαριασμούς e-mail κατά την εγγραφή σου σε διαφορετικές υπηρεσίες του διαδικτύου -** Φρόντισε τον κύριο λογαριασμό να τον γνωρίζουν μόνο αυτοί που επιλέγεις εσύ **(**φίλοι, συγγενείς,...**)**

- **Προστάτευσε τον υπολογιστή σου από κακόβουλο λογισμικό -** Κάνε τακτικές ενημερώσεις του λειτουργικού συστήματος και χρησιμοποίησε προγράμματα προστασίας από ιούς και άλλο κακόβουλο λογισμικό **(antivirus, antispam, antispyware)**.

- **Όταν είσαι στο διαδίκτυο, η κάμερα να είναι αρχικά πάντα σβηστή... -** Να την ανοίγεις μόνο όταν συνομιλείς με πολύ κοντινό σου φίλο. Θυμήσου ότι δεν ξέρεις πάντα ποιος πραγματικά σε βλέπει και μπορεί να καταγράψει ή και να δημοσιεύσει τις εικόνες σου!

- **Να ακολουθείς το ένστικτό σου... -** Αμφιβολία, κακή εντύπωση; Αν κάποια συμπεριφορά σε ενοχλεί κατά τη συνομιλία ή το παιχνίδι... τότε από-συνδέσου...

- **Είναι η ζωή σου!... -** Μην αφήνεις να σε κατακλύζουν με στιγμιαία μηνύματα **(instant messages)** και κλήσεις... Έχεις το δικαίωμα να μη είσαι διαθέσιμος ακόμη και όταν είσαι συνδεδεμένος.

Πώς μπορεί να σε βοηθήσει η Αρχή

Σε περίπτωση που έχεις πέσει θύμα υποκλοπής προσωπικών σου δεδομένων, π.χ. αν κάποιος σε εξαπάτησε και του έδωσες στοιχεία που δεν ήθελες και τα οποία τώρα βλέπεις δημοσιευμένα, επικοινώνησε με την Αρχή για να σε βοηθήσει.

Στοιχεία επικοινωνίας με την Αρχή:

Ταχυδρομική Διεύθυνση:

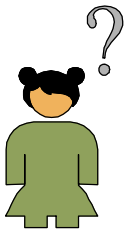
Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Γραφεία: Κηφισίας **1-3**, Τ.Κ. **115 23**, Αθήνα

Τηλεφωνικό Κέντρο: +30 210 6475600

Ηλεκτρονικό Ταχυδρομείο: contact@dpa.gr

Εάν υποψιάζεσαι ότι κάποιος χρησιμοποιεί ψεύτικη ταυτότητα για να σε εξαπατήσει, είναι καλό να το συζητήσεις με τους γονείς σου και να απευθυνθείτε στην αστυνομία **(**Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος**).**

Κουίζ



Επίλεξε την απάντηση που θεωρείς σωστή.
Έλεγξε στο τέλος πόσο καλά τα πήγες.

Ερώτηση 1:

Ποια είναι μια καλή πρακτική για να θυμάμαι τον κωδικό μου **(**για **instant messaging** πρόγραμμα ή για **e-mail)**;

α**)** Επιλέγω ως κωδικό κάτι εύκολο **(**π.χ. το τηλέφωνό μου ή**/**και όνομα του κατοικίδιού μου**)**

β**)** Προσπαθώ να διαλέξω κωδικό που θα είναι εύκολο να τον θυμάμαι**,** αλλά δύσκολο για κάποιον να τον μαντέψει

γ**)** Έχω ρυθμίσει τον υπολογιστή μου να τον **«**θυμάται**»** έτσι ώστε να μην το πληκτρολογώ

Ερώτηση 2:

Δεν πρέπει ποτέ να δεχτείς να συναντήσεις μόνος**/**η κάποιον**/**α που έχει γνωρίσει μέσω **chat,** ακόμα και αν σου φαίνεται συμπαθής**.**

α**)** Σωστό

β**)** Λάθος

γ**)** Εξαρτάται

Ερώτηση 3:

Αν ο πάροχος του ηλεκτρονικού μου λογαριασμού **(e-mail)** μου ζητάει να του στείλω με **e-mail** τον κωδικό μου**,** τότε**:**

α**)** Τον στέλνω σε κάθε περίπτωση

β**)** Τον στέλνω μόνο αν μου αιτιολογεί πλήρως τον λόγο που τον χρειάζεται **(**π.χ. για ανανέωσή του**)**

γ**)** Δεν στέλνω ποτέ με **e-mail** τον κωδικό μου και σε κανέναν**,** για κανέναν λόγο

Ερώτηση 4:

Στο προφίλ μου σε μία ιστοσελίδα κοινωνικής δικτύωσης ή όταν κάνω **chat** μου ζητείται η διεύθυνση που διαμένω. Τι κάνω;

α) Δεν δίνω την πραγματική μου διεύθυνσή ποτέ

β) Τη δίνω μόνο αν είναι κάποια ιστοσελίδα γνωστή (π.χ. στο **Facebook**)

γ) Τη δίνω πάντοτε (δεν θα με πείραζε να μου στέλνουν ταχυδρομικό υλικό)

Ερώτηση 5:

Στο **Msn** ξαφνικά εμφανίζεται ένα μήνυμα από τη φίλη σου Μαρία που σου λέει **«Hey!! Nice Pictures!! Click here: http://real_photos.com/?pic=holiday.jpg»**

α) Δεν πατάω αν πριν δεν έχω επιβεβαιώσει ότι πραγματικά είναι από τη φίλη μου (π.χ. αφού της τηλεφωνήσω ή της στείλω ένα **e-mail**).

β) Πατάω στο **link** άφοβα (αφού μου το στέλνει η φίλη μου)

γ) Συνήθως πατάω ανάλογα με το **link** - κρίνω κατά περίπτωση (αυτό το **link** φαίνεται ενδιαφέρον, αφού είναι εικόνα, αλλά γενικά προσέχω)

Ερώτηση 6:

Μία σοβαρή εταιρεία αποκλείεται να σου ζητήσει να της στείλεις με **e-mail** κρίσιμα προσωπικά σου δεδομένα (όπως π.χ. κωδικούς).

