2ο ΠΕ.Κ.Ε.Σ. Ιονίων Νήσων

Μπαρμπόπουλος Γεώργιος

Συντονιστής Εκπαιδευτικού Έργου κλ. ΠΕ86

Ασφαλής χρήση του Διαδικτύου και των ψηφιακών πόρων e-πολιτειότητα

Δημοσιεύθηκε από European Schoolnet 2014

Νέοι και Διαδίκτυο - Δραστηριότητες από νέους για νέους.

Το Διαδίκτυο που θέλουμε

Το έργο συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση

insafe

saferinternet.gr

Google

LIBERTY GLOBAL

Σκοπός

Να αποκτήσουμε

- **λειτουργικού χαρακτήρα γνώσεις για τη φύση και το είδος των κινδύνων που συνδέονται με τη χρήση των ΤΠΕ, γενικότερα των ψηφιακών πόρων και κυρίως του Διαδικτύου**
- **μερικές βασικές γνώσεις γύρω από τις νέες μορφές *ψηφιακής πολιτειότητας***
- **γνώσεις σχετικά με στρατηγικές διαχείρισης ψηφιακών πληροφοριών από τους μαθητές**
- **γνώσεις διδακτικής οι οποίες θα μας επιτρέψουν να διδάξουμε τα σχετικά θέματα στους μαθητές μας (ψηφιακής πολιτειότητας και διαχείρισης της πληροφορίας)**

Ψηφιακή Πολιτειότητα

Με τον όρο πολιτειότητα νοείται γενικά το δικαίωμα, αλλά και η υποχρέωση του να είναι κανείς πολίτης, δηλαδή νοείται ο πολιτικός, κοινωνικός και νομικός δεσμός που συνδέει κάποιον ως πολίτη ενός κράτους με το κράτος αυτό και συνεπάγεται ορισμένα δικαιώματα και υποχρεώσεις.

Το «βάρος» στην πολιτειότητα δίνεται ακριβώς στο πολιτικό και κοινωνικό σκέλος του ορισμού: αυτό που ενδιαφέρει είναι κατά κύριο λόγο το πώς μπορεί κανείς να διεκδικήσει τα δικαιώματά του και να ανταποκριθεί στις υποχρεώσεις του ως πολίτη, ιδιαίτερα στην ψηφιακή εποχή και στο σύγχρονο ψηφιακό οικοσύστημα.

Στόχοι (1/2)

Να είμαστε σε θέση να προσδιορίσουμε

- **ποιοι θεωρούνται γενικά κίνδυνοι που συνδέονται με τη χρήση και διαχείριση ψηφιακών πόρων και ιδιαίτερα του Διαδικτύου**
- **ποιοι από τους κινδύνους είναι ιδιαίτερα συνδεδεμένοι με τις μικρές ηλικίες, το σχολείο, την εκπαίδευση**

Να αποκτήσουμε γνώσεις και δεξιότητες

- **για την αντιμετώπιση των κινδύνων και τη διδασκαλία των σχετικών θεμάτων είτε με τρόπο άμεσο (οργανώνοντας μαθήματα επί τούτου), είτε έμμεσα (στα πλαίσια δραστηριοτήτων άλλων γνωστικών αντικειμένων)**

Στόχοι (2/2)

Να αποκτήσουμε

- **γνώσεις και δεξιότητες σχετικές με την e- πολιτειότητα, το σύνολο των ψηφιακών πρακτικών που συνδέονται με την ιδιότητα του πολίτη**
- **γνώσεις σχετικά με τη διαχείριση ψηφιακών πληροφοριών (θέματα στρατηγικών αναζήτησης πληροφοριών, αναφοράς πηγών πληροφοριών, ελέγχου της ποιότητας των πληροφοριών, καλών πρακτικών επικοινωνίας και διάχυσης/μεταβίβασης πληροφοριών)**
- **βασικές γνώσεις που θα μας επιτρέψουν να είμαστε διαρκώς ενήμεροι στις νεότερες εξελίξεις για τα θέματα κινδύνων στο Διαδίκτυο, ψηφιακής πολιτειότητας και διαχείρισης των ψηφιακών πληροφοριών**

