Ινστιτούτο Τεχνολογίας Υπολογιστών και Εκδόσεων "Διόφαντος"

Πανελλήνιο Σχολικό Δίκτυο

ΕΚΠΑΙΔΕΥΤΙΚΟ ΥΛΙΚΟ ΑΝΑΦΟΡΑΣ

Θεματική Ενότητα: Υπηρεσίες Πανελλήνιου Σχολικού Δικτύου

Εκπαιδευτικό Αντικείμενο: 22 – Ασφάλεια στο Διαδίκτυο

Ημερομηνία τελευταίας τροποποίησης : 29/03/2013

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Σύντομη Περιγραφή

Στο παρόν εκπαιδευτικό υλικό παρουσιάζονται βασικές πρακτικές και χρήσιμες οδηγίες σχετικά με την Ασφάλεια στο Διαδίκτυο. Αρχικά γίνεται μία εισαγωγή στην έννοια της Ασφάλειας στο Διαδίκτυο και στην πολιτική που ακολουθεί το Υπουργείο Παιδείας και Θρησκευμάτων, Πολιτισμού και Αθλητισμού (ΥΠΑΙΘΠΑ) και το Πανελλήνιο Σχολικό Δίκτυο (ΠΣΔ). Στη συνέχεια περιγράφονται οι κίνδυνοι που ενδεχομένως θα αντιμετωπίσουν οι μαθητές αλλά και οι εκπαιδευτικοί κατά την πλοήγησή τους και προτείνονται τρόποι αντιμετώπισης των παραπάνω κινδύνων καθώς και συμβουλές προς του γονείς και τους ίδιους τους μαθητές. Επίσης, γίνεται αναφορά στα κοινωνικά δίκτυα και στους κινδύνους που εγκυμονούν. Τέλος, παρουσιάζεται ο μηχανισμός γονικού ελέγχου (parental control) και ασφαλούς περιήγησης στους φυλλομετρητές ιστού.

Συγγραφική Ομάδα: ΙΤΥΕ – Διεύθυνση Πανελλήνιο Σχολικού Δικτύου και Δικτυακών Τεχνολογιών – Ομάδα Οργάνωσης Εκπαιδευτικού Υλικού

Χρηματοδότηση

Το παρόν συγχρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και εθνικούς πόρους στο πλαίσιο της πράξης "ΣΤΗΡΙΖΩ - Οριζόντιο έργο υποστήριξης σχολείων, εκπαιδευτικών και

μαθητών στο δρόμο για το ΨΗΦΙΑΚΟ ΣΧΟΛΕΙΟ, νέες υπηρεσίες Πανελλήνιου Σχολικού Δικτύου και Στήριξης του ΨΗΦΙΑΚΟΥ ΣΧΟΛΕΙΟΥ" του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Διά Βίου Μάθηση»

Σκοποί και Στόχοι

Οι σκοποί του παρόντος εκπαιδευτικού υλικού συνοψίζονται παρακάτω:

Γνώσεις

1. Να ενημερωθούν οι εκπαιδευτικοί και οι μαθητές για τους κινδύνους που κρύβει το διαδίκτυο.
2. Να διακρίνουν οι μαθητές και οι γονείς τούς τις διαδικτυακές παγίδες και απειλές.

Δεξιότητες

1. Να εκτελούν οι εκπαιδευτικοί βασικές ενέργειες για τη διαδικτυακή ασφάλεια των μαθητών τους.
2. Να εφαρμόζουν οι μαθητές και οι γονείς τους απλούς κανόνες ασφάλειας.

Πρακτικές

1. Να συνειδητοποιήσουν οι εκπαιδευτικοί τη σπουδαιότητα της ασφαλούς διαδικτυακής πλοήγησης.
2. Να αντιληφθούν οι μαθητές και οι γονείς τους κινδύνους που μπορεί να εγκυμονεί η περιήγηση στο διαδίκτυο.
3. Να κατανοήσουν και να προβάλλουν την βασική αρχή ότι για την προστασία από τους κινδύνους του Διαδικτύου είναι απαραίτητη η κριτική και ενεργητική στάση των άμεσα εμπλεκομένων (μαθητές, εκπαιδευτικοί και γονείς).

Προτεινόμενη Βιβλιογραφία

[1] W. R. Cheswick, S. M. Belovin, A. D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker (2nd Edition),* Addison-Wesley Professional Computing Series, ISBN 978-0201634662, 2003.

[2] Γ. Τσουβέλας, Ο. Γιωτάκος, *Sexting : φαινομενολογία, πρόληψη και προτάσεις για δομικές πολυεπίπεδες παρεμβάσεις σε επίπεδο σχολικής κοινότητας*. Διαθέσιμο στην ακόλουθη ηλεκτρονική διεύθυνση http://blogs.sch.gr/internet-safety/archives/1031. Τελευταία ημερομηνία πρόσβασης 13 Μαρτίου 2013.

[3] K. D. Mitnick, W. L. Simon, S. Wozniak, *The Art of Deception: Controlling the Human Element of Security*, John Wiley & Sons, ISBN 978-0764542800, 2003.

[4] K. D. Mitnick, W. L. Simon, *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*, John Wiley & Sons, ISBN 978-0764569593, 2005.

[5] R. M. Kowalski, S. P. Limber, P. W. Agatston, *Cyber Bullying: Bullying in the Digital Age,* Blackwell Publishing, ISBN 978-1405159920, 2008.

[6] J. J. Myers, D. S. McCaw, L. S. Hemphill, *Responding to Cyber Bullying: An Action Tool for School Leaders, Corwin Press, ISBN 978-1412994842, 2011.*

[7] C. Davies, R. Eynon, *Teenagers and Technology (Adolescence and Society Series),* Routledge, ISBN 978-0415684583, 2012.

[8] Safer Internet Hellas, *Προστασία της ιδιωτικής μας σφαίρας στον ιστοχώρο κοινωνικής δικτύωσης Facebook - Πώς μπορούμε να ελέγχουμε και να ρυθμίζουμε την πρόσβαση στα δεδομένα μας μέσα από τις οθόνες του Facebook*, 1η Έκδοση 2011, Ανακτήθηκε από την ηλεκτρονική διεύθυνση www.saferinternet.gr/index.php?action=download&objId=File472.

[9] Εγκύκλιος, Π*ρόσβαση μαθητών Πρωτοβάθμιας Εκπαίδευσης σε υπηρεσίες κοινωνικής δικτύωσης μέσω διαδικτύου*. Διαθέσιμη στην ακόλουθη ηλεκτρονική διεύθυνση http://www.sch.gr/files/usersanakoinoseis/facebook.pdf. Τελευταία ημερομηνία πρόσβασης 13 Μαρτίου 2013.

Προτεινόμενες Ιστοσελίδες

[1]	http://www.saferinternet.gr/ http://www.saferinternet.org/	Δικτυακός τόπος της Δράσης *Ενημέρωση και Επαγρύπνηση του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου*, υπό την αιγίδα της Ευρωπαϊκής Επιτροπής
[2]	http://internet-safety.sch.gr/	Δικτυακός τόπος του Πανελλήνιου Σχολικού Δικτύου (ΠΣΔ) για την Ασφάλεια στο Διαδίκτυο
[3]	http://www.sch.gr/spam	Δικτυακός τόπος του ΠΣΔ για την προστασία από την ανεπιθύμητη αλληλογραφία
[4]	http://www.sch.gr/virus	Δικτυακός τόπος του ΠΣΔ για την παροχή οδηγιών ασφάλειας και προστασίας από ιούς
[5]	http://www.safeline.gr	Ανοικτή γραμμή καταγγελιών παράνομου περιεχομένου στο διαδίκτυο (SafeLine) και μέλος του INHOPE (Διεθνής Σύνδεσμος Ανοικτών Γραμμών Διαδικτύου)
[6]	http://www.antibullying.eu	Δικτυακός τόπος για την Ευρωπαϊκή καμπάνια κατά του σχολικού εκφοβισμού
[7]	http://www.youth-health.gr/	Δικτυακός τόπος της Μονάδας Εφηβικής Υγείας
[8]	http://creativecommons.org/licenses/by-nc-sa/3.0/gr/	Δικτυακός τόπος της Creative Commons
[9]	http://creativecommons.org/licenses/by-nc-sa/3.0/gr/legalcode	Άδεια χρήσης Creative Commons

Γλωσσάριο – Ακρωνύμια

[1]	ΠΣΔ	Πανελλήνιο Σχολικό Δίκτυο
[2]	ΥΠΑΙΘΠΑ	Υπουργείο Παιδείας Θρησκευμάτων, Πολιτισμού & Αθλητισμού
[3]	CERT	Computer Emergency Response Team
[4]	DoS	Denial of Service
[4]	MMS	Multimedia Messaging Service

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Εισαγωγή

Η χρησιμότητα του Διαδικτύου (Internet) είναι αδιαμφισβήτητη στην Κοινωνία της Πληροφορίας. Το Διαδίκτυο μπορεί να χρησιμοποιηθεί για εκπαιδευτικούς, ενημερωτικούς, επιχειρηματικούς σκοπούς, για έρευνα ή για διασκέδαση, κλπ. Οι υπηρεσίες που προσφέρει το καθιστούν σήμερα πολύτιμο εργαλείο της μαθησιακής διαδικασίας. Ωστόσο, η επιτυχής και ασφαλής αξιοποίησή του από τους μαθητές απαιτεί την ανάπτυξη συγκεκριμένων δεξιοτήτων. Χωρίς να αναιρείται η θετική πλευρά του Διαδικτύου, θα πρέπει να επισημανθεί ότι το Διαδίκτυο από τη φύση του δεν εγγυάται ασφάλεια για τον ανήλικο χρήστη, καθώς οι δημοσιευμένες πληροφορίες δεν χαρακτηρίζονται απαραίτητα από καταλληλότητα και εγκυρότητα ενώ οι ταυτότητες και οι σκοποί των συντακτών δεν είναι πάντα εμφανείς. Οι κίνδυνοι αυτοί ειδικά για τους ανήλικους, αναδεικνύουν την αναγκαιότητα σχεδιασμού μίας πολιτικής προστασίας τους από την έκθεσή τους σε ακατάλληλο περιεχόμενο, το οποίο μπορεί να καταστεί επιβλαβές στην ανάπτυξη της προσωπικότητάς τους. Χωρίς αυτό να υπονοεί ότι θα πρέπει να καταφύγουμε σε ακραίες λύσεις λογοκρισίας ή ασφυκτικούς περιορισμούς, είναι προφανές ότι πρέπει να οριστούν πολιτικές ελέγχου του περιεχομένου στο Διαδίκτυο και μέτρα για την ενημέρωση και την προστασία των ανήλικων χρηστών του.

Πολιτική του Υπουργείου Παιδείας και Θρησκευμάτων, Πολιτισμού και Αθλητισμού

Το ζήτημα της ασφαλούς πρόσβασης των ανηλίκων στο Διαδίκτυο είναι ιδιαίτερα σημαντικό, αφού έχει κοινωνικές, πολιτισμικές, παιδαγωγικές, επιστημονικές και άλλες πτυχές. Το Υπουργείο Παιδείας και Θρησκευμάτων, Πολιτισμού και Αθλητισμού (ΥΠΑΙΘΠΑ) αναγνωρίζει την κρισιμότητα του ζητήματος και εφαρμόζει μέσω του Πανελλήνιου Σχολικού Δικτύου (www.sch.gr) μία συγκεκριμένη πολιτική προστασίας των μαθητών από την έκθεσή τους σε ακατάλληλο περιεχόμενο του Διαδικτύου μέσα από το σχολείο. Η πολιτική είναι εναρμονισμένη με τη διεθνή πρακτική και τις νομικές απαιτήσεις και διαρθρώνεται σε πέντε άξονες:

1. Στον ορισμό των Πολιτικών Αποδεκτής Χρήσης του Διαδικτύου και των Σχολικών Εργαστηρίων Πληροφορικής (ΣΕΠΕΗΥ) από τα σχολεία και τους μαθητές. Για το σκοπό αυτό το ΥΠΑΙΘΠΑ έχει θεσμοθετήσει συλλογικά όργανα, αποτελούμενα από ειδικούς επιστήμονες, τα οποία έχουν την ευθύνη της χάραξης πολιτικής και διαχείρισης του περιεχομένου που διακινείται μέσω του Πανελλήνιου Σχολικού Δικτύου (ΠΣΔ) και των υπηρεσιών του.