α) Αλήθεια

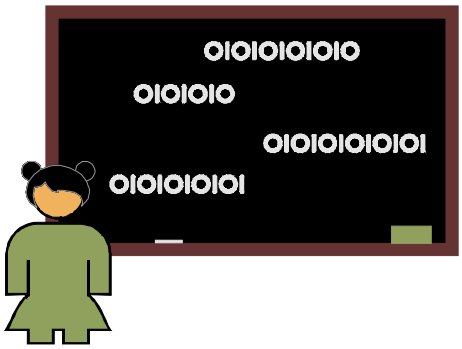
β) Ψέματα

γ) Ίσως

ΑΠΟΤΕΛΕΣΜΑΤΑ

1. β
2. α
3. γ
4. α
5. α
6. α

Εκπαιδευτικό υλικό



Το υλικό που προτείνουμε παρακάτω μπορεί να βοηθήσει στην ενημέρωση των μαθητών για το ζήτημα της πλαστοπροσωπίας στο διαδίκτυο με συγκεκριμένα θέματα συζήτησης και προβληματισμού στην τάξη, καθώς και με χρήση διαδραστικών εργαλείων όπως κουίζ και βίντεο.

Εκπαιδευτική ενότητα: «Γνωρίζω με ποιον μιλώ»

Γενική περιγραφή

Σκοπός της ενότητας αυτής είναι:

1. να κατανοήσουν οι μαθητές τους κινδύνους που απορρέουν από τις δυνατότητες που δίνει το διαδίκτυο (μέσω εφαρμογών όπως **e-mail, instant messaging, blogs, chat, forums,** διαδικτυακά παιχνίδια... κτλ.) για απόκρυψη της πραγματικής ταυτότητας κάποιου.
2. να μάθουν με κάποιες απλές πρακτικές συμβουλές πώς μπορούν να αποφεύγουν κινδύνους που σχετίζονται με πλαστή ταυτότητα.
3. να μάθουν να «ανιχνεύουν» τα **phishing** μηνύματα.

Προτεινόμενη δομή ενημέρωσης

1. Ενημέρωση για θέματα πλαστής/κλοπής ταυτότητας στο διαδίκτυο (από τις σελίδες «Ποιός στα αλήθεια είναι;» και «Γνωριμίες στο διαδίκτυο»)
2. Ενημέρωση για μηνύματα **phishing** και το κακόβουλο λογισμικό (από τη σελίδα «Ψάρεμα στο διαδίκτυο»)
3. Ενημέρωση για τους κινδύνους που ελλοχεύουν στα διαδικτυακά παιχνίδια (από τη σελίδα «Επικίνδυνα... παιχνίδια;»)
4. Στατιστικά και παραδείγματα (από τη σελίδα «Οι αριθμοί μιλούν»)
5. Πρακτικές συμβουλές (από τη σελίδα «Συμβουλές»)

Προτάσεις για συζήτηση / ανταλλαγή απόψεων

Μπορείτε να θέσετε τις παρακάτω ερωτήσεις στην τάξη και να ζητήσετε τις απόψεις-εμπειρίες των μαθητών:

- Τι πληροφορία για τον εαυτό σας δεν θα περιλαμβάνατε ποτέ στο προφίλ σας;
  - και τι στην προσωπική σας ιστοσελίδα ή όταν «κάνετε» **chat;**
- Έχετε ποτέ μιλήσει με κάποιον στο διαδίκτυο του οποίου δεν γνωρίζατε την

ταυτότητα στην πραγματική του ζωή;
  - πιστεύετε ότι κάποιος από αυτούς χρησιμοποιούσε ψεύτικη ταυτότητα;
  - παίρνετε προφυλάξεις για να βεβαιωθείτε ότι το πρόσωπο στο οποίο μιλάτε δεν ψεύδεται για το ποιος/ποια είναι;

- Βρίσκετε ότι είναι πιο εύκολο να προσβάλετε κάποιον στο διαδίκτυο όταν δεν γνωρίζεστε;
  - βρίσκετε όμως ότι είναι πιο αποδεκτό;

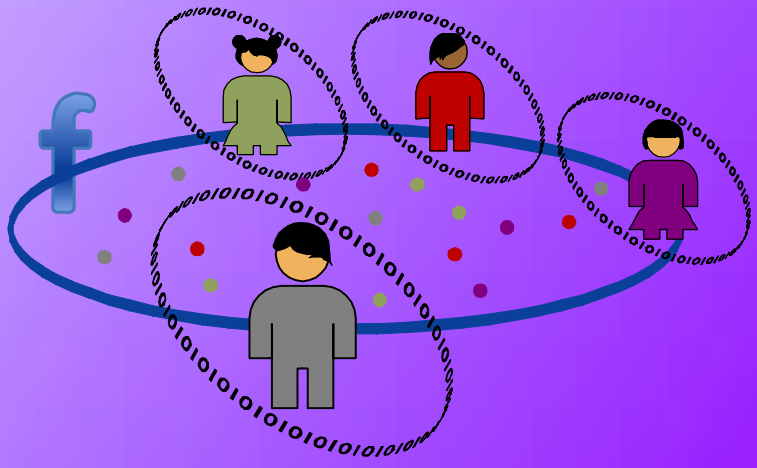
- Είναι σωστό να κανονίσετε συνάντηση με κάποιον που γνωρίσατε μέσω διαδικτύου;
  - φτιάξτε μια λίστα με προφυλάξεις που πρέπει να πάρετε αν πρόκειται να πάτε σε τέτοια συνάντηση.

- Μπορεί να υπάρχουν καλοί λόγοι για να κρύψετε την ταυτότητά σας όταν είστε **online**; Υπάρχουν περιπτώσεις που προσποιείστε ότι είστε κάποιος άλλος;
  - τι είδους ψεύτικη πληροφορία έχετε δώσει για τον εαυτό σας;

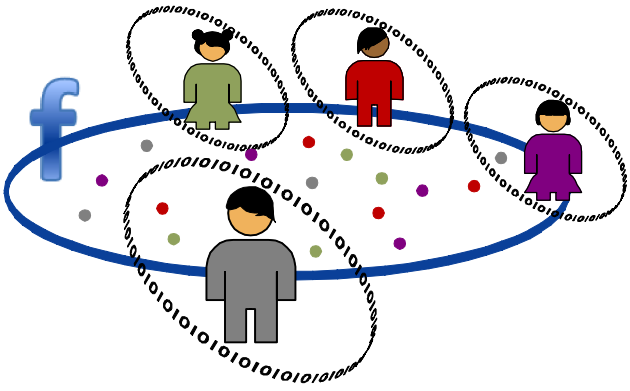
Συζήτηση σχετικά με το αν παίζουν διαδικτυακά παιχνίδια οι μαθητές, ποια είναι αυτά, πόση ώρα αφιερώνουν, με ποιους/πόσους διαδικτυακούς παίκτες μιλάνε. Επίσης συζήτηση για το αν χρησιμοποιούν **chat**, **blogs** και ποια.