Ένταξη του αντικειμένου στο πρόγραμμα σπουδών

- **Το θέμα της ασφαλούς πλοήγησης στο Διαδίκτυο και της γενικά ασφαλούς χρήσης των ψηφιακών πόρων, όπως και το θέμα της e-πολιτειότητας δε συνδέονται με κάποια συγκεκριμένη σχολική τάξη, ούτε και με συγκεκριμένο περιεχόμενο (μάθημα).**

Προκαταρκτικά

- **Η έννοια του κινδύνου (συνδεδεμένη και με την έννοια της «απειλής» αλλά και της αντίθετης εννοίας της «ασφάλειας» και της «προφύλαξης», όπως και με την έννοια της «απαγόρευσης» για την προστασία των ευάλωτων ατόμων) είναι σε μεγάλο βαθμό μια κοινωνική κατασκευή και δεν είναι «σταθερή» στον χρόνο και στον χώρο, σε κάθε κουλτούρα.**

- **Οι έφηβοι συχνά «περνούν τα όρια», έλκονται από τον κίνδυνο και αγνοούν τις απαγορεύσεις. Αυτό ίσως σημαίνει πως όποια μέτρα και αν λάβουν το σχολείο και οι γονείς, οι έφηβοι στον ιδιωτικό τους χώρο και χρόνο θα επισκεφτούν ιστοχώρους που θεωρούνται ακατάλληλοι ή επικίνδυνοι και θα δοκιμάσουν να κάνουν ενέργειες που δεν εγκρίνουν οι ενήλικοι.**

Μερικοί ορισμοί

- ***Οι διαδικτυακοί κίνδυνοι μπορούν να οριστούν ως κάθε τι που μπορεί να προκαλέσει βλάβη σε έναν χρήστη του Διαδικτύου. Η βλάβη αυτή μπορεί να είναι διαφόρων μορφών όπως φυσική, συναισθηματική, ψυχολογική, οικονομική, κοινωνική ή αναφερόμενη στην υπόληψη του χρήστη.*** **M. J. Volkmann, in A. Καμάρης, 2014.**

- ***Οι διαδικτυακοί κίνδυνοι είναι κίνδυνοι που σχετίζονται με το να είναι κάποιος χρήστης του Διαδικτύου. Οι κίνδυνοι αυτοί μπορεί επίσης να αφορούν στην πρόσβαση σε ανεπιθύμητες πληροφορίες. Υπάρχει μεγάλη ποικιλία διαδικτυακών κινδύνων από θέματα ασφάλειας έως διάφορα είδη θυματοποίησης.*** **J. M. Warner-Blankenship, 2011, in A. Καμάρης, 2014.**

Κατηγορίες (1/2)

- Ακατάλληλο – προσβλητικό περιεχόμενο ιστοχώρων (Offensive content).
- Ανεπιθύμητα μηνύματα που αποστέλλονται σε χρήστες (Spam messages).
- Αποξένωση των χρηστών από τον πραγματικό κόσμο (Social isolation). Διαμόρφωση ταυτότητας. Έκθεση στα κοινωνικά δίκτυα.
- Ηλεκτρονική αποπλάνηση χρηστών (Online grooming).
- Βίαια παιχνίδια (Violent games).
- Διαδικτυακός εθισμός ή εξάρτηση των χρηστών (Internet addiction).
- Διαδικτυακός εκφοβισμός (Cyberbullying).
- Παρώθηση σε επιβλαβείς συμπεριφορές.
- Ηλεκτρονικός τζόγος (Online gambling)

Κατηγορίες (2/2)

- **Κακόβουλο λογισμικό που μολύνει ηλεκτρονικούς υπολογιστές (Malware).**
- **Παιδική πορνογραφία (Child pornography).**
- **Παραβίαση της ιδιωτικότητας των χρηστών (Internet privacy).**
- **Παραπληροφόρηση που διαχέεται στο Διαδίκτυο (Misinformation). Ψευδή νέα. Αστικοί μύθοι. Ψηφιακές φάρσες.**
- **Υποκλοπή προσωπικών δεδομένων των χρηστών μέσω «Phishing».**
- **Υποκλοπή προσωπικών δεδομένων των χρηστών μέσω «Pharming».**
- **Φυσικές παθήσεις από παρατεταμένη χρήση του Η/Υ.**