2. Στην ανάπτυξη και εφαρμογή τεχνικών (φίλτρα) που υλοποιούν τις πολιτικές αυτές. Αντίστοιχες τεχνικές εφαρμόζονται διεθνώς στα εκπαιδευτικά δίκτυα πολλών προηγμένων χωρών και αποτρέπουν με σημαντικό δείκτη επιτυχίας την πρόσβαση σε ιστοσελίδες που ανήκουν σε κατηγορίες όπως:
   - «porn» (ιστοσελίδες με πορνογραφικό περιεχόμενο)
   - «gambling» (ιστοσελίδες με τυχερά παιχνίδια)
   - «drugs» (ιστοσελίδες που προωθούν τα ναρκωτικά)
   - «aggressive» (ιστοσελίδες που προπαγανδίζουν την επιθετική συμπεριφορά και το ρατσισμό) και
   - «violence» (ιστοσελίδες που προωθούν την βία)

   Επειδή η ταξινόμηση των ιστοσελίδων στις παραπάνω κατηγορίες γίνεται με τη χρήση αυτοματοποιημένης διαδικασίας (λόγω του τεράστιου πλήθους των ιστοσελίδων στο Διαδίκτυο), είναι πιθανό κάποια ιστοσελίδα να ταξινομηθεί λανθασμένα. Για το λόγο αυτό το ΠΣΔ ακολουθεί τη διεθνή πρακτική και παρέχει τη δυνατότητα στους χρήστες του να ενημερώνουν τους αρμόδιους τεχνικούς όταν διαπιστώσουν οποιαδήποτε δυσλειτουργία της υπηρεσίας, οι οποίοι πλέον χειρωνακτικά διορθώνουν τη βάση δεδομένων.
3. Στη διαρκή πληροφόρηση και ευαισθητοποίηση της σχολικής κοινότητας, καθώς οποιαδήποτε τεχνική λύση είναι αδύνατο να αποδώσει αν δεν είναι σωστά ενημερωμένη και ευαισθητοποιημένη η σχολική κοινότητα. Για το σκοπό αυτό το ΠΣΔ ενημερώνει τους εκπαιδευτικούς, τους γονείς και τους μαθητές μέσω του δικτυακού του τόπου (www.sch.gr/safe) και μέσω της συμμετοχής του σε διάφορες εκδηλώσεις (π.χ., ημερίδες, συνέδρια, κλ,)[1].
4. Στη συνεργασία με ειδικές δράσεις για την ασφάλεια στο Διαδίκτυο, όπως η Ανοικτή Γραμμή Καταγγελιών Παράνομου Περιεχομένου στο Διαδίκτυο (http://www.safeline.gr) και η κοινοτική δράση για την προώθηση της ασφαλέστερης χρήσης του Διαδικτύου, του κινητού τηλεφώνου και άλλων διαδραστικών τεχνολογιών (http://www.saferinternet.org και http://www.saferinternet.gr/).
5. Στη δημιουργία θετικής αντιπρότασης, δηλαδή στην ανάπτυξη αξιόλογου ή/και πιστοποιημένου εκπαιδευτικού υλικού στο οποίο αξίζει να έχουν πρόσβαση οι μαθητές και στη διανομή στην εκπαιδευτική κοινότητα του μέσω των εκπαιδευτικών και δικτυακών πυλών όπως: www.e-yliko.gr, www.sch.gr, www.neagenia.gr, www.kee.gr, www.greeklanguage.gr, www.pi-schools.gr, students.sch.gr, κλπ, οι οποίες λειτουργούν είτε υπό την άμεση ευθύνη του ΥΠΑΙΘΠΑ, είτε υπό την ευθύνη εποπτευόμενων φορέων του.

[1] www.sch.gr/docs

Το πλαίσιο συμπληρώνεται από την εφαρμογή μεθόδων για την προστασία της υπηρεσίας ηλεκτρονικής αλληλογραφίας (e-mail) των σχολείων, των εκπαιδευτικών και των μαθητών από απρόκλητη / διαφημιστική αλληλογραφία (spam) και από κακόβουλο λογισμικό (ιοί - viruses), όπως αναλυτικά παρουσιάζεται στις δικτυακές τοποθεσίες www.sch.gr/spam και www.sch.gr/virus.

Δυνητικοί κίνδυνοι που ενέχει το διαδίκτυο για τους ανήλικους

Γενικά, η πλοήγηση στο διαδίκτυο περιλαμβάνει πολλούς κινδύνους και ακόμη περισσότερους για τους ανήλικους μαθητές. Παρακάτω περιγράφονται οι βασικοί κίνδυνοι που μπορεί να συναντήσει ένας ανήλικος κατά την περιήγησή του στο Διαδίκτυο και είναι οι εξής:

- Προπαγάνδα ιδεών που υποδαυλίζουν το ρατσισμό, το φανατισμό και τη βία.
- Προώθηση χρήσης ναρκωτικών ουσιών και αλκοόλ.
- Προβολή και παρακίνηση συμμετοχής σε τυχερά παιχνίδια.
- Έκθεση σε πορνογραφικό περιεχόμενο.
- Κυκλώματα παιδεραστίας.
- Οικονομική εκμετάλλευση από αποκάλυψη προσωπικών στοιχείων (π.χ., πιστωτικές κάρτες κλπ.)

Ως προς την προστασία που προσφέρεται στο σχολικό εργαστήριο από το ακατάλληλο και παράνομο περιεχόμενο, το ΠΣΔ παρέχει την **Υπηρεσία Ελεγχόμενης Πρόσβασης** (Web-Filtering) στον Παγκόσμιο Ιστό. Όμως για την προστασία από τους κινδύνους του Διαδικτύου δεν αρκεί η χρήση των φίλτρων της παραπάνω υπηρεσίας αλλά είναι απαραίτητη η ενεργητική και κριτική στάση μαθητών, εκπαιδευτικών και γονέων.

Επιπλέον, οι μαθητές και οι εκπαιδευτικοί σε περίπτωση που αντιληφθούν κάποια σελίδα με ακατάλληλο περιεχόμενο μπορούν να επικοινωνήσουν με το διαχειριστή της υπηρεσίας (cachemaster@sch.gr) και να ζητήσουν την απαγόρευση της συγκεκριμένης σελίδας. Αν εντοπίσουν σελίδα που ανήκει στην κατηγορία του παράνομου περιεχομένου, μπορούν να επικοινωνήσουν με την **Ελληνική Γραμμή Αναφοράς Παράνομου Περιεχομένου στο Internet** (http://www.safeline.gr).

Διαδικτυακές Απειλές

Sexting

Το **sexting** ορίζεται ως η πράξη αποστολής, λήψης και διατήρησης μηνυμάτων σεξουαλικού περιεχομένου με φωτογραφικό ή οπτικοακουστικό υλικό μέσω κινητού τηλεφώνου ή άλλου μέσου ψηφιακής τεχνολογίας. Τυπικά το sexting, στα πλαίσια του σχολείου, εμφανίζεται περισσότερο μέσα από τη χρήση κινητών τηλεφώνων, ωστόσο με τις αυξημένες δυνατότητες διαδικτυακής πρόσβασης των σύγχρονων συσκευών (κινητά τηλέφωνα, notebooks, tablets κλπ), τα υβριδικά

μηνύματα πορνογραφικού περιεχομένου (**sexts**) δύναται να μεταδίδονται μέσω e-mail, μέσω ιστοτόπων κοινωνικής δικτύωσης κλπ.

Μια επιφανειακή προσέγγιση του sexting καθιστά προφανές το γεγονός ότι οι εμπλεκόμενοι μαθητές δεν κατανοούν πλήρως όλες τις πτυχές και τους κινδύνους του συγκεκριμένου φαινομένου. Οι εμπλεκόμενοι έφηβοι, συχνά δεν μπορούν να διανοηθούν ότι ένα sext μπορεί να προωθηθεί σε πολλαπλούς αποδέκτες καθώς και ότι κάτι που προορίζονταν στα πλαίσια μιας ιδιαίτερα προσωπικής επικοινωνίας, δύναται να έχει διανεμηθεί σε πολλαπλούς παραλήπτες. Επίσης, οι περισσότεροι έφηβοι αγνοούν ότι η αποστολή ή προώθηση υλικού που απεικονίζει ανήλικο σε γυμνή ή ημίγυμνη φωτογραφία εμπίπτει σε νομικές διατάξεις παιδικής πορνογραφίας. Συνεπώς, για την ελαχιστοποίηση τυπικών παραβιάσεων διατάξεων παιδικής πορνογραφίας αλλά και την αποφυγή καταστάσεων με έντονο κοινωνικό και ψυχολογικό αντίκτυπο κρίνεται απαραίτητη η καθιέρωση δράσεων ενημέρωσης των μαθητών και των γονέων, από τους εκπαιδευτικούς, για αντίστοιχα ζητήματα.

Τρόπος Αντιμετώπισης

Εύλογα αναδύονται ερωτήματα για το πώς το σχολείο μπορεί να αντιμετωπίσει το φαινόμενο sexting και να συμβάλλει στον περιορισμό δυσάρεστων καταστάσεων (π.χ., εκμετάλλευση, εκβιασμός κλπ). Οι τρόποι αντιμετώπισης του φαινομένου κατηγοριοποιούνται ανάλογα με το επίπεδο της πρόληψης. Τα επίπεδα αυτά χωρίζονται στο πρωτογενές (Διευθυντές) και δευτερογενές (προσωπικό σχολικής μονάδας).

Σε επίπεδο πρωτογενούς πρόληψης οι Διευθυντές οφείλουν να εξετάσουν κατά πόσο και σε ποιο βαθμό το σχολείο έχει μία σταθερή πολιτική για την παρενόχληση και τον εκφοβισμό με χρήση της ψηφιακής τεχνολογίας. Ενέργειες που πρέπει να υλοποιηθούν σε αυτό το επίπεδο είναι:

1. Ρητή απαγόρευση του sexting στα πλαίσια του σχολείου,
2. Υιοθέτηση συγκεκριμένης πολιτικής για τη χρήση ψηφιακών μέσων τεχνολογίας στους σχολικούς χώρους, όπως κινητά τηλέφωνα, tablets, φωτογραφικές μηχανές και φορητοί υπολογιστές,
3. Επισήμανση ότι η διανομή και κατοχή υλικού μέσω sexting, τόσο στο πλαίσιο του σχολείου όσο και εκτός σχολείου επιφέρει συγκεκριμένες νομικές επιπτώσεις.

Σε επίπεδο δευτερογενούς πρόληψης:

1. Το προσωπικό του σχολείου οφείλει να είναι ενήμερο για τη νομοθεσία σχετικά με την παιδική πορνογραφία.
2. Οι μαθητές να έχουν λάβει ειδική ενημέρωση αναφορικά με τους κινδύνους που σχετίζονται με το sexting σε νομικό και συναισθηματικό-ψυχολογικό επίπεδο, καθώς και για την πολιτική που υιοθετεί το σχολείο.

3. Το προσωπικό του σχολείου να γνωρίζει τις συντονισμένες ενέργειες που πρέπει να εκτελεστούν στην περίπτωση που αναφερθεί κάποιο περιστατικό sexting.
4. Με τον εντοπισμό του συγκεκριμένου φαινομένου, το προσωπικό που εμπλέκεται στο σχέδιο αντιμετώπισης της κρίσης, πρέπει να γνωρίζει πώς να παρέχει συμβουλές σε θέματα ασφάλειας και ψυχολογικής υποστήριξης των μαθητών και να εξασφαλίζει συμμόρφωση τόσο με την πολιτική του σχολείου όσο και με τη σχετική νομοθεσία.

Σε επίπεδο τριτογενούς πρόληψης οι Διευθυντές των σχολείων, οι Σχολικοί Σύμβουλοι και οι Σχολικοί Ψυχολόγοι πρέπει να έχουν εξειδικευμένες γνώσεις και δεξιότητες για την αξιολόγηση και πρόληψη των πιθανών κινδύνων καθώς και την παροχή συμβουλών έτσι ώστε να ανταποκριθούν επιτυχώς στις ανάγκες των ατόμων και των ομάδων που εμπλέκονται με το sexting.

Οι Διευθυντές των σχολείων και οι Σχολικοί Σύμβουλοι που γνωρίζουν σε μεγαλύτερο βάθος τη σχολική νομοθεσία οφείλουν να συνεργαστούν με Σχολικούς Ψυχολόγους και άλλο ειδικευμένο επιστημονικό προσωπικό, έτσι ώστε να προκύψουν εποικοδομητικές παρεμβάσεις τόσο στο πλαίσιο του σχολείου όσο και της ευρύτερης κοινωνίας. Παράλληλα, θα πρέπει να διερευνήσουν κατά πόσον οι υφιστάμενες πολιτικές του σχολείου (εσωτερικός κανονισμός), του ΥΠΑΙΘΠΑ (σχετικοί εγκύκλιοι) και η αντίστοιχη νομοθεσία, λαμβάνουν υπόψη τους τη μεταβαλλόμενη φύση της ψηφιακής τεχνολογίας και εν συνεχεία να διαμορφώσουν συγκεκριμένο πλαίσιο δράσης και να προτείνουν την υιοθέτηση καλών παραδειγμάτων.

