ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ ΤΜΗΜΑ

ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Ηλεκτρονική Μάθηση.»

Ακαδημαϊκό έτος 2023-2024

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ελένη Καλογεροπούλου ΜΗΜ2322

Σχεδίαση και Ανάπτυξη Διαδικτυακού Μαθήματος για τη Ψηφιακή Ενδυνάμωση Ενηλίκων: Στρατηγικές για την Προαγωγή της Ασφαλούς Πλοήγησης στο Διαδίκτυο

Designing and Developing an Online Course for Digitally Empowering Adults: Strategies for Promoting Safe Internet Browsing

Επιβλέπων Καθηγητής:

Δημήτριος Σάμψων

Πειραιάς, Σεπτέμβριος 2024

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Αυτή η Μεταπτυχιακή Διπλωματική Εργασία υποβάλλεται ως μερική εκπλήρωση των απαιτήσεων του Προγράμματος Μεταπτυχιακών Σπουδών στην «Ηλεκτρονική Μάθηση» του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς.

Δηλώνω υπεύθυνα ότι η συγκεκριμένη Μεταπτυχιακή Διπλωματική Εργασία έχει συγγραφεί από εμένα προσωπικά και δεν έχει υποβληθεί ούτε έχει αξιολογηθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό.

Η εργασία αυτή έχοντας εκπονηθεί από εμένα, αντιπροσωπεύει τις προσωπικές μου απόψεις επί του θέματος. Οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης διπλωματικής αναφέρονται στο σύνολό τους, δίνοντας πλήρεις αναφορές στους συγγραφείς, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το Διαδίκτυο.

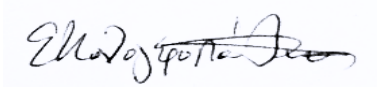
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου. Σε κάθε περίπτωση, αναληθούς ή ανακριβούς δηλώσεως, υπόκειμαι στις συνέπειες που προβλέπονται τις διατάξεις που προβλέπει η Ελληνική και Κοινοτική Νομοθεσία περί πνευματικής ιδιοκτησίας.

Η ΔΗΛΟΥΣΑ

Ονοματεπώνυμο: Ελένη Καλογεροπούλου

Αριθμός Μητρώου: ΜΗΜ2322

Υπογραφή:



Στην κόρη μου, Νικολέττα, για
την αστείρευτη αγάπη, την
κατανόηση και την έμπνευση
που μου προσφέρει
καθημερινά.

Ευχαριστίες

Θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στον επιβλέποντα καθηγητή, Δημήτριο Σάμψων, για την καθοδήγηση και την υποστήριξή του κατά τη διάρκεια των σπουδών μου και της εκπόνησης αυτής της εργασίας. Η εμπειρία και οι συμβουλές του ήταν καθοριστικές για την ολοκλήρωσή της.

Επιπλέον, ευχαριστώ τον Δημήτριο Γκότζο και την υποψήφια διδάκτορα Σοφία Μουγιάκου για την πολύτιμη βοήθειά τους, την ενθάρρυνση και τη στήριξή τους στην εκπόνηση αυτής της εργασίας.

Τέλος, θα ήθελα να εκφράσω την εκτίμησή μου σε όλους τους καθηγητές του μεταπτυχιακού προγράμματος "Ηλεκτρονική Μάθηση" για την αμέριστη υποστήριξή τους στην ανάπτυξη των γνώσεων και των δεξιοτήτων μας.

Θα ήθελα επίσης να ευχαριστήσω θερμά την οικογένειά μου για όλη την υποστήριξη, την υπομονή και την ενθάρρυνση που μου προσέφεραν καθ' όλη τη διάρκεια των σπουδών μου. Σας ευχαριστώ που πάντα πιστεύετε σε εμένα.

Περιεχόμενα

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

Περίληψη

Η παρούσα εργασία επικεντρώνεται στην σχεδίαση και ανάπτυξη ενός διαδικτυακού μαθήματος που στοχεύει στην ψηφιακή ενδυνάμωση ενηλίκων, με έμφαση στις στρατηγικές ασφαλούς πλοήγησης στο διαδίκτυο. Σε έναν κόσμο όπου η ψηφιακή ασφάλεια αποτελεί προτεραιότητα, η εκπαίδευση ενηλίκων για την αναγνώριση και αποφυγή διαδικτυακών απειλών είναι επιτακτική. Το πρόγραμμα περιλαμβάνει μια σειρά από θεωρητικές και πρακτικές ενότητες που καλύπτουν βασικά θέματα όπως η ασφάλεια των προσωπικών δεδομένων, η αναγνώριση phishing επιθέσεων, και η χρήση εργαλείων προστασίας της ιδιωτικότητας.

