Digital Citizenship

Απόρρητο και Ασφάλεια

Μάθημα

Αναγνώσεις | Ασκήσεις | Μελέτες Περιπτώσεων | Κουίζ

Erasmus+
ATHENS LIFELONG LEARNING INSTITUTE
TEAM 4 excellence
SEALL CYPRUS

Στρατηγική σύμπραξη για την ανάπτυξη ανοικτών εκπαιδευτικών πόρων για τη διδασκαλία της ψηφιακής ιθαγένειας

2019-3-RO01-KA205-078053

DIGCIT

D15 - Ψηφιακής Ιθαγένειας "Απόρρητο και Ασφάλεια" Μάθημα

Αναθεώρηση: v.1.1

Πνευματική παραγωγή	IO2 - Εκπαιδευτικό υλικό για την ψηφιακή ιθαγένεια
Δραστηριότητα	Ανάπτυξη προγράμματος σπουδών μαθημάτων
Επικεφαλής του παραδοτέου	Arbeitskreis Ostviertel e. V. , Γερμανία
Ημερομηνία λήξης	15 Μαρτίου 2021
Συγγραφείς	Jan LEYE
Περίληψη	Το μάθημα "Απόρρητο και Ασφάλεια" καλύπτει τους κινδύνους και τα οφέλη για τις προσωπικές πληροφορίες και τα δεδομένα των ψηφιακών πολιτών. Ενώ τα κοινωνικά οφέλη από την άσκηση δικαιωμάτων και υποχρεώσεων, τα χόμπι και τις κοινωνικές αλληλεπιδράσεις στο διαδίκτυο είναι τεράστια, όλο και περισσότερες απειλές για την ιδιωτική ζωή κάθε πολίτη εμφανίζονται συνεχώς. Το μάθημα αυτό διδάσκει τις σημαντικότερες πτυχές της ασφαλούς συμπεριφοράς και τη σημασία της προστασίας της ιδιωτικής ζωής.
Λέξεις κλειδιά	Πρότυπο μάθημα- ψηφιακή ιθαγένεια- σχέδιο μαθήματος- ιδιωτικότητα- ασφάλεια- ψηφιακά περιβάλλοντα- κοινωνικά δίκτυα- κίνδυνοι ασφάλειας στο διαδίκτυο- υλικό- λογισμικό- εκπαίδευση- προβληματισμός- αναστοχαστική σκέψη

Αναγνώριση

Το παρόν έγγραφο χρηματοδοτήθηκε από την Ευρωπαϊκή Επιτροπή στο πλαίσιο της Συμφωνίας Επιχορήγησης-2019-3-RO01-KA205-078053, έργο στρατηγικής εταιρικής σχέσης ERASMUS+ "Στρατηγική εταιρική σχέση για την ανάπτυξη ανοικτών εκπαιδευτικών πόρων για τη διδασκαλία της ψηφιακής ιθαγένειας".

Αποποίηση ευθύνης

"Η υποστήριξη της Ευρωπαϊκής Επιτροπής για την παραγωγή της παρούσας δημοσίευσης δεν συνιστά έγκριση του περιεχομένου, το οποίο αντανακλά τις απόψεις μόνο των συγγραφέων, και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν."

Σημείωση περί πνευματικών δικαιωμάτων

Περιεχόμενα

Εισαγωγή 6
1. Ενότητα 1 - Εισαγωγή στην ιδιωτικότητα 7
Επισκόπηση μαθημάτων 7
Ο ορισμός της ιδιωτικής ζωής 8
Ψηφιακό απόρρητο 10
Η σημασία της ιδιωτικής ζωής 11
Μελέτη περίπτωσης - Ιδιωτικότητα μέσω σχεδιασμού 11
Άσκηση 1: Ιδιωτική συνάντηση στο World Café 12
2. Ενότητα 2 - Εισαγωγή στην ασφάλεια 14
Επισκόπηση μαθημάτων 14
Ο ορισμός της ασφάλειας 15
Η σημασία της ασφάλειας 15
Μελέτη περίπτωσης - STOP.THINK.CONNECT 16
Άσκηση 2: Σχεδιάζοντας τη γραμμή 16
3. Ενότητα 3 - Ιδιωτικότητα σε ψηφιακό περιβάλλον 19
Επισκόπηση μαθημάτων 19
Η προϋπόθεση των ψηφιακών περιβαλλόντων 20
Κίνδυνοι από τα κοινωνικά δίκτυα και τους αγγελιοφόρους σε ένα ψηφιακό περιβάλλον 20
Μελέτη περίπτωσης - Μέσα κοινωνικής δικτύωσης και κλοπή ταυτότητας 23
Άσκηση 3: Κοινότητα 24
4. Ενότητα 4 - Κίνδυνοι ασφάλειας σε ένα ψηφιακό περιβάλλον 26
Επισκόπηση μαθημάτων 26
Εισαγωγή στο υλικό 27
Εισαγωγή στο λογισμικό 27
Απειλές για το υλικό και το λογισμικό 28
Μελέτη περίπτωσης - Ο αγαπημένος απατεώνας της γιαγιάς μου 29
Άσκηση 4: Η εισβολή 30
5. Ενότητα 5 - Συμβουλές ασφαλείας για το ψηφιακό περιβάλλον 32
Επισκόπηση μαθημάτων 32
Συμβουλές για την ασφάλεια υλικού 33
Συμβουλές για την ασφάλεια λογισμικού 33
Συμβουλές σχετικά με την ασφάλεια των χρηστών 34
Μελέτη περίπτωσης - Lorrie Faith Cranor: Τι έχει ο πατέρας σου; 34
Άσκηση 5: Ασφαλείς μαζί 35

6. Κουίζ αξιολόγησης 37
7. Αναφορές 41
Παράρτημα 42
Φύλλα ελέγχου κουίζ αξιολόγησης 42
Λίστα ελέγχου αναθεώρησης διδακτικού σχεδιασμού για τους εργαζόμενους στον τομέα της νεολαίας 43
Ανατροφοδότηση σχετικά με το θέμα για τους μαθητές 44

Εισαγωγή

Το απόρρητο και η ασφάλεια είναι παλιοί όροι, αλλά η σημασία τους αυξήθηκε τα τελευταία χρόνια. Η ενότητα "Ιδιωτικότητα και ασφάλεια" εξηγεί τη σύγχρονη ερμηνεία της ιδιωτικότητας ως ανθρώπινο δικαίωμα στην ψηφιοποιημένη εποχή.

Το Εκπαιδευτικό Εγχειρίδιο Ψηφιακής Ιθαγένειας του Συμβουλίου της Ευρώπης ορίζει την ιδιωτική ζωή ως ένα δικαίωμα που *"αφορά κυρίως την προσωπική προστασία των δικών μας και των πληροφοριών των άλλων στο διαδίκτυο, ενώ η ασφάλεια σχετίζεται περισσότερο με την επίγνωση των διαδικτυακών ενεργειών και συμπεριφορών του ατόμου".*

Το απόρρητο και η ασφάλεια εξαρτώνται το ένα από το άλλο, πολύ περισσότερο σε ένα ψηφιακό περιβάλλον. Αντιμετωπίζοντας απειλές που σχετίζονται με το υλικό, το λογισμικό και τον ίδιο τον χρήστη, η προστασία της ιδιωτικής ζωής αποτελεί συνεχή πρόκληση και ευθύνη για κάθε ψηφιακό πολίτη.

Η ενότητα αυτή αποσκοπεί στην ευαισθητοποίηση σχετικά με τη σημασία της ιδιωτικής ζωής σε σχέση με μια ολοκληρωμένη ζωή και τα απαραίτητα μέτρα που πρέπει να ληφθούν για την προστασία της ιδιωτικής ζωής. Θα παρουσιάσει γνώσεις και πρακτικές συμβουλές σχετικά με τις βασικές αρχές της σύγχρονης ασφάλειας απέναντι στους σύγχρονους κινδύνους. Οι ενότητες θα καλύψουν τα ακόλουθα θέματα κ.ά:

- Τι είναι η ιδιωτικότητα;
- Τι είναι η ασφάλεια;
- Τι είναι τα ψηφιακά περιβάλλοντα;
- Πώς επηρεάζει η ιδιωτικότητα τη ζωή μας;
- Πώς λειτουργεί μια ψηφιακή συσκευή;
- Πώς να συμπεριφέρεστε με ασφάλεια και υπευθυνότητα;

1. Ενότητα 1 - Εισαγωγή στην ιδιωτικότητα

Πηγή: Unsplash

Επισκόπηση μαθημάτων

Περίληψη: Αυτή η ενότητα καλύπτει τις βασικές αρχές της ιδιωτικότητας, τον ορισμό της και τον ρόλο της στο σημερινό ψηφιακό περιβάλλον. Παρουσιάζει επίσης τη σημασία της ιδιωτικής ζωής ως ανθρώπινο δικαίωμα.

Δομή:

- Επισκόπηση μαθημάτων
- Ο ορισμός της ιδιωτικής ζωής
- Ψηφιακό απόρρητο
- Η σημασία της ιδιωτικής ζωής
- Μελέτη περίπτωσης
- Συμπληρωματική ανάγνωση
- Άσκηση
- Ανατροφοδότηση
- E-Quiz

Μαθησιακοί στόχοι:

- Κατανόηση του ορισμού της ιδιωτικής ζωής
- Αναγνωρίζουν τη σημασία της ιδιωτικής ζωής
- Εξηγήστε τη σημασία της ιδιωτικής ζωής

Ο ορισμός της ιδιωτικής ζωής

Δεν υπάρχει ένας παγκοσμίως αναγνωρισμένος ορισμός της ιδιωτικής ζωής, επειδή ο όρος μπορεί να έχει διαφορετικές έννοιες ανάλογα με τον πολιτισμό, την ιστορία ή την προσωπική εμπειρία. Κατά τη διάρκεια αυτού του μαθήματος, θα χρησιμοποιήσουμε έναν ορισμό που θα πρέπει να ισχύει επαρκώς για τις περισσότερες δυτικές δημοκρατίες:

Ιδιωτικότητα είναι η ικανότητα κάποιου να βρίσκεται σε μια κατάσταση χωρίς παρέα και χωρίς παρατήρηση, ή εν συντομία: είναι το δικαίωμα να τον αφήνουν ήσυχο. Το να βρίσκεται κανείς σε ιδιωτική ζωή σημαίνει να κρατά μυστικές τις προσωπικές πληροφορίες και τα προσωπικά του θέματα και να μοιράζεται προσωπικές πληροφορίες και θέματα μόνο με τη θέλησή του. Η προστασία της ιδιωτικής ζωής, επομένως, σημαίνει την ελευθερία από μη εξουσιοδοτημένη εισβολή στον προσωπικό χώρο, τις πληροφορίες και τα θέματα κάποιου.

Η σύγχυση οφείλεται συχνά στο γεγονός ότι οι όροι "προστασία της ιδιωτικής ζωής" και "προστασία των δεδομένων" χρησιμοποιούνται ως συνώνυμα. Συνδέονται και οι δύο μεταξύ τους, αλλά ενώ η ιδιωτική ζωή αναφέρεται άμεσα στον προσωπικό χώρο ή την προσωπική σφαίρα ενός ατόμου, η προστασία των δεδομένων αναφέρεται συγκεκριμένα στην προστασία "κάθε πληροφορίας που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό (ζωντανό) πρόσωπο".[1] Η ιδιωτικότητα καλύπτει όλες τις πτυχές της προσωπικής σφαίρας, όπως η φυσική προστασία του σπιτιού σας. Για παράδειγμα, αν πέσετε θύμα ανεπιθύμητης σωματικής επαφής, θίγεται το δικαίωμά σας στην ιδιωτική ζωή, αλλά όχι το δικαίωμά σας στην προστασία των δεδομένων.

Το δικαίωμα στην ιδιωτική ζωή αποτελεί ανθρώπινο δικαίωμα, όπως αναφέρεται στο άρθρο 12 της Οικουμενικής Διακήρυξης των Ανθρωπίνων Δικαιωμάτων (ΟΔΑΔ) του 1948:

> *"Κανείς δεν πρέπει να υποβάλλεται σε αυθαίρετες παρεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε σε επιθέσεις κατά της τιμής και της υπόληψής του. Καθένας έχει δικαίωμα στην προστασία του νόμου έναντι τέτοιων παρεμβάσεων ή επιθέσεων".*[2]

Πηγή: Πηγή: Public domain

[1] https://edps.europa.eu/data-protection_en
[2] https://www.un.org/en/about-us/universal-declaration-of-human-rights

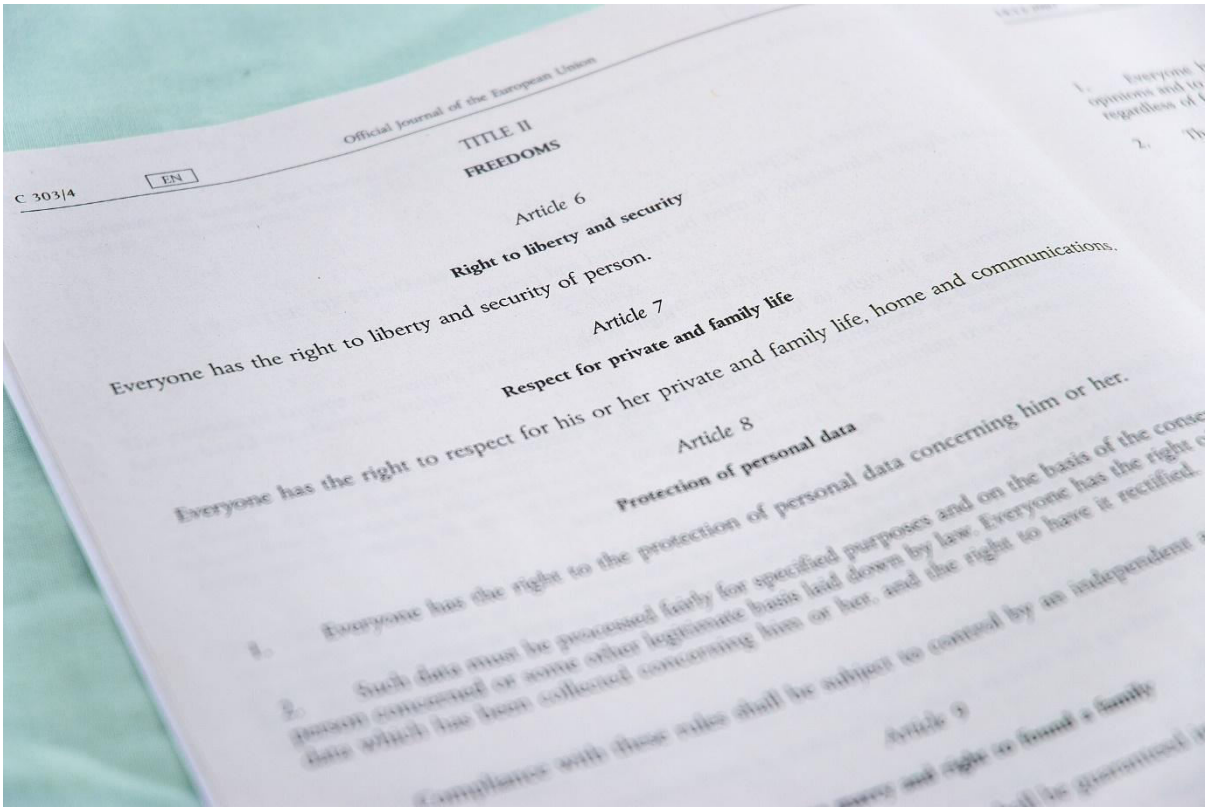
Η προστασία της ιδιωτικής ζωής αναγνωρίστηκε ρητά από το Συμβούλιο της Ευρώπης όταν υπογράφηκε η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ) το 1950 και τέθηκε σε ισχύ τον Σεπτέμβριο του 1953. Το άρθρο 8 της ΕΣΔΑ τιτλοφορείται "Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής" και αναφέρει:

> *"1. Καθένας έχει δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής του ζωής, της κατοικίας του και της αλληλογραφίας του.*
>
> *2. Δεν επιτρέπεται η παρέμβαση δημόσιας αρχής στην άσκηση του δικαιώματος αυτού, εκτός αν είναι σύμφωνη με το νόμο και αναγκαία σε μια δημοκρατική κοινωνία για λόγους εθνικής ασφάλειας, δημόσιας ασφάλειας ή οικονομικής ευημερίας της χώρας, για την πρόληψη της αναταραχής ή του εγκλήματος, για την προστασία της υγείας ή των ηθών ή για την προστασία των δικαιωμάτων και ελευθεριών των άλλων."*[3]

Επιπλέον, η Ευρωπαϊκή Ένωση αναγνωρίζει το δικαίωμα στην ιδιωτική ζωή στα άρθρα 7 και 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΧΘΔ), ο οποίος συντάχθηκε το 2000 και τέθηκε σε ισχύ τον Δεκέμβριο του 2009:

> *"Άρθρο 7*
>
> *Σεβασμός της ιδιωτικής και οικογενειακής ζωής*
>
> *Καθένας έχει το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής του ζωής, της κατοικίας και των επικοινωνιών του.*
>
> *Άρθρο 8*
>
> *Προστασία προσωπικών δεδομένων*
>
> 1. *Καθένας έχει δικαίωμα στην προστασία των προσωπικών δεδομένων που τον αφορούν.*
> 2. *Τα δεδομένα αυτά πρέπει να υποβάλλονται σε δίκαιη επεξεργασία για συγκεκριμένους σκοπούς και βάσει της συγκατάθεσης του ενδιαφερόμενου προσώπου ή βάσει άλλης νόμιμης βάσης που προβλέπεται από τον νόμο. Καθένας έχει το δικαίωμα πρόσβασης στα δεδομένα που έχουν συλλεχθεί και τον αφορούν, καθώς και το δικαίωμα διόρθωσής τους.*
> 3. *Η συμμόρφωση με τους κανόνες αυτούς υπόκειται στον έλεγχο ανεξάρτητης αρχής."*[4]

[3] https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=DE



Πηγή: Wikimedia

Ψηφιακό απόρρητο

Η ψηφιακή εποχή έφερε νέες ευκαιρίες και προκλήσεις. Όταν μιλάμε για την ιδιωτικότητα σε ένα ψηφιακό περιβάλλον χρησιμοποιούμε συνήθως τον όρο "ψηφιακή ιδιωτικότητα". Η ψηφιακή ιδιωτικότητα περιλαμβάνει το δικαίωμα στην ιδιωτική ζωή και όλους τους ισχύοντες ορισμούς του από τον αναλογικό κόσμο, καθώς και την προστασία των δεδομένων.