Συζήτηση σχετικά με το αν γνωρίζουν πώς να προστατεύουν τους προσωπικούς τους υπολογιστές από κακόβουλο λογισμικό.

"Δικτυώνομαι" με ασφάλεια



Είναι όλοι φίλοι σου;



Εκατομμύρια άνθρωποι στον κόσμο χρησιμοποιούν σήμερα υπηρεσίες κοινωνικής δικτύωσης **(**ή αλλιώς κοινωνικά δίκτυα**),** όπως το **Facebook,** το **Twitter** ή το **MySpace,** για να επικοινωνούν μεταξύ τους**.**

Οι υπηρεσίες αυτές σου επιτρέπουν να μοιράζεσαι πληροφορίες με πολλούς ανθρώπους γρήγορα και εύκολα**...**

Μπορείς να ανεβάσεις τις φωτογραφίες ή τα **video** των διακοπών σου όσο είσαι ακόμα στο νησί από το κινητό σου**!** Και μπορείς να ελέγξεις τα προφίλ των φίλων σου και να διαβάσεις τα μηνύματα και τα σχόλιά τους**.**

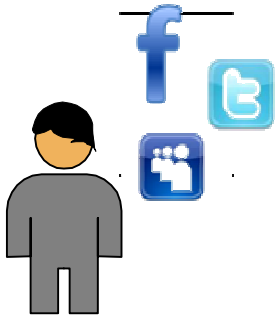
Μήπως όμως οι πληροφορίες σου είναι τελικά διαθέσιμες σε πολλούς περισσότερους από όσους πραγματικά θα ήθελες**;** Μήπως κάποιες θα προτιμούσες να μην τις είχες ποτέ δημοσιοποιήσει**;**

Είσαι σίγουρος ότι είναι όλοι **«**φίλοι**»** σου**;**

Πριν δημιουργήσεις ένα καινούργιο προφίλ στο **Facebook** ή πριν ανεβάσεις μια φωτογραφία ή ανακοινώσεις σε όλο τον κόσμο τι κάνεις αυτή τη στιγμή**,** αναρωτήσου πόσο ασφαλής θα είσαι αν το κάνεις**...**

Αν δεν είσαι προσεκτικός μπορεί να βάζεις την ιδιωτική σου ζωή ή ακόμα και την προσωπική σου ασφάλεια σε κίνδυνο**...**

Λίγα λόγια για τις υπηρεσίες κοινωνικής δικτύωσης



Σε μια υπηρεσία κοινωνικής δικτύωσης **(social network)** μπορείς να **«**ανεβάζεις**»** πληροφορίες, φωτογραφίες και **video**, να κρατάς επαφή με τους φίλους σου και να γνωρίζεις άτομα που έχουν τα ίδια ενδιαφέροντα με εσένα. Η πιο δημοφιλής υπηρεσία κοινωνικής δικτύωσης παγκοσμίως **(**και στην Ελλάδα**)** είναι το **Facebook**.

Διάβασε και μάθε για τις υπηρεσίες κοινωνικής δικτύωσης με τις παρακάτω ερωτήσεις - απαντήσεις.

Πώς λειτουργεί μια υπηρεσία κοινωνικής δικτύωσης;

Η λειτουργία μιας τέτοιας υπηρεσίας βασίζεται στα **«**προφίλ**»** των χρηστών της. Μπορείς να δημιουργήσεις ένα προφίλ, καταχωρώντας προσωπικά σου δεδομένα, όπως το όνομά σου, τη διεύθυνση ηλεκτρονικού ταχυδρομείου **(e-mail)**, καθώς και άλλες προαιρετικές πληροφορίες, όπως ενδιαφέροντα, προσωπική κατάσταση, εργασία, φίλοι, κλπ. Η υπηρεσία κοινωνικής δικτύωσης σου παρέχει συνήθως τη δυνατότητα να μοιράζεσαι δεδομένα με παλιούς και νέους φίλους, ανάλογα με τις επιλογές που κάνεις στο προφίλ σου.

Στις περισσότερες περιπτώσεις οι υπηρεσίες κοινωνικής δικτύωσης παρέχονται δωρεάν στους χρήστες. Η χρηματοδότησή τους γίνεται από δίκτυα διαφημίσεων, τα οποία, σε αντάλλαγμα, μπορούν να μεταδίδουν στοχευμένες διαφημίσεις στους χρήστες βάσει των προφίλ τους.

Ποιοι είναι οι κίνδυνοι από τη χρήση υπηρεσιών κοινωνικής δικτύωσης;

Όταν δημοσιοποιείς προσωπικά δεδομένα στο διαδίκτυο, υπάρχει πάντα ο κίνδυνος αυτή η πληροφορία να **«**διαβαστεί**»** από κάποιους που δεν θέλεις ή να πέσει σε λάθος χέρια. Η πληροφορία του προφίλ σου σε μια υπηρεσία κοινωνικής δικτύωσης μπορεί να αποκαλύπτει πολλά προσωπικά σου στοιχεία, όπως λεπτομέρειες της ζωής σου ή φωτογραφίες από ιδιωτικές σου στιγμές. Και είναι όλη συγκεντρωμένη σε ένα και μοναδικό σημείο στο διαδίκτυο**...**

Είναι δυνατό κάποιος να υποκλέψει το προφίλ μου;

Είναι πολύ εύκολο για κάποιον να **«**κατεβάσει**»** και να αποθηκεύσει προφίλ χρηστών. Αρκεί να τον κάνεις φίλο σου ή να είναι φίλος κάποιου φίλου σου **(**ή ίσως να μην απαιτείται ούτε καν αυτό**)...** κι εσύ να μην έχεις κάνει τις απαιτούμενες ρυθμίσεις ασφάλειας στο προφίλ σου.