Η μεθοδολογία που χρησιμοποιήθηκε περιλαμβάνει την ανάπτυξη διαδραστικού περιεχομένου με ασκήσεις αυτοαξιολόγησης που ενισχύουν την εμπλοκή των συμμετεχόντων. Το μάθημα σχεδιάστηκε με στόχο να προσφέρει πρακτικές γνώσεις και δεξιότητες που θα ενισχύσουν την αυτοπεποίθηση των ενηλίκων στη χρήση του διαδικτύου. Επιπλέον, εξετάζεται η σημασία της ψηφιακής ηθικής και της υπευθυνότητας στη διαδικτυακή αλληλεπίδραση.

Αυτή η εργασία αναδεικνύει τη σημασία της ψηφιακής εκπαίδευσης και της ευαισθητοποίησης για την ασφάλεια στο διαδίκτυο, προτείνοντας ένα ολοκληρωμένο πρόγραμμα που μπορεί να λειτουργήσει ως πρότυπο για μελλοντική εκπαίδευση ενηλίκων. Οι ευρήματα της έρευνας δείχνουν ότι η ψηφιακή ενδυνάμωση μπορεί να συμβάλει στην καλύτερη διαχείριση των διαδικτυακών κινδύνων, προάγοντας έναν ασφαλέστερο ψηφιακό κόσμο.

Λέξεις-κλειδιά: ψηφιακή ενδυνάμωση, διαδικτυακό μάθημα, ασφαλής πλοήγηση, ψηφιακή ασφάλεια, εκπαίδευση ενηλίκων.

Abstract

This paper focuses on the design and development of an online course aimed at the digital empowerment of adults, with an emphasis on strategies for safe internet navigation. In a world where digital security is a priority, educating adults on recognizing and avoiding online threats is imperative. The program includes a series of theoretical and practical modules covering essential topics such as personal data security, phishing attack recognition, and the use of privacy protection tools.

The methodology employed involves the creation of interactive content, simulation scenarios, and self-assessment exercises that enhance participant engagement. The course is designed to provide practical knowledge and skills that will boost adults' confidence in using the internet. Additionally, the importance of digital ethics and responsibility in online interactions is examined.

This work highlights the significance of digital education and awareness for internet safety, proposing a comprehensive program that can serve as a model for future adult education initiatives. The research findings indicate that digital empowerment can contribute to better management of online risks, promoting a safer digital environment.

Keywords: digital empowerment, online course, safe navigation, digital security, adult education.

Κεφάλαιο 1. Εισαγωγή της εργασίας «Σχεδίαση και Ανάπτυξη Διαδικτυακού Μαθήματος για τη Ψηφιακή Ενδυνάμωση Ενηλίκων: Στρατηγικές για την Προαγωγή της Ασφαλούς Πλοήγησης στο Διαδίκτυο»

1.1 Εισαγωγή

Ο βασικός σκοπός αυτής της εργασίας που αφορά τη σχεδίαση και ανάπτυξη διαδικτυακού μαθήματος για τη ψηφιακή ενδυνάμωση ενηλίκων, επικεντρωμένος στις στρατηγικές προαγωγής της ασφαλούς πλοήγησης στο διαδίκτυο, είναι η ενίσχυση της ψηφιακής ικανότητας και της ασφάλειας των ενηλίκων χρηστών στο ψηφιακό περιβάλλον. Στον σύγχρονο κόσμο, η διαδικτυακή παρουσία είναι ουσιώδης, αλλά με την αύξηση των διαδικτυακών απειλών και κινδύνων, η εκπαίδευση των ενηλίκων σχετικά με την ασφαλή πλοήγηση είναι πιο σημαντική από ποτέ.

Πρώτον, ο σκοπός αυτός περιλαμβάνει την ενημέρωση των ενηλίκων για τις βασικές αρχές ασφαλούς πλοήγησης. Αυτό περιλαμβάνει τη γνώση σχετικά με την αναγνώριση και αποφυγή phishing, κακόβουλων λογισμικών και άλλων διαδικτυακών επιθέσεων, καθώς και την κατανόηση της σημασίας των ισχυρών κωδικών πρόσβασης και της προστασίας των προσωπικών τους στοιχείων. Μέσω της εκπαίδευσης, οι συμμετέχοντες θα είναι σε θέση να αναγνωρίζουν τους κινδύνους και να εφαρμόζουν τις κατάλληλες στρατηγικές για την προστασία τους.

