ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Προγράμματα Συμπληρωματικής Εκπαίδευσης

Με τη χρήση καινοτόμων μεθόδων εξ αποστάσεως εκπαίδευσης

ΑΡΙΑΔΝΗ:
ΠΡΟΓΡΑΜΜΑ ΚΑΤΑΡΤΙΣΗΣ ΕΠΑΓΓΕΛΜΑΤΙΩΝ ΨΥΧΙΚΗΣ ΥΓΕΙΑΣ ΓΙΑ ΤΟ ΦΑΙΝΟΜΕΝΟ ΤΟΥ «ΕΘΙΣΜΟΥ» ΤΩΝ ΕΦΗΒΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΘΩΣ ΚΑΙ ΓΙΑ ΤΟΥΣ ΚΙΝΔΥΝΟΥΣ ΠΟΥ ΑΝΤΙΜΕΤΩΠΙΖΟΥΝ ΤΑ ΠΑΙΔΙΑ ΚΑΙ ΟΙ ΕΦΗΒΟΙ ΑΠΟ ΤΗΝ ΑΝΕΞΕΛΕΓΚΤΗ ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

ΤΗΛΕΚΠΑΙΔΕΥΣΗ Α' ΜΕΡΟΣ: ΚΟΙΝΩΝΙΚΗ ΔΙΚΤΥΩΣΗ – CYBERBULLYING -PHISHING ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΠΙΧΕΙΡΕΙΝ

Π Ε Ρ Ι Ε Χ Ο Μ Ε Ν Α

Σκοπός της Διδακτικής Ενότητας

Σκοπός της διδακτικής ενότητας είναι να καταδείξει την κοινωνική δικτύωση όσο πιο συνοπτικά γίνεται, να αναφέρει ενδεικτικά ιστοχώρους κοινωνικής δικτύωσης, και να αναδείξει τα ζητήματα και κυρίως την αντιμετώπιση περιστατικών ασφαλείας. Θα παρουσιαστεί επίσης το φαινόμενο του κυβερνοεκφοβισμού (ή δικτυακού εκφοβισμού, ή ηλεκτρονικής παρενόχλησης), θα προταθούν συμβουλές και θα αναδειχθούν τρόποι προστασίας για το συγκεκριμένο ζήτημα. Τέλος, η ενότητα θα παρουσιάσει το φαινόμενο του phishing σε όλες του τις μορφές, και θα προτείνει τρόπους προστασίας απέναντι στο πρόβλημα που έχει ανακύψει κυρίως μέσω του ηλεκτρονικού επιχειρείν, θα παρουσιάσει παραδείγματα και θα προτείνει λύσεις στο συγκεκριμένο θέμα. Επίσης, θα παρουσιάσει περιπτώσεις κακόβουλου λογισμικού το οποίο χρησιμοποιείται σε αυτές τις περιπτώσεις -και όχι μόνο.

Προσδοκώμενα αποτελέσματα

Όταν ολοκληρωθεί η παρουσίαση της ενότητας οι εκπαιδευόμενοι θα είναι σε θέση:

- να γνωρίζουν την επικοινωνία μεταξύ των χρηστών στο Διαδίκτυο: chat, instant messaging στο πλαίσιο της κοινωνικής δικτύωσης,
- να αναγνωρίζουν το φαινόμενο grooming,
- να είναι ενήμεροι για τα ακρωνύμια emoticons και την γραφή σε greeklish,
- να αναζητούν ζητήματα ασφάλειας στο διαδίκτυο σε ιστοχώρους κοινωνικής δικτύωσης,
- να γνωρίζουν τα περί δημοσίευσης φωτογραφιών ή βίντεο,
- να καταδείξουν πώς γίνεται αναφορά ύποπτης, ανάρμοστης και παράνομης δραστηριότητας.
- να γνωρίζουν τι είναι ο διαδικτυακός εκφοβισμός,
- να είναι ενήμεροι και ευαισθητοποιημένοι για τις επιπτώσεις του φαινομένου cyberbullying στον τομέα ευθύνης τους,
- να αναγνωρίζουν τα προβλήματα που ανακύπτουν και την προστασία που προτείνεται για την αποφυγή του φαινομένου (και μέσω κινητού)
- να γνωρίζουν τα περί happy slapping και sexting.
- να γνωρίζουν τι είναι το ηλεκτρονικό επιχειρείν,
- να γνωρίζουν το φαινόμενο phishing με τις παραλλαγές του,
- να είναι ενήμεροι για τα προβλήματα που είναι πιθανό να αντιμετωπίσουν στις online συναλλαγές,

- να γνωρίζουν πώς μπορούν να κάνουν ηλεκτρονικές συναλλαγές με ασφάλεια, και
- να γνωρίζουν βασικές συμβουλές για την προστασία μας από ενδεχόμενες online απάτες.

