Γραμματισμός Μέσων στον Ψηφιακό Κόσμο: Υποστήριξη των Εκπαιδευτικών μέσω μιας ολιστικής σχολικής προσέγγισης

MeLDE

Co-funded by the Erasmus+ Programme of the European Union

Emphasys CENTRE

UNIVERSITY OF WOLVERHAMPTON

ANTI

BÜRGERHAUS ENNOHAUS

DEMOKRITOS

Ενότητα 4: Διαδικτυακή Ασφάλεια

ΠΕΡΙΓΡΑΦΗ

Η θεματική ενότητα αυτή αποσκοπεί να εισάγει τους εκπαιδευτικούς σε ένα ευρύ φάσμα περιπτώσεων και τρόπων για να παραμείνουν ασφαλείς στο διαδίκτυο. Θα συζητηθούν θέματα, όπως κίνδυνοι και υποχρεώσεις στο διαδίκτυο, προστασία προσωπικών δεδομένων, διαδικτυακή παραπληροφόρηση και επιβλαβές περιεχόμενο, ψηφιακά πνευματικά δικαιώματα και αποτελεσματικές και αναποτελεσματικές πρακτικές για το διαδικτυακό εκφοβισμό.

Ενότητα 4: Διαδικτυακή Ασφάλεια

MeLDE

ΛΙΣΤΑ ΜΕ ΤΑ ΘΕΜΑΤΑ

ΘΕΜΑ 1 ΔΙΑΔΙΚΤΥΑΚΟΙ ΚΙΝΔΥΝΟΙ ΚΑΙ ΕΥΘΥΝΕΣ

ΘΕΜΑ 2 ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΘΕΜΑ 3 ΨΗΦΙΑΚΑ ΠΝΕΥΜΑΤΙΚΑ ΔΙΚΑΙΩΜΑΤΑ

ΘΕΜΑ 4 ΔΙΑΔΙΚΤΥΑΚΗ ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗ ΚΑΙ ΕΠΙΒΛΑΒΕΣ ΠΕΡΙΕΧΟΜΕΝΟ

ΘΕΜΑ 5 ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ

Ενότητα 4: Διαδικτυακή Ασφάλεια

MeLDE

ΠΕΡΙΕΧΟΜΕΝΑ

Θέμα 1: Διαδικτυακοί κίνδυνοι και υποχρεώσεις

- Πιθανές απειλές για το υλικό και το λογισμικό
- Απειλές για τα Δεδομένα και τις Πληροφορίες
- Τρόποι αναφοράς Διαδικτυακών απατεώνων
- Διαδικτυακά δικαιώματα και υποχρεώσεις

Θέμα 2: Προστασία προσωπικών δεδομένων

- Δημιουργία και Διατήρηση ισχυρών κωδικών
- Η σημασία ενός ενημερωμένου λειτουργικού συστήματος και ενός ενημερωμένου λογισμικού, ενάντια σε κακόβουλα λογισμικά
- Ευαλωτότητα των Κινητών Συνσκευών και Τρόποι να τις διατηρήσεις Ασφαλείς
- Κακόβουλη ηλεκτρονική Αλληλογραφία
- Τρόποι πραστασίας Προσωπικών Δεδομένων στις σελίδες Κοινωνικού Δικτύου

Θέμα 3: Ψηφιακά πνευματικά δικαιώματα

- Συζήτηση νέων νομικών και πολιτικών εξελίξεων του νόμου περί πνευματικών δικαιωμάτων και κατανόηση της υιοθέτησής του στην ψηφιακή εποχή
- Κατανόηση της προστασίας του ψηφιακού περιεχομένου που δημιουργήθηκε και δημοσιεύτηκε από τους μαθητές σου
- Κατανόηση της λογοκλοπής και αποφυγή της στην εποχή της υπερφορτωμένης πληροφορίας, όπου το περιεχόμενο μπορεί να χρησιμοποιηθεί και να επαναχρησιμοποιηθεί με ποικίλους τρόπους από αναρίθμητες πηγές.
- Εξερεύνηση μιας σειράς πηγών ελεύθερων σε πρόσβαση και κατανόηση του γιατί και του πότε μπορεί να χρησιμοποιηθεί και να επαναχρησιμοποιηθεί το ψηφιακό υλικό για εκπαιδευτικούς σκοπούς
- Εργασία σε ομάδες για παραγωγή μικρού και ευανάγνωστου εγχειριδίου σχετικά με τα πνευματικά δικαιώματα για τα σχολεία των ομάδων αυτών.