1. Δεν δίνουμε τα προσωπικά μας στοιχεία σε ένα δωμάτιο συνομιλίας. Ποτέ δεν μπορούμε να είμαστε σίγουροι για την ταυτότητα του συνομιλητή μας.
2. Δεν συναντούμε κάποιο ξένο, τον οποίο γνωρίσαμε σε ένα δωμάτιο συνομιλίας. Αν μάς ζητηθεί κάτι τέτοιο το συζητάμε αμέσως με κάποιο ενήλικα.
3. Μπορούμε να αποθηκεύουμε τις ηλεκτρονικές μας συνομιλίες. Αν μια συνομιλία μας έκανε να νιώσουμε άβολα ή μας έφερε σε δύσκολη θέση, κρατάμε αντίγραφο. Αυτό θα μας βοηθήσει να καταγγείλουμε τον επιτήδειο που προσπάθησε να μας παραπλανήσει.
4. Διαβάζουμε τους όρους χρήσης, τον κώδικα επικοινωνίας και τη δήλωση απορρήτου στη διαδικτυακή τοποθεσία συνομιλίας, προτού αρχίσουμε τη συνομιλία.

Grooming: Σεξουαλική Αποπλάνηση

Ο όρος **Grooming** αναφέρεται στην αποπλάνηση και συμβαίνει όταν άγνωστοι εκμεταλλεύονται κακόβουλα το στοιχείο της ανωνυμίας στο Διαδίκτυο για να προσεγγίσουν ανήλικους με στόχο τη σεξουαλική παρενόχληση. Γενικά, στο Διαδίκτυο ποτέ δεν μπορούμε να είμαστε σίγουροι ποιος είναι ο συνομιλητής μας στις ηλεκτρονικές μας επικοινωνίες, ακόμα και αν βλέπουμε τη φωτογραφία του ή αν χρησιμοποιούμε ψηφιακή κάμερα. Έτσι, πολλοί επιτήδειοι εκμεταλλεύονται το γεγονός αυτό, δίνουν ψεύτικα στοιχεία (π.χ., ηλικία) και ξεκινούν συζητήσεις με τα πιθανά θύματά τους με στόχο να αναπτύξουν φιλική σχέση και να αποσπάσουν όσο το δυνατό περισσότερες πληροφορίες (π.χ.,

τόπο διαμονής, τα ενδιαφέροντά τους, τις σεξουαλικές τους εμπειρίες κλπ). Το Grooming αποτελεί ένα είδος ψυχολογικού χειρισμού και για το λόγο αυτό είναι σημαντικό **να εξηγήσουμε στους γονείς** πως οφείλουν να είναι ενημερωμένοι για τις διαδικτυακές γνωριμίες των παιδιών τους ώστε, όταν παρατηρήσουν κάτι ύποπτο, να μπορέσουν να τα συμβουλέψουν αποτελεσματικά και να δράσουν άμεσα.

Κατηγορίες Θυμάτων

Τα θύματα του Grooming είναι συνήθως έφηβοι ηλικίας 11 έως 17 ετών, ενώ σύμφωνα με έρευνες το κορίτσια είναι πιο ευάλωτα σε αυτό το φαινόμενο από τα αγόρια. Έχουν, όμως, αναφερθεί και συγκεκριμένες κατηγορίες παιδιών που τα καθιστούν ακόμα πιο ευάλωτα σε αυτήν τη διαδικασία:

1. Παιδιά με χαμηλή αυτοεκτίμηση και έλλειψη αυτοπεποίθησης.
2. Παιδιά με συναισθηματικά προβλήματα ή με προβλήματα στις σχέσεις με γονείς, σχολείο και συνομήλικους.
3. Παιδιά που δείχνουν αφελή και υπερβολική εμπιστοσύνη στους άλλους.
4. Έφηβοι, καθότι τους απασχολούν και τους ενδιαφέρουν τα σεξουαλικά ζητήματα.

Επιπλέον, οι ακόλουθες κατηγορίες παρουσιάζονται ως ιδιαίτερα ευάλωτες σε πιθανή διαδικτυακή σεξουαλική παρενόχληση:

1. Κορίτσια
2. Έφηβοι ηλικίας 14 έως 17 ετών.
3. Νέοι που έχουν βιώσει κάποιο αρνητικό γεγονός στο στενό οικογενειακό τους περιβάλλον καθώς και νέοι με καταθλιπτικό συναίσθημα.
4. Τακτικοί χρήστες του διαδικτύου (που δαπανούν πάνω από δύο ώρες ημερησίως και πάνω από τέσσερις μέρες την εβδομάδα στο διαδίκτυο ενώ αξιολογούν ότι το διαδίκτυο έχει μεγάλη σημασία για τη ζωή τους).
5. Συμμετέχοντες σε διαδικτυακά δωμάτια συνομιλιών (chat rooms) ενώ επιδεικνύουν επικίνδυνη διαδικτυακή συμπεριφορά (π.χ., παρέχουν προσωπικές και εμπιστευτικές πληροφορίες, σχολιάζουν με άκομψο και προκλητικό τρόπο, ενοχλούν άλλους χρήστες, συζητούν για σεξουαλικά ζητήματα με κάποιον που δεν γνωρίζουν, επισκέπτονται εκουσίως πορνογραφικούς διαδικτυακούς τόπους κλπ).

Αναφορά προβλήματος

Σε αρκετές περιπτώσεις η παρενόχληση γίνεται από παιδιά προς παιδιά. Σε αυτή την περίπτωση, καλό είναι να αναζητήσουμε τον θύτη και να μιλήσουμε με τους γονείς του. Αν το πρόβλημα δεν μπορεί να λυθεί με τη δική μας παρέμβαση και κρίνεται απαραίτητη η λήψη δραστικότερων μέτρων μπορούμε να **καταγγείλουμε** το περιστατικό στην ανοιχτή γραμμή SafeLine (http://www.safeline.gr στην ηλεκτρονική διεύθυνση report@safeline.gr) ή στο τηλέφωνο **2811 391615** από τις **9.00 έως τις 16.00** (εργάσιμες ημέρες).

Cyber-Bulling: Διαδικτυακός εκφοβισμός

Ο όρος **διαδικτυακός εκφοβισμός** (Cyber-bullying) αφορά τον εκφοβισμό που είναι δυνατό να πραγματοποιηθεί μέσω του Διαδικτύου και περιλαμβάνει εσκεμμένη, επαναλαμβανόμενη και εχθρική συμπεριφορά απέναντι σε συγκεκριμένο άτομο ή ομάδα ατόμων με σκοπό την πρόκληση συναισθηματικής και ψυχολογικής βλάβης. Ο διαδικτυακός εκφοβισμός συνήθως έχει τη μορφή ενός εκφοβιστικού, ρατσιστικού, ή προσβλητικού ηλεκτρονικού μηνύματος, φωτογραφίας ή βίντεο και ενδεχομένως μπορεί να οδηγήσει στην περιθωριοποίηση και τον κοινωνικό αποκλεισμό των θυμάτων. Γενικά, ο εκφοβισμός αυτός είναι δύσκολο να ελεγχθεί, αφού δεν υπάρχει περιορισμός των μηνυμάτων που διανέμονται ηλεκτρονικά (περίπτωση ανεπιθύμητης αλληλογραφίας[2]) καθώς και του αριθμού των παραληπτών που μπορούν να γίνουν δέκτες αυτών των μηνυμάτων.

Τρόποι Αντιμετώπισης

Ενδεικτικοί τρόποι αντιμετώπισης του παραπάνω διαδικτυακού κινδύνου επισημαίνονται παρακάτω:

1. Εάν πέσουμε θύμα εκφοβισμού, σταματάμε αμέσως την επικοινωνία με το θύτη.
2. Εμπιστευόμαστε στους γονείς μας ή σε κάποιο ενήλικα τον εκφοβισμό που έχουμε δεχθεί.
3. Δεν προωθούμε εκφοβιστικά μηνύματα.
4. Αν γνωρίζουμε κάποιο φίλο που είναι θύτης τον συμβουλεύουμε να σταματήσει.
5. Φιλτράρουμε ηλεκτρονικά μηνύματα από άτομα που μάς παρενοχλούν και μπλοκάρουμε την πρόσβασή τους σε προσωπικούς δικτυακούς χώρους (π.χ., ιστολόγιο).

Είναι χρήσιμο να επισημανθεί ότι στην ηλεκτρονική διεύθυνση http://www.antibullying.eu παρουσιάζεται η Ευρωπαϊκή καμπάνια κατά του σχολικού εκφοβισμού σε όλες του τις μορφές (π.χ., διαδικτυακός εκφοβισμός) που υλοποιείται στα πλαίσια του κοινοτικού προγράμματος Daphne III[3]. Ο στόχος του συγκεκριμένου προγράμματος συνίσταται στη δημιουργία μιας ενιαίας πολιτικής στην καταγραφή και διαχείριση του σχολικού εκφοβισμού και την δημιουργία μιας Ευρωπαϊκής πλατφόρμας για την ενημέρωση των παιδιών, γονέων, εκπαιδευτικών και κάθε άμεσα ενδιαφερόμενου για το συγκεκριμένο πρόβλημα.

Υπερβολική Ενασχόληση με το διαδίκτυο (Εθισμός)

Εθισμός στο Διαδίκτυο μπορεί να προκύψει με την πολύωρη ενασχόληση ατόμων σε διάφορες διαδικτυακές δραστηριότητες (π.χ., on-line παιχνίδια, δωμάτια συζητήσεων, ιστότοποι ηλεκτρονικού τζόγου κλπ). Ένα άτομο είναι εθισμένο όταν παρουσιάζει τουλάχιστον τρία από τα ακόλουθα χαρακτηριστικά:

1. Χρήση του Διαδικτύου για υπερβολικά μεγάλο χρονικό διάστημα.

[2] Για περισσότερες πληροφορίες για την αντιμετώπιση της ανεπιθύμητης πληροφορίας μπορείτε να ανατρέξετε στο **ΕΑ13 - Ηλεκτρονικό ταχυδρομείο**.
[3] http://ec.europa.eu/justice/grants/programmes/daphne/index_en.htm

2. Κατανάλωση υπερβολικού χρόνου ή/και χρημάτων σε δραστηριότητες σχετικές με το Διαδίκτυο (π.χ., τυχερά παιχνίδια).
3. Συμπτώματα Συνδρόμου Απόσυρσης (π.χ., ψυχοκινητική διέγερση, άγχος, τάση διαρκούς ενασχόλησης με το Διαδίκτυο χωρίς ουσιαστικό λόγο κλπ).
4. Χρήση Διαδικτύου προκειμένου να αποφευχθούν συμπτώματα απόσυρσης.
5. Συστηματικό περιορισμό βασικών καθημερινών λειτουργιών όπως ο ύπνος, το φαγητό, η ξεκούραση, προσωπική φροντίδα και υγιεινή κλπ, δεδομένου ότι το διαδίκτυο παρέχει ένα ευρύ πεδίο δραστηριοποίησης (π.χ., on-line παιχνίδι, δυναμική επικοινωνία, ακρόαση μουσικής, αναζήτηση πληροφορίας, ηλεκτρονικές αγορές κλπ).
6. Συνέχιση χρήσης του Διαδικτύου παρά τη γνώση των παραπάνω δυσλειτουργιών.

Κατηγορίες θυμάτων

Σύμφωνα με στατιστικά στοιχεία της Μονάδας Εφηβικής Υγείας (Μ.Ε.Υ., http://www.youth-health.gr/) στην Ελλάδα, το φαινόμενο είναι συχνότερο σε αγόρια, σε δυσλειτουργικές οικογένειες και σε παιδιά με καταθλιπτικά συναισθήματα ή σύνδρομο υπερκινητικότητας.

Τρόποι Αντιμετώπισης

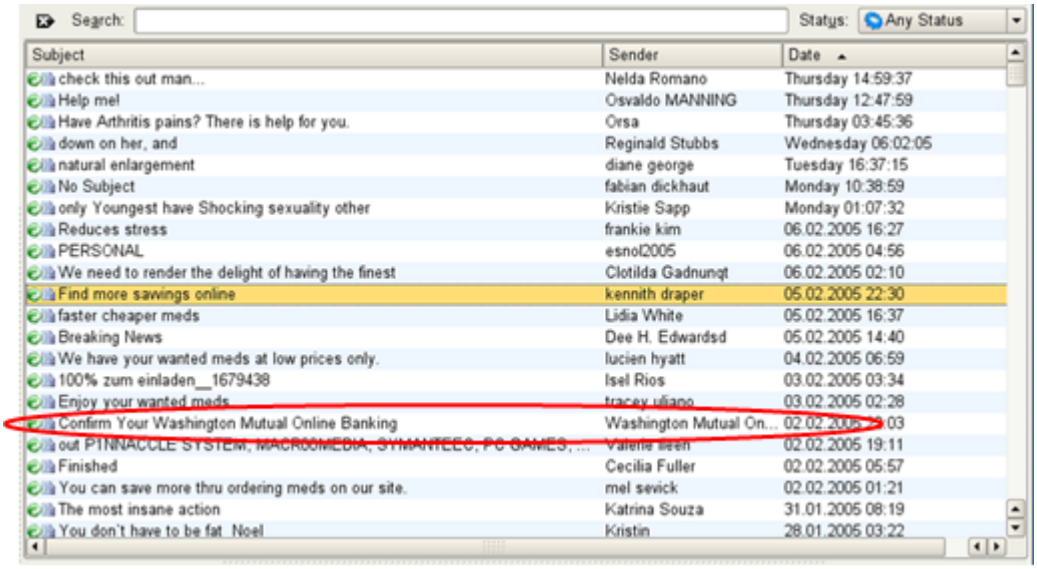
1. Ευαισθητοποίηση και ενημέρωση για το φαινόμενο του εθισμού.
2. Χρήση του Διαδικτύου με σύνεση, ενσωματώνοντας στο καθημερινό πρόγραμμα διάφορες δραστηριότητες (π.χ., ενασχόληση με ομαδικό άθλημα).
3. Υιοθέτηση καλών πρακτικών αξιοποίησης του Διαδικτύου.
4. Εάν παρατηρήσουμε υπερβολική χρήση καθώς και συμπεριφορές εθισμού αναζητούμε βοήθεια στην ιστοσελίδα http://www.saferinternet.gr ή στο τηλέφωνο 800 11 800 15.