Η ψηφιακή ιδιωτικότητα μπορεί να είναι ένας όρος που προκαλεί σύγχυση, επειδή η ιδιωτικότητα ως νομικός όρος καλύπτει ήδη όλους τους τομείς εφαρμογής: Δεν έχει σημασία αν η ιδιωτική ζωή κινδυνεύει στον πραγματικό κόσμο ή σε ψηφιακό περιβάλλον, διότι η προστασία της εφαρμόζεται ανεξάρτητα από την τεχνολογία, τον τόπο ή τον χρόνο. Όταν μιλάμε για "ψηφιακή" ή "ηλεκτρονική" ιδιωτικότητα, θέλουμε βασικά να δώσουμε έμφαση σε συγκεκριμένους κινδύνους και κινδύνους για την ιδιωτικότητα που προέρχονται από νέες(ες) τεχνολογίες όπως το διαδίκτυο, τα κοινωνικά δίκτυα ή τις νέες συσκευές.

Η Ευρωπαϊκή Ένωση θέσπισε δύο βασικά σύνολα κανόνων που προστατεύουν ειδικά τα δικαιώματα προστασίας της ιδιωτικής ζωής και των δεδομένων σε ψηφιακά ή ηλεκτρονικά περιβάλλοντα: την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες[5] (πλήρης τίτλος: οδηγία για την προστασία της ιδιωτικής ζωής και τις ηλεκτρονικές επικοινωνίες) και τον γενικό κανονισμό για την προστασία των δεδομένων[6] (ΓΚΠΔ). Και οι δύο προσπαθούν να αντιμετωπίσουν τις ανησυχίες για την προστασία της ιδιωτικής ζωής και των δεδομένων που σχετίζονται με το διαδίκτυο, για παράδειγμα απαιτώντας μεγαλύτερη διαφάνεια στο πλαίσιο του μάρκετινγκ ή της παρακολούθησης των προσωπικών δεδομένων.

[5] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
[6] https://eur-lex.europa.eu/eli/reg/2016/679/oj

Η σημασία της ιδιωτικής ζωής

Το δικαίωμα στην ιδιωτική ζωή αποτελεί προϋπόθεση για την ελεύθερη ανάπτυξη της προσωπικότητας, όπως αναφέρεται στο άρθρο 22 της ΕΣΔΑ:

> *"Καθένας, ως μέλος της κοινωνίας, έχει δικαίωμα στην κοινωνική ασφάλιση και δικαιούται να πραγματοποιήσει, μέσω της εθνικής προσπάθειας και της διεθνούς συνεργασίας και σύμφωνα με την οργάνωση και τους πόρους κάθε κράτους, τα οικονομικά, κοινωνικά και πολιτιστικά δικαιώματα που είναι απαραίτητα για την αξιοπρέπειά του και την ελεύθερη ανάπτυξη της προσωπικότητάς του."*[7]

Ορισμένα κράτη μέλη της Ευρωπαϊκής Ένωσης, όπως η Γερμανία ή οι Κάτω Χώρες, αναγνωρίζουν ρητά το δικαίωμα στην προσωπικότητα στα αντίστοιχα συντάγματά τους, όπως για παράδειγμα το άρθρο 2 του γερμανικού συντάγματος που ορίζει:

> *"(1) Κάθε πρόσωπο έχει δικαίωμα στην ελεύθερη ανάπτυξη της προσωπικότητάς του, εφόσον δεν παραβιάζει τα δικαιώματα των άλλων ούτε προσβάλλει τη συνταγματική τάξη ή τον ηθικό νόμο."*[8]

Άλλα κράτη, όπως η Γαλλία, επέλεξαν διαφορετικά μέσα στη δικαιοδοσία τους για την προστασία της ανάπτυξης της προσωπικότητας.

Ωστόσο, όλες μοιράζονται μια γενική αντίληψη για τη σημασία της προσωπικότητας, την προστασία της και την εγγενή σύνδεσή της με την ιδιωτική ζωή. Χωρίς την προστασία της ιδιωτικής ζωής, ο άνθρωπος δεν μπορεί να αναπτυχθεί και να ζήσει ελεύθερα.

Μελέτη περίπτωσης - Ιδιωτικότητα μέσω σχεδιασμού

Απόρρητο από το σχεδιασμό: Συλλογή δεδομένων με κοινωνικά υπεύθυνο τρόπο χωρίς παρενέργειες στην ιδιωτική ζωή

Σε αυτό το βίντεο από την Εβδομάδα Προστασίας Προσωπικών Δεδομένων 2017 στη Βιέννη, η Konark Modi εξηγεί τις επικίνδυνες "παρενέργειες" του σημερινού βιομηχανικού προτύπου που εφαρμόζουν οι τεχνολογικοί κολοσσοί, οι οποίοι συλλέγουν όσο το δυνατόν περισσότερα δεδομένα.

[7] https://www.un.org/en/about-us/universal-declaration-of-human-rights
[8] https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0023

https://media.ccc.de/v/pw17-158-privacy_by_design#t=74

Ο Modi αποδεικνύει ότι η ιδιωτική ζωή μπορεί να γίνει σεβαστή κατά το σχεδιασμό διαδικτυακών υπηρεσιών και παρουσιάζει μια εναλλακτική έκδοση του "Google Analytics" που σέβεται την ιδιωτική ζωή.

Ερώτηση αυτοαναστοχασμού: Τι είναι μια παρενέργεια στο πλαίσιο της συλλογής δεδομένων;

Άσκηση 1: Ιδιωτική συνάντηση στο World Café

Στόχοι:

- Κατανόηση των συνηθειών σας σχετικά με την ανάρτηση προσωπικών δεδομένων
- Αναγνώριση πιθανών κινδύνων και κινδύνων για την ιδιωτική σας ζωή

Διάρκεια: 30 λεπτά

Εργαλεία: στυλό και χαρτί

Μέθοδοι: ολομέλεια, ομαδική εργασία

Περιγραφή της άσκησης: Οι μαθητές χωρίζονται σε τέσσερις ομάδες. Κάθε ομάδα ανατίθεται σε ένα τραπέζι με μόνιμους μαρκαδόρους/χαρτί ή σε μια αίθουσα διαλείμματος με εικονικό πίνακα. Σε κάθε τραπέζι/αίθουσα έχει ανατεθεί ένα από τα ακόλουθα ζητήματα προστασίας της ιδιωτικής ζωής: (1) Κλοπή ταυτότητας. (2) Δικαίωμα στη λήθη. (3) Προσωπικότητα. (4) Κατασκοπευτικό λογισμικό. Σε κάθε ομάδα δίνονται 5 λεπτά για να προβληματιστεί σχετικά με αυτά τα θέματα (Τι σημαίνουν; Ποια είναι η σύνδεσή τους με την ιδιωτικότητα; Γνωρίζουμε παραδείγματα; Είναι επικίνδυνα ή ωφέλιμα για μένα;) και να καταγράψουν τις ιδέες τους στο χαρτί/τον εικονικό πίνακα. Μετά από 5 λεπτά, οι ομάδες αρχίζουν να εναλλάσσονται. Το καφενείο κλείνει μόλις κάθε ομάδα συζητήσει κάθε θέμα. Κάθε ομάδα ορίζει έναν ομιλητή ο οποίος παρουσιάζει τα αντίστοιχα αποτελέσματα για την ομάδα του.

Καθήκοντα:

- Χωριστείτε σε ομάδες.
- Συζητήστε κάθε θέμα για πέντε λεπτά.
- Μοιραστείτε τα αποτελέσματά σας με την τάξη (έχετε υπόψη σας ότι δεν χρειάζεται να μοιραστείτε οποιαδήποτε πληροφορία που μπορεί να σας κάνει να νιώσετε άβολα).

Ενημέρωση: Ο εκπαιδευτής θα πρέπει να τονίσει την καθολική σημασία της ιδιωτικής ζωής και ότι επηρεάζει πολλά μέρη της ζωής μας και της ευημερίας μας.

Διδάγματα: Η προστασία της ιδιωτικής ζωής είναι ένα πολύπλοκο θέμα και απαιτεί ενεργό προβληματισμό.

Συμπληρωματική ανάγνωση

- **Η Ημέρα Προστασίας Δεδομένων (κάθε χρόνο στις 28 Ιανουαρίουth)**: "Φέτος, η 28η Ιανουαρίου είναι μια πολύ ιδιαίτερη ημέρα, όχι μόνο για το Συμβούλιο της Ευρώπης, αλλά για ολόκληρη την παγκόσμια κοινότητα προστασίας δεδομένων και, πάνω απ' όλα, για κάθε άτομο που προστατεύεται από αυτό το θεμελιώδες δικαίωμα." https://www.coe.int/en/web/data-protection/data-protection-day

E-Quiz

Online κουίζ			
Τίτλος μαθήματος:	Απόρρητο και ασφάλεια		
Τίτλος ενότητας:	Εισαγωγή της ιδιωτικότητας		
Σωστό ή Λάθος	Σημειώστε αν οι ακόλουθες δηλώσεις είναι σωστές (Σ) ή λανθασμένες (Λ)		
Δηλώσεις		T	F
1	Σύμφωνα με τα Ηνωμένα Έθνη, η ιδιωτική ζωή αποτελεί ανθρώπινο δικαίωμα		
2	Το απόρρητο είναι το δικαίωμα να κρατάτε μυστικές όλες τις πληροφορίες για τον εαυτό σας, ακόμη και για την κυβέρνηση.		
3	Η Ευρωπαϊκή Ένωση δεν αναγνωρίζει ρητά την ιδιωτική ζωή ως δικαίωμα		
4	Οι όροι "προστασία της ιδιωτικής ζωής" και "προστασία των δεδομένων" είναι λίγο πολύ συνώνυμα.		
5	GDPR σημαίνει "Γενική οδηγία για τα δικαιώματα προστασίας της ιδιωτικής ζωής".		
6	Ορισμένες δικαιοδοσίες αναγνωρίζουν την ιδιωτική ζωή ως προϋπόθεση για την ελεύθερη ανάπτυξη της προσωπικότητας		
7	Ο σεβασμός των νόμων περί προστασίας της ιδιωτικής ζωής και ο σχεδιασμός σύγχρονου λογισμικού είναι αμοιβαία αποκλειόμενοι		
8	Η προστασία των δεδομένων αναφέρεται στην προστασία κάθε πληροφορίας που αφορά ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό (ζωντανό) πρόσωπο.		

2. Ενότητα 2 - Εισαγωγή στην ασφάλεια

Πηγή: Pixabay

Επισκόπηση μαθημάτων

Περίληψη: Αυτή η ενότητα καλύπτει τις βασικές αρχές της ασφάλειας. Εξηγεί τον βασικό ορισμό της, τη σχέση της με την ιδιωτικότητα και παρουσιάζει τη σημασία της ασφάλειας σε ψηφιακά περιβάλλοντα.

Δομή:

- Επισκόπηση μαθημάτων
- Ο ορισμός της ασφάλειας
- Η σημασία της ασφάλειας
- Μελέτη περίπτωσης
- Συμπληρωματική ανάγνωση
- Άσκηση
- Ανατροφοδότηση
- E-Quiz

Μαθησιακοί στόχοι:

- Κατανόηση του ορισμού της ασφάλειας
- Αναγνωρίζουν τη σημασία της ασφάλειας

- Εξηγήστε τη σημασία της ασφάλειας στο πλαίσιο της ιδιωτικής ζωής

Ο ορισμός της ασφάλειας

Ασφάλεια σημαίνει ελευθερία από κινδύνους που προκαλούνται από εξωτερικές απειλές ή από φόβο ή άγχος για βλάβη ή κίνδυνο. Τα ανθρώπινα δικαιώματα βασίζονται εν μέρει στην αρχή ότι οι άνθρωποι επιθυμούν να είναι ασφαλείς.

Στο πλαίσιο της ψηφιακής ιθαγένειας, ασφάλεια σημαίνει την ελευθερία από τον κίνδυνο που μπορεί να προκληθεί από τις πράξεις, τις αδράνειες και τη συμπεριφορά του ατόμου σε ένα ψηφιακό ή διαδικτυακό περιβάλλον. Είναι βαθιά συνδεδεμένη με την ιδιωτικότητα, διότι χωρίς την εφαρμογή κατάλληλων μέτρων ασφαλείας η ιδιωτική σας ζωή τίθεται σε κίνδυνο. Το Συμβούλιο της Ευρώπης αναφέρει στην ιστοσελίδα του:

> *"Για να γίνει κάποιος ψηφιακός πολίτης, αναμένεται να αναπτύξει μια κριτική και ηθική προσέγγιση για να περιηγηθεί στο ψηφιακό περιβάλλον με αυτοπεποίθηση και σαφήνεια και να ενεργήσει αναλόγως".*[9]

Επομένως, για να είναι ασφαλής, ο ψηφιακός πολίτης πρέπει να γνωρίζει τους πιθανούς κινδύνους και τις απειλές που μπορούν να βλάψουν όχι μόνο τον εαυτό του, αλλά και άλλους ανθρώπους. Για να κατανοήσουμε καλύτερα τη δυνητική βλάβη που προκαλείται από την έλλειψη ασφάλειας, μπορούμε να δούμε ένα παράδειγμα λίστας προσωπικών δεδομένων:

- Όνομα και επώνυμο
- Διεύθυνση κατοικίας
- Αριθμός τηλεφώνου
- Διεύθυνση ηλεκτρονικού ταχυδρομείου
- Δεδομένα γεωγραφικού εντοπισμού
- Διευθύνσεις IP
- Αναγνωριστικά cookie

Η διαρροή οποιουδήποτε από αυτά τα δεδομένα μπορεί να οδηγήσει σε μικρή ή/και σοβαρή βλάβη.

Η σημασία της ασφάλειας

Τα ψηφιακά περιβάλλοντα θέτουν νέους και συχνά αρκετά αόρατους κινδύνους για τα άτομα. Για να εξηγήσουμε τη σημασία της ψηφιακής ασφάλειας, μπορούμε να εξετάσουμε την πανδημία Corona: Όσο περισσότεροι άνθρωποι μολύνονται από τον ιό, τόσο αυξάνεται η πιθανότητα να μολυνθούν και άλλοι άνθρωποι. Φανταστείτε ότι η συσκευή σας έχει προσβληθεί από κακόβουλο λογισμικό. Ανάλογα με τον τύπο του κακόβουλου λογισμικού, μπορεί να αποτελέσει κίνδυνο όχι μόνο για τη δική σας ιδιωτική ζωή αλλά και για την ιδιωτική ζωή άλλων ανθρώπων και να επηρεάσει αρνητικά τη ζωή τους.