Ενότητα 4: Διαδικτυακή Ασφάλεια

MeLDE

ΠΕΡΙΕΧΟΜΕΝΑ

Θέμα 4: Διαδικτυακή παραπληροφόρηση και επιβλαβές περιεχόμενο

- Η διαφορά ανάμεσα σε μια γνήσια ιστοσελίδα και σε ένα αντίγραφο
- Αξιολόγηση και αναφορά ιστοσελίδων απάτης
- Η έννοια της 'ψεύτικης είδησης' και πώς να την αξιολογήσεις και να την αναγνωρίσεις
- Γιατί είναι σημαντικό να αναφέρεις τις ιστοσελίδες απάτης και ο επιβλαβής αντίκτυπος τους στη δημοκρατία, την κοινωνία, αλλά και σε ατομικό επίπεδο

Θέμα 5: Διαδικτυακός Εκφοβισμός

- Τι είναι διαδικτυακός εκφοβισμός και γιατί είναι σημαντικός
- Διαφορετικές μορφές διαδικτυακού εκφοβισμού
- Αναγνώριση μαθητών που έπεσαν θύματα διαδικτυακού εκφοβισμού με πολλαπλούς τρόπους
- Δράσεις που θα βοηθήσουν τους μαθητές που έπεσαν θύματα διαδικτυακού εκφοβισμού
- Η σημασία της παρεμβατικής και αποτρεπτικής στρατηγικής στα σχολεία σε σχέση με το διαδικτυακό εκφοβισμό

Θέμα 2: Προστασία προσωπικών δεδομένων

ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΚΑΙ ΥΠΟΚΑΤΗΓΟΡΙΕΣ

Αυτή η θεματική ενότητα αποσκοπεί στο να εισάγει τους εκπαιδευτικούς στα πιο κοινά μέτρα ασφαλείας, όπως οι ισχυροί κωδικοί, το λογισμικό ενάντια στα κακόβουλα προγράμματα, τα αντίγραφα ασφαλείας των δεδομένων, η κρυπτογράφηση, προγράμματα προστασίας και ασφαλείς διαδικτυακές αγορές. Θα ασχοληθούμε επίσης με το πως να παραμείνεις ασφαλής στα κοινωνικά δίκτυα, πως να κρατήσεις ασφαλείς τις κινητές συσκευές, πως να αποφύγεις επιβλαβές ή επιθετικό περιεχόμενο στα κοινωνικά δίκτυα και πώς να εντοπίσεις τις ψεύτικες ειδήσεις.

Θα συζητηθούν τα ακόλουθα:

- Δημιουργία και Διατήρηση ισχυρών κωδικών
- Η σημασία ενός ενημερωμένου λειτουργικού συστήματος και ενός ενημερωμένου λογισμικού, ενάντια σε κακόβουλα λογισμικά
- Ευαλωτότητα των Κινητών Συνσκευών και Τρόποι να τις διατηρήσεις Ασφαλείς
- Κακόβουλη ηλεκτρονική Αλληλογραφία
- Τρόποι πραστασίας Προσωπικών Δεδομένων στις σελίδες Κοινωνικού Δικτύου

Θέμα 2: Προστασία προσωπικών δεδομένων

MeLDE

ΔΗΜΙΟΥΡΓΙΑ ΚΑΙ ΔΙΑΤΗΡΗΣΗ ΙΣΧΥΡΩΝ ΚΩΔΙΚΩΝ

Η δημιουργία ισχυρών κωδικών για τους διαδικτυακούς σου λογαριασμούς, είναι ένας από τους πιο αποτελεσματικούς τρόπους για να προστατέψεις τα προσωπικά σου δεδομένα και τις πληροφορίες και να κρατήσεις τον εαυτό σου ασφαλή από διαδικτυακές επιθέσεις.