Κι αν σβήσω τελείως το προφίλ μου;

Ακόμα κι αν σβήσεις πληροφορία από το προφίλ σου ή κι αν διαγράψεις ολόκληρο το προφίλ, δεν μπορείς να είσαι σίγουρος ότι η πληροφορία έχει διαγραφεί εντελώς από το διαδίκτυο. Για παράδειγμα, το **Facebook** διατηρεί όλο το προφίλ σου - ακόμα και μετά τη διαγραφή - για την περίπτωση που ζητήσεις ξανά να γίνεις μέλος του.

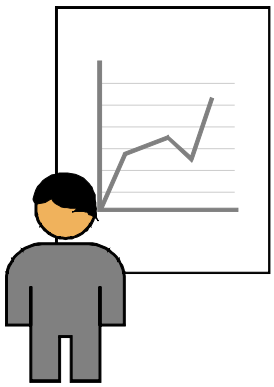
Μπορεί κάποιος να υποδυθεί ότι είμαι εγώ;

Φυσικά. Αν φτιάξει ένα ψεύτικο δικό σου προφίλ... Κι αν εσύ ποτέ δεν το ελέγξεις...

Σε ποιόν ανήκουν τα δεδομένα του προφίλ μου;

Όταν δημιουργήσεις ένα προφίλ, επιτρέπεις στην υπηρεσία κοινωνικής δικτύωσης να διατηρεί όλες τις πληροφορίες που καταχωρείς και να τις χρησιμοποιεί, π.χ. για διαφήμιση. Αυτό μπορεί να ισχύει ακόμα και όταν διαγράψεις το προφίλ σου, ανάλογα με τα αναφερόμενα στους όρους χρήσης της υπηρεσίας. Πρόσεξε ότι το **Facebook** διατηρεί το δικαίωμα να αλλάζει τους όρους χρήσης της υπηρεσίας του, όποτε το επιθυμεί...

Οι αριθμοί μιλούν...



Το **57%** των παιδιών ηλικίας **9-16** ετών στην Ευρώπη έχουν προφίλ σε πλατφόρμα κοινωνικής δικτύωσης, ενώ αυτό ισχύει για το **24%** των παιδιών μεταξύ **9-10** ετών, το **48%** των παιδιών **11-12** ετών, το **72%** όσων είναι **13-14** ετών και το **81%** όσων είναι **15-16** ετών. Αξίζει να σημειωθεί ότι στους όρους χρήσης του **Facebook** αναφέρεται ότι η εγγραφή στην υπηρεσία επιτρέπεται μόνο για άτομα άνω των **13** ετών.

Η κοινωνική δικτύωση είναι πιο δημοφιλής μεταξύ των νέων στην Ολλανδία **(78%)**, τη Σλοβενία **(76%)**, τη Λιθουανία **(75%)**, και λιγότερο δημοφιλής στη Ρουμανία και την Τουρκία. Το ποσοστό κοινωνικής δικτύωσης στην Ελλάδα είναι **54%**. Το **29%** έχει περισσότερες από **100** επαφές, ενώ πολλοί έχουν λιγότερες.

Ανάμεσα σε όσους έχουν προφίλ σε πλατφόρμες κοινωνικής δικτύωσης, το **29%** έχει δημόσιο προφίλ (ανοικτό) και αυτό συμβαίνει κυρίως στην Ουγγαρία **(53%)**, την Τουρκία **(45%)** και τη Ρουμανία **(44%)** και σε μικρότερο βαθμό στη χώρα μας **(37%)**.

Πηγή: Έρευνα του Δικτύου ***EU Kids Online*** **(http://www.eukidsgreece.gr/)**

Έχει συμβεί...

Παρακάτω αναφέρονται λίγα μόνο από τα πολλά σενάρια που εύκολα έγιναν πραγματικές ιστορίες...

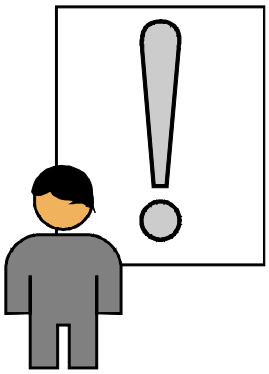
- Η Μαρία είναι νέος χρήστης του **Facebook**. Στο προφίλ της έχει βάλει διάφορα στοιχεία, όπως την ημερομηνία γέννησής της και διάφορες φωτογραφίες της. Μια μέρα κάνει κατά λάθος **«φίλο»** κάποιον που δεν γνωρίζει, αλλά δεν δίνει ιδιαίτερη σημασία στο συμβάν. Την επόμενη μέρα δεν μπορεί να εισέλθει στο λογαριασμό της. Διαπιστώνει όμως πως κάποιος χρησιμοποιεί το προφίλ της προσποιούμενος ότι είναι η ίδια, συνομιλεί και στέλνει μηνύματα στους φίλους της. Τρομάζει και αναρωτιέται πώς έγινε η υποκλοπή του λογαριασμού της. Μήπως φταίει ότι το συνθηματικό που χρησιμοποιούσε ήταν η ημερομηνία γέννησής της; Και μήπως δεν θα έπρεπε να κάνει **«φίλους»** άτομα που δεν γνωρίζει;

- Ο Αντώνης είναι **«τρελός»** για την Ελένη. Δεν μπορεί να αντέξει το γεγονός ότι τον χώρισε. Για να την εκδικηθεί δημιουργεί ανοικτό πλαστό προφίλ στο όνομα της και δημοσιεύει αποκαλυπτικές φωτογραφίες της. Η Ελένη ενημερώνεται από φίλους της μια βδομάδα αργότερα και απευθύνεται στην Ασφάλεια. Το προφίλ τελικά διαγράφεται, αλλά το κακό για την Ελένη έχει ήδη γίνει...

- Ο Γιώργος διασκεδάζει πολύ ανεβάζοντας φωτογραφίες από τα πάρτυ στο **Facebook**. Κάποιες είναι πολύ αστείες, όπως αυτή που μεθυσμένος βγάζει τα ρούχα του χορεύοντας πάνω στο μπαρ. Δεν είχε φανταστεί βέβαια ότι την φωτογραφία αυτή θα την έβλεπε ο φίλος του πατέρα του... Μήπως δεν έπρεπε να ανεβάσει όλες εκείνες τις φωτογραφίες; Και μήπως δεν έπρεπε το προφίλ του στο **Facebook** να είναι ανοικτό σε όλους;

- Η Ειρήνη είναι τακτικός χρήστης του **Facebook**. Της αρέσει να ενημερώνει συνεχώς τους φίλους της για το πού βρίσκεται και τι κάνει. Χθες το βράδυ έγραψε ότι ήταν μόνη στο σπίτι. Ο Βαγγέλης και ο Χάρης σκέφτηκαν ότι ήταν ευκαιρία για πλάκα κι έτσι πέρασαν από εκεί και της χτυπούσαν επίμονα το κουδούνι. Η Ειρήνη τρόμαξε. Δεν είναι λίγο να σε ενοχλεί κάποιος έτσι τα μεσάνυχτα...