Η ασφάλεια δεν πρέπει να θεωρείται προνόμιο, επιλογή ή εθελοντική προσφορά. Αντίθετα, ένας υπεύθυνος ψηφιακός πολίτης πρέπει να αντιλαμβάνεται την ασφάλεια ως μια αστική ευθύνη για τον εαυτό του και τους άλλους πολίτες. Η τήρηση των βασικών αρχών της ψηφιακής ασφάλειας (βλ. ενότητα 4) αποτελεί ενεργό συμβολή σε ένα δικαιότερο και θετικότερο ψηφιακό περιβάλλον.

[9] https://www.coe.int/en/web/digital-citizenship-education/privacy-and-security

Η ασφάλεια δεν αφορά ποτέ μόνο την προστασία του εαυτού σας. Πρόκειται για την προστασία όλων μας, συμπεριλαμβανομένων των φίλων και των οικογενειών σας.

Μελέτη περίπτωσης - STOP.THINK.CONNECT

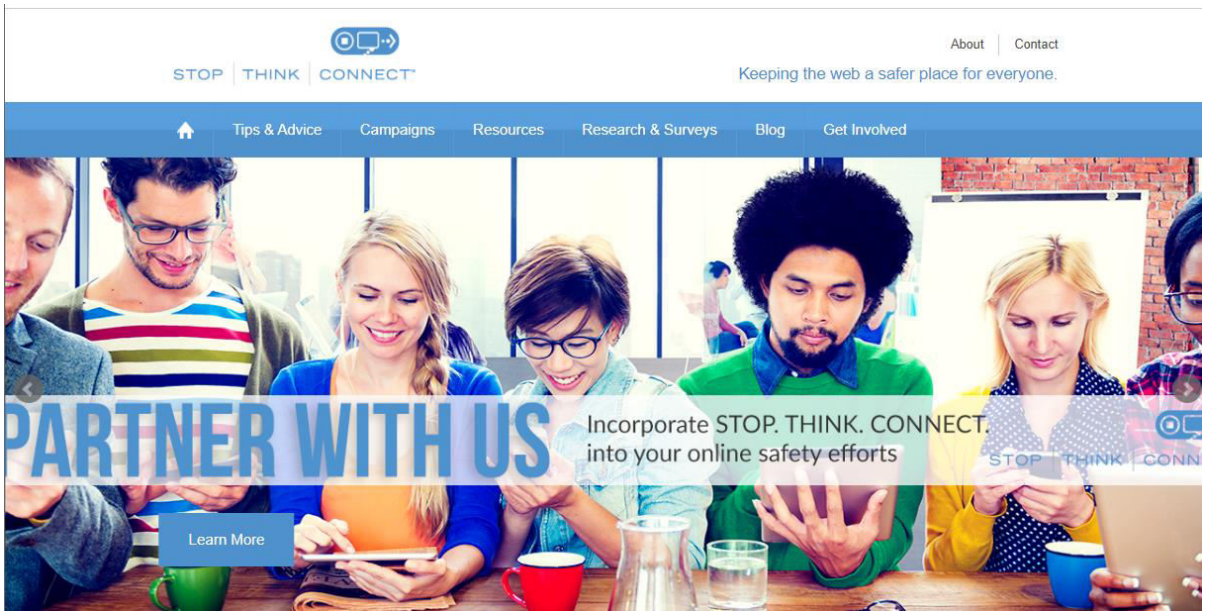
Το STOP.THINK.CONNECT. είναι η πρώτη παγκόσμια εκστρατεία ευαισθητοποίησης του κοινού που αναπτύχθηκε για να βοηθήσει όλους τους χρήστες του Διαδικτύου να διατηρούν τις προσωπικές τους πληροφορίες, τις επικοινωνίες και τις συναλλαγές τους πιο ασφαλείς στο διαδίκτυο.

Η οργάνωση "National Cybersecurity Alliance" με έδρα τις ΗΠΑ και η "APWG Public Education Initiative" διοργάνωσαν αυτή την παγκόσμια εκστρατεία ευαισθητοποίησης για την ασφάλεια στο διαδίκτυο με τίτλο "STOP. THINK. CONNECT.". Συνιστούν τρεις βασικές αρχές που σχετίζονται με την ψηφιακή ασφάλεια:

"**STOP:** Πριν χρησιμοποιήσετε το Διαδίκτυο, αφιερώστε χρόνο για να κατανοήσετε τους κινδύνους και να μάθετε πώς να εντοπίζετε πιθανά προβλήματα.

ΣΚΕΦΤΕΙΤΕ: Αφιερώστε ένα λεπτό για να βεβαιωθείτε ότι ο δρόμος μπροστά σας είναι καθαρός. Προσέξτε για προειδοποιητικά σημάδια και σκεφτείτε πώς οι ενέργειές σας στο διαδίκτυο θα μπορούσαν να επηρεάσουν την ασφάλειά σας ή την ασφάλεια της οικογένειάς σας.

CONNECT: Απολαύστε το Διαδίκτυο με μεγαλύτερη αυτοπεποίθηση, γνωρίζοντας ότι έχετε λάβει τα σωστά μέτρα για την προστασία του εαυτού σας και του υπολογιστή σας (και άλλων συσκευών)".



https://www.stopthinkconnect.org/

Περισσότερες από 800 εμπορικές επιχειρήσεις, εκπαιδευτικά ιδρύματα, κυβερνητικές υπηρεσίες και ΜΚΟ έχουν υιοθετήσει το STOP. THINK. CONNECT. ™. Δεκατρία εθνικά υπουργεία και ΜΚΟ εθνικής εμβέλειας έχουν αναπτύξει εθνικές εκστρατείες.

Διαβάστε το ενημερωτικό δελτίο https://education.apwg.org/safety-messaging-convention/ και σκεφτείτε πώς οι οργανισμοί μπορούν να συμμετάσχουν στην εκστρατεία.

Άσκηση 2: Σχεδιάζοντας τη γραμμή

Στόχοι:

- Κατανόηση της διαφοράς μεταξύ προσωπικών δεδομένων και δημόσιων δεδομένων

- Αναγνωρίστε τις δικές σας ανάγκες σχετικά με την προστασία των δεδομένων
- Αιτιολογήστε τη χρήση των προσωπικών σας δεδομένων

Διάρκεια: 20 λεπτά

Εργαλεία: στυλό και χαρτί

Μέθοδοι: ολομέλεια, δημιουργική εφαρμογή, γραφή

Περιγραφή της άσκησης: Σκεφτείτε τα ακόλουθα παραδείγματα προσωπικών δεδομένων: Το όνομα, η ηλικία, το μέγεθος των παπουτσιών, το βάρος, τα χόμπι, ο μισθός, η μάρκα σαμπουάν, το όνομα του πρώτου σας κατοικίδιου, το χρώμα των εσωρούχων σας, η βαθμολογία των τελευταίων εξετάσεων/αξιολόγησης της εργασίας σας, ο μισθός σας, η ώρα που βγαίνετε από το σπίτι σας. Αναθέστε καθένα από αυτά τα δεδομένα σε μία από τις ακόλουθες τέσσερις κατηγορίες: (1) Αυτά τα δεδομένα είναι προσωπικά- δεν θα τα μοιραστώ. (2) Αυτά τα δεδομένα μπορούν να μοιραστούν μόνο με τους φίλους μου. (3) Αυτά τα δεδομένα μπορούν να δημοσιοποιηθούν. (4) Δεν ξέρω πού να αναθέσω αυτά τα δεδομένα.

Καθήκοντα:

- Δημιουργήστε έναν πίνακα στο χαρτί σας, όπου κάθε γραμμή αντιπροσωπεύει μία από τις τέσσερις κατηγορίες.
- Αναθέστε όλα τα παραδείγματα σε μία από τις τέσσερις κατηγορίες εντός 5 λεπτών.
- Μοιραστείτε τα αποτελέσματά σας με την τάξη (έχετε υπόψη σας ότι δεν χρειάζεται να μοιραστείτε οποιαδήποτε πληροφορία που μπορεί να σας κάνει να νιώσετε άβολα).

Ενημέρωση: Ο εκπαιδευτής θα πρέπει να τονίσει τους λόγους για τους οποίους ορισμένα παραδείγματα προσωπικών δεδομένων είναι προτιμότερο να μην κοινοποιούνται στο κοινό από τους περισσότερους συμμετέχοντες. Η ολομέλεια θα πρέπει να εξάγει συμπεράσματα και κοινούς λόγους σχετικά με τα προσωπικά δεδομένα και την ιδιωτική ζωή.

Διδάγματα: Τα προσωπικά δεδομένα χρειάζονται προστασία. Θα πρέπει να παίρνω το χρόνο μου και να σκέφτομαι πριν μοιραστώ προσωπικά δεδομένα.

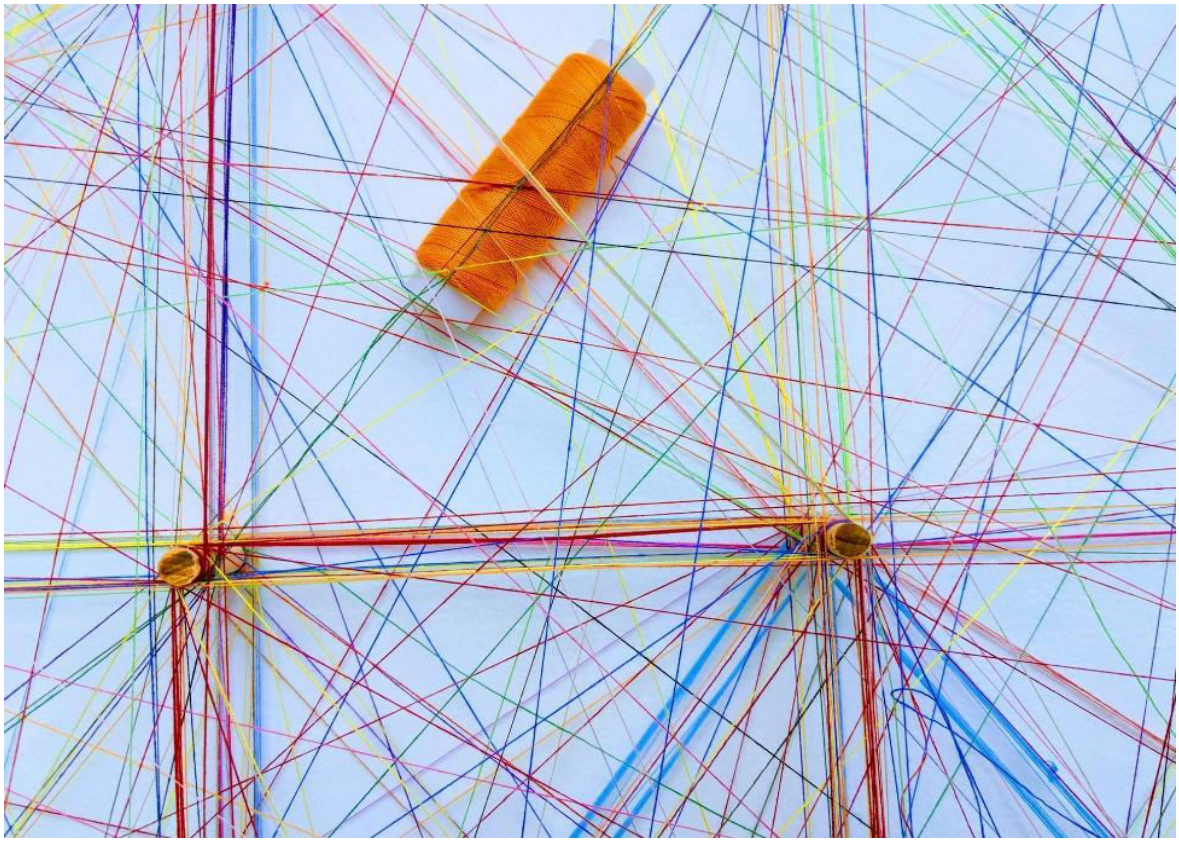
Συμπληρωματική ανάγνωση

- **Διαρροή δεδομένων Facebook**: Διαρροή δεδομένων από το Facebook, που αφορά περίπου 533 εκατομμύρια χρήστες του Facebook από όλο τον κόσμο. https://twitter.com/UnderTheBreach/status/1349671294808285184

E-Quiz

Online κουίζ			
Τίτλος μαθήματος:	Απόρρητο και ασφάλεια		
Τίτλος ενότητας:	Εισαγωγή της ασφάλειας		
Σωστό ή Λάθος	Σημειώστε αν οι ακόλουθες δηλώσεις είναι σωστές (Σ) ή λανθασμένες (Λ)		
Δηλώσεις		T	F
1	Η έλλειψη ασφάλειας μπορεί να θέσει σε κίνδυνο την ιδιωτική σας ζωή		
2	Η διεύθυνση IP του smartphone σας είναι μέρος των προσωπικών σας δεδομένων		
3	Η ασφάλεια αναφέρεται στην ελευθερία σας να αποκτήσετε πρόσβαση στις ιδιωτικές σφαίρες άλλων ανθρώπων.		
4	Εάν εφαρμόζετε σωστή ευαισθητοποίηση για την ασφάλεια, προστατεύετε και άλλους ανθρώπους.		
5	Η ασφάλεια αποτελεί ευθύνη των πολιτών για τους ψηφιακούς πολίτες		
6	Η κριτική και ηθική συμπεριφορά σε ένα ψηφιακό περιβάλλον αποτελεί μέρος της ασφάλειας		

3. Ενότητα 3 - Ιδιωτικότητα σε ψηφιακό περιβάλλον



Πηγή: Unsplash

Επισκόπηση μαθημάτων

Περίληψη: Αυτή η ενότητα εξηγεί την έννοια των ψηφιακών περιβαλλόντων. Επικεντρώνεται στα κοινωνικά περιβάλλοντα και τα περιβάλλοντα επικοινωνίας και τους αντίστοιχους κινδύνους για την ιδιωτικότητα του χρήστη. Σε σχέση με την προστασία της ιδιωτικής ζωής, εξετάζει κριτικά τη σημασία και τα ζητήματα των μεγαλύτερων ιστότοπων κοινωνικής δικτύωσης.

Δομή:

- Επισκόπηση μαθημάτων
- Η προϋπόθεση των ψηφιακών περιβαλλόντων
- Κίνδυνοι από τα κοινωνικά δίκτυα και τους αγγελιοφόρους σε ένα ψηφιακό περιβάλλον
- Μελέτη περίπτωσης
- Συμπληρωματική ανάγνωση
- Άσκηση
- Ανατροφοδότηση
- E-Quiz

Μαθησιακοί στόχοι:

- Κατανόηση του ορισμού των ψηφιακών περιβαλλόντων
- Αναγνωρίστε την επιρροή των ιστότοπων κοινωνικής δικτύωσης

- Προσδιορισμός των πολυεπίπεδων απειλών για την ιδιωτικότητα σε ψηφιακά περιβάλλοντα

Η προϋπόθεση των ψηφιακών περιβαλλόντων

Σήμερα, ο τεχνικός ορισμός του ψηφιακού περιβάλλοντος αναφέρεται συνήθως σε ψηφιακά και ηλεκτρονικά συστήματα που είναι ολοκληρωμένα, συνδεδεμένα και προσβάσιμα μέσω του παγκόσμιου ιστού ή άλλων διαδικτυακών προσβάσεων. Για τους ψηφιακούς πολίτες, ωστόσο, τα ψηφιακά περιβάλλοντα συχνά ορίζονται από τα συμφραζόμενα και βιώνονται ως συνδεδεμένοι διαδικτυακοί χώροι, που ενεργοποιούνται από την τεχνολογία και τις ψηφιακές συσκευές.[10]

Τα ψηφιακά περιβάλλοντα μπορούν να χρησιμοποιηθούν για την ευαισθητοποίηση για τα ανθρώπινα δικαιώματα ή για θέματα που αφορούν την κοινωνία των πολιτών, συνδέοντας ο ένας τον άλλον και εκφράζοντας τη γνώμη σας. Οι ψηφιακοί πολίτες αποκτούν πρόσβαση στα ψηφιακά περιβάλλοντα με τη βοήθεια ψηφιακών συσκευών, όπως τα smartphones ή οι φορητοί υπολογιστές. Αποκτούν πρόσβαση σε διάφορα στοιχεία των ψηφιακών περιβαλλόντων που εξυπηρετούν διαφορετικές λειτουργίες.