Για να δημιουργήσεις ισχυρούς κωδικούς, πρέπει να κάνεις τα ακόλουθα:

- Χρησιμοποίησε κωδικούς με φράσεις αντί για λέξεις
- Χρησιμοποίησε κωδικούς που περιέχουν κεφαλαία και μικρά γράμματα, νούμερα και ειδικούς χαρακτήρες
- Χρησιμοποίησε κωδικούς με μέγεθος μεγαλύτερο των 8 χαρακτήρων
- Απόφυγε τη χρήση εύκολα προβλέψιμων λέξεων ή αλφαριθμητικούς συνδυασμούς (π.χ. ονόματα παιδιών ή κατοικιδίων, ημερομηνίες γέννησης, διευθύνσεις, νούμερα κοινωνικής ασφάλισης)
- Χρησιμοποίησε λέξεις που δεν υπάρχουν στο λεξικό

Θέμα 2: Προστασία προσωπικών δεδομένων

MeLDE

ΔΗΜΙΟΥΡΓΙΑ ΚΑΙ ΔΙΑΤΗΡΗΣΗ ΙΣΧΥΡΩΝ ΚΩΔΙΚΩΝ

Για να δημιουργήσεις ισχυρούς κωδικούς, πρέπει να κάνεις τα ακόλουθα:

- Μην αποθηκεύεις κωδικούς στο λάπτοπ ή το κινητό σου τηλέφωνο
- Μην αποθηκεύεις κωδικούς στο πρόγραμμα περιήγησης
- Μην καταγράφεις τους κωδικούς σου
- Αν κάποιος χρειαστεί πρόσβαση για μια μοναδική, μεμονωμένη περίπτωση, άλλαξε τον κωδικό σου όταν τελειώσει και δε χρειάζεται άλλο πρόσβαση
- Χρησιμοποιήστε ένα διαχειριστή κωδικών πρόσβασης, που μπορεί να κάνει κοινή χρήση πιστοποιήσεων μίας σύνδεσης με άλλα άτομα, χωρίς τα τελευταία να μπορούν να δουν ή να ερμηνεύουν τα στοιχεία σύνδεσης
- Μη χρησιμοποιείς τους ίδιους κωδικούς σε παραπάνω από μία υπηρεσία ή λογαριασμό
- Οργάνωσε τους κωδικούς σου σε λογικές ομαδοποιήσεις
- Μη στέλνεις κωδικούς ή πιστοποιήσεις σύνδεσης λογαριασμού μέσω δημόσιων ή μη ασφαλών συνδέσεων Wi-Fi
- Άλλαξε τον κωδικό σου μόλις παραβιαστεί η ασφάλεια σου και αφού μπλοκαριστεί ο εισβολέας

Θέμα 2: Προστασία προσωπικών δεδομένων

Η ΣΗΜΑΣΙΑ ΕΝΟΣ ΕΝΗΜΕΡΩΜΕΝΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ΚΑΙ ΕΝΟΣ ΕΝΗΜΕΡΩΜΕΝΟΥ ΛΟΓΙΣΜΙΚΟΥ, ΕΝΑΝΤΙΑ ΣΕ ΚΑΚΟΒΟΥΛΑ ΛΟΓΙΣΜΙΚΑ

ΕΝΗΜΕΡΩΣΗ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ ΕΝΑΝΤΙΑ ΣΕ ΚΑΚΟΒΟΥΛΑ ΠΡΟΓΡΑΜΜΑΤΑ- ANTIMALWARE

Καθώς το ηλεκτρονικό έγκλημα αυξάνεται, είναι πολύ σημαντικό να κατεβάσουμε και να εγκαταστήσουμε τις πιο πρόσφατες ενημερώσεις. Δεδομένου ότι οι Antimalware εταιρείες είναι πολύ γρήγορες στο να προσθέσουν κι άλλη προστασία απέναντι σε νέες απειλές και διαθέτουν αυτές τις ενημερώσεις στους πελάτες τους και δεδομένου επίσης, πως οι περισσότερες απειλές μεταδίδονται σχετικά αργά, οι περισσότερες εταιρείες και τα περισσότερα άτομα έχουν χρόνο για να προστατευτούν από αυτές τις νέες απειλές, με το να διατηρούν τις εφαρμογές ενάντια στο κακόβουλο λογισμικό (Antimalware) ενημερωμένες.