Ακατάλληλο περιεχόμενο

Το περιεχόμενο ενός ιστοχώρου (λεκτικό, οπτικό ή ακουστικό) θεωρείται ακατάλληλο ή προσβλητικό όταν παραβιάζει τα κοινωνικά, θρησκευτικά ή πολιτισμικά πρότυπα ή τις προσωπικές και οικογενειακές αξίες του ατόμου. Είναι προφανές ότι όλες αυτές οι διατυπώσεις πρέπει να λαμβάνονται υπόψη μέσα στη σχετικότητά τους, αφού τα πολιτισμικά, κοινωνικά ή θρησκευτικά πρότυπα δεν έχουν καθολικό χαρακτήρα. Έτσι, η ακαταλληλότητα του περιεχομένου ενός ψηφιακού πόρου και ο βαθμός επικινδυνότητάς του σχετίζεται με τα ατομικά χαρακτηριστικά του χρήστη.

Ανεπιθύμητα μηνύματα (Spam)

Αγαπητέ πελάτη,
Έχετε λάβει ένα νέο μήνυμα,
Κάντε *κλικ* εδώ για να το διαβάσετε.
(αληθινό μήνυμα)

Είναι προφανές ότι πρόκειται για μήνυμα που αποσκοπεί στην εξαπάτηση του χρήστη. Εξάλλου ο υπερσύνδεσμος (στο κλικ) οδηγεί σε έναν άσχετο με οιαδήποτε Τράπεζα και πιθανότατα επικίνδυνο ιστότοπο (για να το διαπιστώσει, αρκεί να «περάσει» κανείς με το ποντίκι πάνω από τον υπερσύνδεσμο χωρίς να κάνει «κλικ»).

Αποξένωση των χρηστών

Παρατηρείται κυρίως σε νεαρά άτομα, αλλά όχι αποκλειστικά. Οι χρήστες ασχολούνται σταδιακά ολοένα και περισσότερο με διαδικτυακά και γενικότερα ψηφιακά παιχνίδια, με την άμεση online συνομιλία (chat rooms), με σελίδες κοινωνικής δικτύωσης κ.ά. και αποξενώνονται από τον φυσικό και κοινωνικό τους περίγυρο. Ο χρόνος που αφιερώνουν στις ενασχολήσεις αυτές γίνεται τελικά τόσο μεγάλος, που αποκλείει άλλου είδους δραστηριότητες ατομικές ή ομαδικές.

Διαδικτυακός εκφοβισμός (Cyberbullying) (1/2)

«μια επιθετική, σκόπιμη και επαναλαμβανόμενη πράξη η οποία πραγματοποιείται από ένα άτομο ή μια ομάδα ατόμων, μέσω της χρήσης ηλεκτρονικών μορφών επικοινωνίας, εναντίον ενός ατόμου που δεν μπορεί εύκολα να υπερασπιστεί τον εαυτό του»

Διαδικτυακός εκφοβισμός (Cyberbullying) (2/2)

- Η διακωμώδηση ή/και εξευτελισμός του θύματος.
- Η αποστολή προσβλητικών και άσεμνων μηνυμάτων μέσω Διαδικτυακών εφαρμογών.
- Το άσεμνο περιεχόμενο κατά τη διάρκεια συνομιλιών.
- Ο εξευτελισμός ενός νεαρού ατόμου με τη δημιουργία ενός προφίλ ή ιστολογίου το οποίο περιλαμβάνει σκόπιμα λανθασμένα στοιχεία ή εξευτελιστικό περιεχόμενο.
- Η αποστολή απειλητικών μηνυμάτων.
- Η δημοσιοποίηση προσωπικών βίντεο ή φωτογραφιών χωρίς τη συγκατάθεση του ατόμου.

Παραπληροφόρηση (Misinformation)

Το Διαδίκτυο παρέχει πόρους και ευκαιρίες μάθησης, αλλά δε διαθέτει τις απαραίτητες δικλείδες ασφαλείας για τον έλεγχο της εγκυρότητας των πληροφοριών που δημοσιεύονται. Σε κάποιες περιπτώσεις με τη δημοσίευση αναληθών, τροποποιημένων ή ελλιπών πληροφοριών, ο χρήστης μπορεί να οδηγηθεί σε λανθασμένα, αναξιόπιστα συμπεράσματα.