Γενικά, τόσο οι γονείς όσο και οι εκπαιδευτικοί θα πρέπει να επαγρυπνούν για το χρόνο που αφερώνει το παιδί στο διαδίκτυο και να είναι ενήμεροι για τα θέματα που μπορεί να οδηγήσουν σε ακραίες συμπεριφορές εξάρτησης με το διαδίκτυο και έκπτωσης της λειτουργικότητάς του σε προσωπικό, οικογενειακό και κοινωνικό επίπεδο.

Phishing

Αποτελεί συνηθισμένη διαδικασία παραπλάνησης των διαδικτυακών χρηστών για την υποκλοπή εμπιστευτικών πληροφοριών, όπως οι κωδικοί πρόσβασης ηλεκτρονικών τραπεζικών λογαριασμών (βλ. **Εικόνα 1**). Η τεχνική Phishing συνήθως περιλαμβάνει τη χρήση ηλεκτρονικών ή άμεσων μηνυμάτων που φαίνονται αληθινά και σε συνδυασμό με πλαστές ιστοσελίδες πραγματοποιούν κατάλληλες αιτήσεις για παροχή πληροφοριών (*ψάρεμα δεδομένων*). Αντίστοιχες πρακτικές για την

εκμαίευση κρίσιμων πληροφοριών ακολουθούνται στα πλαίσια της κοινωνικής μηχανικής (social engineering)[4].



Εικόνα 1. *Τυπικό παράδειγμα ηλεκτρονικού μηνύματος για την υποκλοπή κρίσιμων δεδομένων*

Οδηγίες προς τους μαθητές για την Ασφαλή Χρήση του Διαδικτύου

Συμβουλές ασφαλούς χρήσης του Διαδικτύου

Παρακάτω παρουσιάζονται χρήσιμες πρακτικές για την ασφαλή πλοήγηση στο Διαδίκτυο:

- Μη δίνετε ποτέ προσωπικά σας στοιχεία καθώς και ψηφιακό υλικό (π.χ., φωτογραφίες) σε άλλους χρήστες του Διαδικτύου. Επιπλέον, μη παρέχετε πληροφορίες που αφορούν τους φίλους σας, την οικογένεια σας καθώς και το σχολείο σας.
- Μη γνωστοποιείτε μέσω του Διαδικτύου τα στοιχεία επικοινωνίας σας σε αγνώστους.
- Μην αποκαλύπτετε τους κωδικούς πρόσβασης (password) που χρησιμοποιείτε σε κρίσιμες διαδικτυακές υπηρεσίες (π.χ., Webmail, τραπεζικοί λογαριασμοί, ιστότοποι δημόσιων υπηρεσιών, κλπ).
- Μην επιχειρείτε συναλλαγές (π.χ., χρήση πιστωτικής κάρτας) μέσω του Διαδικτύου από άγνωστους ή τυχαίους ιστοτόπους για την αγορά προϊόντων. Αντίθετα, αναζητήστε διαδεδομένους ιστοτόπους που παρέχουν τους κατάλληλους μηχανισμούς για ασφαλείς διαδικτυακές αγορές, τμήμα εξυπηρέτησης πελατών, προβλεπόμενη διαδικασία επιστροφής προϊόντος κλπ. Για την πρώτη σας διαδικτυακή συναλλαγή είναι ιδιαιτέρως χρήσιμη η φυσική παρουσία και καθοδήγηση κάποιου χρήστη με μεγαλύτερη εμπειρία.

[4] http://en.wikipedia.org/wiki/Social_engineering_(security)

- Κατά την επίσκεψή σας σε τυχαίους δικτυακούς τόπους μη συμπληρώνετε φόρμες με τα προσωπικά σας στοιχεία.
- Τα άτομα που γνωρίζετε στο Διαδίκτυο δεν είναι πάντοτε αυτά που ισχυρίζονται ότι είναι, ενδεχομένως να λένε ψέματα για να κερδίσουν την εμπιστοσύνη σας και να αποσπάσουν χρήσιμες πληροφορίες.
- Μη συναντάτε μόνοι σας άτομα που γνωρίσατε από το Διαδίκτυο.
- Να συζητάτε με τους δασκάλους σας, τους γονείς σας καθώς και με πρόσωπα που εμπιστεύεστε για τις δραστηριότητες σας στο Διαδίκτυο, ιδιαίτερα αν αντιμετωπίσετε οποιαδήποτε περίεργη ή ασυνήθιστη κατάσταση.
- Να έχετε πάντα υπόψη σας ότι τα προϊόντα της πνευματικής δημιουργίας/ιδιοκτησίας (μουσική, λογοτεχνία, κινηματογράφος, λογισμικό κλπ) προστατεύονται από τη σχετική νομοθεσία και η διανομή τους μέσω του Διαδικτύου είναι παράνομη πράξη. Έργα (π.χ., λογοτεχνία, μουσική) και προϊόντα (π.χ., λογισμικό) που υπόκεινται σε καθεστώς πνευματικής ιδιοκτησίας (copyright), προστατεύονται από τη σχετική νομοθεσία και η διανομή τους μέσω Διαδικτύου θεωρείται παράνομη πράξη.
- Όπως επισημαίνεται παραπάνω, παράνομη πράξη θεωρείται και η διακίνηση εφαρμογών λογισμικού (software) εκτός και αν ανήκουν στην κατηγορία του Ελεύθερου Λογισμικού (open source software). Σε κάθε περίπτωση θα πρέπει να έχετε κατανοήσει τους όρους χρήσης και τις προϋποθέσεις για την τροποποίηση και την ελεύθερη διακίνησή τους. Σχετικές πληροφορίες μπορείτε να αντλήσετε στην ακόλουθη ηλεκτρονική διεύθυνση http://opensource.org/.
- Μη χρησιμοποιείτε άκριτα οποιοδήποτε πρόγραμμα βρίσκεται στο Διαδίκτυο ακόμη και αν αποτελεί κάποιο παιχνίδι, διότι μπορεί να περιέχει κακόβουλο λογισμικό (π.χ., trojan horse) και να επιφέρει σημαντικές δυσλειτουργίες στο υπολογιστικό σύστημα (π.χ., διαγραφή αρχείων, απενεργοποίηση firewall, επανεκκίνηση ή τερματισμός Η/Υ κλπ).
- Μην ανοίγετε e-mail από άγνωστους αποστολείς με τα ακόλουθα χαρακτηριστικά: (α) χωρίς θέμα (subject), (β) με περίεργο θέμα και (γ) περιέχουν επισυναπτόμενο/α αρχείο/α (π.χ., σε εκτελέσιμη μορφή, αρχείο/α .zip κλπ), διότι είναι πολύ πιθανό να περιέχουν κακόβουλο λογισμικό ή να αποτελούν μέρος στοχευμένης προσπάθειας Phishing (βλ. παραπάνω).

Πέρα από τις παραπάνω συμβουλές επισημαίνονται ακολούθως και βασικές οδηγίες καλής χρήσης του Διαδικτύου σχετικά με τα μηνύματα Ηλεκτρονικού Ταχυδρομείου και τις πληροφορίες που αποστέλλουν οι μαθητές με οποιοδήποτε τρόπο σε χρήστες ή ομάδες χρηστών του Πανελλήνιου Σχολικού Δικτύου καθώς και του Διαδικτύου γενικότερα:

- Το περιεχόμενο των πληροφοριών **δεν** πρέπει:
  - να προσβάλλει άλλους χρήστες του Διαδικτύου, αλλά να ακολουθεί τους νόμους, τα χρηστά ήθη και τα ήθη χρήσης του Διαδικτύου.
  - να προσβάλλει τα ανθρώπινα δικαιώματα και τις διάφορες μειονότητες.

- να σχετίζεται με παράνομες πράξεις (π.χ., τυχερά παιχνίδια, διακίνηση εμπορικού λογισμικού κλπ).
- να έχει υβριστικό χαρακτήρα ή διαφημιστική χροιά (παρά μόνο ενημερωτική).

- **Μην διακινείτε** πληροφορίες και **μην προωθείτε ή προβάλλετε** δικτυακούς τόπους που:
  - προπαγανδίζουν την βίαιη και επιθετική συμπεριφορά, το μίσος και το ρατσισμό.
  - προωθούν τα ναρκωτικά, το αλκοόλ και τα τυχερά παιχνίδια.
  - περιέχουν πορνογραφικό περιεχόμενο.
  - αναφέρονται σε παραβιάσεις ασφάλειας διαφόρων υπολογιστικών συστημάτων ή και εφαρμογών.
  - αφορούν στην παράνομη διανομή λογισμικού, ταινιών ή μουσικής.
  - περιέχουν οπτικοακουστικό υλικό που αποτελεί προϊόν πνευματικής δημιουργίας.
  - αφορούν σε υλικό με διαφημιστικά banners.

Επιπλέον, θα πρέπει να ελέγχετε το περιεχόμενο των ηλεκτρονικών μηνυμάτων σας για την πιθανή απομάκρυνση ιών ή άλλων κακόβουλων τμημάτων λογισμικού που μπορούν εν δυνάμει να βλάψουν άλλους χρήστες. Για το λόγο αυτό, προτείνεται στο υπολογιστικό σύστημα να υπάρχει εγκατεστημένο **λογισμικό προστασίας** από ιούς (antivirus) και κακόβουλο λογισμικό, το οποίο να είναι **ενεργό** και να ανανεώνεται **αυτόματα** από τον κατασκευαστή του με τις πληροφορίες για νέους ιούς ή απειλές.

Οδηγίες προς τους εκπαιδευτικούς για την ασφαλή παρουσία των μαθητών στο Διαδίκτυο

Το ΠΣΔ στα πλαίσια καθιέρωσης ενός λειτουργικού πλαισίου για την ασφαλή παρουσία των μαθητών στο Διαδίκτυο κατέγραψε μια σειρά από συμβουλές και πρακτικές οι οποίες παρουσιάζονται παρακάτω:

- Φροντίστε να ενημερώνεστε τακτικά για το Διαδίκτυο και τα οφέλη που προσφέρει (π.χ., στην εκπαιδευτική διαδικασία) αλλά και τους πιθανούς κινδύνους που υπάρχουν.
- Αντιμετωπίστε το Διαδίκτυο και τις συνολικές υπηρεσίες που παρέχει ως ένα πολύτιμο εργαλείο της μαθησιακής διαδικασίας..
- Συζητήστε με τους μαθητές για τα οφέλη αλλά και τους κινδύνους του Διαδικτύου και διαμορφώστε ένα λειτουργικό και ασφαλές πλαίσιο αξιοποίησής του.
- Δημιουργήστε μία λίστα δικτυακών τόπων με κατάλληλο περιεχόμενο που θα προωθεί το σεβασμό των ανθρώπινων αξιών και θα προαγάγει το γνωστικό και πνευματικό επίπεδο των μαθητών.
- Προσπαθήστε μέσω συνεχών ενημερώσεων, γόνιμων συζητήσεων και της επίδειξης καλών πρακτικών, για την ανάπτυξη από τους μαθητές δεξιοτήτων κριτικής χρήσης του Διαδικτύου.
- Ουσιαστική επίβλεψη του περιεχομένου που προσπελαύνουν οι μαθητές και έλεγχος των ιστοσελίδων που επισκέπτονται οι μαθητές μέσω των Αγαπημένων (bookmarks) και του

Ιστορικού (history) των φυλλομετρητών (browsers). Για ειδικές περιπτώσεις και όπου κριθεί απαραίτητο μπορείτε να προβείτε σε σχετικές συστάσεις και παρατηρήσεις.