Οι συντάκτες των ιών και οι κατασκευαστές επιβλαβών κωδικών βρίσκουν συνεχώς τρόπους γύρω από τα χαρακτηριστικά της νέας τεχνολογίας και τα κενά στα λειτουργικά συστήματα, που τους κάνουν πιο εύκολο το έργο τους. Για αυτό το λόγο, αν χρησιμοποιείς κάποιο λογισμικό ασφάλειας και δεν το έχεις ενημερώσει για πολύ καιρό, είναι σαν να μην έχεις εγκαταστήσει κανένα αντιιικό πρόγραμμα –Antivirus και κανένα λογισμικό ενάντια στο κακόβουλο υλικό- Antimalware. Όσο το λογισμικό ασφαλείας είναι ξεπερασμένο, οι ηλεκτρονικοί εγκληματίες θα βρίσκουν σφάλματα και ζητήματα για να εκμεταλλευτούν.

Επίσης, εάν ο Η/Υ ή το λάπτοπ σου μολυνθεί από κάποιον ιό ή κάποιο κακόβουλο λογισμικό, μπορεί να επηρεαστεί όχι μόνο ο σκληρός δίσκος και τα δεδομένα σου, αλλά και να μεταδοθεί σε άλλες συσκευές μέσω δικτύων ή μηνυμάτων ηλεκτρονικής αλληλογραφίας. Οι ηλεκτρονικοί εγκληματίες μπορούν να χρησιμοποιήσουν τις προσωπικές σου πληροφορίες, όπως διεύθυνση ηλεκτρονικής αλληλογραφίας, ή διαδικτυακούς λογαριασμούς, για να διαπράξουν ηλεκτρονικά εγκλήματα στο όνομα σου. Σε τέτοια περίπτωση δε, μπορεί να χρειαστεί να πληρώσεις χρήματα για να τις πάρεις πίσω. Στη χειρότερη περίπτωση, μπορεί να πληρώσεις και παρόλα αυτά να μην τις πάρεις πίσω.

Θέμα 2: Προστασία προσωπικών δεδομένων

MeLDE

Η ΣΗΜΑΣΙΑ ΕΝΟΣ ΕΝΗΜΕΡΩΜΕΝΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ ΚΑΙ ΕΝΟΣ ΕΝΗΜΕΡΩΜΕΝΟΥ ΛΟΓΙΣΜΙΚΟΥ, ΕΝΑΝΤΙΑ ΣΕ ΚΑΚΟΒΟΥΛΑ ΛΟΓΙΣΜΙΚΑ

ΕΝΗΜΕΡΩΣΗ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ

Οι Hackers μπορούν να εκμεταλλευτούν την ευαλωτότητα ενός λογισμικού, που μπορεί να είναι μια τρύπα/ αδυναμία στην ασφάλεια, η οποία βρέθηκε στο λογισμικό/ λειτουργικό σύστημα, συντάσσοντας έναν κωδικό για να στοχεύσει στο ευάλωτο σημείο και να κλέψεουν έτσι προσωπικές πληροφορίες και να διαπράξουν εγκλήματα στο όνομά σου ή να τις πουλήσουν στο σκοτεινό διαδίκτυο - dark web και να επιτρέψουν έτσι σε άλλους να διαπράξουν παράνομες ενέργειες.