Συμβουλές



Τα κοινωνικά δίκτυα είναι πλέον μέρος της καθημερινότητάς σου. Μάθε λοιπόν να τα χρησιμοποιείς με ασφάλεια:

- **Σκέψου πριν «ανεβάσεις»:** Πριν δημοσιοποιήσεις μια φωτογραφία, ένα βίντεο ή απλά τις απόψεις σου στο προφίλ σου, σκέψου την εντύπωση που θα προκαλέσεις. Θα έκανες το ίδιο στον πραγματικό κόσμο; Πώς θα ένιωθες αν έβλεπαν αυτά τα δεδομένα οι γονείς σου, οι καθηγητές σου ή ένας πιθανός εργοδότης σου; Μήπως, τελικά, είναι πολύ λίγα τα άτομα με τα οποία θα μοιραζόσουν αυτά τα δεδομένα;

- **Πρόσεξε τι «ανεβάζεις» για τους άλλους:** Πριν ανεβάσεις οποιαδήποτε πληροφορία που μπορεί να περιλαμβάνει δεδομένα και άλλων ατόμων **(**π.χ. φωτογραφίες φίλων σου**)**, φρόντισε να έχεις ενημερώσει τα άτομα αυτά και να σου έχουν πει ότι συμφωνούν. Έχε πάντα στο μυαλό σου ότι δεν πρέπει να εκθέτεις προσωπικά δεδομένα άλλων ατόμων χωρίς τη συγκατάθεσή τους.

- **Ενεργοποίησε τις ρυθμίσεις απορρήτου (privacy settings) στο λογαριασμό σου:** Οι ρυθμίσεις απορρήτου σου επιτρέπουν να ελέγχεις τι μπορούν να δουν οι άλλοι για σένα. Έλεγξε το επίπεδο των ρυθμίσεων αυτών για το προφίλ σου. Μήπως οι ρυθμίσεις είναι τέτοιες που επιτρέπουν σε όλους να έχουν πρόσβαση στις πληροφορίες σου; Προσπάθησε να επιλέξεις όσο το δυνατόν αυστηρότερες ρυθμίσεις **(**π.χ. μόνο οι φίλοι σου να μπορούν να δουν το αναλυτικό προφίλ σου και όχι οι φίλοι των φίλων σου**...)**. Θυμήσου ότι δεν μπορείς να πάρεις πίσω την πληροφορία όταν κάποιος την έχει δει**...** ενώ μπορείς πάντα να δώσεις περισσότερη πληροφορία όταν θα νιώθεις πιο άνετα με κάποιον. Μάθε περισσότερα για τις ρυθμίσεις απορρήτου στο **Facebook** στην αντίστοιχη ενότητα στη συνέχεια.

- **Έλεγχε την πολιτική ιδιωτικότητας και τους όρους χρήσης:** Πριν εγγραφείς σε οποιοδήποτε υπηρεσία κοινωνικής δικτύωσης, διάβασε προσεκτικά την πολιτική ιδιωτικότητας και τους όρους χρήσης **(**συνήθως υπάρχει κάποιος σύνδεσμος **- link** στο κάτω μέρος της κεντρικής σελίδας**)**. Μήπως υπάρχει κάποιος κρυφός όρος για διαβίβαση των προσωπικών σου στοιχείων σε διαφημιστικές εταιρείες; Διάβασε για παράδειγμα για το **Facebook: http://el-gr.facebook.com/terms.php?ref=pf**

- **Να είσαι επιφυλακτικός με άτομα που δεν ξέρεις:** Κάποιες πληροφορίες σου μπορεί να χρησιμοποιηθούν από άλλους για να σου κάνουν κακό. Μην αποκαλύπτεις τη διεύθυνσή σου, τον τηλεφωνικό σου αριθμό, την ημέρα γέννησής σου ή τον τόπο εργασίας σου στο προφίλ σου. Πρόσεχε πολύ ποιους κάνεις **«**φίλους**»** σου.

- **Χρησιμοποίησε ασφαλές συνθηματικό για το λογαριασμό σου:** Προσπάθησε να αποφεύγεις συνθηματικά που μπορούν εύκολα να μαντέψουν οι άλλοι. Επίσης, προσπάθησε να μην χρησιμοποιείς συνθηματικά που ήδη έχεις σε κάποιες άλλες υπηρεσίες, όπως π.χ. το λογαριασμό ηλεκτρονικού ταχυδρομείου σου. Αν μπορείς χρησιμοποίησε μία ξεχωριστή διεύθυνση **e-mail** ειδικά για το προφίλ σου, ώστε να μη χρειάζεται να δίνεις τα άλλα στοιχεία επικοινωνίας σου.

- **Ανάφερε περιστατικά παραβίασης του προφίλ σου ή του προφίλ κάποιου φίλου σου:** Μάθε πώς μπορείς να το κάνεις για το **Facebook** στην αντίστοιχη ενότητα στη συνέχεια.

Ρυθμίσεις απορρήτου στο Facebook

Για να καθορίσεις τις ρυθμίσεις απορρήτου στο **Facebook**, πήγαινε στο λογαριασμό σου **(account) -** ρυθμίσεις απορρήτου **(privacy settings).** Στη σελίδα αυτή μπορείς να ελέγξεις τις ρυθμίσεις που αφορούν:

- Κοινοποίηση στο **Facebook**: Από αυτήν την ενότητα ελέγχεις ποιος **(**π.χ. όλοι**,** μόνο οι φίλοι σου**,** οι φίλοι των φίλων σου**,** κ.ο.κ**)** μπορεί να δει όλο το περιεχόμενο που δημοσιεύεις σε καθημερινή βάση **(**π.χ. ενημερώσεις κατάστασης**,** φωτογραφίες και βίντεο**).** Επίσης**,** αυτή η ενότητα περιλαμβάνει κάποια πράγματα που κοινοποιείς σχετικά με τον εαυτό σου **(**γενέθλια και στοιχεία επικοινωνίας**),** καθώς και περιεχόμενο που κοινοποιούν οι άλλοι για εσένα **(**σχόλια σε δημοσιεύσεις σου**,** καθώς και φωτογραφίες ή βίντεο όπου εμφανίζεσαι**).** Με την επιλογή **«**Προσαρμογή ρυθμίσεων**»** εμφανίζεται μια πλήρης λίστα**,** ώστε να ελέγχεις το επίπεδο προσωπικού απορρήτου σε κάθε κατηγορία πληροφοριών**.**