Αντιμετώπιση του κυβερνοεκφοβισμού (1/5)

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

- **Αν έλαβε ποτέ κάποιο email ή γραπτό μήνυμα που το αναστάτωσε.**
- **Αν ανάρτησε κανείς στο διαδίκτυο μια φωτογραφία ή ένα βίντεο με το παιδί, χωρίς να του ζητήσει την άδεια.**
- **Αν συμμετείχε στον εκφοβισμό κάποιου άλλου στο διαδίκτυο ή μέσω του κινητού του.**

Αντιμετώπιση του κυβερνοεκφοβισμού (2/5)

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

- **Καθησυχάστε το πως έπραξε ορθά λέγοντάς σας τι συμβαίνει.**
- **Εξηγήστε ότι δεν πρέπει να απαντά στον εκφοβισμό, καθώς αυτό θα μπορούσε να χειροτερέψει τα πράγματα.**
- **Καθίστε με το παιδί να καταγράψετε το περιστατικό εκφοβισμού και να συλλέξετε στοιχεία, π.χ. σώζοντας γραπτά μηνύματα ή εκτυπώνοντας email και στιγμιότυπα οθόνης από ιστοτόπους. Μη σβήσετε τίποτε.**
- **Εκμεταλλευθείτε στο μέγιστο τα ενσωματωμένα εργαλεία στις υπηρεσίες διαδικτύου ή κινητής τηλεφωνίας του παιδιού σας, ώστε να αποτρέψετε περαιτέρω εκφοβισμό. Για παράδειγμα, μπορείτε να αφαιρέσετε από τις λίστες των «φίλων» αυτόν που διέπραξε τον εκφοβισμό και να ρυθμίσετε το προφίλ κοινωνικής δικτύωσης του παιδιού σας ώστε να είναι «απόρρητο», αν δεν είναι ήδη.**

Αντιμετώπιση του κυβερνοεκφοβισμού (3/5)

- **Επικοινωνήστε με τον πάροχο των υπηρεσιών διαδικτύου, κινητής τηλεφωνίας ή κοινωνικής δικτύωσης. Αν ό,τι συνέβη παραβαίνει τους Όρους Χρήσης ή τις Οδηγίες Κοινότητας του παρόχου, αυτός μπορεί να αναστείλει τον λογαριασμό του ατόμου που διέπραξε τον εκφοβισμό, να καταργήσει περιεχόμενο ή να εγκαταστήσει νέο αριθμό κινητού, για παράδειγμα.**
- **Αν το παιδί σας πιστεύει πως αυτός που διέπραξε τον εκφοβισμό είναι συμμαθητής του, μιλήστε στον δάσκαλό του.**
- **Αν πιστεύετε ότι διεπράχθη έγκλημα ή αν ανησυχείτε ότι το παιδί σας διατρέχει άμεσο κίνδυνο, επικοινωνήστε με την αστυνομία και συγκεκριμένα με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος.**

Αντιμετώπιση του κυβερνοεκφοβισμού (4/5)