Ωστόσο, η ασφαλής συμμετοχή όλων των ψηφιακών πολιτών στα κοινωνικά και επικοινωνιακά περιβάλλοντα συνδέεται με έναν απαραίτητο βαθμό παιδείας στα μέσα επικοινωνίας.

Για την εμπειρία της ψηφιακής ιθαγένειας, η επικοινωνία και οι κοινωνικές υπηρεσίες μέσα στα ψηφιακά περιβάλλοντα είναι πολύ σημαντικές, όπως για παράδειγμα οι ιστότοποι, οι πλατφόρμες κοινωνικής δικτύωσης ή οι αγγελιοφόροι. Ο Εκπαιδευτικός, Επιστημονικός και Πολιτιστικός Οργανισμός των Ηνωμένων Εθνών αναφέρει στην έκθεσή του για τον "Πολιτισμό στο ψηφιακό περιβάλλον":

> *"Αυτό περιλαμβάνει την ικανότητα κριτικής ανάλυσης της ποικιλίας των πληροφοριών που δεχόμαστε (δηλαδή του οπτικοακουστικού περιεχομένου), τη διαμόρφωση αυτόνομων απόψεων, την ενεργό συμμετοχή σε θέματα της κοινότητας και την κατάκτηση νέων μορφών κοινωνικής αλληλεπίδρασης".*[11]

Δεδομένου ότι τα ψηφιακά περιβάλλοντα τείνουν να αλλάζουν γρήγορα τις διεπαφές, τις προσβάσεις, τις λειτουργίες και τις συμπεριφορές τους, είναι σημαντικό να τα συμπεριλάβουμε ενεργά στις τυπικές και μη τυπικές εκπαιδευτικές διαδικασίες για άτομα όλων των ηλικιών.

Κίνδυνοι από τα κοινωνικά δίκτυα και τους αγγελιοφόρους σε ένα ψηφιακό περιβάλλον

Το ψηφιακό περιβάλλον εγκυμονεί κινδύνους για τους ψηφιακούς πολίτες όλων των ηλικιών και με την άνοδο των ιστότοπων κοινωνικής δικτύωσης και των άμεσων μηνυμάτων, τα ζητήματα προστασίας της ιδιωτικής ζωής φαίνεται να εμφανίζονται πιο συχνά από ποτέ.

> *"Το 2020, πάνω από 3,6 δισεκατομμύρια άνθρωποι χρησιμοποιούσαν τα μέσα κοινωνικής δικτύωσης παγκοσμίως, αριθμός που αναμένεται να αυξηθεί σε σχεδόν 4,41 δισεκατομμύρια το 2025".*[12]

Εάν οι υπηρεσίες αυτές χρησιμοποιούνται με απερίσκεπτο τρόπο, ο χρήστης μπορεί να υποστεί κοινωνικές, οικονομικές, συναισθηματικές, επαγγελματικές ή νομικές συνέπειες. Ο παρακάτω

[10] "Handbook of Research on Educational Design and Cloud Computing in Modern Classroom Settings", σελ. 79, 2017, Yannis Kotsanis (Doukas School, Greece), ISBN13: 9781522530534
[11] https://en.unesco.org/creativity/sites/creativity/files/dce-policyresearch-book2-en-web.pdf
[12] https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

κατάλογος παρέχει τις σημαντικότερες ανησυχίες για την προστασία της ιδιωτικής ζωής σε σχέση με τους ιστότοπους κοινωνικής δικτύωσης:

- **Απώλεια της κυριαρχίας των δεδομένων**: Η απώλεια της δυνατότητάς σας να ελέγχετε την επεξεργασία των προσωπικών σας δεδομένων
- **Έλλειψη διαφάνειας**: Η έλλειψη της δυνατότητάς σας να ενημερώνεστε για τον χειρισμό των προσωπικών σας δεδομένων
- **Λανθασμένη αντίληψη των οφελών**: Μια κατάσταση κατά την οποία το αντιληπτό όφελος από την αποκάλυψη κομματιών των προσωπικών σας δεδομένων φαίνεται να είναι μεγαλύτερο από τον αντιληπτό κίνδυνο από την ανταλλαγή πληροφοριών σε μια διαδικτυακή πλατφόρμα.
- **Χαλαρή συμπεριφορά**: Η υποτίμηση των συνεπειών που μπορεί να προκαλέσει η κοινοποίηση προσωπικών δεδομένων
- **Διαρκής διατήρηση των πληροφοριών:** Το γεγονός ότι οι προσωπικές σας πληροφορίες είναι πιθανό να είναι μόνιμα διαθέσιμες στο διαδίκτυο (σχετίζεται με το "δικαίωμα στη λήθη" στην Ευρωπαϊκή Ένωση).
- **Προφίλ**: Η απειλή δημιουργίας ενός προφίλ για εσάς με τη χρήση διαθέσιμων προσωπικών πληροφοριών ή/και μεταδεδομένων, για παράδειγμα στο πλαίσιο στοχευμένης διαφήμισης.

Στις μέρες μας, μία από τις μεγαλύτερες απειλές είναι η χαλαρή συμπεριφορά σε ιστότοπους κοινωνικής δικτύωσης όπως το Facebook, το Twitter, το Instagram ή το TikTok. Καθένας από αυτούς τους ιστότοπους προσφέρει διαφορετικό βαθμό προστασίας της ιδιωτικής ζωής. Ιστοσελίδες όπως το Facebook συχνά αναγκάζουν τους χρήστες τους να χρησιμοποιούν το πραγματικό τους όνομα, αλλιώς οι λογαριασμοί τους μπορεί να κλείσουν, ενώ άλλες ιστοσελίδες κοινωνικής δικτύωσης ενθαρρύνουν τη χρήση ψευδωνύμων. Ωστόσο, κάθε ιστότοπος κοινωνικής δικτύωσης μπορεί δυνητικά να παρέχει αρκετές προσωπικές πληροφορίες που να καθιστούν εσάς ή άλλους αναγνωρίσιμους, για παράδειγμα με τη χρήση των ίδιων εικόνων προφίλ σε διαφορετικά δίκτυα, με τη δημοσίευση φωτογραφιών με αναγνωρίσιμα περιβάλλοντα ή με την κοινοποίηση πληροφοριών τοποθεσίας με το προφίλ σας.

Το 2020, η αμερικανική εταιρεία λιανικής πώλησης δορυφορικού διαδικτύου "Viasat Savings" διεξήγαγε έρευνα σε 1.000 ενήλικες Αμερικανούς πολίτες, ρωτώντας πόσοι άνθρωποι στους ιστότοπους κοινωνικής δικτύωσης διατηρούν το προφίλ τους ιδιωτικό:

> *"Αποδεικνύεται ότι είναι ισομερώς μοιρασμένο: σχεδόν το 50% των ατόμων που ερωτήσαμε διατηρούν τους λογαριασμούς τους σε ιδιωτική λειτουργία, ενώ οι υπόλοιποι μισοί επέλεξαν να είναι δημόσιοι. Σύμφωνα με την Kyrsten Holland, εμπειρογνώμονα διαδικτύου της Viasatsavings.com, "οι νέοι και οι ηλικιωμένοι έχουν ένα κοινό: οι άνθρωποι 18-24 και 54+ είναι οι ηλικιακές ομάδες που είναι πιο πιθανό να δημοσιοποιήσουν τους λογαριασμούς τους στα μέσα κοινωνικής δικτύωσης".*[13]

Αλλά ακόμη και όταν διατηρείτε το προφίλ σας ιδιωτικό, οι σημαντικότεροι ιστότοποι κοινωνικής δικτύωσης ανήκουν σε ιδιωτικές εταιρείες με σκοπό την πραγματοποίηση κερδών. Ως εκ τούτου, διατηρούν συνήθως το δικαίωμα να χρησιμοποιούν, να συνδυάζουν (ιδιαίτερα πολύτιμο αν κατέχουν πολλαπλές υπηρεσίες, όπως για παράδειγμα το Facebook, το Instagram και το WhatsApp) ή/και να πωλούν τις προσωπικές σας πληροφορίες -που με τη θέλησή σας δώσατε- σε άλλες

[13] https://www.viasatsavings.com/news/blog/are-more-people-public-or-private-on-social-media/

εταιρείες, οι οποίες στη συνέχεια μπορούν να κατευθύνουν τη διαφήμισή τους (συμπεριλαμβανομένων των πολιτικών εκστρατειών) προς τα συμφέροντά σας.

Ταυτόχρονα, η εμπειρία μάς διδάσκει ότι καμία εταιρεία δεν μπορεί να εμπιστευτεί την ασφαλή αποθήκευση των προσωπικών σας δεδομένων όλη την ώρα. Όλοι οι μεγάλοι ιστότοποι κοινωνικής δικτύωσης έπεσαν θύματα διαρροής δεδομένων στο παρελθόν:

- **Instagram, TikTok, YouTube**: "Η ομάδα έρευνας ασφαλείας της Comparitech αποκάλυψε σήμερα πώς μια μη ασφαλής βάση δεδομένων άφησε εκτεθειμένα στο διαδίκτυο σχεδόν 235 εκατομμύρια προφίλ χρηστών του Instagram, του TikTok και του YouTube, σε κάτι που μπορεί να περιγραφεί μόνο ως μαζική διαρροή δεδομένων".[14]
- **Facebook:** "Η ομάδα κυβερνοκινδύνων της UpGuard μπορεί τώρα να αναφέρει ότι δύο ακόμη σύνολα δεδομένων εφαρμογών του Facebook που αναπτύχθηκαν από τρίτους βρέθηκαν εκτεθειμένα στο δημόσιο διαδίκτυο. Το ένα, προερχόμενο από την εταιρεία μέσων ενημέρωσης Cultura Colectiva με έδρα το Μεξικό, ζυγίζει 146 gigabytes και περιέχει πάνω από 540 εκατομμύρια εγγραφές που περιλαμβάνουν λεπτομερώς σχόλια, συμπάθειες, αντιδράσεις, ονόματα λογαριασμών, FB IDs και άλλα".[15]
- **Twitter**: "Ένα τέταρτο του ενός εκατομμυρίου χρηστών του Twitter υπέστησαν παραβίαση των λογαριασμών τους στην τελευταία από μια σειρά παραβιάσεων ασφαλείας υψηλού προφίλ σε εταιρείες του διαδικτύου. Ανώνυμοι χάκερς ενδέχεται να κατάφεραν να αποκτήσουν πρόσβαση σε περίπου 250.000 λογαριασμούς στον ιστότοπο κοινωνικής δικτύωσης, συμπεριλαμβανομένων των ονομάτων χρήστη, των διευθύνσεων ηλεκτρονικού ταχυδρομείου και των κωδικών πρόσβασης".[16]

Οι ακόλουθες συμβουλές θα πρέπει να ακολουθούνται κατά την αντιμετώπιση ζητημάτων προστασίας της ιδιωτικής ζωής σε ένα ψηφιακό κοινωνικό ή επικοινωνιακό περιβάλλον:

- Ακολουθείτε πάντα τις αρχές της αποφυγής και της ελαχιστοποίησης των δεδομένων: Ποτέ μην παρέχετε προσωπικά δεδομένα και αν πρέπει, παρέχετε όσο το δυνατόν λιγότερα (σχετικό: ενεργοποιείτε πάντα όσο το δυνατόν περισσότερες ρυθμίσεις προστασίας της ιδιωτικής ζωής).
- Ποτέ μην ανεβάζετε περιεχόμενο (π.χ. φωτογραφίες ή βίντεο) για το οποίο δεν έχετε τα δικαιώματα.
- Ποτέ μην μοιράζεστε προσωπικές πληροφορίες ή δεδομένα άλλων ανθρώπων (π.χ. προσωπικές φωτογραφίες, βίντεο ή μηνύματα) χωρίς τη ρητή συγκατάθεσή τους.
- Να επαληθεύετε πάντα τα αιτήματα φίλων ή συγγενών εκτός σύνδεσης
- Να αναφέρετε πάντα τους ύποπτους χρήστες που προσπαθούν να σας πείσουν να μοιραστείτε τις προσωπικές σας πληροφορίες - άλλοι μπορεί να μην είναι τόσο έξυπνοι!

Μια γερμανική μελέτη του 2012 σχετικά με την ψηφιακή ιδιωτικότητα[17] δείχνει ότι ειδικά οι νέοι χρήστες υιοθετούν μια πολύ ατομική προσέγγιση για την ψηφιακή τους ιδιωτικότητα. Συχνά συμμετέχουν σε ψηφιακά κοινωνικά και επικοινωνιακά περιβάλλοντα σε μια διελκυστίνδα μεταξύ

[14] https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=e35b1371111e
[15] https://www.upguard.com/breaches/facebook-user-data-leak

[16] https://www.theguardian.com/technology/2013/feb/02/twitter-hacked-accounts-reset-security
[17] https://www.medienanstalt-nrw.de/fileadmin/lfm-nrw/Forschung/LfM-Band-71.pdf

της ανάγκης τους για κοινωνική συμμετοχή και του φόβου τους για την ιδιωτική τους ζωή. Η μελέτη εντοπίζει τρεις τύπους χρηστών με διαφορετικές στρατηγικές προστασίας της ιδιωτικής ζωής:

- **Τα αποκαλυπτικά πρόσωπα**: Αυτή είναι η μικρότερη ομάδα μεταξύ των υποκειμένων της μελέτης. Χαρακτηρίζονται από το γεγονός ότι έχουν ανοιχτές ρυθμίσεις απορρήτου στους διαδικτυακούς λογαριασμούς τους, ενώ ταυτόχρονα μοιράζονται πολλές προσωπικές πληροφορίες. Υπάρχουν σχετικά περισσότερα αποκαλυπτικά άτομα μεταξύ των νεότερων ατόμων και των ατόμων με χαμηλότερο επίπεδο τυπικής εκπαίδευσης. Η μελέτη υποδηλώνει ότι αυτή η ομάδα είτε μοιράζεται οικειοθελώς τα δεδομένα της είτε ότι δεν διαθέτει την ικανότητα και την ευαισθητοποίηση για ασφαλείς ρυθμίσεις απορρήτου.
- **Τα επιφυλακτικά άτομα**: Αυτή η ομάδα ανθρώπων έχει συγκριτικά περιοριστικές ρυθμίσεις απορρήτου και αποφεύγει να μοιράζεται προσωπικές πληροφορίες. Αποτελούν τον αντίποδα των αποκαλυπτικών ατόμων. Παρόλο που επισκέπτονται συχνά το κοινωνικό δίκτυο που προτιμούν, πιθανότατα δεν θέλουν να χάσουν σημαντικές κοινωνικές πληροφορίες.
- **Οι διαχειριστές απορρήτου:** Αυτή η ομάδα ανθρώπων είναι συνεχώς ενεργή όσον αφορά την ανάρτηση ενημερώσεων κατάστασης και σχολίων στα κοινωνικά δίκτυα. Διαθέτουν ένα τεράστιο δίκτυο επαφών και γνωρίζουν πολλούς από αυτούς και στην πραγματική ζωή. Φαίνεται ότι είναι ειδικοί στην προστασία της ιδιωτικής ζωής σε ένα ψηφιακό περιβάλλον και μπορούν να σταθμίσουν τις συνήθειες κοινής χρήσης τους σε σχέση με την προστασία της ιδιωτικής τους ζωής.

Η μελέτη καταλήγει στο συμπέρασμα ότι οι πιθανές απειλές για την προστασία της ιδιωτικής ζωής ελάχιστα επηρεάζουν τη συμπεριφορά του χρήστη. Είναι ενδιαφέρον ότι οι αρχές της ίδιας της ψηφιακής ιθαγένειας δεν αναζητούνται ενεργά.

Μελέτη περίπτωσης - Μέσα κοινωνικής δικτύωσης και κλοπή ταυτότητας

Ένα άρθρο που εξετάζει τη σύγχρονη εφαρμογή της κλοπής ταυτότητας με τη χρήση των ιστότοπων κοινωνικής δικτύωσης. Παρουσιάζει τέσσερις περιπτώσεις κλοπής ταυτότητας και παρέχει συμβουλές για το πώς μπορείτε να προστατευτείτε από αυτό το είδος απάτης.