- Αν συναντήσετε κάποια ιστοσελίδα με ακατάλληλο περιεχόμενο επικοινωνήστε με τον διαχειριστή της υπηρεσίας (cachemaster@sch.gr) του ΠΣΔ.
- Ιδιαίτερη προσοχή πρέπει να δοθεί στην απεικόνιση των μαθητών στις σχολικές ιστοσελίδες. Εφόσον υπάρχουν αντίστοιχες φωτογραφίες θα πρέπει να είναι με αλλοιωμένα χαρακτηριστικά, ενώ σε καμία περίπτωση δεν πρέπει να αντιστοιχίζεται φωτογραφία μαθητή με τα προσωπικά του στοιχεία (ονοματεπώνυμο, τάξη κλπ). Για την επεξεργασία ψηφιακών φωτογραφιών (αλλοίωση χαρακτηριστικών) και την μετέπειτα ανάρτησή τους στις σχολικές ιστοσελίδες μπορείτε να χρησιμοποιήσετε διαδεδομένα προγράμματα επεξεργασίας εικόνας, όπως το Gimp (http://www.gimp.org), το οποίο αποτελεί μια εφαρμογή ανοικτού λογισμικού και είναι διαθέσιμο σε διάφορες υπολογιστικές πλατφόρμες (π.χ., Linux, Mac Os, Windows).
- Συστρατευτείτε στην καταπολέμηση του παράνομου περιεχομένου στο Διαδίκτυο καταγγέλλοντας οποιαδήποτε ιστοσελίδα με παράνομο περιεχόμενο στην **Ελληνική Γραμμή Αναφοράς Παράνομου Περιεχομένου στο Internet** (www.safeline.gr). Επιπλέον αναζήτηστε και διαδώστε αντίστοιχες δράσεις (σε εθνικό και ευρωπαϊκό επίπεδο) λαμβάνοντας ως σημείο εκκίνησης τις ηλεκτρονικές διευθύνσεις που επισημάνθηκαν στο παρόν κείμενο.
- Δραστηριοποίηση των μαθητών με την θέσπιση και διάδοση αντίστοιχων μαθητικών ημερίδων για την παρουσίαση και προβολή απόψεων και εμπειριών για την προστασία από παράνομο και επιβλαβές ψηφιακό περιεχόμενο, την υιοθέτηση καλών πρακτικών πλοήγησης κλπ.

Συγκεκριμένα, όσο αφορά την Πρωτοβάθμια Εκπαίδευση κατόπιν εισήγησης της Επιτροπής Πολιτικής, Διαχείρισης και Δεοντολογίας Περιεχομένου του ΠΣΔ, για την προστασία των μαθητών της Πρωτοβάθμιας Εκπαίδευσης από την έκθεσή τους σε σοβαρούς διαδικτυακούς κινδύνους, η πρόσβαση μέσω των λογαριασμών του ΠΣΔ των σχολείων πρωτοβάθμιας εκπαίδευσης σε κοινωνικά δίκτυα, όπως άλλωστε συμβαίνει στις περισσότερες χώρες της Ευρώπης, **δεν θα παρέχεται ανεξέλεγκτα**. Διευθυντές σχολικών μονάδων Πρωτοβάθμιας μπορούν να ζητούν **εγγράφως με αίτημά τους** προς το Πανελλήνιο Σχολικό Δίκτυο (ΠΣΔ) προσδιορισμένη χρονικά πρόσβαση σε κάποιο κοινωνικό δίκτυο, **στο πλαίσιο συμμετοχής τους σε συγκεκριμένο εκπαιδευτικό πρόγραμμα**, τεκμηριώνοντας αυτή την αναγκαιότητα.

Οι εκπαιδευτικοί εκτός από την επαρκή ενημέρωση των μαθητών, θα πρέπει να συμβουλεύουν και να καθοδηγούν και τους γονείς με βάση και τις οδηγίες που επισημάνθηκαν παραπάνω. Προς αυτή την κατεύθυνση μπορούν να λειτουργήσουν συμπληρωματικά και οι οδηγίες που περιγράφονται στην επόμενη ενότητα.

- **Ας μιλάμε με τα παιδιά για τις δραστηριότητές τους στο διαδίκτυο.** Ας γίνουμε μέρος της ψηφιακής διαδικτυακής τους ζωής και με ειλικρινές ενδιαφέρον ας αναζητήσουμε με τη σύμφωνη γνώμη τους ποιούς ιστοχώρους επισκέπτονται και τί είναι αυτό που τους αρέσει. Είναι σημαντικό να έχουμε υπόψη μας ότι όταν τα παιδιά ξέρουν και νιώθουν ότι τα καταλαβαίνουμε, είναι πιο πιθανό να απευθυνθούν σε εμάς εάν αντιμετωπίσουν οποιοδήποτε πρόβλημα.
- **Ας είμαστε ενημερωμένοι.** Τα παιδιά αναπτύσσουν συνεχώς καινούργιες δεξιότητες ιδιαίτερα σε ότι σχετίζεται με τις ψηφιακές τεχνολογίες. Είναι ιδιαίτερα σημαντικό για τους γονείς να αποβάλλουν οποιαδήποτε τεχνοφοβικά σύνδρομα ή προκαταλήψεις και να παρουσιάσουν αντίστοιχη προσαρμοστικότητα στις ραγδαίες τεχνολογικές εξελίξεις, έτσι ώστε να αντιμετωπιστεί επιτυχώς το ψηφιακό χάσμα που αναπόφευκτα δημιουργείται.
- **Ας θέσουμε όρια στον ψηφιακό και διαδικτυακό κόσμο όπως ακριβώς θα κάναμε και στον πραγματικό.** Ας αναλογιστούμε τον τεράστιο όγκο ψηφιακής πληροφορίας που μπορούν να προσπελάσουν στο διαδίκτυο, τί μπορεί να μοιραστούν, με ποιούς επικοινωνούν και πόσο χρόνο αφιερώνουν (π.χ., σε ημερήσια βάση) στον Η/Υ καθώς και σε άλλες έξυπνες ψηφιακές συσκευές. Ο σεβασμός στην αυτονομία και τις πρωτοβουλίες των παιδιών, ο περιορισμός υπερβολικών αντιδράσεων, η επισήμανση της προσωπικής ευθύνης για την διαχείριση των προσωπικών στοιχείων, μπορούν να αποτελέσουν τον οδηγό και το βασικό πλαίσιο οικογενειακών κανόνων για την οριοθέτηση των δραστηριοτήτων των παιδιών στον ψηφιακό κόσμο.
- **Ας δώσουμε έμφαση στο να κατανοήσουν τα παιδιά ότι αυτό που διατυπώνουν και ο τρόπος που παρουσιάζονται οι διάφοροι χρήστες στο διαδίκτυο δεν ανταποκρίνεται πάντα στην πραγματικότητα.** Είναι σημαντικό να βεβαιωθούμε ότι τα παιδιά έχουν κατανοήσει ότι δεν πρέπει να συναντηθούν, ειδικά χωρίς την φυσική παρουσία ενήλικα, με κάποιο χρήστη που γνώρισαν στο διαδίκτυο. Επίσης, είναι σημαντικό με την κατάλληλη καθοδήγηση να αναπτύξουν κριτικό πνεύμα και να αξιολογούν συστηματικά το περιεχόμενο κάθε πληροφορίας που παρουσιάζεται στο Διαδίκτυο (π.χ., περιπτώσεις διαδικτυακής απάτης).
- **Ας γνωρίζουμε ποιές ψηφιακές συσκευές συνδέονται στο διαδίκτυο και πώς.** Στις μέρες μας υπάρχει πλήθος ψηφιακών συσκευών (π.χ., tablets, smartphones, netbooks) με δυνατότητες σύνδεσης στο διαδίκτυο. Είναι πολύ σημαντικό να είμαστε ενημερωμένοι για το ποιές συσκευές χρησιμοποιούν τα παιδιά για να συνδέονται στο διαδίκτυο (π.χ., κινητά τηλέφωνα, κονσόλες παιχνιδιών κλπ), ενώ είναι κρίσιμο να υπάρχει εποπτεία στην διαχείριση και ασφάλεια των κωδικών πρόσβασης/ενεργοποίησης και να μην κοινοποιούνται σε τρίτους (π.χ., διάφοροι χρήστες στο Διαδικτύο)

- **Ας ενθαρρύνουμε τη χρήση φίλτρων γονεϊκού ελέγχου σε όλες τις ψηφιακές συσκευές που συνδέονται στο διαδίκτυο.** Τα φίλτρα δεν αφορούν μόνο τον **αποκλεισμό** ή **κλείδωμα** ακατάλληλου περιεχομένου και ιστοτόπων, αλλά αποτελούν και ένα εργαλείο που μπορεί να βοηθήσει στη θέσπιση συγκεκριμένων ορίων καθώς τα παιδιά αναπτύσσουν και βελτιώνουν τις δεξιότητές τους στις ψηφιακές τεχνολογίες. Θα πρέπει να έχουμε υπόψη ότι η χρήση των συγκεκριμένων φίλτρων δεν αποτελεί τη λύση για την ψηφιακή ασφάλεια των παιδιών, αλλά διαμορφώνει το κατάλληλο πλαίσιο για την εδραίωσή της.
- **Τοποθετήστε τον υπολογιστή σε ένα κοινόχρηστο χώρο του σπιτιού.** Προτείνεται η τοποθέτηση του υπολογιστικού συστήματος, με δυνατότητες πρόσβασης στο Διαδίκτυο, σε ένα κοινόχρηστο χώρο του σπιτιού (π.χ., σαλόνι ή το καθιστικό) έτσι ώστε να πραγματοποιείται ουσιαστικότερος έλεγχος για τη χρήση του σε καθημερινή βάση. Εάν αυτό δεν είναι εφικτό και πρέπει να τοποθετηθεί στο υπνοδωμάτιο του παιδιού θα πρέπει να μεριμνήσετε για τον εντοπισμό καταστάσεων όπως υπνηλία κατά τη διάρκεια της ημέρας, δυσκολία στον πρωινό ξύπνημα κλπ που πιθανώς να υποδηλώνουν υπερβολική χρήση του Η/Υ και του Διαδικτύου κατ' επέκταση.

Υπηρεσίες Κοινωνικής Δικτύωσης και Μαθητές

Σύμφωνα με μία έρευνα, ένα στα δυο παιδιά στην Ελλάδα δηλώνει ότι παρέχει πολλές προσωπικές πληροφορίες στο Διαδίκτυο και συγκεκριμένα στους ιδιαίτερα δημοφιλείς ιστοχώρους κοινωνικής δικτύωσης, όπως το Facebook (http://www.facebook.com). Επίσης, θεωρούν ότι η ηλεκτρονική κοινωνική δικτύωση είναι ο βολικότερος τρόπος επικοινωνίας, που θα αντικαταστήσει συμβατικές μορφές επικοινωνίας και διάδρασης (π.χ., email). Κανονίζουν τα ραντεβού τους μέσω του Facebook αντί να τηλεφωνήσουν, συζητούν γι' αυτό με τους φίλους τους και χρησιμοποιούν την ηλεκτρονική ιδιόλεκτο (αργκό). Επιπλέον, πολλοί μαθητές δήλωσαν ότι αυτό που τους συναρπάζει στο Facebook είναι ότι γνωρίζουν άτομα που μοιράζονται τα ίδια ενδιαφέροντα, ότι έχουν πρόσβαση σε πληροφορίες που τους ενδιαφέρουν, ακόμη και ότι συγκροτούν ομάδες μελέτης για διάφορες εκπαιδευτικές δραστηριότητες.

Από τα παραπάνω γίνεται αντιληπτό ότι οι εκπαιδευτικοί θα πρέπει να συζητούν με τους μαθητές και να τους προστατεύουν σε ότι σχετίζεται με τις καθημερινές τους δραστηριότητες σε ιστοχώρους κοινωνικής δικτύωσης. Τα παιδιά πρέπει να αντιληφθούν ότι οι άνθρωποι στο Διαδίκτυο, ακόμα και αυτοί με τους οποίους αλληλογραφούν ή συνομιλούν, ακόμα και για πολύ καιρό, αλλά δεν τους γνωρίζουν στο φυσικό κόσμο, δεν είναι πάντοτε αυτοί που φαίνεται ότι είναι. Οι άνθρωποι δεν λένε πάντοτε την αλήθεια στο Διαδίκτυο, οπότε πρέπει να αντιμετωπίζονται με τη δέουσα προσοχή και να υιοθετείται μια κριτική στάση στην διαδικτυακή τους συμπεριφορά.

Πρέπει να βεβαιωθείτε ότι οι μαθητές σας δεν πρέπει να συναντήσουν κάποιο άτομο που γνωρίζουν μόνο μέσω του Διαδικτύου. Ακόμα και αν τα παιδιά επιμένουν ότι έχουν δει φωτογραφία του ατόμου αυτού, εξηγήστε τους ότι η φωτογραφία αυτή μπορεί να είναι πλαστή, για να τα παραπλανήσει και να επιτύχει ευκολότερα να συναντηθεί μαζί τους. Ακόμα και αν δουν κάποιον μέσω web κάμερας, πάλι διατρέχουν τον ίδιο κίνδυνο από πιθανά παιδοφιλικά ή άλλα κυκλώματα, τα οποία, ενδεχομένως, να έχουν επιστρατεύσει και ανήλικα παιδιά με σκοπό να προσελκύσουν άλλα παιδιά.