Έννοιες Κλειδιά

• Chat	• Instant messaging
• Κοινωνική δικτύωση	• Grooming
• Emoticons	• Greeklish
• Δημοσίευση	• Cyberbullying
• Happy slapping	• Sexting
• Phishing	• Ηλεκτρονικό επιχειρείν
• Pharming	• Κακόβουλο λογισμικό (malware)
• Ανεπιθύμητη αλληλογραφία	

Εισαγωγικές Παρατηρήσεις

Σε αυτήν τη διδακτική ενότητα προσεγγίζεται η κοινωνική δικτύωση, το φαινόμενο grooming και γενικά ζητήματα ασφάλειας σε ανάλογους ιστοχώρους. Αναλύεται η αναγκαιότητα περιορισμού του κυβερνοεκφοβισμού, καθώς πρόκειται για ένα φαινόμενο αυξανόμενης σημασίας. Όλο και περισσότερο υπάρχει η ανησυχία για την επικράτηση του κυβερνοεκφοβισμού, τη θεωρούμενη αποδοχή του, και τον αντίκτυπο στην κοινωνία.

Επιπλέον, μετά το τέλος του αντικειμένου εκπαίδευσης, οι εκπαιδευόμενοι θα είναι σε θέση να γνωρίζουν τι είναι το ηλεκτρονικό «ψάρεμα», τα προβλήματα που ανακύπτουν και βασικές συμβουλές για την προστασία του από ενδεχόμενες απάτες του είδους.

Η πρώτη υποενότητα αναλύει την επικοινωνία μεταξύ των χρηστών, τους όρους χρήσης και την πολιτική απορρήτου και κλείνει με το δεκάλογο της ασφαλούς χρήσης σε ιστοχώρους κοινωνικής δικτύωσης. Αναλύει επίσης το φαινόμενο του κυβερνοεκφοβισμού, είτε μέσω Διαδικτύου είτε μέσω κινητής τηλεφωνίας, καθώς και τα επιμέρους παράπλευρα και μεταγενέστερα φαινόμενα του grooming, happy slapping και sexting.

Η δεύτερη υποενότητα αναλύει κυρίως το φαινόμενο του phishing, καθώς και τις επιμέρους παράπλευρα και μεταγενέστερα παραλλαγές του spear phishing, και pharming. Σε αυτή την υποενότητα προσεγγίζεται η αναγκαιότητα περιορισμού e-mails τα οποία εντάσσονται στη λογική των παραπλανητικών μηνυμάτων τύπου phishing.

Επίσης, γίνεται ιδιαίτερη αναφορά στο ηλεκτρονικό εμπόριο, με παραδείγματα και βασικές συμβουλές για την προστασία από ενδεχόμενες online απάτες. Τέλος, αναλύονται οι περιπτώσεις κακόβουλου λογισμικού, ανεπιθύμητης αλληλογραφίας και προστασίας από το malware τέτοιου τύπου.

Στην τρίτη υποενότητα παρατίθενται άρθρα από τον ενημερωτικό κόμβο για την Ασφάλεια στο Διαδίκτυο του Πανελλήνιου Σχολικού Δικτύου http://internet-safety.sch.gr για το χρονικό διάστημα από τον Σεπτέμβριο 2010 έως τον Σεπτέμβριο 2011.

Η πρώτη και δεύτερη υποενότητα βασίζονται σε υλικό που έγραψε η Δρ. Βερόνικα Σαμαρά, Μηχανικός Πληροφορικής. Στα εδάφια 1.2.1 και 1.5 *συνέβαλε με συγγραφή η κ. Μ. Χριστοδουλάκη, δικηγόρος*.

Το εδάφιο 1.7 καθώς και την τρίτη υποενότητα συγκέντρωσε και επιμελήθηκε ο Άρης Λούβρης, Εκπαιδευτικός Πληροφορικής.