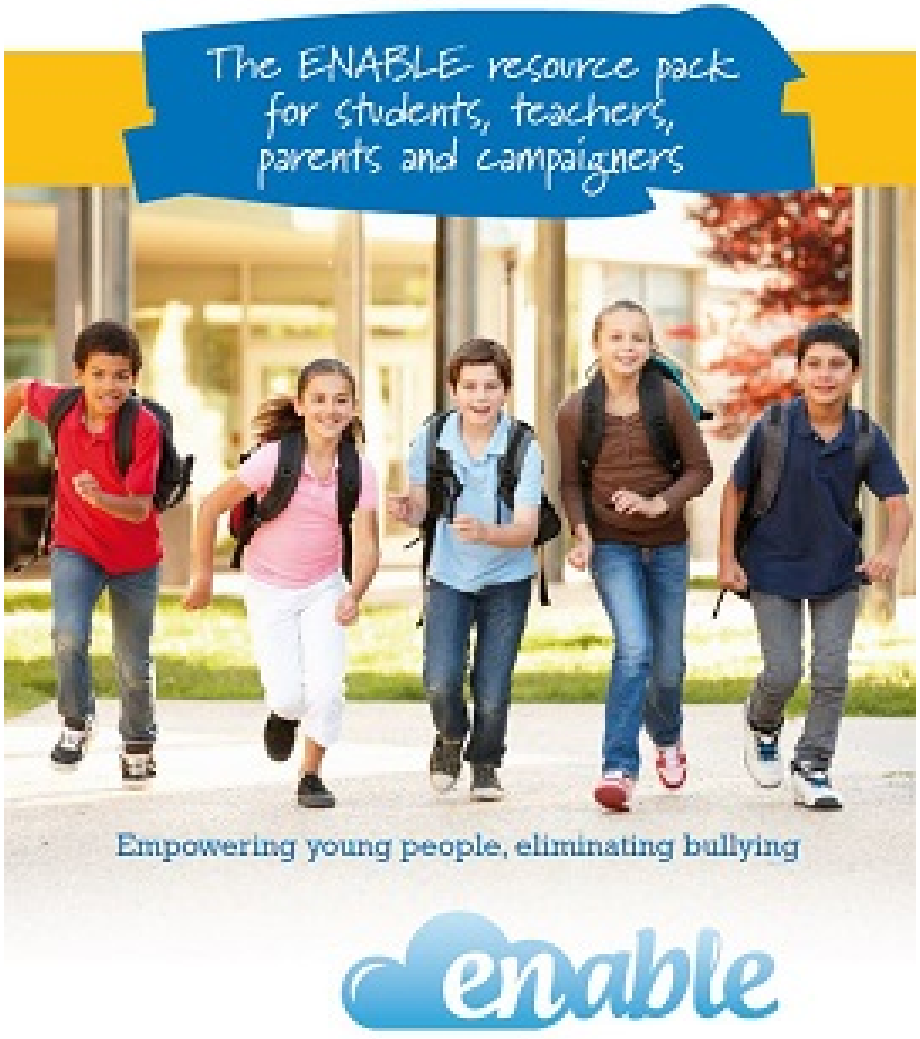
Αν πιστεύετε ότι το παιδί σας θα μπορούσε να χρησιμοποιεί νέες τεχνολογίες για να εκφοβίσει κάποιον άλλον:

- **Μιλήστε του σχετικά με τον διαδικτυακό εκφοβισμό και εξηγήστε γιατί αυτό είναι απαράδεκτο και πρέπει να σταματήσει.**
- **Συζητήστε ανοιχτά με το παιδί σας. Ρωτήστε το γιατί το κάνει κι ακούστε τι έχει να σας πει.**
- **Αν δεν είχε συνειδητοποιήσει πως αυτό που έκανε ήταν εκφοβισμός, εξηγήστε του ότι ο εκφοβισμός δεν είναι απλώς σωματικός. Το να χρησιμοποιείς την τεχνολογία για να πειράζεις, να εξευτελίζεις και να διαβάλλεις, είναι επίσης εκφοβιστική συμπεριφορά.**

Αντιμετώπιση του κυβερνοεκφοβισμού (5/5)

- **Μιλήστε στον δάσκαλό του σχετικά με το τι συμβαίνει και δείξτε του ότι είστε πρόθυμος να συνεργαστείτε με το σχολείο ώστε να εξασφαλίσετε πως δεν θα ξανασυμβεί.**
- **Καθησυχάστε το παιδί σας πως ακόμη το αγαπάτε, αλλά ξεκαθαρίστε του ότι η συμπεριφορά του πρέπει να αλλάξει.**
- **Προτρέψτε το να μιλήσει σε εσάς ή σε έναν δάσκαλο, για οποιονδήποτε εκφοβισμό στον οποίον είναι μάρτυρας, συμπεριλαμβανομένων των περιστατικών διαδικτυακού εκφοβισμού.**

Επιπλέον Υλικό



Εγχειρίδιο Καταπολέμησης του Σχολικού Εκφοβισμού για Γονείς και Κηδεμόνες

Σας ευχαριστούμε