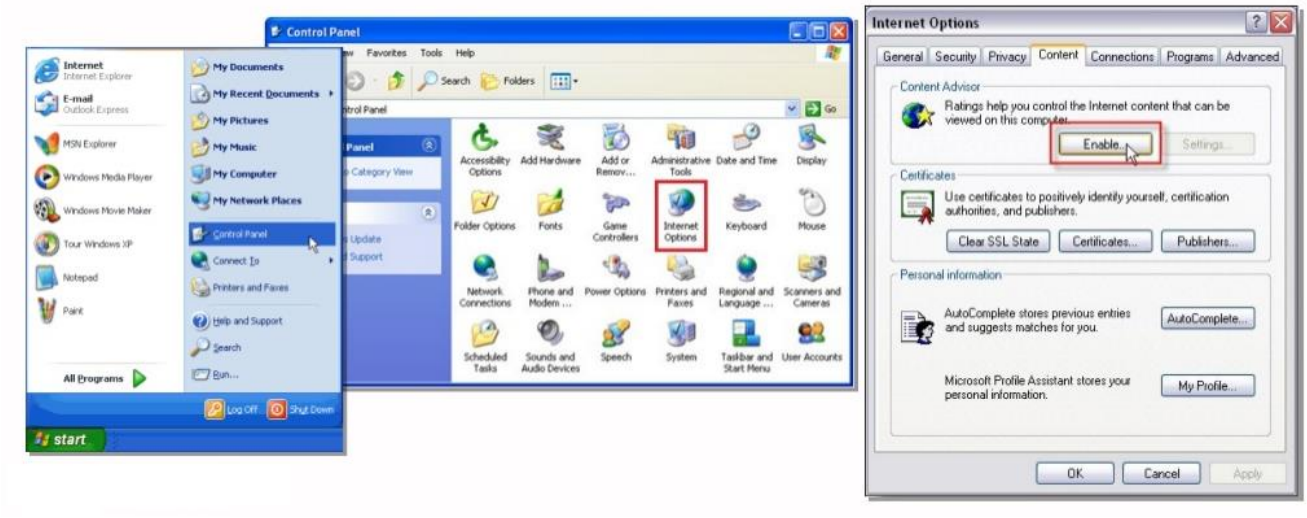
Γονικός Έλεγχος (Parental Control)

Στη συγκεκριμένη ενότητα περιγράφονται τα βήματα ρύθμισης του γονικού ελέγχου σε Windows XP και Windows 7.

Ρύθμιση γονικού ελέγχου σε Windows XP

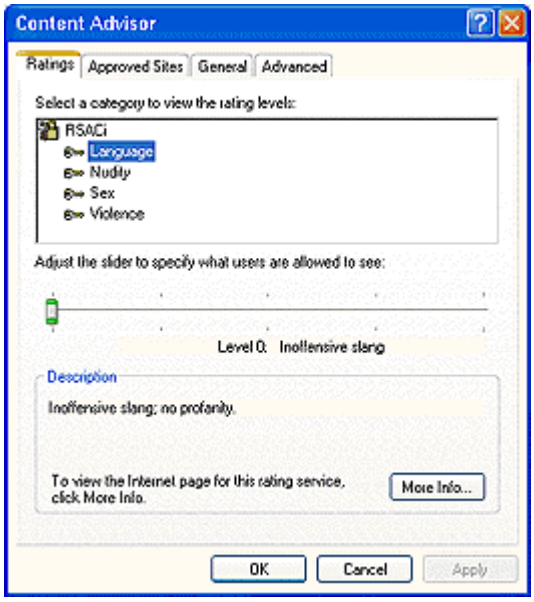
Για να ρυθμίσετε το γονικό έλεγχο σε **Windows XP** ακολουθήστε τα παρακάτω βήματα:

1. Πατήστε στην **«Έναρξη/Start»** και έπειτα επιλέξτε **«Πίνακας Ελέγχου/Control Panel»**.
2. Κάντε κλικ στο εικονίδιο **«Επιλογές Internet/Internet Options»**.
3. Στο πλαίσιο διαλόγου επιλέξτε **«Περιεχόμενο/Content»** και μετά **«Ενεργοποίηση/Enable»**.



Εικόνα 2. *Βήματα 1 – 3 γονικού ελέγχου σε Windows XP*

4. Στο νέο πλαίσιο διαλόγου επιλέξτε την καρτέλα **«Χαρακτηρισμοί/Ratings»** και επιλέγοντας μία-μία τις επιλογές (*Language*, *Nudity* κ.ά.) μπορείτε να μετακινήσετε την κυλιομένη μπάρα στο επιθυμητό επίπεδο προστασίας.
5. Τέλος στην καρτέλα **«Γενικά/General»** μπορείτε να επιλέξετε να μπορεί να βλέπει κανείς σελίδες αμφιβόλου περιεχομένου μετά την εισαγωγή του κωδικού πρόσβασης (τον οποίο τον ορίζετε εσείς από την αντίστοιχη επιλογή).



Εικόνα 3. *Βήματα 4 - 5 γονικού ελέγχου σε Windows XP*

Ρύθμιση γονικού ελέγχου σε Windows 7

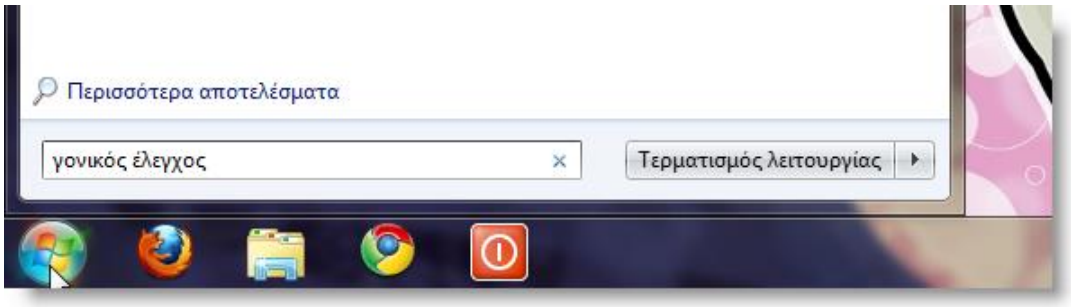
Για να ρυθμίσετε το γονικό έλεγχο σε **Windows 7** ακολουθήστε τα παρακάτω βήματα:

(*Απαραίτητη προϋπόθεση για να εφαρμοστεί ο γονικός έλεγχος σε* Windows 7 *είναι να έχετε ορίσει κωδικό πρόσβασης στο λογαριασμό του διαχειριστή*)

1. Πατήστε **«Έναρξη/Start»** και επιλέξτε **«Πίνακας Ελέγχου/Control Panel»**.
    - Στο επόμενο παράθυρο επιλέξτε **«Λογαριασμοί Χρηστών & Οικ. Ασφάλεια / User Accounts and Family Safety»** και έπειτα **«Λογαριασμοί Χρηστών/User Accounts»**.
    - Επιλέξτε **«Δημιουργία κωδικού πρόσβασης για τον λογαριασμό σας/Create password for your account»**
2. Στο παράθυρο που εμφανίζεται εισάγετε δύο φορές τον επιθυμητό κωδικό και πατήστε **«Δημιουργία Κωδικού πρόσβασης/Create password».**
3. Θα πρέπει να δημιουργήσετε λογαριασμό παιδιού.
4. Εκτελέστε ξανά τις επιμέρους ενέργειες του πρώτου βήματος.
5. Επιλέξτε **«Δημιουργία ενός νέου λογαριασμού/Create a new account»**

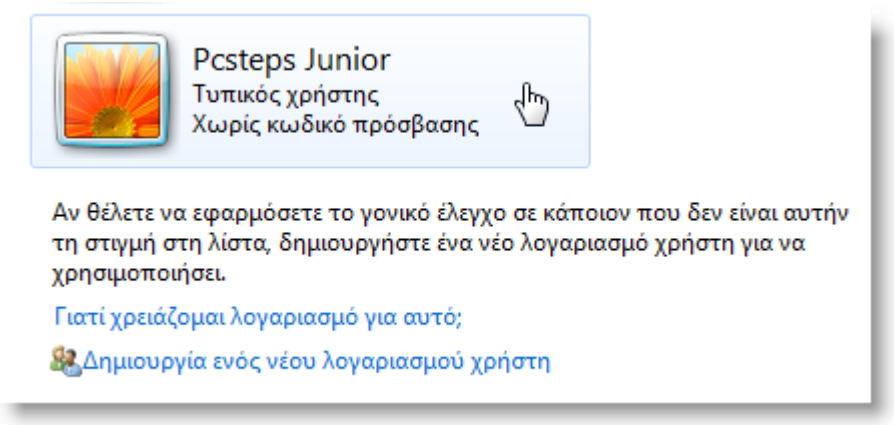
***Εικόνα 4.**– Δημιουργία Λογαριασμού*

6. Πληκτρολογήστε το όνομα του νέου λογαριασμού και πατήστε **«Δημιουργία λογαριασμού/Create account»**.
7. Για να ανοίξετε τη διαχείριση του Γονικού Ελέγχου πληκτρολογήστε στο πεδίο «Αναζήτηση» του μενού έναρξης τη φράση: **«Γονικός έλεγχος/Parental Controls»** και πατήστε Enter.



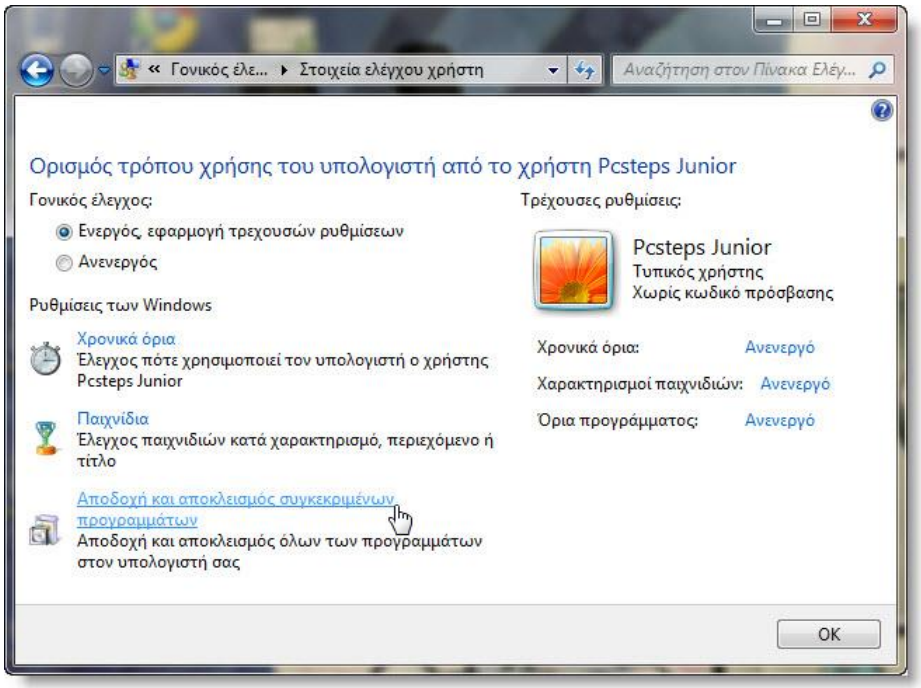
***Εικόνα 5.** Αναζήτηση ρύθμισης γονικού ελέγχου*

8. Όταν ανοίξει το παράθυρο του γονικού ελέγχου κάντε κλικ στο λογαριασμό που θέλετε να παραμετροποιήσετε.



Εικόνα 6. *Επιλογή λογαριασμού χρήστη για παραμετροποίηση*

9. Στο παράθυρο παραμετροποίησης του γονικού ελέγχου επιλέξτε (radio button): **«Ενεργός, εφαρμογή τρεχουσών ρυθμίσεων/ On, enforce current settings»**.