Jessica Velasco για το socialnomics.net, 13/01/2016: https://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft/

> *"Μελέτη περίπτωσης: Sarah Palins".*
>
> *Η πρώην κυβερνήτης της Αλάσκας Σάρα Πέιλιν δεν είναι άγνωστη στις διαμάχες, ούτε στους απατεώνες λογαριασμούς στο Twitter. Το 2011, ο τότε επίσημος λογαριασμός της Πέιλιν στο Twitter, AKGovSarahPalin (τώρα@SarahPalinUSA), βρέθηκε να χάνεται όλο και περισσότερο σε μια θάλασσα από ψεύτικους λογαριασμούς.*
>
> *Σε ένα ιδιαίτερα αξιοσημείωτο περιστατικό, ένας μιμητής της Πέιλιν έστειλε στο Twitter μια ανοιχτή πρόσκληση στο σπίτι της οικογένειας της Σάρα Πέιλιν για μπάρμπεκιου. Ως αποτέλεσμα, το προσωπικό ασφαλείας της Πέιλιν χρειάστηκε να αποσταλεί στην κατοικία της στην Αλάσκα για να αποτρέψει τους επίδοξους επισκέπτες του πάρτι.*
>
> *Το φαινόμενο αυτό δεν περιορίζεται μόνο στη Σάρα Πέιλιν. Πολλά δημόσια πρόσωπα και πολιτικοί, ιδιαίτερα αμφιλεγόμενοι, όπως ο υποψήφιος για τις προεδρικές εκλογές του 2016*

Ντόναλντ Τραμπ, έχουν πλήθος ψεύτικων λογαριασμών που υποδύονται την ταυτότητά τους. "

Ερώτηση αυτοαναστοχασμού: Σας αφήνει εκτεθειμένους στον κίνδυνο κλοπής ταυτότητας;

Άσκηση 3: Κοινότητα

Στόχος:

- Κατανόηση και εφαρμογή τρόπων προστασίας της ιδιωτικής σας ζωής σε διαδικτυακές κοινότητες

Διάρκεια: 25 λεπτά

Εργαλεία: ψηφιακές συσκευές με ενεργή σύνδεση στο διαδίκτυο, στυλό και χαρτί

Μέθοδοι: ολομέλεια, έρευνα, ομαδική εργασία

Περιγραφή της άσκησης: Οι μαθητές εργάζονται μαζί σε μικρές ομάδες (το πολύ 4 άτομα). Η ομάδα επιλέγει έναν ιστότοπο κοινωνικής δικτύωσης με μεγάλο όγκο επικοινωνίας (π.χ. Facebook, Twitter, Instagram, Twitch, TikTok). Ιδανικά, όλοι οι μαθητές είναι ήδη ενεργοί στον επιλεγμένο ιστότοπο. Στη συνέχεια, προσπαθούν να βρουν μια λύση για καθεμία από τις ακόλουθες προκλήσεις: (1) Πώς μπορώ να ενεργοποιήσω τις πιο περιοριστικές ρυθμίσεις απορρήτου στο προφίλ μου; (2) Πώς μπορώ να αφαιρέσω μια ενοχλητική φωτογραφία μου που μοιράστηκαν άλλοι στην πλατφόρμα; (3) Πώς μπορώ να αναφέρω ή να μπλοκάρω άλλους χρήστες; (4) Πού μπορώ να βρω τους όρους παροχής υπηρεσιών και τι αναφέρουν σχετικά με το απόρρητό μου; (5) Πώς μπορώ να διαγράψω το προφίλ μου και χάθηκε πραγματικά;

Καθήκοντα:

- Μέσα σε 3 λεπτά, επιλέξτε έναν ιστότοπο κοινωνικού δικτύου
- Επισκεφθείτε τους ιστότοπους για δεκαπέντε λεπτά και απαντήστε στις 5 ερωτήσεις με τη βοήθεια του ιστότοπου ή της έρευνας.
- Μοιραστείτε τα αποτελέσματά σας με την τάξη (έχετε υπόψη σας ότι δεν χρειάζεται να μοιραστείτε οποιαδήποτε πληροφορία που μπορεί να σας κάνει να νιώσετε άβολα).

Ενημέρωση: Ο εκπαιδευτής θα πρέπει να εστιάσει στα εμπόδια που δημιουργούν οι ιστότοποι κοινωνικής δικτύωσης για να διατηρήσουν την πρόσβαση στα προσωπικά δεδομένα των χρηστών τους. Ο εκπαιδευτής θα πρέπει επίσης να ενσωματώσει πραγματικές εμπειρίες που κάποιοι από τους μαθητές μπορεί να έχουν ήδη κάνει σχετικά με ορισμένες από τις προκλήσεις.

Διδάγματα: Μόλις οι πληροφορίες δημοσιοποιηθούν, είναι δύσκολο να τις πάρεις πίσω. Να είστε προσεκτικοί όταν συμμετέχετε σε μεγάλα κοινωνικά δίκτυα, δεν είναι φίλοι σας.

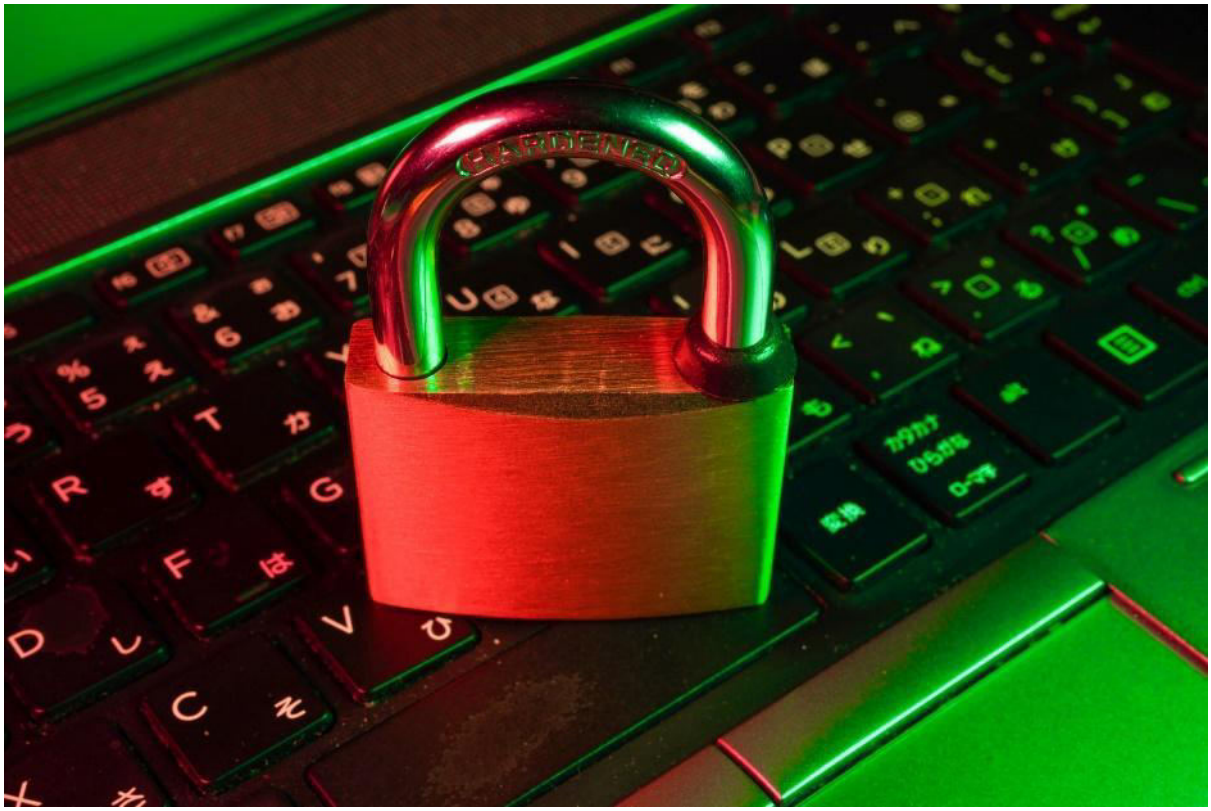
Συμπληρωματική ανάγνωση

- **Γιατί είμαστε εθισμένοι στα μέσα κοινωνικής δικτύωσης: Η ψυχολογία των likes**: "Τα likes στα μέσα κοινωνικής δικτύωσης είναι εθιστικά επειδή επηρεάζουν τον εγκέφαλό σας, παρόμοια με τη λήψη χημικών ουσιών. Τα likes συμβολίζουν ένα κέρδος σε φήμη, προκαλώντας σας να συγκρίνετε συνεχώς τον εαυτό σας με τους συνομηλίκους σας." https://steverosephd.com/why-we-are-addicted-to-likes/.

E-Quiz

Online κουίζ			
Τίτλος μαθήματος:	Απόρρητο και ασφάλεια		
Τίτλος ενότητας:	Ιδιωτικότητα σε ένα ψηφιακό περιβάλλον		
Σωστό ή Λάθος	Σημειώστε αν οι ακόλουθες δηλώσεις είναι σωστές (Σ) ή λανθασμένες (Λ)		
Δηλώσεις		T	F
1	Δεν υπάρχει κοινωνικό όφελος από τα ψηφιακά περιβάλλοντα		
2	Περισσότεροι από 3 δισεκατομμύρια άνθρωποι χρησιμοποιούν πλέον ιστότοπους κοινωνικής δικτύωσης		
3	Το Facebook διαγράφει αυτόματα τα προσωπικά μου δεδομένα μετά από ορισμένο χρονικό διάστημα		
4	Οι μεγάλες εταιρείες τεχνολογίας μπορούν γενικά να εμπιστευτούν ότι χειρίζονται προσεκτικά τα προσωπικά μου δεδομένα		
5	Η εφαρμογή της αποφυγής δεδομένων είναι ο ασφαλέστερος τρόπος για να διατηρήσω τα προσωπικά μου δεδομένα ασφαλή		
6	Το Facebook μπορεί να χρησιμοποιήσει τα δεδομένα μου για να εξατομικεύσει την εμπειρία μου σύμφωνα με τους όρους παροχής υπηρεσιών του.		
7	Η κατάρτιση προφίλ αποτελεί κίνδυνο για την ιδιωτική μου ζωή		
8	Η κλοπή ταυτότητας αποτελεί σημαντική απειλή για τους άπειρους χρήστες των μέσων κοινωνικής δικτύωσης		

4. Ενότητα 4 - Κίνδυνοι ασφάλειας σε ένα ψηφιακό περιβάλλον



Πηγή: Unsplash

Επισκόπηση μαθημάτων

Περίληψη: Αυτή η ενότητα εισάγει τις βασικές αρχές και τις διάφορες απειλές για το υλικό και το λογισμικό. Επικεντρώνεται στους κινδύνους της καθημερινής ζωής και στο ρόλο του χρήστη ως κρίσιμο μέρος των τυπικών τρωτών σημείων ασφαλείας.

Δομή:

- Επισκόπηση μαθημάτων
- Εισαγωγή στο υλικό
- Εισαγωγή στο λογισμικό
- Απειλές για το υλικό και το λογισμικό
- Μελέτη περίπτωσης
- Συμπληρωματική ανάγνωση
- Άσκηση
- Ανατροφοδότηση
- E-Quiz

Μαθησιακοί στόχοι:

- Να κατανοήσουν το ρόλο του υλικού και του λογισμικού στα ψηφιακά περιβάλλοντα
- Προσδιορίστε τους επιμέρους κινδύνους από τη χρήση υλικού και λογισμικού
- Αναγνώριση των κινδύνων που σχετίζονται με τον χρήστη και αφορούν τη χρήση υλικού και λογισμικού

Εισαγωγή στο υλικό

Καθημερινά έχουμε να κάνουμε με διαφορετικές συσκευές για να συμμετέχουμε σε ένα ψηφιακό περιβάλλον, για παράδειγμα, με smartphones, επιτραπέζιους υπολογιστές ή ATM. Υλικό είναι ο όρος που χρησιμοποιείται για να περιγράψει τα φυσικά εξαρτήματα αυτών των συσκευών. Ενώ το ίδιο το υλικό μπορεί να αποτελεί κρίσιμη ευπάθεια, τα μέτρα ασφαλείας ελήφθησαν κυρίως για θέματα λογισμικού και χρηστών (βλ. επόμενο θέμα).

Ο συνδυασμός πολλαπλών εξαρτημάτων υλικού κάνει τις συσκευές μας να λειτουργούν:

- Η CPU (Κεντρική Μονάδα Επεξεργασίας) είναι υπεύθυνη για την εκτέλεση των διαφόρων εντολών και υπολογισμών που είναι απαραίτητες για την ορθή λειτουργία των συσκευών μας. Θα βρείτε μια CPU στο smartphone σας, στο φορητό σας υπολογιστή, στον επιτραπέζιο υπολογιστή ή στο tablet σας, για παράδειγμα.
- Η GPU (Μονάδα επεξεργασίας γραφικών) είναι υπεύθυνη για όλες τις διεργασίες που απαιτούν γραφικά, όπως η ροή βίντεο ή τα βιντεοπαιχνίδια. Οι GPU υψηλού φόρτου εργασίας απαιτούν μεγάλη ισχύ και μπορούν να επεξεργαστούν ακόμη και πολύπλοκους και μακροχρόνιους υπολογισμούς σε σύντομο χρονικό διάστημα.
- Ο σκληρός δίσκος HDD (Hard Disk Drive) και ο SSD (Solid State Drive) είναι συσκευές αποθήκευσης. Χρησιμοποιούνται για την αποθήκευση δεδομένων ή λογισμικού. Η διαφορά τους έγκειται στην αρχιτεκτονική τους: Οι σκληροί δίσκοι χρησιμοποιούν τεχνολογία μαγνητικής αποθήκευσης, ενώ οι SSD και όλες οι κινητές συσκευές χρησιμοποιούν τεχνολογία μνήμης flash.
- Η μητρική πλακέτα ή κεντρική πλακέτα είναι το βασικό κομμάτι κάθε υπολογιστή ή κινητής συσκευής. Συνδέει όλα τα ηλεκτρονικά εξαρτήματα της συσκευής.
- Η κάρτα RAM (μνήμη τυχαίας προσπέλασης) είναι μια μορφή μνήμης υπολογιστή. Η συσκευή αποθηκεύει τα τρέχοντα προγράμματα που εκτελούνται, τα μέρη του προγράμματος και τα δεδομένα στη μνήμη RAM. Η ταχύτητα πρόσβασης της RAM και το μέγεθος των αποθηκευτικών της δυνατοτήτων μπορούν να βελτιώσουν δραστικά την ταχύτητα μιας συσκευής.

Εισαγωγή στο λογισμικό

Το λογισμικό αναφέρεται σε όλα τα είδη προγραμμάτων ή εφαρμογών που μπορούμε να εγκαταστήσουμε στις συσκευές μας, όπως το LibreOffice Writer, το πρόγραμμα αναπαραγωγής VLC ή την προσωπική σας τραπεζική εφαρμογή. Ενώ το υλικό είναι υπεύθυνο για την εκτέλεση της εργασίας, μπορούμε να χρησιμοποιήσουμε το λογισμικό για να καθορίσουμε την εργασία που πρέπει να κάνουν οι συσκευές μας.

Υπάρχουν διαφορετικοί τύποι λογισμικού για διαφορετικούς σκοπούς:

- Το λογισμικό συστήματος αναφέρεται σε όλα τα προγράμματα και τα δεδομένα που χρησιμοποιούνται για τον έλεγχο των διαδικασιών που κάνουν έναν υπολογιστή να λειτουργεί. Το λογισμικό συστήματος είναι στενά συνδεδεμένο με το υλικό της αντίστοιχης συσκευής και ελέγχει τη χρήση των πόρων- ως εκ τούτου, παρέχει την υποδομή στον υπολογιστή. Παραδείγματα για το λογισμικό συστήματος είναι:
    - λειτουργικά συστήματα, όπως Linux, Windows, Android ή iOS
    - προγράμματα οδήγησης συσκευών για εξωτερικό υλικό, όπως εκτυπωτές ή ηχεία.
- Το λογισμικό εφαρμογών αναφέρεται σε όλα τα προγράμματα που εκτελούν συγκεκριμένες εργασίες για τους χρήστες, οι οποίες δεν σχετίζονται με το λογισμικό συστήματος ή το

βοηθητικό λογισμικό. Όλες οι σύγχρονες συσκευές μπορούν να εκτελέσουν μια σειρά από διαφορετικά λογισμικά εφαρμογών:

- Media players, για παράδειγμα το VLC player
- Επεξεργαστές κειμένου, για παράδειγμα LibreOffice Writer
- Λογισμικό μοντάζ, για παράδειγμα Adobe Premiere Pro
- Προγράμματα ηλεκτρονικού ταχυδρομείου, για παράδειγμα Mozilla Thunderbird
- Φυλλομετρητές ιστού, για παράδειγμα Mozilla Firefox.