Ο χρήστης ενός ενημερωμένου λειτουργικού συστήματος, επωφελείται από τις διορθωμένες τρύπες στην ασφάλεια, από τα λογισμικά επιδιόρθωσης και από την αποκατάσταση ή απομάκρυνση των σφαλμάτων ασφαλείας. Η ενημέρωση του λειτουργικού συστήματος μπορεί να προσθέσει και επιπλέον χαρακτηριστικά στη συσκευή σου και να αφαιρέσει τα ξεπερασμένα που δεν είναι σε ισχύ.

Ένας ακόμα σημαντικός λόγος για να ενημερώνεις το λειτουργικό σου σύστημα, είναι για να μη μένεις πίσω στην τεχνολογική εξέλιξη, χρησιμοποιώντας ξεπερασμένα προγράμματα και εφαρμογές, που είναι ζωτικής σημασίας για την επιτυχία σου στο σχολείο, το σπίτι , την εργασία κ.τ.λ.

Τέλος, όλα τα λειτουργικά συστήματα και κάθε κομμάτι πολύπλοκου λογισμικού, δεν είναι απαλλαγμένα από σφάλματα. Για το λόγο αυτό, οι συχνές ενημερώσεις είναι σημαντικές, για να διορθώσουν τα σφάλματα που ανακαλύπτονται μετά την κυκλοφορία του λειτουργικού συστήματος/ προγράμματος/ εφαρμογής.

Θέμα 2: Προστασία προσωπικών δεδομένων

MeLDE

ΕΥΑΛΩΤΟΤΗΤΑ ΤΩΝ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ ΚΑΙ ΤΡΟΠΟΙ ΝΑ ΤΙΣ ΔΙΑΤΗΡΗΣΕΙΣ ΑΣΦΑΛΕΙΣ

Οι Hackers σήμερα στοχεύουν smartphones και κινητές συσκευές γενικότερα, για να κερδίσουν πρόσβαση σε προσωπικές πληροφορίες από μηνύματα, το Facebook και άλλες εφαρμογές κοινωνικής δικτύωσης, σε τραπεζικά δεδομένα και δεδομένα αγορών, σε μηνύματα ηλεκτρονικής αλληλογραφίας, κ.τ.λ.

Για να αποφύγουν ή να αντιμετωπίσουν μια τέτοια επίθεση στο smartphone ή την κινητή συσκευή, οι χρήστες μπορούν να ακολουθήσουν τα παρακάτω βήματα:

- Κλείδωσε το κινητό σου τηλέφωνο
  - Όλα τα smartphones διαθέτουν δυνατότητα κλειδώματος, οπότε βεβαιώσου ότι το χρησιμοποιείς και άλλαζε τον κωδικό σου ανά 3 με 6 μήνες. Μια εύκολη εναλλακτική του κλειδώματος με κωδικό, είναι ο σχεδιασμός μοτίβου, ή η αναγνώριση προσώπου, φωνής ή δακτυλικού αποτυπώματος.
- Ενεργοποίησε την εντολή του εντοπισμού της συσκευής
  - Αν κλέψουν το smartphone σου, μπορείς να ελέγξεις την τοποθεσία από αυτή την εντολή. Επιπρόσθετα, μπορείς και να κλειδώσεις το τηλέφωνο σου από μακριά, με μια εφαρμογή εντοπισμού.
- Ενημέρωσε το λειτουργικό σύστημα
  - Βεβαιώσου ότι έχεις τις τελευταίες ενημερώσεις στο smartphone’, για να γλιτώσεις διαρροές που ενδεχομένως έχουν ανακαλύψει οι hackers.
- Πρόσεχε ποιές εφαρμογές κατεβάζεις
  - Βεβαιώσου ότι κατεβάζεις εφαρμογές από το App Store (για iOS) ή από την Google Play (για Android), που πιστοποιούν την αυθεντικότητα των εφαρμογών που προσφέρουν.