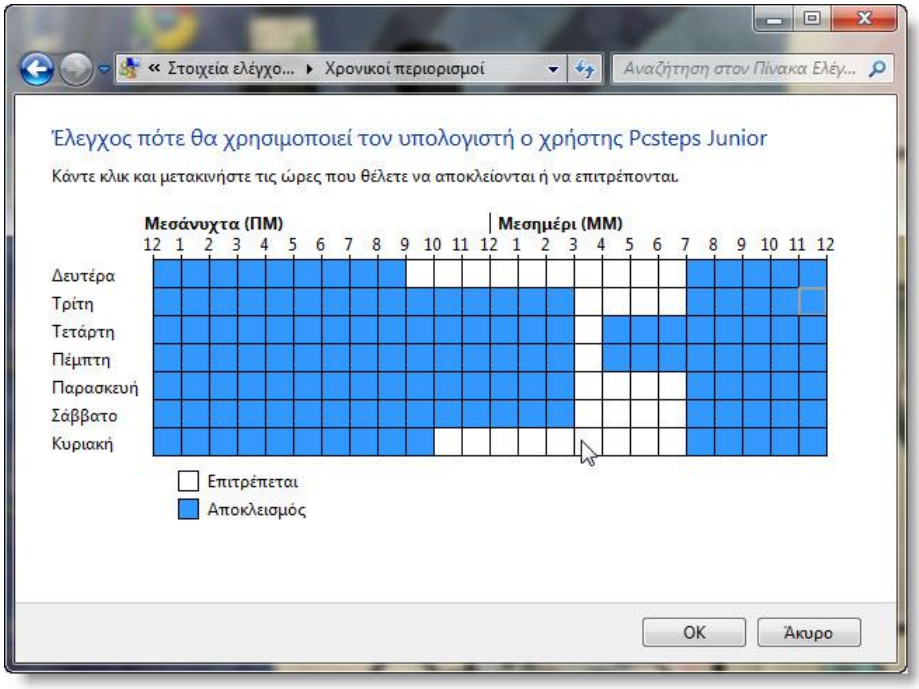


Εικόνα 7. *Παράθυρο παραμετροποίησης γονικού ελέγχου*

Χαρακτηριστικά

Ρύθμιση χρονικών ορίων

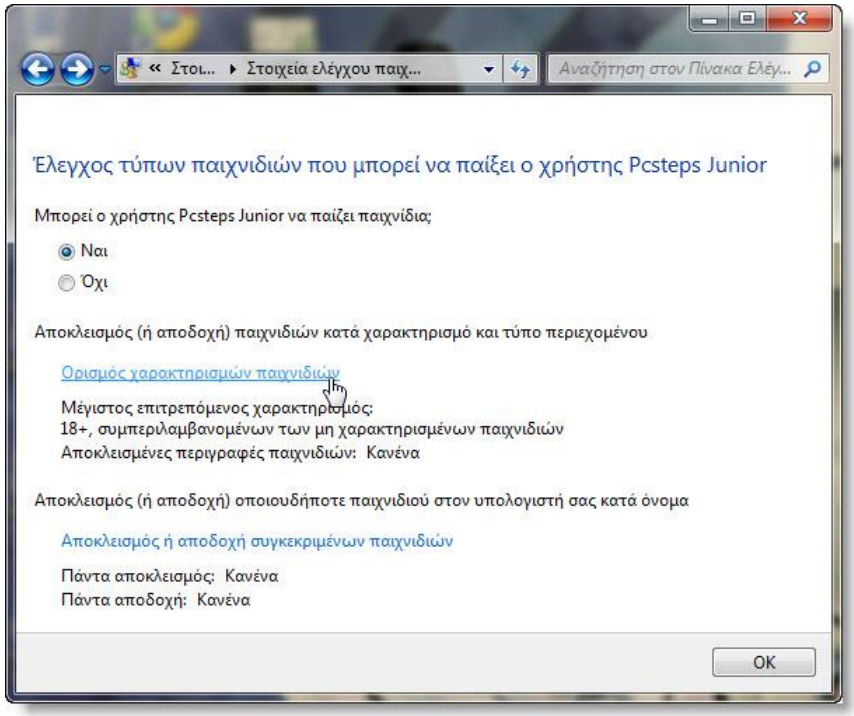
Σε αυτή τη ρύθμιση **(Χρονικά Όρια /Time limits)** μπορείτε να ελέγξετε πότε και για πόση ώρα θα μπορεί ο χρήστης να χρησιμοποιεί τον υπολογιστή. Το μόνο που πρέπει να κάνετε είναι ένα κλικ σε κάποιο από τα *κουτάκια* και να το σύρετε μέχρι αυτά να γίνουν **μπλε**. Τα μπλε κουτάκια είναι οι **ώρες** τις οποίες ο χρήστης **δεν** μπορεί να χρησιμοποιήσει τον υπολογιστή.



Εικόνα 8. *Παράθυρο χρονοπρογραμματισμού χρήσης υπολογιστή*

Ρύθμιση παιχνιδιών

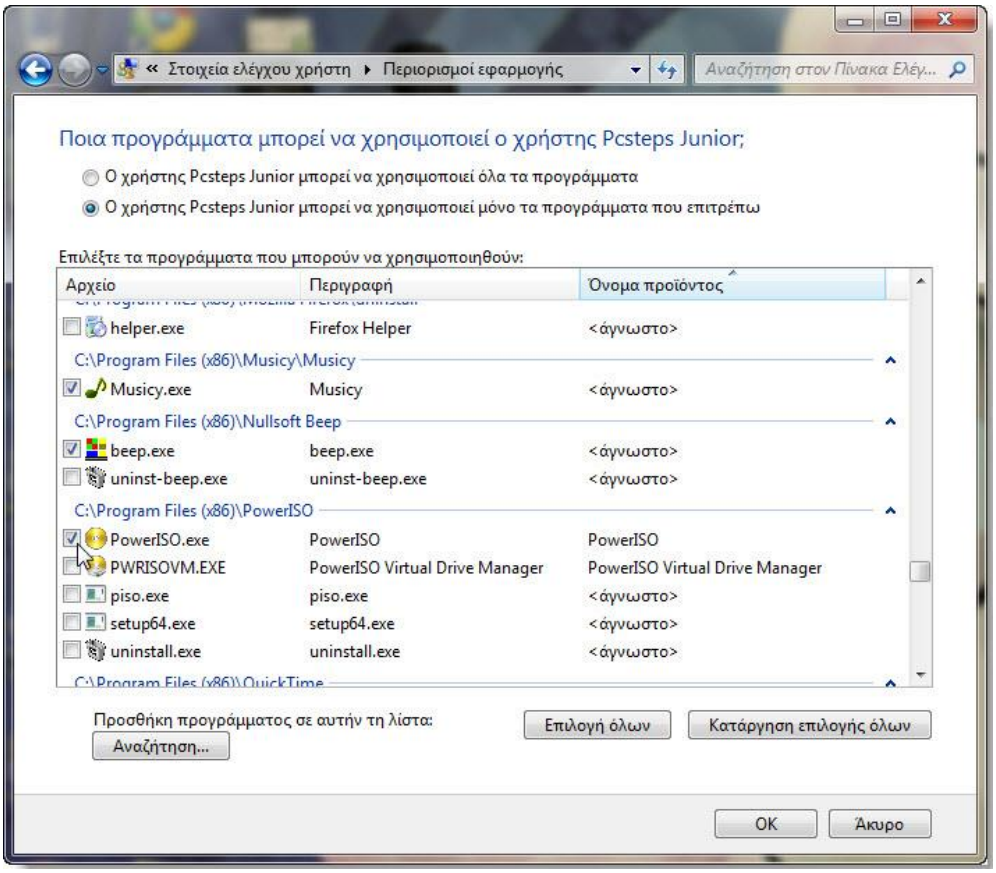
Εδώ μπορείτε να ελέγξετε ποια παιχνίδια μπορεί να παίζει ο χρήστης ανάλογα με την ηλικία του ή άλλων περιορισμών. Κάντε κλικ στην επιλογή **«Ορισμός χαρακτηρισμών παιχνιδιών/Set game ratings»**.



Εικόνα 9*. – Καθορισμός παιχνιδιών στα οποία έχει πρόσβαση συγκεκριμένος χρήστης*

Ρύθμιση πρόσβασης σε προγράμματα

Σε αυτή τη ρύθμιση **«Αποδοχή και αποκλεισμός συγκεκριμένων προγραμμάτων/Allow and block specific programs»** μπορείτε να επιλέξετε ποια προγράμματα μπορεί να χρησιμοποιεί ο χρήστης. Τσεκάρετε από τη λίστα τα επιθυμητά προγράμματα και πατήστε OK.



Εικόνα 10. *– Παράθυρο ρύθμισης πρόσβασης σε συγκεκριμένα προγράμματα*

Μετά από αυτό ο γονικός έλεγχος έχει ρυθμιστεί με επιτυχία.

Κατάσταση Ανώνυμης/Ιδιωτικής Περιήγησης

Η ανώνυμη περιήγηση είναι ένας τρόπος λειτουργίας των φυλλομετρητών ιστού κατά τον οποία δεν αποθηκεύεται καμία πληροφορία ή προσωπικά δεδομένα του χρήστη στον υπολογιστή που χρησιμοποιεί καθώς πλοηγείται στο διαδίκτυο. Συνίσταται να εφαρμόζεται σε κοινόχρηστους υπολογιστές, όπως τους υπολογιστές του σχολείου ή ενός internet café.

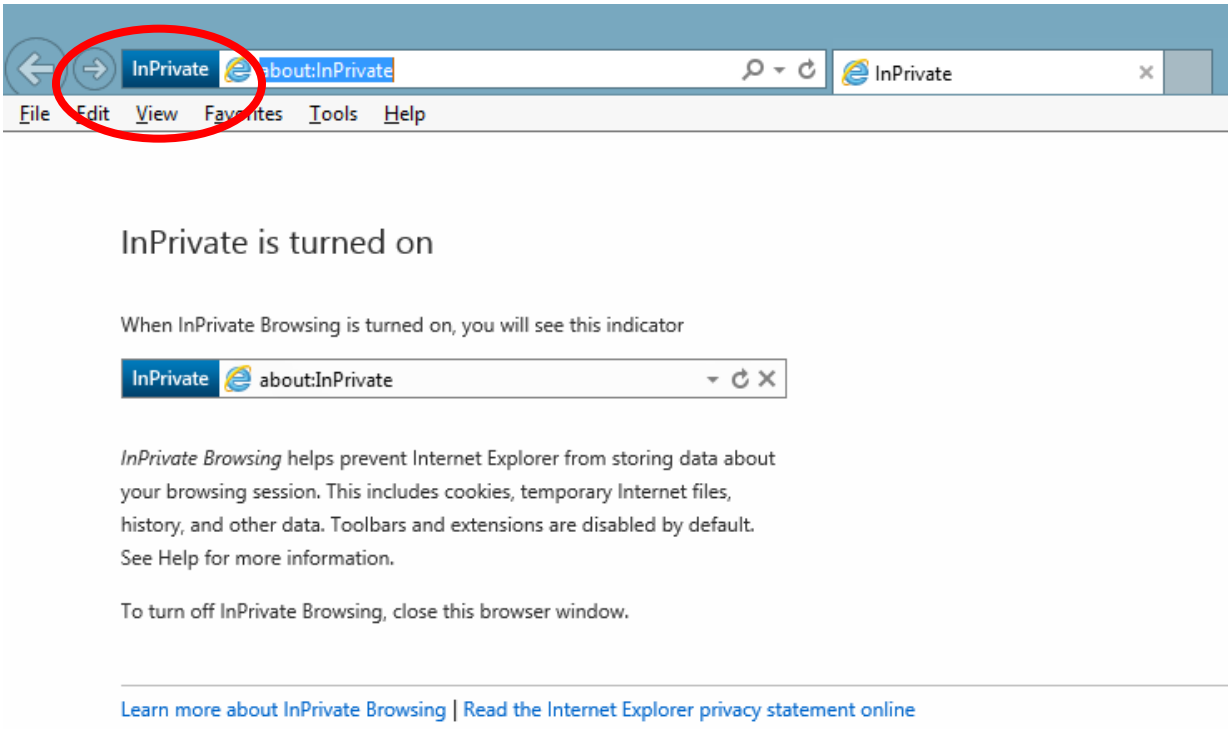
- Όσο χρησιμοποιείτε την ανώνυμη περιήγηση, δεν καταγράφονται στο ιστορικό σας περιήγησης και λήψεων οι ιστοσελίδες που ανοίγετε και τα αρχεία για τα οποία πραγματοποιείτε λήψη αντίστοιχα.

- Όλα τα νέα cookies διαγράφονται μόλις κλείσετε όλα τα παράθυρα ανώνυμης περιήγησης που είχατε ανοίξει.

Στους περισσότερους φυλλομετρητές ιστού η ανώνυμη περιήγηση ενεργοποιείται πατώντας ταυτόχρονα ***Ctrl+Shift+P***.