Το λογισμικό εφαρμογών μπορεί είτε να εγκατασταθεί από τον χρήστη, το οποίο στις περισσότερες περιπτώσεις λειτουργεί με τη λήψη των δεδομένων του προγράμματος από μια διαδικτυακή πηγή, είτε είναι προεγκατεστημένο και συνοδεύει ορισμένες συσκευές, όπως τα smartphones.

- Το βοηθητικό λογισμικό αναφέρεται σε λογισμικό που υποστηρίζει την υποδομή, τα λειτουργικά συστήματα ή το λογισμικό εφαρμογών με πρόσθετες λειτουργίες. Το βοηθητικό λογισμικό συχνά ενσωματώνεται στα λειτουργικά συστήματα με ορισμένα από αυτά να λειτουργούν στο παρασκήνιο, επομένως η διάκριση μεταξύ του λογισμικού συστήματος και του βοηθητικού λογισμικού δεν είναι πάντα σαφής. Τυπικά παραδείγματα για γνωστό βοηθητικό λογισμικό είναι:
  - Προγράμματα κατά των ιών
  - Προγράμματα ανάκτησης δεδομένων
  - Διαχειριστές αρχείων

Απειλές για το υλικό και το λογισμικό

Όπως καθορίσαμε στις προηγούμενες ενότητες, πρέπει να δίνουμε ιδιαίτερη προσοχή στα προσωπικά μας δεδομένα και πληροφορίες. Τα οφέλη και οι ανακουφίσεις από την εκτέλεση πολλών εργασιών ή καθημερινών ρουτινών της ζωής στο διαδίκτυο μπορεί να απειλήσουν την ιδιωτική μας ζωή, για παράδειγμα:

- Μπορεί να είστε άρρωστοι και να θέλετε να επισκεφθείτε έναν γιατρό. Αναζητάτε έναν εξειδικευμένο γιατρό χρησιμοποιώντας το Google στο smartphone σας. Στη συνέχεια, προχωράτε στην κλήση του γιατρού, χρησιμοποιώντας το smartphone σας και κλείνοντας ένα ραντεβού, το οποίο αποθηκεύετε στην εφαρμογή ημερολογίου του smartphone σας. Την ημέρα του ραντεβού, χρησιμοποιείτε το smartphone σας για να αγοράσετε ένα εισιτήριο για το τραμ και τους χάρτες Google για να φτάσετε στον προορισμό σας. Μετά το ραντεβού, επισκέπτεστε το πλησιέστερο φαρμακείο και αγοράζετε τα συνταγογραφούμενα φάρμακα χρησιμοποιώντας το Google Pay με το smartphone σας.
- Αναζητάτε ενδιαφέροντα άτομα στην εφαρμογή γνωριμιών Tinder. Αφού συνομιλήσετε για λίγο με ένα ενδιαφέρον άτομο, χρησιμοποιώντας το smartphone σας, ανταλλάσσετε τις διευθύνσεις ηλεκτρονικού ταχυδρομείου σας. Χρησιμοποιείτε μια εφαρμογή-πελάτη ηλεκτρονικού ταχυδρομείου στο smartphone σας και μετά από λίγο, ανταλλάσσετε τους αριθμούς τηλεφώνου σας. Προχωράτε στη χρήση του WhatsApp και τηλεφωνείτε ο ένας στον άλλον κατά διαστήματα. Τέλος, συναντιέστε για το πρώτο σας ραντεβού στην πραγματική ζωή. Η εφαρμογή ημερολογίου στο smartphone σας σας υπενθυμίζει το ραντεβού σας και χρησιμοποιείτε το PayPal στο smartphone σας για να πληρώσετε τα εισιτήρια του κινηματογράφου. Αργότερα το βράδυ, χρησιμοποιείτε τις επιλογές πληρωμής του smartphone σας για να πληρώσετε τα ποτά στο μπαρ, προτού αποχαιρετήσετε ο ένας τον άλλον και καλέσετε ένα Uber για να πάτε σπίτι.

Όπως δείχνουν τα παραδείγματα, συχνά χρησιμοποιούμε την ίδια συσκευή για διαφορετικούς σκοπούς, ενώ ταυτόχρονα μοιραζόμαστε και αποθηκεύουμε ευαίσθητες, προσωπικές πληροφορίες. Αν κάποιος αποκτήσει πρόσβαση σε αυτή τη συσκευή, εύκολα θα μάθει ή τουλάχιστον θα ανακατασκευάσει τις πιο προσωπικές λεπτομέρειες της ιδιωτικής σας ζωής.

1. **Κίνδυνοι υλικού**

   Καθώς η τεχνολογία εξελίσσεται, ο σχεδιασμός εξαρτημάτων υλικού γίνεται όλο και πιο πολύπλοκος. Ένα πρόσφατο παράδειγμα από το 2018 παρουσιάζει δύο παραδείγματα κρίσιμων ευπαθειών υλικού: Το "Meltdown" και το "Spectre" εκμεταλλεύονται αμφότερα ευπάθειες στα σύγχρονα τσιπ CPU και μπορούν να χρησιμοποιηθούν για πρόσβαση σε δεδομένα σε προγράμματα και λειτουργικά συστήματα. Οι ευπάθειες μπορούν να αξιοποιηθούν σε smartphones, επιτραπέζιους υπολογιστές και ουσιαστικά σε κάθε συσκευή που χρησιμοποιεί ένα από αυτά τα τσιπ CPU. Υπάρχουν και άλλα παραδείγματα επιθέσεων σε στοιχεία υλικού, π.χ. "RAMbleed", αλλά είναι συνήθως δύσκολο να εκτελεστούν και απαιτούν συγκεκριμένες προϋποθέσεις.

   Ενώ υπάρχουν τρόποι να προστατευτείτε από τέτοιου είδους ευπάθειες (βλ. επόμενη ενότητα), η μεγαλύτερη απειλή για το υλικό σας είναι η άμεση πρόσβαση. Ενώ δεν είναι πιθανό να αποκτήσει πρόσβαση στον επιτραπέζιο υπολογιστή σας στο σπίτι κάποιος εισβολέας, είναι εύκολο να χάσετε ένα στικάκι USB ή το smartphone σας (δεν εξαρτάται πάντα από αμέλεια του χρήστη - τα ακριβά smartphones προσελκύουν κλέφτες, για παράδειγμα).

2. **Κίνδυνοι λογισμικού και δικτύου**

   Οι κίνδυνοι από το λογισμικό και το δίκτυο μπορεί να απειλήσουν την ασφάλεια ολόκληρης της συσκευής σας. Συχνά προκύπτουν είτε από σφάλματα λογισμικού (π.χ. οι προγραμματιστές έκαναν κάποιο λάθος κατά τη δημιουργία του λογισμικού), είτε από επιθέσεις μέσω διαδικτύου ή/και από διάφορους τύπους κακόβουλου λογισμικού (λογισμικό που ενεργεί σκόπιμα ενάντια στα συμφέροντα του χρήστη βλάπτοντας τον υπολογιστή), συμπεριλαμβανομένων ιών, σκουληκιών, trojans, spyware ή adware.

3. **Κίνδυνοι που σχετίζονται με τον χρήστη**

   Οι χρήστες μπορούν να αποτελέσουν τη μεγαλύτερη απειλή με απρόσεκτη, αφελή ή απληροφόρητη συμπεριφορά κατά τη χρήση των συσκευών τους, η οποία συχνά σχετίζεται με την κακή διαχείριση κωδικών πρόσβασης ή τη χρήση προσωπικών οικονομικών δεδομένων. Οι κίνδυνοι που σχετίζονται με τους χρήστες περιλαμβάνουν έννοιες εγκλήματος στον κυβερνοχώρο, όπως η ψηφιακή κοινωνική μηχανική, για παράδειγμα μέσω του phishing. Σε αυτή την περίπτωση, ο επιτιθέμενος προσποιείται έναν έμπιστο συνεργάτη επικοινωνίας για να αποκτήσει πρόσβαση σε προσωπικά δεδομένα ή για να χειραγωγήσει το θύμα του ώστε να εκτελέσει μια κακόβουλη πράξη.

Μελέτη περίπτωσης - Ο αγαπημένος απατεώνας της γιαγιάς μου

Μια 88χρονη Κινέζα γιαγιά πείθεται από έναν απατεώνα ότι μια επίλεκτη κυβερνητική ομάδα εργασίας χρειάζεται τη βοήθειά της για να αποκαλύψει ένα διεθνές κύκλωμα εγκλήματος. Χρησιμοποιώντας μόνο τηλεφωνήματα, μια "μυστική συνάντηση" σε ένα απομακρυσμένο ξενοδοχείο και μια περίτεχνη ιστορία που αφορά τις ανάγκες της "Λαολάο", ο απατεώνας

καταφέρνει να αδειάσει τους τραπεζικούς της λογαριασμούς και να της πάρει τις οικονομίες της ζωής της.

Άρθρο γνώμης του Frankie Huang στους New York Times, 07/12/2019:
https://www.nytimes.com/2019/12/07/opinion/sunday/china-bank-scam-grandmother.html

Ερώτηση αυτοαναστοχασμού: Ποια είναι τα θύματα των οικονομικών απατεώνων;

Άσκηση 4: Η εισβολή

Στόχοι

- Κατανοήστε γιατί η ασφάλεια είναι σημαντική
- Προσδιορισμός των συνεπειών της ανεπαρκούς ασφάλειας
- Ανάλυση των ζητημάτων ασφαλείας

Διάρκεια: 20 λεπτά

Εργαλεία: smartphones ή υπολογιστές με ενεργή σύνδεση στο διαδίκτυο, στυλό και χαρτί

Μέθοδοι: παιχνίδι ρόλων, ολομέλεια, δημιουργική εφαρμογή, πρακτική εφαρμογή

Περιγραφή της άσκησης: Συνδεθείτε στη συσκευή σας και φανταστείτε ότι κάποιος άλλος έχει πλήρη πρόσβαση σε αυτήν. Εργαστείτε μέσα από τις εφαρμογές σας, τα αρχεία πολυμέσων και τα περιεχόμενα του messenger, ενώ απαντάτε στις ακόλουθες τρεις ερωτήσεις: (1) Τι είδους ιδιωτικές, επαγγελματικές ή οικονομικές πληροφορίες θα μπορούσε να μάθει ο επιτιθέμενος για εσάς; (2) Τι είδους ιδιωτικές, επαγγελματικές ή οικονομικές πληροφορίες θα μπορούσε να μάθει ο επιτιθέμενος για την οικογένεια και τους φίλους σας; (3) Ποιες πληροφορίες θα ήταν πιο ενοχλητικές για να τις μοιραστείτε με έναν ξένο;

Καθήκοντα:

- Απαντήστε και στις τρεις ερωτήσεις όσο το δυνατόν περισσότερο μέσα σε δεκαπέντε λεπτά.
    - Γράψτε τις απαντήσεις σε κουκκίδες.
    - Μοιραστείτε τα αποτελέσματά σας με την τάξη (έχετε υπόψη σας ότι δεν χρειάζεται να μοιραστείτε οποιαδήποτε πληροφορία που μπορεί να σας κάνει να νιώσετε άβολα).

Ενημέρωση: Ο εκπαιδευτής θα πρέπει να βρει μια ισορροπία μεταξύ της νεοαποκτηθείσας γνώσης και του συναισθηματικού χαρακτήρα της εργασίας. Ο εκπαιδευτής θα πρέπει να εξάγει συγκεκριμένα συμπεράσματα για τη βελτίωση της ασφάλειας των συσκευών όλων.

Διδάγματα: Η ασφάλεια των συσκευών είναι σημαντική σε πολλαπλά επίπεδα και μας προστατεύει από βλάβες.

Συμπληρωματική ανάγνωση

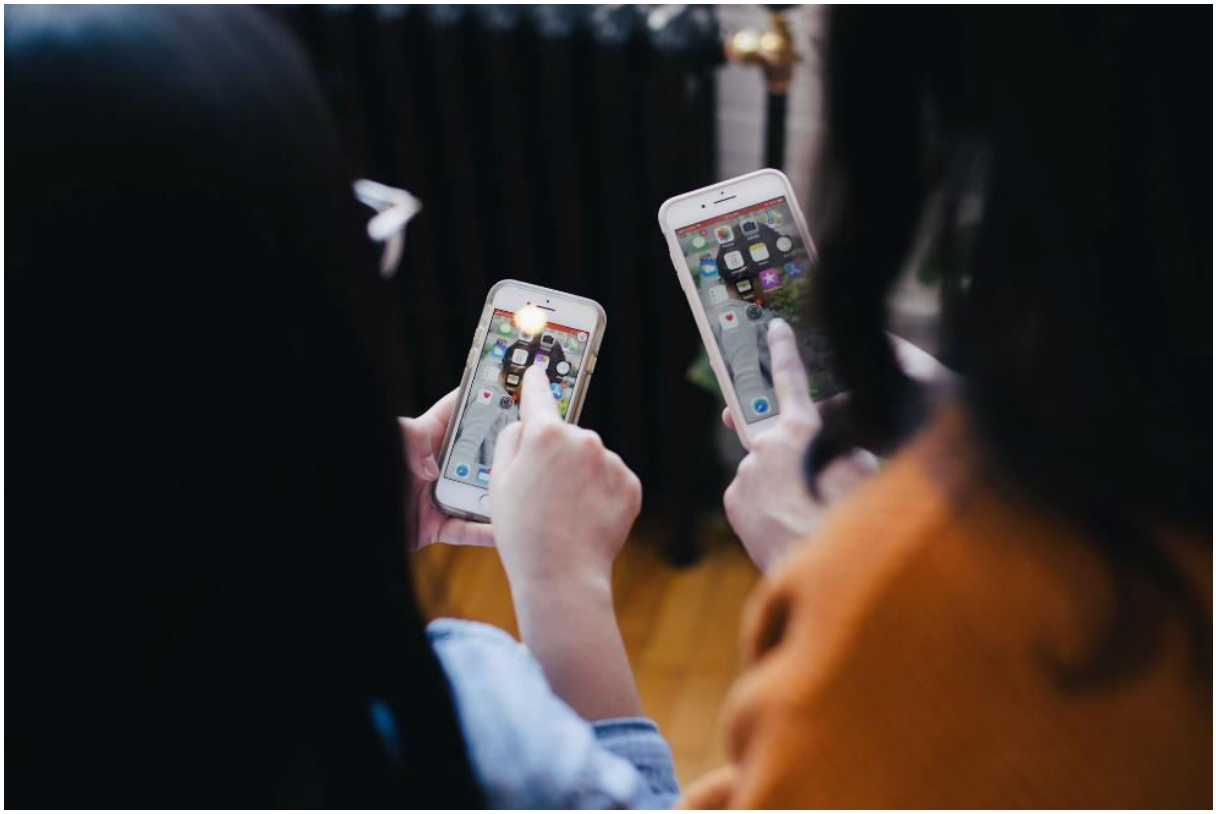
- **Project Zero**: "Το Project Zero δημιουργήθηκε το 2014 και είναι μια ομάδα ερευνητών ασφαλείας της Google που μελετούν τις ευπάθειες μηδενικής ημέρας στα συστήματα υλικού και λογισμικού από τα οποία εξαρτώνται οι χρήστες σε όλο τον κόσμο." https://googleprojectzero.blogspot.com/
- **Firefox Monitor**: Το ίδρυμα Mozilla συλλέγει διαρροές δεδομένων. Εισάγοντας μια διεύθυνση ηλεκτρονικού ταχυδρομείου, το Firefox Monitor ελέγχει αν η διεύθυνση αυτή

περιλαμβάνεται σε προηγούμενες διαρροές δεδομένων. Αυτές οι πληροφορίες μπορεί να σας βοηθήσουν να προστατεύσετε καλύτερα τον εαυτό σας ή άλλους από, για παράδειγμα, επιθέσεις κοινωνικής μηχανικής. https://monitor.firefox.com/

E-Quiz

Online κουίζ			
Τίτλος μαθήματος:	Απόρρητο και ασφάλεια		
Τίτλος ενότητας:	Κίνδυνοι ασφάλειας σε ένα ψηφιακό περιβάλλον		
Σωστό ή Λάθος	Σημειώστε αν οι ακόλουθες δηλώσεις είναι σωστές (Σ) ή λανθασμένες (Λ)		
Δηλώσεις		T	F
1	Το λειτουργικό μου σύστημα είναι ένα λογισμικό εφαρμογών		
2	Τα τρωτά σημεία ασφαλείας στην ψηφιακή μου συσκευή σχετίζονται πάντα με το λογισμικό		
3	Μπορώ να ανοίξω έναν λογαριασμό που μου έστειλε ο πάροχος υπηρεσιών διαδικτύου σε αρχείο .zip χωρίς δισταγμό.		
4	Η κοινή χρήση των δεδομένων γεωγραφικού εντοπισμού μου θέτει σε κίνδυνο την ιδιωτική μου ζωή		
5	Οι ίδιοι οι χρήστες είναι συχνά υπεύθυνοι για διαρροές ασφαλείας		
6	Το Adware προστατεύει τη συσκευή μου από ανεπιθύμητες διαφημίσεις		

5. Ενότητα 5 - Συμβουλές ασφαλείας για το ψηφιακό περιβάλλον



Πηγή: Unsplash

Επισκόπηση μαθημάτων

Περίληψη: Αυτή η ενότητα παρέχει προσιτές συμβουλές σχετικά με θέματα ασφάλειας υλικού, λογισμικού και χρηστών, εστιάζοντας σε πρακτικές συμβουλές ως σημαντικό μέρος της προστασίας της ιδιωτικής ζωής.