Θέμα 2: Προστασία προσωπικών δεδομένων

MeLDE

ΕΥΑΛΩΤΟΤΗΤΑ ΤΩΝ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ ΚΑΙ ΤΡΟΠΟΙ ΝΑ ΤΙΣ ΔΙΑΤΗΡΗΣΕΙΣ ΑΣΦΑΛΕΙΣ

- Πρόσεχε τα μηνύματα από ξένους
  - Μην ανοίγεις οποιοδήποτε μήνυμα λαμβάνεις από κάποιον ξένο, από άγνωστο αριθμό ή από αριθμό που σου φαίνεται περίεργος και διάγραψέ το.
  - Μην ανοίγεις κανέναν σύνδεσμο που στέλνεται από ξένα μηνύματα
  - Μην κατεβάσεις καμία εφαρμογή που στέλνεται από ξένα μηνύματα
- Να είσαι προσεκτικός με τα δημόσια WiFi
  - Πρόσεχε τα μη ασφαλή ασύρματα δίκτυα.
  - Αν δε χρησιμοποιείς τις διαδικτυακές υπηρεσίες κάποιου παρόχου, αλλά μία ασύρματη σύνδεση, κινδυνεύεις να εκθέσεις τα δεδομένα σου σε hackers.
  - Βεβαιώσου ότι έχεις συνδεθεί σε μια δημόσια σύνδεση μιας επιχείρησης, γιατί η ελεύθερη πρόσβαση σε WiFi μπορεί να είναι το σχέδιο ενός hacker, για να κλέψει προσωπικά, ιδιωτικά δεδομένα σε πολυπληθής περιοχές.
- Χρησιμοποίησε προστασία Antivirus
  - Το smartphone διαθέτει λειτουργικό σύστημα, προγράμματα (εφαρμογές), πρόγραμμα περιήγησης στο διαδίκτυο, οπότε θεωρείται στην ουσία υπολογιστής, που χρειάζεται προστασία από τους hackers.

Θέμα 2: Προστασία προσωπικών δεδομένων

MeLDE

ΑΝΑΓΝΩΡΙΣΗ ΤΗΣ ΚΑΚΟΒΟΥΛΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΑΛΛΗΛΟΓΡΑΦΙΑΣ

1. Ο αποστολέας δεν είναι σωστός
   - Έλεγξε, αν η διεύθυνση ταιριάζει με το όνομα του αποστολέα.
   - Έλεγξε, αν ο τομέας της εταιρείας του αποστολέα είναι ορθός.

   Για να μπορέσεις να ελέγξεις τα παραπάνω, ο πελάτης σου πρέπει να εμφανίζει και τη διεύθυνση – email του αποστολέα και όχι μόνο το όνομα του.
2. Ο αποστολέας δε σε γνωρίζει
   - Έλεγξε, αν ο αποστολέας σου απευθύνεται με τον τρόπο που θα περίμενες.
   - Έλεγξε ,αν η υπογραφή του αποστολέα ταιριάζει με αυτή που στέλνει συνήθως στα emails του.

   Για παράδειγμα, η τράπεζά σου θα σου απευθυνόταν κανονικά με το επίθετο σε ένα email, και όχι με μία γενικευμένη προσφώνηση (“Αγαπητέ πελάτη”).
3. Συνημμένοι σύνδεσμοι έχουν ύποττα URLs
   - Περιεργάσου τους συνδέσμους πριν τους ανοίξεις. Έλεγξε, αν ο προορισμός τους ταιριάζει με την ιστοσελίδα στην οποία αναφέρεται το email.
4. Η ορθογραφία και η γραμματική είναι ασυνήθιστες
   - Έλεγξε, αν το email είναι γεμάτο με ορθογραφικά και γραμματικά λάθη., σαν κάποιος να χρησιμοποίησε αυτόματο διαδικτυακό μεταφραστή για τη δική σου γλώσσα.
5. Το περιεχόμενο δεν είναι πιστευτό ή είναι περίεργο
   - Αν το email υπόσχεται μεγάλα κέρδη ως ανταπόδοση μικρών επενδύσεων ή και δωρεάν, πρόκειται συνήθως για phishing email.