- Σύνδεση μέσω **Facebook**: Στην ενότητα αυτή μπορείς να ρυθμίζεις ποιες λειτουργίες μέσω **Facebook (**π.χ. δυνατότητα να σου στέλνουν μηνύματα**,** δυνατότητα να σε βρίσκουν μέσα από το **Facebook**, κ.ο.κ**)** μπορούν να είναι ενεργοποιημένες για το προφίλ σου και για ποιους **(**π.χ. όλους**,** μόνο τους φίλους σου**,** κ.ο.κ**).** Πρόσεξε ότι οι λειτουργίες αυτές είναι από προεπιλογή ενεργοποιημένες και διαθέσιμες για όλους. Αν θες αυτό να το αλλάξεις**,** μπορείς να το κάνεις μέσω της συγκεκριμένης ενότητας**.** Πρόσεξε επίσης ότι κάποια στοιχεία σου είναι υποχρεωτικά διαθέσιμα σε όλους και δεν μπορείς αυτό να το αλλάξεις. Τα στοιχεία αυτά είναι: όνομα**,** φωτογραφία προφίλ**,** φύλο και δίκτυα**.**

- Εφαρμογές και Ιστοσελίδες: Το τμήμα αυτό ελέγχει ποιες πληροφορίες κοινοποιούνται σε ιστοσελίδες και εφαρμογές**,** περιλαμβανομένων των μηχανών αναζήτησης**.** Πρόσεξε ότι από προεπιλογή όλες οι εφαρμογές και ιστοσελίδες που εσύ και οι φίλοι σου χρησιμοποιείτε έχουν ήδη πρόσβαση στο όνομά σου**,** την φωτογραφία προφίλ**,** το φύλο**,** τα δίκτυα**,** τον κατάλογο των φίλων σου και οποιεσδήποτε άλλες πληροφορίες μοιράζεσαι με όλους. Αν θέλεις αυτό να το αλλάξεις**,** θα πρέπει να μπεις στη συγκεκριμένη σελίδα και να επιλέξεις τις ρυθμίσεις που επιθυμείς για κάθε εφαρμογή**.**

- Λίστες αποκλεισμού: Σε αυτήν την ενότητα μπορείς να αποκλείσεις άτομα**,** ώστε να μην έχουν επαφή μαζί σου ή να μην βλέπουν τις πληροφορίες σου στο **Facebook.** Μπορείς επίσης να ορίσεις τους φίλους που θα αγνοείς όταν σου στέλνουν προσκλήσεις για εφαρμογές**,** καθώς και να δεις μια λίστα εφαρμογών στις οποίες δεν επιτρέπεις να έχουν πρόσβαση στις πληροφορίες σου και να επικοινωνούν μαζί σου**.**

Δώσε επίσης προσοχή στα εξής:

- **Έλεγξε κάθε δημοσίευσή σου**: Μπορείς να ελέγχεις ποιος βλέπει κάθε δημοσίευση σου. Πριν δημοσιεύσεις μια ενημέρωση κατάστασης**,** ένα σύνδεσμο**,** ένα άλμπουμ φωτογραφιών σου ή οτιδήποτε άλλο**,** κάνε κλικ στο εικονίδιο λουκέτου για να επιλέξεις ποιος μπορεί να δει το περιεχόμενο. Πρόσεξε ότι μπορείς να επιλέξεις να γίνει η δημοσίευση ακόμα και σε συγκεκριμένα άτομα **(**και όχι στο σύνολο των φίλων σου**).**

- **Έλεγχε τις ετικέτες (tags) με τις οποίες εμφανίζεσαι**: Εσύ ελέγχεις ποιος μπορεί να δει τις φωτογραφίες και τα βίντεο με τις ετικέτες σου**,** τα οποία εμφανίζονται στο προφίλ σου. Θα πρέπει να γνωρίζεις ότι ο κάτοχος μιας φωτογραφίας μπορεί ακόμη να μοιράζεται τη φωτογραφία αυτή με άτομα που δεν είναι φίλοι σου. Αν δεν θέλεις να εμφανίζεσαι με ετικέτα**,** αφαίρεσέ τη από τη φωτογραφία ή από το βίντεο. Έτσι**,** δεν θα εμφανίζεται ούτε στο προφίλ σου**.**

- **Προστάτευσε τον κατάλογο ηλεκτρονικών διευθύνσεων των φίλων σου:** Κατά την εγγραφή σου, το **Facebook** ζητά να «κατεβάσει» τον κατάλογο διευθύνσεων ηλεκτρονικού ταχυδρομείου σου (π.χ. από τον λογαριασμό σου στο **Hotmail, Yahoo** ή άλλες συχνά χρησιμοποιούμενες υπηρεσίες **e-mail** χρησιμοποιείς). Στη συνέχεια μπορεί να χρησιμοποιήσει τις διευθύνσεις αυτές για να στείλει μηνύματα σε φίλους σου (π.χ. πρόσκληση να γίνουν κι εκείνοι χρήστες του **Facebook** αν δεν είναι ήδη). Απενεργοποίησε αυτή τη δυνατότητα. Σκέψου ότι κάποιοι φίλοι σου μπορεί να μην ήθελαν το **Facebook** να έχει το **e-mail** τους και να τους στέλνει μηνύματα (ειδικά αν δεν είναι οι ίδιοι χρήστες του **Facebook**).

Διάβασε περισσότερα και δες σχετικές οδηγίες και βίντεο στο **Facebook:** **http://el-gr.facebook.com/privacy/explanation.php**.

Δες περισσότερες οδηγίες από την ιστοσελίδα της Ομάδας Δράσης για την Ψηφιακή Ασφάλεια **(DART): http://kids.dart.gov.gr/kidsdefault.aspx**.