Δομή:

- Επισκόπηση μαθημάτων
- Συμβουλές για την ασφάλεια υλικού
- Συμβουλές για την ασφάλεια λογισμικού
- Συμβουλές σχετικά με την ασφάλεια των χρηστών
- Μελέτη περίπτωσης
- Συμπληρωματική ανάγνωση
- Άσκηση
- Ανατροφοδότηση
- E-Quiz

Μαθησιακοί στόχοι:

- Υπενθυμίζουμε τα βασικά μέσα ασφάλειας σε ψηφιακά περιβάλλοντα
- Ανάπτυξη μιας βασικής στρατηγικής ασφάλειας για την προστασία της ιδιωτικής ζωής του ιδίου και άλλων προσώπων
- Ανάπτυξη μιας στάσης που προωθεί συνειδητές και υπεύθυνες διαδικτυακές συμπεριφορές και αλληλεπιδράσεις

- Να εφαρμόζει μέτρα ασφαλείας στις συσκευές, τους λογαριασμούς και τις ψηφιακές αλληλεπιδράσεις του.

Η διατήρηση της ασφάλειας των προσωπικών σας πληροφοριών και δεδομένων δεν είναι εύκολη υπόθεση, αλλά αξίζει τον κόπο για να προστατεύσετε τον εαυτό σας και τους άλλους από διάφορους τύπους βλάβης, που επηρεάζουν αρνητικά την επαγγελματική ή/και την ιδιωτική σας ζωή. Αυτός ο κατάλογος περιέχει γενικούς κανόνες που πρέπει πάντα να ακολουθείτε:

Συμβουλές για την ασφάλεια υλικού

- **Αγοράστε υλικό από αξιόπιστους κατασκευαστές**: Είναι σχεδόν αδύνατο για τον μέσο χρήστη να ανακαλύψει ευπάθειες σε καταναλωτικές συσκευές όπως smartphones, φορητούς υπολογιστές ή δρομολογητές. Ένα καλό σημείο εκκίνησης είναι η τοποθεσία και η αντίστοιχη δικαιοδοσία του κατασκευαστή του υλικού, η οποία μπορεί να απαιτεί από αυτόν να σέβεται τους νόμους για την προστασία της ιδιωτικής ζωής και την ασφάλεια.
- **Μην αφήνετε τις συσκευές χωρίς επιτήρηση**: Μην μεταφέρετε ευαίσθητες πληροφορίες σε φορητές συσκευές, όπως smartphones ή μονάδες USB. Εάν είναι απαραίτητο, βεβαιωθείτε ότι οι συσκευές σας προστατεύονται τουλάχιστον με κωδικό πρόσβασης ή PIN ή ακόμη καλύτερα κρυπτογραφούνται με τη χρήση λογισμικού κρυπτογράφησης, για παράδειγμα VeraCrypt. Εάν χρησιμοποιείτε επιτραπέζιο υπολογιστή, κλειδώνετε πάντα την οθόνη σας ή κλείστε τον όταν δεν τον χρησιμοποιείτε.
- **Απενεργοποιήστε τις ρυθμίσεις γεωεντοπισμού και Bluetooth**: Εφόσον δεν τις χρειάζεστε, δεν υπάρχει λόγος να τις κρατάτε ενεργοποιημένες, αφού ενδεχομένως παρέχουν πολλές μεταπληροφορίες για εσάς.
- **Μην εισάγετε συσκευές άγνωστης προέλευσης**: Ο κανόνας αυτός είναι ιδιαίτερα σημαντικός σε ένα επαγγελματικό περιβάλλον εργασίας. Ποτέ μην εισάγετε μονάδες USB ή άλλα φορητά μέσα αποθήκευσης στον επιτραπέζιο υπολογιστή σας, εάν δεν έχει προηγηθεί έλεγχος για πιθανούς κινδύνους ασφαλείας.
- **Αγοράστε εφεδρικές συσκευές**: Η απώλεια σημαντικών δεδομένων μπορεί να προκαλέσει μεγάλη ζημιά στην επαγγελματική ή την ιδιωτική σας ζωή (για παράδειγμα, χάνοντας τη διατριβή σας). Να αφιερώνετε πάντα χρόνο για να δημιουργείτε τακτικά αντίγραφα ασφαλείας σημαντικών δεδομένων και να βρίσκετε έναν ασφαλή φυσικό χώρο για να αποθηκεύετε αυτό το αντίγραφο ασφαλείας.

Συμβουλές για την ασφάλεια λογισμικού

- **Διατηρείτε το λογισμικό σας ενημερωμένο**: Αυτό περιλαμβάνει το λογισμικό συστήματος, το βοηθητικό λογισμικό και το λογισμικό εφαρμογών. Ενεργοποιήστε τις αυτόματες ενημερώσεις για τα προγράμματα, τις εφαρμογές και το λειτουργικό σας σύστημα, ανεξάρτητα από τη συσκευή που χρησιμοποιείτε.
- **Χρησιμοποιήστε λογισμικό από αξιόπιστες πηγές**: Για παράδειγμα, ο Firefox ως πρόγραμμα περιήγησης στο διαδίκτυο ή το LibreOffice για εφαρμογές γραφείου. Να είστε ιδιαίτερα προσεκτικοί όταν κατεβάζετε εφαρμογές στην κινητή συσκευή σας που δεν έχουν ελεγχθεί από το PlayStore ή το AppStore.
- **Προστατέψτε το πρόγραμμα περιήγησής σας**: Είναι εξαιρετικά σημαντικό να το διατηρείτε πάντα όσο το δυνατόν πιο ασφαλές. Τα περισσότερα προγράμματα περιήγησης υποστηρίζουν την εγκατάσταση επεκτάσεων, όπως αποκλειστές διαφημίσεων (π.χ. uBlock

Origin), αποκλειστές παρακολούθησης (π.χ. Facebook Container), τείχη προστασίας (π.χ. uMatrix) ή αυτόματες ανακατευθύνσεις σε σελίδες https (π.χ. HTTPS everywhere).

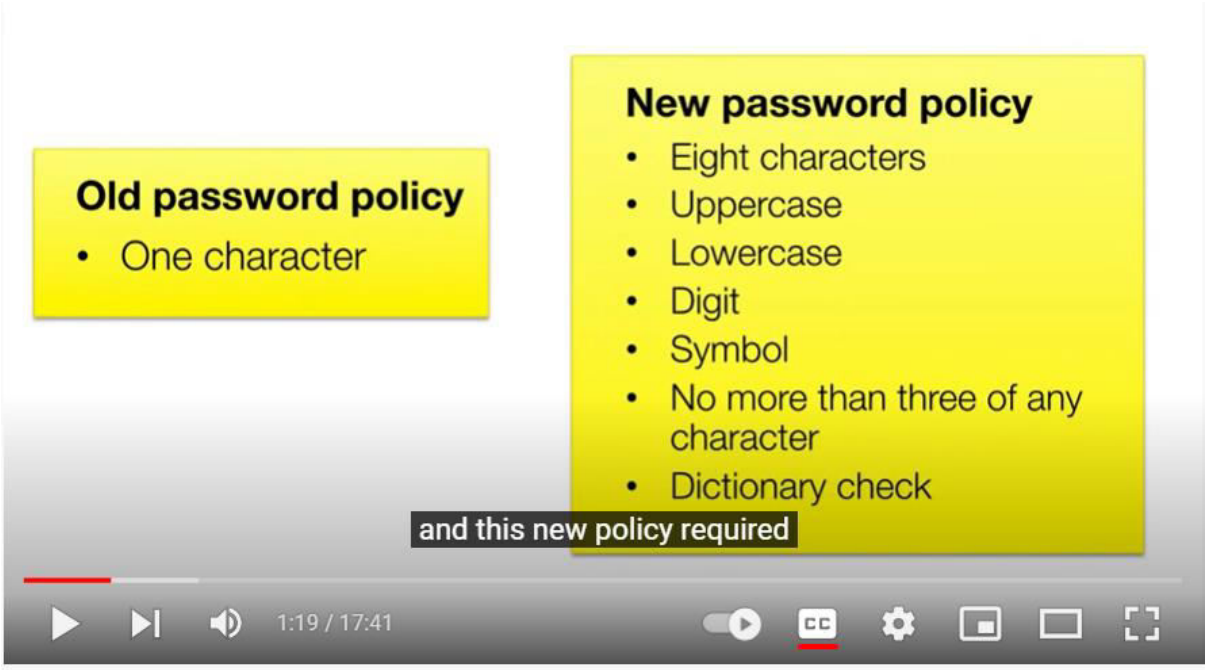
- **Εγκαταστήστε λογισμικό προστασίας από κακόβουλο λογισμικό (προαιρετικά)**: Τα οφέλη του λογισμικού anti-malware αμφισβητούνται, δεδομένου ότι τα ίδια τα προγράμματα ενέχουν δυνητικούς και πραγματικούς κινδύνους για την ασφάλεια. Για να προστατεύσει το σύστημά σας, το λογισμικό προστασίας από ιούς απαιτεί συνήθως βαθιά πρόσβαση στο σύστημά σας - αλλά αν το ίδιο το λογισμικό προστασίας από ιούς τεθεί σε κίνδυνο, το σύστημά σας είναι ξαφνικά ανοιχτό σε επιθέσεις που δεν θα είχαν πραγματοποιηθεί εξαρχής χωρίς το λογισμικό προστασίας από ιούς. Επιπλέον, αν είστε υπεύθυνος χρήστης, δεν θα πρέπει ποτέ να έρθετε σε επαφή με λογισμικό κακόβουλου λογισμικού ούτως ή άλλως. Το λογισμικό προστασίας από ιούς μπορεί ακόμα να είναι επωφελές για τους άπειρους χρήστες που μπορεί να είναι πιο επιρρεπείς σε παγίδες κακόβουλου λογισμικού, όπως τα συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου.

Συμβουλές σχετικά με την ασφάλεια των χρηστών

- **Να είστε προσεκτικοί με άγνωστες πηγές:** Ποτέ μην κάνετε κλικ σε συνδέσμους ή συνημμένα αρχεία από ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου ή άλλα μηνύματα σε οποιαδήποτε συσκευή.
- **Διαχειριστείτε σωστά τον κωδικό πρόσβασης:** Χρησιμοποιήστε έναν διαχειριστή κωδικών πρόσβασης (π.χ. KeyPass) για τη δημιουργία ασφαλών κωδικών πρόσβασης και την ασφαλή αποθήκευση αυτών των κωδικών πρόσβασης. Ποτέ μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης δύο φορές.
- **Μειώστε στο ελάχιστο τη χρήση προσωπικών πληροφοριών:** Θα πρέπει πάντα να επανεξετάζετε αν είναι απαραίτητη η μη ζητηθείσα κοινοποίηση προσωπικών πληροφοριών και δεδομένων σε ψηφιακό περιβάλλον, για παράδειγμα στα κοινωνικά δίκτυα. Συνήθως δεν υπάρχει κανένα όφελος από κάτι τέτοιο, αλλά μπορεί να σας βλάψει αργότερα, π.χ. πέφτοντας θύμα απόπειρας κοινωνικής μηχανικής.
- **Αποφύγετε τις απάτες:** Μάθετε να μην εμπιστεύεστε αγνώστους στο διαδίκτυο ή σε ένα τηλεφώνημα. Η κοινωνική μηχανική στο ψηφιακό περιβάλλον είναι ιδιαίτερα επικίνδυνη για τους ηλικιωμένους, όπως για παράδειγμα η διαβόητη απάτη με τον παππού και τη γιαγιά. Ενημερώστε τον εαυτό σας και τους άλλους και βεβαιωθείτε ότι **δεν** μοιράζεστε **ποτέ** προσωπικά δεδομένα και πληροφορίες μέσω μη ασφαλών ψηφιακών καναλιών, όπως μη κρυπτογραφημένα μηνύματα ηλεκτρονικού ταχυδρομείου, συνομιλίες messenger ή τηλεφωνικές κλήσεις.

Μελέτη περίπτωσης - Lorrie Faith Cranor: Τι έχει ο πατέρας σου;

"Η Lorrie Faith Cranor μελέτησε χιλιάδες πραγματικούς κωδικούς πρόσβασης για να ανακαλύψει τα εκπληκτικά, πολύ συνηθισμένα λάθη που κάνουν οι χρήστες - και οι ασφαλείς ιστότοποι - για να θέσουν σε κίνδυνο την ασφάλεια. Και πώς, θα αναρωτηθείτε, μελέτησε χιλιάδες πραγματικούς κωδικούς πρόσβασης χωρίς να θέσει σε κίνδυνο την ασφάλεια κανενός χρήστη; Αυτό είναι μια ιστορία από μόνο του. Πρόκειται για μυστικά δεδομένα που αξίζει να γνωρίζετε, ειδικά αν ο κωδικός πρόσβασής σας είναι 123456 ..."



Κυκλοφόρησε από τον οργανισμό TED στις 24/06/2014: https://www.youtube.com/watch?v=0SkdP36wiAU

Ερώτηση αυτοαναστοχασμού: Πόσο ισχυροί είναι οι κωδικοί σας;

Άσκηση 5: Ασφαλείς μαζί

Στόχοι:

- Κατανοήστε γιατί η ασφάλεια είναι σημαντική
- Παρουσίαση των σημαντικότερων μέτρων ασφαλείας

Διάρκεια: 20 λεπτά

Εργαλεία: στυλό και χαρτί

Μέθοδοι: ολομέλεια, δημιουργική εφαρμογή, παρουσίαση

Περιγραφή της άσκησης: Κάθε μαθητής φαντάζεται ένα παλιό μέλος της οικογένειας που αγόρασε τον πρώτο του φορητό υπολογιστή για να επωφεληθεί επιτέλους από τη σύγχρονη τεχνολογία. Αυτό το μέλος της οικογένειας γνωρίζει πώς να εκκινήσει το νέο του φορητό υπολογιστή και ζητάει τη βοήθεια του μαθητή για (1) τη δημιουργία μιας διεύθυνσης ηλεκτρονικού ταχυδρομείου, (2) την έναρξη ηλεκτρονικών τραπεζικών συναλλαγών, (3) τη δημιουργία ενός προφίλ στο Facebook, (4) την εγκατάσταση της εφαρμογής WhatsApp για την επιφάνεια εργασίας, (5) τη δουλειά σε μια καφετέρια κάθε πρωί και την είσοδο στο διαδίκτυο από εκεί. Κάθε μαθητής προετοιμάζει μια μικρή παρουσίαση και επικεντρώνεται στις πιο σημαντικές πτυχές της ασφάλειας που θέλει να δείξει στο μέλος της οικογένειάς του.

Καθήκοντα:

- Γράψτε τουλάχιστον τρία σημεία με τις σημαντικότερες πτυχές ασφάλειας για κάθε ένα από τα 5 σενάρια σε 15 λεπτά.

- Μοιραστείτε τα αποτελέσματά σας με την τάξη (έχετε υπόψη σας ότι δεν χρειάζεται να μοιραστείτε οποιαδήποτε πληροφορία που μπορεί να σας κάνει να νιώσετε άβολα).