Θέμα 2: Προστασία προσωπικών δεδομένων

MeLDE

ΤΙ ΝΑ ΚΑΝΕΙΣ ΑΝ ΚΛΙΚΑΡΕΣ ΣΕ ΕΝΑ ΣΥΝΔΕΣΜΟ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

1. Μην καταχωρήσεις προσωπικά δεδομένα αν σου ζητηθεί.
2. Μην καταχωρήσεις κανένα πιστοποιητικό σύνδεσης.

   Οι ηλεκτρονικοί εγκληματίες θα τα χρησιμοποιήσουν για να μπουν στον πραγματικό λογαριασμό.
3. Αποσυνδέσου από το διαδίκτυο όσο το δυνατόν γρηγορότερα για να περιορίσεις τη μόλυνση από κακόβουλο υλικό.
   - Κλείνοντας τη διαδικτυακή σύνδεση από τη συσκευή σου.
   - Βγάζοντας το καλώδιο της σύνδεσης.
4. Σάρωσε τη συσκευή με ένα antivirus ή/ και ένα antimalware λογισμικό με μία πλήρη σάρωση.
   - Παρέμεινε αποσυνδεδεμένος από το διαδίκτυο όσο γίνεται η σάρωση.
5. Άλλαξε τους κωδικούς στην πραγματική σελίδα ή οπουδήποτε χρησιμοποιείς αυτό το email με τον ίδιο κωδικό.
6. Κράτα αντίγραφα ασφαλείας των αρχείων σου σε διαφορετικές συσκευές.

Θέμα 2: Προστασία προσωπικών δεδομένων

MeLDE

ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΑ ΚΟΙΝΩΝΙΚΗ ΔΙΚΤΥΑ

1. Απόφυγε τη συμπλήρωση των πεδίων που αφορούν τον εαυτό σου.
   - Τα περισσότερα κοινωνικά δίκτυα, όπως το Facebook, διατηρούν το πεδίο με τις πληροφορίες για τον εαυτό σου προαιρετικό. Δίνε μόνο γενικές πληροφορίες ή αφησε το πεδίο αυτό εντελώς κενό.
2. Εξοικειώσου με τις ρυθμίσεις ιδιωτικότητας.
   - Εξερεύνησε τις ρυθμίσεις ιδιωτικότητας και δοκίμασε διαφορετικές επιλογές, για να βρεις τι ταιριάζει καλύτερα στις προτιμήσεις σου. Προτίμησε να περιορίσεις το κοινό που μπορεί να βλέπει τις δημοσιεύσεις σου, στους ανθρώπους που γνωρίζεις. Έχε στο νου ότι ακόμα και να φαίνονται κάποιες φωτογραφίες ως ‘’προσωπικές’’, μπορεί να εμφανιστούν δημόσια στις εικόνες του Google, οπότε αν δε θες να δημοσιευτεί κάτι δημόσια, απλώς μην το ανεβάζεις.
3. Δέξου αιτήματα φιλίας από ανθρώπους που γνωρίζεις και εμπιστεύεσαι.
   - Όσο περισσότερους φίλους έχεις στα κοινωνικά δίκτυα, τόσο πιο δύσκολο είναι να διαχειριστείς τις πληροφορίες που δημοσιεύεις. Μη διστάσεις να μπλοκάρεις κάποιον, αν φοβάσαι ότι θα εκμεταλλευτεί εσένα και τις πληροφορίες σου.
4. Απόφυγε τη λειτουργία “πρόσθεσε την τοποθεσία σου”.
   - Κάποιοι εγκληματίες μπορεί να σε εκμεταλλευτούν και να σου κάνουν ακόμα και κακό, αν γνωρίζουν την ακριβή τοποθεσία που βρίσκεσαι.
   - Κάποιοι εγκληματίες μπορεί να διαρρήξουν και το σπίτι σου, αν γνωρίζουν ότι είσαι μακριά από αυτό.