Αναφορά περιστατικού παραβίασης στο Facebook

Αν διαπιστώσεις ότι κάποιος έχει δημιουργήσει ένα ψευδές προφίλ για εσένα ή ότι κάποιος έχει υποκλέψει το προφίλ σου, μπορείς να το αναφέρεις στο **Facebook** ως εξής: μπαίνεις στο ψευδές προφίλ και πατάς το κουμπί **«**Αναφορά**/**αποκλεισμός ατόμου**» (Report/block this person)** που βρίσκεται στο κάτω μέρος της αριστερής στήλης**.**

Εναλλακτικά**,** μπορείς να αναφέρεις το περιστατικό στο **email login [at] facebook [dot] com.**

Διάβασε περισσότερα και δες σχετικές οδηγίες στο **Facebook:**

http://www.facebook.com/help/?search=report+fake+profile

Πώς μπορεί να σε βοηθήσει η Αρχή

Σε περίπτωση που θέλεις να διαγράψεις προσωπικά δεδομένα από το προφίλ σου, συμβουλεύσου πρώτα τις οδηγίες χρήσης της υπηρεσίας κοινωνικής δικτύωσης. Αν χρειάζεσαι περισσότερη βοήθεια, επικοινώνησε με την Αρχή για να σε κατευθύνει σχετικά.

Αν θέλεις να διαγράψεις προσωπικά σου δεδομένα που είναι αναρτημένα σε προφίλ άλλου ατόμου, προσπάθησε πρώτα να επικοινωνήσεις με το άτομο αυτό και να του το ζητήσεις. Αν το πρόβλημα συνεχίζεται, μπορείς να επικοινωνήσεις με την Αρχή για περαιτέρω βοήθεια.

Στοιχεία επικοινωνίας με την Αρχή:

Ταχυδρομική Διεύθυνση:

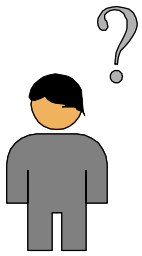
Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Γραφεία: Κηφισίας **1-3**, Τ.Κ. **115 23**, Αθήνα

Τηλεφωνικό Κέντρο: +30 210 6475600

Ηλεκτρονικό Ταχυδρομείο: contact@dpa.gr

Αν διαπιστώσεις ότι κάποιος έχει υποκλέψει το προφίλ σου ή έχει δημιουργήσει ένα ψεύτικο προφίλ με τα στοιχεία σου, ενημέρωσε αμέσως τους φίλους σου και ανάφερε αμέσως το περιστατικό στην υπηρεσία κοινωνικής δικτύωσης **(**δες τις Συμβουλές για το **Facebook)**. Αν το πρόβλημα παραμένει μπορείς να επικοινωνήσεις με την Αρχή για να σε βοηθήσει. Επίσης, μπορείς να αναφέρεις το περιστατικό στην αστυνομία **(**Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος**)** για περαιτέρω ενέργειες.

Κουίζ



Επίλεξε την απάντηση που θεωρείς σωστή **(**Σωστό ή Λάθος**).**
Έλεγξε στο τέλος πόσο καλά τα πήγες**!**

Ερώτηση 1:

Το προφίλ σου σε μία υπηρεσία κοινωνικής δικτύωσης είναι αρχικά ρυθμισμένο έτσι ώστε να μπορούν να το βλέπουν μόνο οι φίλοι σου. Έτσι, είσαι σίγουρος ότι τα προσωπικά σου δεδομένα είναι απόλυτα ασφαλή.

α) Σωστό

β) Λάθος

Ερώτηση 2:

Ο κολλητός σου κάνει πάρτυ αυτό το σαββατοκύριακο και όλοι οι φίλοι σας είναι καλεσμένοι. Σου φαίνεται ωραία ιδέα να ανεβάσεις την ημερομηνία, ώρα και μέρος στο προφίλ σου, ώστε όλοι να δουν εύκολα τις πληροφορίες.

α) Σωστό

β) Λάθος

Ερώτηση 3:

Κάποιοι φίλοι σου θεωρούν πολύ καλό να έχουν εκατοντάδες **«**φίλους**»** στο προφίλ τους στο **Facebook.** Μερικές φορές σου ζητούν να γίνεται **«**φίλοι**» (friend request)** άτομα που δεν ξέρεις. Συνήθως όμως είσαι επιφυλακτικός και προτιμάς να απορρίπτεις αυτά τα αιτήματα και ας μην έχεις τόσο πολλούς **«**φίλους**».**

α) Σωστό

β) Λάθος

Ερώτηση 4:

Μπορείς πάντα να έχεις τον έλεγχο των φωτογραφιών που **«**ανεβάζεις**»** στο προφίλ σου.

α) Σωστό

Λάθος

Ερώτηση 5:

Κάποιος έχει δημιουργήσει ένα ψεύτικο προφίλ με το όνομα σου. Σκέφτεσαι ότι πρέπει να κάνεις κάτι άμεσα γι' αυτό.

α) Σωστό

β) Λάθος

ΑΠΟΤΕΛΕΣΜΑΤΑ

Ερώτηση 1:

Λάθος ! Η πληροφορία που δημοσιεύεις δεν είναι ποτέ απόλυτα ασφαλής. Ακόμα κι αν έχεις επιλέξει τις αυστηρότερες ρυθμίσεις απορρήτου, τα προσωπικά σου δεδομένα είναι διαθέσιμα στους φίλους σου. Πρόσεχε πάντα τι δημοσιεύεις! Και πρόσεχε ποιους θεωρείς «φίλους» στο διαδίκτυο!

Ερώτηση 2:

Λάθος ! Αντί να δημοσιεύσεις την πληροφορία στο προφίλ σου, προτίμησε να στείλεις μήνυμα σε όσους φίλους είναι καλεσμένοι. Σκέψου ότι η έννοια του «φίλου» στο **Facebook** δεν είναι ίδια με το φίλο στην ζωή. Και δεν θα ήθελες να έρθουν στο πάρτυ ανεπιθύμητοι καλεσμένοι...

Ερώτηση 3:

Σωστό ! Όσο πιο πολλές σχέσεις έχεις με κάποιον στον πραγματικό κόσμο, τόσο πιο σίγουρος μπορείς να είσαι γι' αυτόν όταν μοιράζεσαι μαζί του πληροφορίες. Θυμήσου ότι υπάρχουν απατεώνες με ψεύτικα προφίλ που προσπαθούν να υποκλέψουν προσωπικές σου πληροφορίες. Στο διαδίκτυο δεν είσαι ποτέ **100%** σίγουρος με ποιόν «μιλάς», οπότε αν δεν ξέρεις αρκετά καλά το άτομο που σου κάνει αίτημα φιλίας, προτίμησε να μην το δεχτείς.