Ενημέρωση: Ο εκπαιδευτής θα πρέπει να τονίσει ποια συμπεράσματα μπορούν να βγάλουν οι μαθητές από την άσκηση για τις δικές τους συνήθειες ασφαλείας. Θα πρέπει επίσης να απευθύνει έκκληση στο αίσθημα της κοινότητας να βοηθάει ο ένας τον άλλον να παραμείνει ασφαλής.

Διδάγματα: Η ασφάλεια είναι σημαντική για την προστασία μας από βλάβες και πρέπει να υποστηρίζουμε ο ένας τον άλλον για να παραμείνουμε ασφαλείς.

Συμπληρωματική ανάγνωση

- **Γουίλ Στάιλερ**: "Θυμάστε λοιπόν τη διατριβή πάνω στην οποία δούλευα; [...] Λοιπόν, ένα μεγάλο μέρος της δουλειάς που έκανα χάθηκε, επειδή πήρα κάποιες κακές αποφάσεις και είχα κάποια πολύ κακή τύχη. Θα ήθελα να μοιραστώ μαζί σας τι έκανα λάθος και πώς να μην είστε σαν εμένα." https://wstyler.ucsd.edu/posts/lost_dissertation_files.html

E-Quiz

Online κουίζ			
Τίτλος μαθήματος:	Απόρρητο και ασφάλεια		
Τίτλος ενότητας:	Συμβουλές ασφαλείας για το ψηφιακό περιβάλλον		
Σωστό ή Λάθος	Σημειώστε αν οι ακόλουθες δηλώσεις είναι σωστές (Σ) ή λανθασμένες (Λ)		
Δηλώσεις		T	F
1	Η χρήση του ίδιου κωδικού πρόσβασης παντού είναι αρκετά ασφαλής αν δεν τον μοιράζεστε ποτέ.		
2	Οι αυτόματες ενημερώσεις ασφαλείας μπορούν να προστατεύσουν το λειτουργικό μου σύστημα		
3	Τα προγράμματα κατά του κακόβουλου λογισμικού κάνουν πάντα τη συσκευή μου πιο ασφαλή		
4	Τα τρωτά σημεία ασφαλείας στην ψηφιακή μου συσκευή σχετίζονται πάντα με το λογισμικό		
5	Το smartphone μου είναι ασφαλές αν προστατεύεται με PIN		
6	Μπορώ να εκτελέσω με ασφάλεια ένα αρχείο APK στο smartphone μου που κατέβασα από έναν ιστότοπο		

6. Κουίζ αξιολόγησης

Ενότητα 1

1) Ποια από τις παρακάτω προτάσεις ταιριάζει περισσότερο σε μια περιγραφή της ασφάλειας στο διαδίκτυο και όχι της ιδιωτικής ζωής στο διαδίκτυο;
   a) Η προσωπική προστασία των δικών μας
   b) Η προστασία των διαδικτυακών πληροφοριών άλλων
   c) Η δική σας επίγνωση των διαδικτυακών ενεργειών και συμπεριφορών

2) Ποια από τα ακόλουθα σύνολα κανόνων προστατεύουν την ιδιωτική ζωή σε ψηφιακά ή ηλεκτρονικά περιβάλλοντα;
   a) Η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες
   b) Η οδηγία για την ηλεκτρονική ασφάλεια
   c) Η οδηγία για το απόρρητο και την ασφάλεια

3) Ποιος είναι ο πλήρης τίτλος του συνόλου κανόνων της οδηγίας ePrivacy;
   a) Οδηγία για την προστασία των προσωπικών δεδομένων και τις επιγραμμικές συμπεριφορές
   b) Οδηγία για την προστασία της ιδιωτικής ζωής και την ασφάλεια στο διαδίκτυο
   c) Οδηγία για την προστασία της ιδιωτικής ζωής και τις ηλεκτρονικές επικοινωνίες

4) Τι σημαίνει ο GDPR;
   a) Γενικός κανονισμός για το απόρρητο των δεδομένων
   b) Γενικός κανονισμός για την προστασία δεδομένων
   c) Γενικοί κανόνες προστασίας δεδομένων

Ενότητα 2

1) Πότε είναι η Ημέρα Προστασίας Δεδομένων;
   a) 28 Ιανουαρίου
   b) 28 Ιουνίου
   c) 28 Δεκεμβρίου

2) Ποιο είναι το όνομα της παγκόσμιας εκστρατείας ευαισθητοποίησης για την ασφάλεια στο διαδίκτυο που διοργανώνεται από την Εθνική Συμμαχία για την Κυβερνοασφάλεια και την Πρωτοβουλία Δημόσιας Εκπαίδευσης της APWG;
   a) STOP. ΣΚΕΦΤΕΙΤΕ. CONNECT

b) STOP. Ξανασκέψου. ΕΠΙΚΟΙΝΩΝΙΑ

c) START. ΣΚΕΦΤΕΙΤΕ. ΣΧΟΛΙΟ

3) Ποιο περιεχόμενο επιτρέπεται να δημοσιεύετε στο διαδίκτυο;

a) Οποιεσδήποτε φωτογραφίες που λαμβάνονται από το google

b) Φωτογραφίες τραβηγμένες από τους φίλους μου

c) Οι δικές μου φωτογραφίες

4) Ποιος από τους ακόλουθους τύπους χρηστών ενδιαφέρεται λιγότερο για τις ρυθμίσεις απορρήτου;

a) Τα επιφυλακτικά άτομα

b) Τα αποκαλυπτικά πρόσωπα

c) Οι διαχειριστές απορρήτου

Ενότητα 3

1) Ποιος από τους ακόλουθους είναι υπεύθυνος για την εκτέλεση των διαφόρων εντολών και υπολογισμών που είναι απαραίτητοι για την ορθή λειτουργία των συσκευών;

a) CPU (κεντρική μονάδα επεξεργασίας)

b) GPU (Μονάδα επεξεργασίας γραφικών)

c) HDD (σκληρός δίσκος)

2) Τι σημαίνει RAM;

a) Απομακρυσμένη πρόσθετη μνήμη

b) Μνήμη τυχαίας προσπέλασης

c) Εύρος Ποσό Μέτρα

3) Ποια από τα παρακάτω αναφέρονται σε βοηθητικό λογισμικό;

a) Linux

b) VLC Player

c) Πρόγραμμα Anti-virus

4) Τι είναι το "Meltdown";

a) Μια ευπάθεια υλικού

b) Ένα λογισμικό εφαρμογής

c) Λογισμικό συστήματος

Ενότητα 4

1) Τι είδους κίνδυνοι συνδέονται με το κακόβουλο λογισμικό, το spyware και το adware;
   a) Κίνδυνοι υλικού
   b) Κίνδυνοι λογισμικού και δικτύου
   c) Κίνδυνοι που σχετίζονται με τον χρήστη

2) Η χρήση ενός διαχειριστή κωδικών πρόσβασης σχετίζεται με ποιο είδος ασφάλειας;
   a) Ασφάλεια υλικού
   b) Ασφάλεια λογισμικού
   c) Ασφάλεια που σχετίζεται με τον χρήστη

3) Τι κάνει το adware;
   a) Δημιουργεί αυτόματα διαδικτυακές διαφημίσεις
   b) Αποκλεισμός αυτόματων διαφημίσεων
   c) Βοηθά στη διαμόρφωση του υλικού σας

4) Ποια από τα ακόλουθα αναφέρονται στο λογισμικό εφαρμογών;
   a) Φυλλομετρητές Web
   b) Λειτουργικά συστήματα
   c) Προγράμματα ανάκτησης δεδομένων

Ενότητα 5

1) Ποια από τα ακόλουθα ΔΕΝ χρησιμοποιούνται ως συσκευές αποθήκευσης;
   a) HDD (σκληρός δίσκος)
   b) SSD (Solid State Drive)
   c) GPU (Μονάδα επεξεργασίας γραφικών)

2) Ποια από τις ακόλουθες προτάσεις είναι σωστή;
   a) Οι ρυθμίσεις των μέσων κοινωνικής δικτύωσης μου παρέχουν πλήρη προστασία των δεδομένων μου
   b) Πρέπει να προσαρμόσω τις ρυθμίσεις απορρήτου στα μέσα κοινωνικής δικτύωσης για την προστασία των δεδομένων μου

c) Τα δεδομένα μου στα μέσα κοινωνικής δικτύωσης είναι πλήρως προστατευμένα από τη στιγμή που δημοσιεύω μόνο τις δικές μου φωτογραφίες

3) Με ποιους κινδύνους σχετίζεται το έγκλημα στον κυβερνοχώρο;

a) Κίνδυνοι που σχετίζονται με τον χρήστη

b) Κίνδυνοι λογισμικού

c) Κίνδυνοι υλικού

4) Πού μπορεί να εμφανιστεί απάτη;

a) Μόνο εκτός σύνδεσης

b) Μόνο online

c) Offline και online

7. Αναφορές

Συμβούλιο της Ευρώπης (2014). Οδηγός ανθρωπίνων δικαιωμάτων για τους χρήστες του διαδικτύου

Netter, M., Herbst, S., Pernul, G. (2013). Διεπιστημονική ανάλυση των επιπτώσεων της ιδιωτικότητας στα κοινωνικά δίκτυα

Ladan, M. I. (2015). Κοινωνικά δίκτυα: Κοινωνικά δίκτυα: Θέματα προστασίας προσωπικών δεδομένων και προφυλάξεις

Schenk, M., Niemann, J., Reinmann, G., Roßnagel, A. (2012). Digitale Privatsphäre: Sozialen Netzwerkplattformen: Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen.

Gross, R., Acquisti, A. (2005). Αποκάλυψη πληροφοριών και ιδιωτικότητα στα διαδικτυακά κοινωνικά δίκτυα (Η περίπτωση του Facebook).

Cranor, L.F. (2014). What's wrong with your pa$$w0rd? https://www.youtube.com/watch?v=0SkdP36wiAU

Velasco, J. (2016). for socialnomics.net, 4 Case Studies in Fraud: Social Media and Identity Theft, https://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft/.

The New York Times (2019). Ο αγαπημένος απατεώνας της γιαγιάς μου. https://www.nytimes.com/2019/12/07/opinion/sunday/china-bank-scam-grandmother.html

APWG (2010). STOP. THINK. CONNECT.™ public-awarenress campaign. https://education.apwg.org/safety-messaging-convention/

Media.ccc.de (2017). Privacy by Design: Συλλογή δεδομένων με κοινωνικά υπεύθυνο τρόπο χωρίς παρενέργειες στην ιδιωτική ζωή. https://media.ccc.de/v/pw17-158-privacy_by_design#t=74.

Παράρτημα

Φύλλα ελέγχου κουίζ αξιολόγησης

Κουίζ αξιολόγησης Φύλλο ελέγχου ενότητας 1 - σωστές απαντήσεις

1c

2a

3c

4b

Κουίζ αξιολόγησης Φύλλο ελέγχου ενότητας 2 - σωστές απαντήσεις

1a

2a

3c

4b

Κουίζ αξιολόγησης Φύλλο ελέγχου ενότητας 3 - σωστές απαντήσεις

1a

2b

3c

4a

Κουίζ αξιολόγησης Φύλλο ελέγχου ενότητας 4 - σωστές απαντήσεις

1b

2c

3a

4a

Κουίζ αξιολόγησης Φύλλο ελέγχου ενότητας 5 - σωστές απαντήσεις

1c

2b

3a

4c

Λίστα ελέγχου αναθεώρησης διδακτικού σχεδιασμού για τους εργαζόμενους στον τομέα της νεολαίας

Όχι	Κριτήρια	Ναι	Όχι
1. Στόχοι			
1.1	Οι στόχοι δηλώνονται με σαφήνεια για τον εκπαιδευόμενο;		
1.2	Οι απαιτήσεις του μαθήματος συνάδουν με τους στόχους;		
1.3	Τα κεφάλαια/θέματα καλύπτουν διεξοδικά τους στόχους του μαθήματος;		
1.4	Ταιριάζουν οι μαθησιακοί στόχοι με τα μαθησιακά αποτελέσματα;		
1.5	Ανταποκρίνεται το συνολικό περιεχόμενο και η δομή του μαθήματος στους διδακτικούς στόχους του;		
2. Δομή			
2.1	Διαθέτει το μάθημα συνοπτική και περιεκτική επισκόπηση ή πρόγραμμα σπουδών;		
2.2	Περιλαμβάνει το μάθημα παραδείγματα, αναλογίες, μελέτες περιπτώσεων, προσομοιώσεις, γραφικές αναπαραστάσεις και διαδραστικές ερωτήσεις;		
2.3	Η δομή του μαθήματος χρησιμοποιεί κατάλληλες μεθόδους και διαδικασίες για τη μέτρηση της επίδοσης των μαθητών;		
3. Περιεχόμενο			
3.1	Το περιεχόμενο ρέει απρόσκοπτα, χωρίς γραμματικά, συντακτικά και τυπογραφικά λάθη;		
3.2	Είναι το περιεχόμενο ενημερωμένο;		
3.3	Είναι το περιεχόμενο ευθυγραμμισμένο με το πρόγραμμα σπουδών;		
3.4	Ενσωματώνονται τα επιθυμητά αποτελέσματα στο περιεχόμενο;		
3.5	Είναι το περιεχόμενο σύμφωνο με τους νόμους περί πνευματικών δικαιωμάτων και αναφέρεται σωστά όλο το παρατιθέμενο υλικό του;		
3.6	Το μάθημα εμπλέκει τους μαθητές σε κριτική και αφηρημένη σκέψη;		
3.7	Το μάθημα έχει προαπαιτούμενα ή απαιτεί τεχνικό υπόβαθρο;		
4. Αξιολόγηση			
4.1	Είναι οι εργασίες σχετικές, αποτελεσματικές και εμπλέκουν τους μαθητές σε ποικιλία τύπων επιδόσεων και δραστηριοτήτων;		
4.2	Είναι οι ερωτήσεις πρακτικής και αξιολόγησης διαδραστικές;		
4.3	Οι ασκήσεις πρακτικής και αξιολόγησης επικεντρώνονται στους στόχους του μαθήματος;		
5. Τεχνολογία - Σχεδιασμός			
5.1	Είναι ο σχεδιασμός σαφής και συνεπής, με τις κατάλληλες κατευθύνσεις;		
5.2	Είναι οι εικόνες και τα γραφικά υψηλής ποιότητας και κατάλληλα για το μάθημα;		
5.3	Είναι εύκολη η πλοήγηση στο μάθημα και προσφέρει βοήθεια με την τεχνική διαχείριση και τη διαχείριση του μαθήματος;		
5.4	Είναι συνεπής και αξιόπιστη η δομή πλοήγησης στο μάθημα;		
5.5	Είναι η πορεία καθορισμένη από υλικό και λογισμικό;		
5.6	Είναι ο ήχος και το κείμενο στην οθόνη συγχρονισμένα;		
5.7	Η αρχιτεκτονική του μαθήματος επιτρέπει στους εκπαιδευτές να προσθέτουν περιεχόμενο, δραστηριότητες και επιπλέον αξιολογήσεις;		

Ανατροφοδότηση σχετικά με το θέμα για τους μαθητές

Αξιολόγηση της ενότητας						
Τίτλος μαθήματος:						
Τίτλος ενότητας:						
Μέρος Α:	Σε κλίμακα 1-5, όπου το 1 είναι το χαμηλότερο και το 5 το υψηλότερο επίπεδο συμφωνίας, αναφέρετε πώς αισθάνεστε για τα ακόλουθα					
Παρατηρήσεις		1	2	3	4	5
1	Το θέμα ήταν ενδιαφέρον					
2	Πιστεύω ότι τα θέματα που καλύφθηκαν ήταν σημαντικά					
3	Θα ήθελα να μάθω περισσότερα για την περιοχή					
4	Έμαθα νέα πράγματα τα οποία είναι πιθανό να εφαρμόσω στο μέλλον					
5	Θα ήθελα να βελτιώσω τις δεξιότητές μου στον τομέα					
6	Είναι πιθανό να συστήσω αυτό το μάθημα					
Μέρος Β:	Στον προβλεπόμενο χώρο μπορείτε να συμπεριλάβετε τα σχόλια και τις συστάσεις που επιθυμείτε.					
Μέρος Γ:	Στον προβλεπόμενο χώρο μπορείτε να συμπεριλάβετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας, αν θέλετε να ενημερώνεστε για το έργο αυτό.					