Θέμα 2: Προστασία προσωπικών δεδομένων

MeLDE

ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΑ ΚΟΙΝΩΝΙΚΗ ΔΙΚΤΥΑ

5. Αποσυνδέσου από τα κοινωνικά δίκτυα όταν τελειώσεις.
   - Αν χρησιμοποιείς μία δημόσια συσκευή για να συνδεθείς, ή ακόμα και τη δική σου συσκευή, η αποσύνδεση από τα κοινωνικά δίκτυα, διασφαλίζει ότι δε θα πέσεις θύμα χακαρίσματος, από κάποιον που έχει άμεση πρόσβαση στη συσκευή που είσαι ήδη συνδεδεμένος και μπορεί να επιτεθεί λεκτικά σε φίλους, να δημοσιεύσει προσβλητικό περιεχόμενο εκ μέρους σου ή ακόμα χειρότερα να αλλάξει τις προσωπικές σου πληροφορίες, τον κωδικό σου και να μην έχεις πια πρόσβαση στον ίδιο σου το λογαριασμό.
6. Δημιούργησε ισχυρούς, κρυφούς κωδικούς.
   - Οι ισχυροί κωδικοί περιέχουν συνδυασμούς κεφαλαίων και μικρών γραμμάτων, αριθμών, ειδικών χαρακτήρων, που είναι εύκολο να τους θυμάσαι εσύ, αλλά δύσκολο για κάποιον άλλο να τους σπάσει ή να τους μαντέψει.
   - Απόφυγε τη χρήση εύκολων και κοινών κωδικών, όπως ημερομηνίες γενεθλίων, επετείων και ονόματα των κατοικιδίων σου.
   - Κράτα τους κωδικούς σου ιδιωτικούς, μην τους γράψεις σε χαρτί και τους αφήσεις κοντά στη συσκευή για να μπορείς να συνδεθείς. *Primary School Teacher, Special Educator at KESY (Public Assessment and Support Centre for Children who face learning difficulties) and E-safety Ambassador at eSafety Label Project*

Θέμα 2: Προστασία προσωπικών δεδομένων

MeLDE

ΠΑΡΑΠΟΜΠΕΣ

- Protection of personal data. Retrieved from

  https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en

- De Groot, J. (2019, December). 101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2020. Retrieved from

  https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

- How to create a good password. Retrieved from

  https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/how-to-create-a-good-password/

- McDonald, J. (2006, October). The Importance of Updating Antivirus Definitions. Retrieved from

  https://www.symantec.com/connect/blogs/importance-updating-antivirus-definitions

- Graham-Smith, D. (2017, March). 12 ways to hack-proof your smartphone. Retrieved from

  https://www.theguardian.com/technology/2017/mar/26/12-ways-to-hack-proof-your-smartphone-privacy-data-thieveshttps://www.mcafee.com/blogs/consumer/consumer-threat-notices/how-to-tell-if-your-smartphone-has-been-hacked/

Θέμα 2: Προστασία προσωπικών δεδομένων

MeLDE

ΓΛΩΣΣΑΡΙ

Όρος	Έννοια
ΚΩΔΙΚΟΣ	Μία μυστική λέξη ή έκφραση που χρησιμοποιείται για την είσοδο, πρόσβαση σε μια μηχανή, σελίδα, κ.τ.λ.
ANTIMALWARE	Antimalware είναι ένας τύπος προγράμματος λογισμικού που σχεδιάζεται για την αποτροπή, εύρεση και απομάκρυνση κακόβουλου λογισμικού σε συστήματα πληροφορικής, όπως και σε ατομικές συσκευές.
ANTIVIRUS	Το λογισμικό Antivirus είναι ένας τύπος προγράμματος που σχεδιάζεται και αναπτύσσεται για την προστασία των Η/Υ από κακόβουλο υλικό, όπως ιοί, σκουλήκια υπολογιστών (computer worms), ηλεκτρονική κατασκοπεία (spyware), botnets, rootkits, καταγραφή πληκτρολόγησης (keyloggers), κ.τ.λ.
MALICIOUS URL	Το Malicious URL είναι ένας σύνδεσμος που δημιουργείται για λόγους προώθησης ηλεκτρονικής αλληλογραφίας, απάτης και επιθέσεων.