Ερώτηση 4:

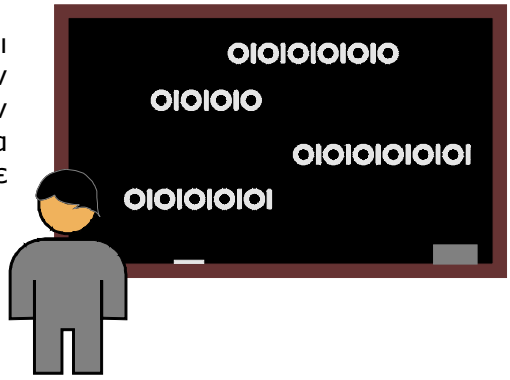
Λάθος ! Όταν «ανεβάζεις» φωτογραφίες στο προφίλ σου ή σε οποιαδήποτε άλλη ιστοσελίδα ίσως να δίνεις το δικαίωμα σε άλλους να τις κατεβάζουν χωρίς την έγκρισή σου και πιθανά να τις αλλοιώνουν με τρόπο που σε προσβάλει! Πρόσεχε πάντα ποιες φωτογραφίες δημοσιεύεις και ποιοι έχουν πρόσβαση σε αυτές!

Ερώτηση 5:

Σωστό ! Όταν διαπιστώσεις παραβίαση του προφίλ σου πρέπει αμέσως να αναφέρεις το περιστατικό στην υπηρεσία κοινωνικής δικτύωσης και να ενημερώσεις τους φίλους σου. Αν το πρόβλημα δεν επιλύεται, επικοινώνησε με την Αρχή Προστασίας Δεδομένων για να σε βοηθήσει.

Εκπαιδευτικό υλικό

Το υλικό που προτείνουμε παρακάτω μπορεί να βοηθήσει στην ενημέρωση των μαθητών για την προστασία των προσωπικών τους δεδομένων κατά τη χρήση υπηρεσιών κοινωνικής δικτύωσης με συγκεκριμένα θέματα συζήτησης και προβληματισμού στην τάξη, καθώς και με χρήση διαδραστικών εργαλείων όπως κουίζ και βίντεο.



Εκπαιδευτική ενότητα: «Δικτυώνομαι με ασφάλεια»

Γενική περιγραφή

Σκοπός της ενότητας αυτής είναι:

Α) να κατανοήσουν οι μαθητές τους κινδύνους από τη χρήση των υπηρεσιών κοινωνικής δικτύωσης,

Β) να μάθουν με κάποιες απλές πρακτικές συμβουλές πώς μπορούν να κάνουν χρήση αυτών των υπηρεσιών με ασφάλεια. Ιδιαίτερη έμφαση δίνεται στο **Facebook** ειδικά ως προς το θέμα των ρυθμίσεων απορρήτου και της αναφοράς περιστατικών παραβίασης προφίλ.

Προτεινόμενη δομή ενημέρωσης

1. Εισαγωγή στις υπηρεσίες κοινωνικής δικτύωσης: τι είναι, ποιους αφορά, κλπ. **(**από τις σελίδες **«**Είναι όλοι φίλοι σου;**»** και **«**Λίγα λόγια για τις υπηρεσίες κοινωνικής δικτύωσης**»).**

2. Κίνδυνοι κατά τη χρήση υπηρεσιών κοινωνικής δικτύωσης **-** συγκεκριμένα παραδείγματα **(**από τις σελίδες **«**Λίγα λόγια για τις υπηρεσίες κοινωνικής δικτύωσης**»** και **«**Έχει συμβεί**»).**

3. Πρακτικές συμβουλές γενικά για τη χρήση των υπηρεσιών κοινωνικής δικτύωσης **(**από τις σελίδες **«**Συμβουλές**»** και **«**Πώς μπορεί να σε βοηθήσει η Αρχή**»).**

4. Πρακτικές συμβουλές ειδικά για τις ρυθμίσεις απορρήτου και την αναφορά παραβίασης λογαριασμού στο **Facebook -** με χρήση υπολογιστή **(**από τη σελίδα **«**Συμβουλές**»).**

Συζήτηση στην τάξη

1. Ζητήστε από τους μαθητές να διατυπώσουν τις απόψεις τους για τις υπηρεσίες κοινωνικής δικτύωσης. Υπάρχουν κίνδυνοι για τα προσωπικά δεδομένα; Ποιοι είναι αυτοί; Υπάρχουν κάποιοι κανόνες ηθικής για το τι μπορείς να κάνεις ή να πεις σε μια υπηρεσία κοινωνικής δικτύωσης, όπως το **Facebook**;

2. Κάντε μία γρήγορη δημοσκόπηση στην τάξη**:** πόσοι από τους μαθητές είναι μέλη σε κάποια υπηρεσία κοινωνικής δικτύωσης**;** Είναι μόνο στο **Facebook** ή και σε κάποια άλλη**;** Έχουν **«**ανοικτό**»** ή **«**κλειστό**»** προφίλ ή αλλιώς είναι διαθέσιμη η πληροφορία τους σε όλους ή μόνο στους φίλους**;** Γνωρίζει κανείς τις δυνατότητες ρυθμίσεων απορρήτου στο **Facebook;**

3. Ζητήστε από τους μαθητές να σκεφτούν τι θα έκαναν αν κάποιος ανέβαζε προσβλητικές πληροφορίες γι**'** αυτούς στο **Facebook.** Έχουν βρεθεί ποτέ σε τέτοια θέση**;** Έχουν ποτέ δημοσιεύσει πληροφορίες για φίλους τους χωρίς να τους ρωτήσουν **(**τους φίλους**);**

Εργαλεία

- Δείξτε **-** με υπολογιστή **-** τη χρήση των ρυθμίσεων απορρήτου στο **Facebook.** Διαβάστε μαζί με τους μαθητές τους όρους χρήσης του **Facebook.**
- Χρησιμοποιείστε τα προτεινόμενα βίντεο και κόμικ για να δώσετε περισσότερη έμφαση στους κινδύνους από την αποκάλυψη προσωπικών δεδομένων σε υπηρεσίες κοινωνικής δικτύωσης**.**
- Κάντε μαζί με τους μαθητές το τεστ για τις υπηρεσίες κοινωνικής δικτύωσης που προτείνουμε**.**

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