Διαφορετικά από το Menu επιλογών:

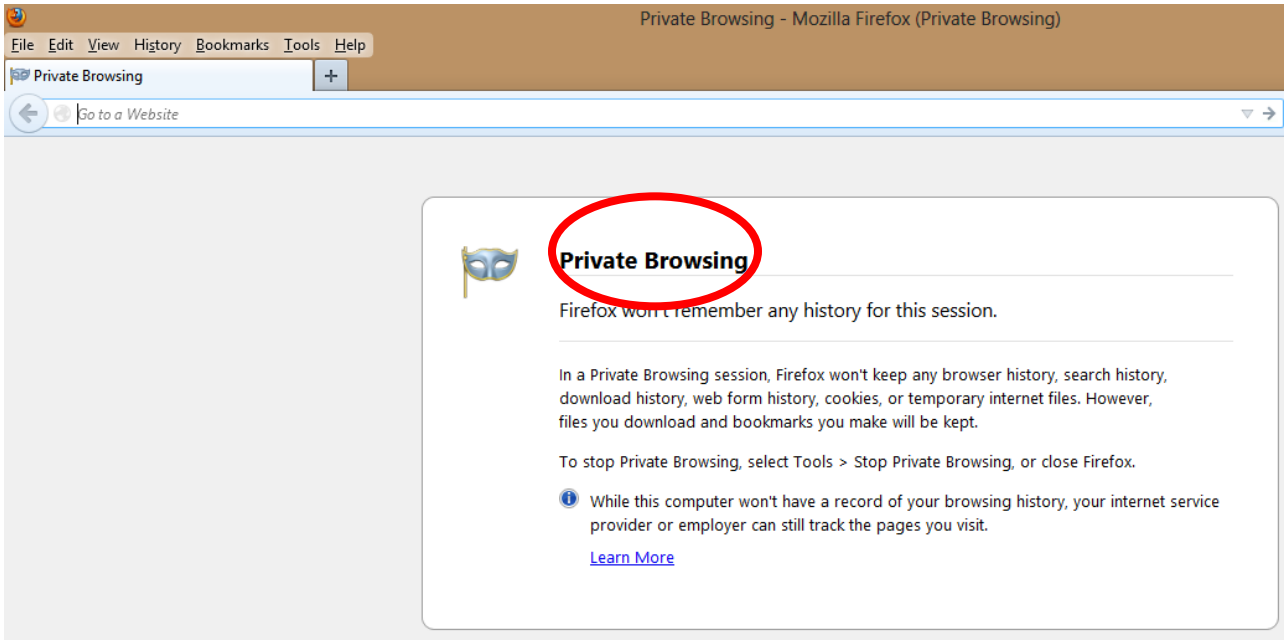
- **Internet Explorer 10:**
  Εργαλεία > Ιδιωτική Περιήγηση (Ctrl+Shift+P)



Εικόνα 11. *Ανώνυμη περιήγηγηση στον Internet Explorer*

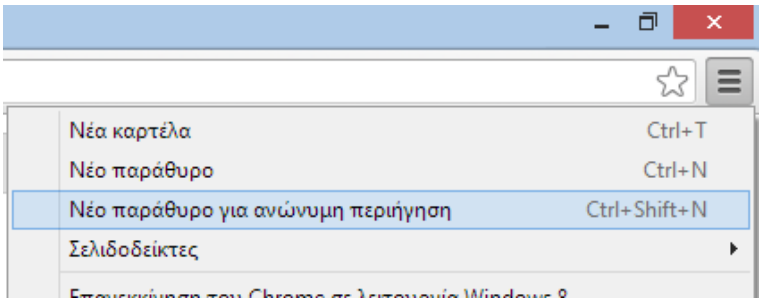
Εμφανίζεται μια νέα καρτέλα του περιηγητή η οποία φέρει το διακριτικό της ανώνυμης περιήγησης.

- **Mozilla Firefox:**
  Εργαλεία > Έναρξη Ανώνυμης Περιήγησης (Ctrl+Shift+P)

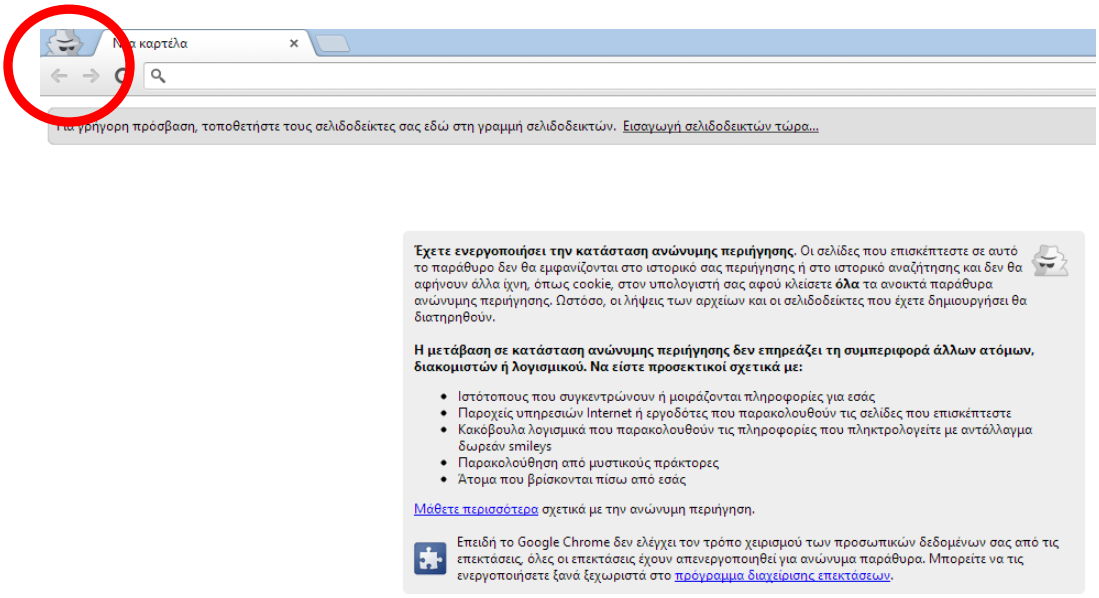


Εικόνα 12. *Ανώνυμη περιήγηση στον Mozilla Firefox*

- **Google Chrome:**
  Εργαλεία > Νέο παράθυρο για ανώνυμη περιήγηση (Ctrl+Shift+N)



Εικόνα 13 *– Έναρξη ανώνυμης περιήγησης στον Google Chrome*



***Εικόνα 14**. Καρτέλα ανώνυμης περιήγησης στον Google Chrome*

Γλωσσάρι ειδικών όρων

Σε αυτή την ενότητα παρατίθενται κάποιοι βασικοί όροι που σχετίζονται με την ασφάλεια στο διαδίκτυο.

Adware

Λογισμικό που εμφανίζει διαφημιστικό περιεχόμενο στον υπολογιστή. Κάποια είδη adware εκτελούνται με την πλήρη γνώση και συγκατάθεσή του χρήστη, ενώ κάποια άλλα όχι. Συνήθως, είναι περισσότερο ενοχλητικά παρά επικίνδυνα, ωστόσο τα προγράμματα adware μπορούν να παρακολουθήσουν τις δραστηριότητές του χρήστη στο διαδίκτυο και να αποστείλουν αυτές τις πληροφορίες σε κάποιον άλλο μέσω του διαδικτύου.

Botnet ή zombie armies

Μια ομάδα υπολογιστών που έχουν παραβιαστεί και βρίσκονται υπό τον έλεγχο ενός τρίτου ατόμου. Αυτό το άτομο χρησιμοποιεί το κακόβουλο λογισμικό που έχει εγκατασταθεί στους παραβιασμένους υπολογιστές προκειμένου να εξαπολύσει επιθέσεις άρνησης εξυπηρέτησης (Denial of Service, DoS), να στείλει μηνύματα spam ή να εκτελέσει άλλες κακόβουλες ενέργειες.

Cookie

Ένα μικρό αρχείο κειμένου που αποθηκεύεται στον υπολογιστή σας όταν επισκέπτεστε μία ιστοσελίδα. Χρησιμοποιείται ώστε η ιστοσελίδα να θυμάται το χρήστη και τις προτιμήσεις του όταν την επισκεφθεί ξανά ή για να καταγράψει τις δραστηριότητές του κατά την πλοήγηση. Τα αρχεία

cookie επιτρέπουν τη χρήση εικονικών καλαθιών σε ηλεκτρονικά καταστήματα, την προσαρμογή διαφόρων σελίδων και τη στοχευμένη διαφήμιση. Δεν είναι προγράμματα και δεν μπορούν να διαβάσουν το σκληρό δίσκο ή να προκαλέσουν ζημιά στον υπολογιστή του χρήστη.

Electronic Footprint

Το ψηφιακό αποτύπωμα που παραμένει στον υπολογιστή και περιλαμβάνει μία καταγραφή από όλες τις σελίδες που επισκέφθηκε ο χρήστης, τα μηνύματα που έστειλε και όλες τις δραστηριότητές του στο διαδικτυακό περιβάλλον.

Griefer

Παίχτης σε ένα διαδικτυακό παιχνίδι που σκόπιμα ενοχλεί και παρενοχλεί άλλους παίχτες του παιχνιδιού.

Identity theft

Σε αυτήν την περίπτωση ένα άτομο αποκτά προσωπικές πληροφορίες ενός άλλου ατόμου (π.χ., πιστωτική κάρτα, αριθμός τραπεζικού λογαριασμού) κυρίως για να κλέψει κάποιο χρηματικό ποσό.

Keylogger

Λογισμικό που παρακολουθεί και καταγράφει οτιδήποτε γράφει ο χρήστης στο πληκτρολόγιο του υπολογιστή. Χρησιμοποιείται για παροχή τεχνικής υποστήριξης και για παρακολούθηση. Ωστόσο, μπορεί να ενσωματωθεί σε κακόβουλο λογισμικό και να χρησιμοποιηθεί για την υποκλοπή κωδικών πρόσβασης, ονομάτων χρήστη και άλλες προσωπικές πληροφορίες.

Malware

Προέρχεται από τις λέξεις "malicious software" (Κακόβουλο λογισμικό). Λογισμικό σχεδιασμένο για να βλάψει, καταστρέφοντας συστήματα και δεδομένα, παραβιάζοντας την ιδιωτικό απόρρητο, υποκλέπτοντας πληροφορίες, ή παραβιάζοντας υπολογιστές χωρίς άδεια. Σε αυτά περιλαμβάνονται ιοί, worm, Trojan horse, κάποια προγράμματα keylogger, προγράμματα spyware, adware, και bot.

Netiquette- Κώδικας δεοντολογικής συμπεριφοράς στο Διαδίκτυο

Το σύνολο των κανόνων που ορίζουν την αποδεκτή συμπεριφορά μεταξύ δύο ή περισσότερων χρηστών του Διαδικτύου κατά την ηλεκτρονική τους επικοινωνία.

URL spoofing

Προσπάθεια *μεταμφίεσης* ή *απομίμησης* της διεύθυνσης URL που εμφανίζεται στη γραμμή διεύθυνσης του προγράμματος πλοήγησης. Χρησιμοποιείται σε επιθέσεις phishing και άλλες διαδικτυακές απάτες προκειμένου να κάνει τις πλαστές ιστοσελίδες να μοιάζουν σαν νόμιμες. Αυτός

που πραγματοποιεί την επίθεση στην ουσία κρύβει την πραγματική διεύθυνση URL καλύπτοντάς την με μία φαινομενικά νόμιμη διεύθυνση ή με τη χρήση μίας παρόμοιας διεύθυνσης URL.

Σύνοψη

Στο παρόν εκπαιδευτικό υλικό παρουσιάστηκε το βασικό πλαίσιο πρακτικές, οδηγιών και πολιτικών που μπορούν να εδραιώσουν την Ασφάλεια στο διαδίκτυο. Επισημάνθηκαν κάποιοι βασικοί άξονες που ακολουθεί το ΠΣΔ και προτάθηκαν ορισμένες συμβουλές προς τους εκπαιδευτικούς και τους μαθητές. Τέλος, περιγράφηκε η πολιτική που ακολουθεί το ΠΣΔ και στο τέλος κατεγράφησαν κάποιοι βασικοί όροι που συναντώνται πολύ συχνά και σχετίζονται με την ασφάλεια στο διαδίκτυο.

Λίστα Ελέγχου Γνώσεων

Με την ολοκλήρωση του παρόντος εκπαιδευτικού αντικειμένου, ελέγξτε κατά πόσο:

- Μπορείτε να περιγράψετε την έννοια της ασφάλειας στο διαδίκτυο.
- Έχετε εμπεδώσει ότι η φύση του Διαδικτύου δεν εγγυάται ασφάλεια στον τελικό χρήστη.
- Έχετε κατανοήσει τις συμβουλές για την ασφάλεια των μαθητών.
- Έχετε κατανοήσει ότι οι δημοσιευμένες πληροφορίες στο Διαδίκτυο δεν χαρακτηρίζονται πάντα από καταλληλότητα και εγκυρότητα.
- Μπορείτε να δείξετε στους γονείς των μαθητών τη διαδικασία εφαρμογής του γονικού ελέγχου.
- Μπορείτε να κάνετε τις απαραίτητες υποστηρικτικές ενέργειες σε περίπτωση παραβίασης της διαδικτυακής ασφάλειας ενός μαθητή.

Σημαντική Παρατήρηση

Το παρόν εκπαιδευτικό υλικό θα πρέπει να θεωρηθεί σημείο εκκίνησης. Η συγγραφή του ολοκληρώθηκε τον Μάρτιο του 2013. Το συγκεκριμένο υλικό επικαιροποιείται ανά τακτά χρονικά διαστήματα, οι αλλαγές δημοσιεύονται στο www.sch.gr και στον δικτυακό τόπο http://internet-safety.sch.gr/.