Δεύτερον, ο σχεδιασμός ενός τέτοιου μαθήματος πρέπει να περιλαμβάνει πρακτικές εφαρμογές και σενάρια που θα επιτρέπουν στους συμμετέχοντες να εξασκηθούν σε πραγματικές καταστάσεις. Αυτό θα ενισχύσει την αυτοπεποίθησή τους και θα τους βοηθήσει να αναπτύξουν τις δεξιότητες που απαιτούνται για τη διαχείριση των διαδικτυακών τους αλληλεπιδράσεων. Για παράδειγμα, η εκπαίδευση μπορεί να περιλαμβάνει ασκήσεις σχετικά με την αναγνώριση ασφαλών και μη ασφαλών ιστότοπων, τη χρήση εργαλείων προστασίας της ιδιωτικότητας και τη σωστή χρήση κοινωνικών δικτύων.

Επιπλέον, η ευαισθητοποίηση σχετικά με την ψυχολογική διάσταση της διαδικτυακής αλληλεπίδρασης είναι εξίσου σημαντική. Οι συμμετέχοντες θα πρέπει να κατανοήσουν τις επιπτώσεις της διαδικτυακής συμπεριφοράς τους, την ανάγκη για ψηφιακή ηθική και την ευθύνη τους απέναντι στους άλλους χρήστες του διαδικτύου.

Τέλος, ο σκοπός της εργασίας αυτής είναι να προάγει μια κουλτούρα ασφαλούς πλοήγησης που θα ενισχύσει τη συνολική εμπειρία των ενηλίκων στο διαδίκτυο. Με την κατάλληλη εκπαίδευση, οι ενήλικες θα μπορέσουν να αξιοποιούν τις δυνατότητες του διαδικτύου με ασφάλεια και αυτοπεποίθηση, συμβάλλοντας έτσι και στη γενικότερη ψηφιακή ενδυνάμωση της κοινωνίας.

1.2 Τεκμηρίωση της Ανάγκης για την Ανάπτυξη των Ικανοτήτων που έχουν Επιλεγεί

Η ανάπτυξη των ικανοτήτων που επιλέχθηκαν για αυτό το μάθημα στοχεύει στην ενδυνάμωση των ατόμων ώστε να:

- **Αναγνωρίζουν και να αξιολογούν** τους κινδύνους και τις απειλές στο διαδίκτυο, όπως το ηλεκτρονικό "ψάρεμα", το κακόβουλο λογισμικό και την παραπληροφόρηση.
- **Προστατεύουν** τα προσωπικά τους δεδομένα και τους online λογαριασμούς τους, δημιουργώντας ισχυρούς κωδικούς πρόσβασης και εφαρμόζοντας ασφαλείς πρακτικές.
- **Χρησιμοποιούν** τα κοινωνικά δίκτυα με υπευθυνότητα και σεβασμό, αποφεύγοντας τη διαδικτυακή παρενόχληση και προωθώντας ένα θετικό διαδικτυακό περιβάλλον.
- **Δημιουργούν** ένα ασφαλές διαδικτυακό περιβάλλον για τα παιδιά και τις οικογένειές τους, μέσω της εκπαίδευσης και της ανοιχτής επικοινωνίας.

Με την απόκτηση αυτών των ικανοτήτων, οι εκπαιδευόμενοι θα είναι σε θέση να αξιοποιήσουν τις δυνατότητες του διαδικτύου με ασφάλεια και αυτοπεποίθηση, συμβάλλοντας παράλληλα στη δημιουργία ενός πιο ασφαλούς και υπεύθυνου ψηφιακού κόσμου για όλους.

1.3 Η Αξιοποίηση Μαζικών Ανοικτών Διαδικτυακών Μαθημάτων (MOOC) ως Πρόσφορη Εκπαιδευτική Μέθοδος

Τα Μαζικά Ανοικτά Διαδικτυακά Μαθήματα (MOOCs) έχουν αναδειχθεί σε μια ισχυρή εκπαιδευτική μέθοδο, προσφέροντας ευκαιρίες μάθησης σε ένα ευρύ κοινό, ανεξαρτήτως γεωγραφικής θέσης, οικονομικής κατάστασης ή προηγούμενων γνώσεων. Η αξιοποίησή τους για την ανάπτυξη προσωπικών ή επαγγελματικών ικανοτήτων, ειδικά στον τομέα της ψηφιακής ασφάλειας, παρουσιάζει σημαντικά πλεονεκτήματα.

1.3.1 Πλεονεκτήματα των MOOCs:

- **Ευελιξία και Προσβασιμότητα:** Τα MOOCs παρέχουν τη δυνατότητα ασύγχρονης μάθησης, επιτρέποντας στους εκπαιδευόμενους να προσαρμόσουν το πρόγραμμα σπουδών στις ανάγκες και τον διαθέσιμο χρόνο τους. Επιπλέον, η δωρεάν πρόσβαση σε ποιοτικό εκπαιδευτικό υλικό εξαλείφει τους οικονομικούς φραγμούς, καθιστώντας τη μάθηση προσιτή σε όλους (Shah, 2020; Siemens, 2013).
- **Ποικιλία και Εξειδίκευση:** Τα MOOCs καλύπτουν ένα ευρύ φάσμα θεματικών περιοχών, επιτρέποντας στους εκπαιδευόμενους να επιλέξουν μαθήματα που ανταποκρίνονται στα ενδιαφέροντα και τους στόχους τους. Ειδικά για την ψηφιακή ασφάλεια, τα MOOCs μπορούν να προσφέρουν εξειδικευμένη γνώση σε συγκεκριμένους τομείς, όπως η προστασία προσωπικών δεδομένων, η ασφάλεια συναλλαγών ή η κυβερνοασφάλεια για παιδιά (Liyanagunawardena, Adams, & Williams, 2013).
- **Διαδραστικότητα και Δημιουργία Κοινότητας:** Τα MOOCs ενσωματώνουν διαδραστικά στοιχεία, όπως κουίζ, φόρουμ συζήτησης και εργασίες, που ενισχύουν την ενεργή συμμετοχή των εκπαιδευόμενων και την αφομοίωση της γνώσης. Επιπλέον, η δημιουργία μιας online κοινότητας μάθησης προάγει την ανταλλαγή απόψεων και την αλληλοϋποστήριξη(Kizilcec & Schneider, 2015).
- **Συνεχής Ενημέρωση:** Ο ψηφιακός κόσμος εξελίσσεται ραγδαία, με νέες απειλές και προκλήσεις να εμφανίζονται συνεχώς. Τα MOOCs μπορούν να ενημερώνονται τακτικά, διασφαλίζοντας ότι οι εκπαιδευόμενοι έχουν πρόσβαση στις πιο πρόσφατες πληροφορίες και πρακτικές για την ψηφιακή ασφάλεια (Chuang & Ho, 2016).

1.3.2Προκλήσεις των MOOCs

- **Υψηλά ποσοστά εγκατάλειψης:** Η έλλειψη άμεσης καθοδήγησης και η ανάγκη για αυτοπειθαρχία μπορεί να οδηγήσουν σε υψηλά ποσοστά εγκατάλειψης (Shah, 2020).

- **Έλλειψη πιστοποίησης:** Αν και πολλά MOOCs προσφέρουν πιστοποιητικά ολοκλήρωσης, αυτά δεν αναγνωρίζονται πάντα επίσημα από εκπαιδευτικά ιδρύματα ή εργοδότες(Liyanagunawardena et al., 2013).

Παρά τις προκλήσεις, τα MOOCs αποτελούν ένα πολύτιμο εργαλείο για την ανάπτυξη ικανοτήτων ψηφιακής ασφάλειας, προσφέροντας ευελιξία, προσβασιμότητα, ποικιλία και διαδραστικότητα. Με την κατάλληλη σχεδίαση και υποστήριξη, τα MOOCs μπορούν να συμβάλουν σημαντικά στην ενίσχυση της ψηφιακής παιδείας και στην προετοιμασία των ατόμων για τις προκλήσεις του ψηφιακού κόσμου (Siemens, 2013).

1.4 Επιλογή της Μικρο-μάθησης για την Σχεδίαση του Διαδικτυακού Μαθήματος (MOOC)

Η μικρο-μάθηση, ως σύγχρονη εκπαιδευτική προσέγγιση, αναδεικνύεται ως ιδανική επιλογή για τη σχεδίαση του προτεινόμενου διαδικτυακού μαθήματος (MOOC) για την ψηφιακή ασφάλεια, καθώς ανταποκρίνεται στις ανάγκες του σύγχρονου εκπαιδευόμενου και μεγιστοποιεί την αποτελεσματικότητα της μαθησιακής διαδικασίας (Pappas, 2016).

Πλεονεκτήματα της Μικρο-μάθησης:

- **Αυξημένη Συγκέντρωση και Αφομοίωση:** Η μικρο-μάθηση βασίζεται στην παρουσίαση σύντομων, στοχευμένων μαθησιακών ενοτήτων, που διαρκούν συνήθως από λίγα λεπτά έως το πολύ 15 λεπτά. Αυτή η προσέγγιση επιτρέπει στους εκπαιδευόμενους να διατηρούν υψηλό επίπεδο συγκέντρωσης και να αφομοιώνουν αποτελεσματικότερα τις πληροφορίες, χωρίς να κατακλύζονται από μεγάλο όγκο δεδομένων (Hug, 2005).
- **Ευελιξία και Προσαρμοστικότητα:** Η μικρο-μάθηση προσφέρει ευελιξία στους εκπαιδευόμενους, επιτρέποντάς τους να επιλέξουν τις ενότητες που τους ενδιαφέρουν περισσότερο ή να επαναλάβουν συγκεκριμένες ενότητες ανάλογα με τις ανάγκες τους. Επιπλέον, η προσέγγιση αυτή μπορεί να προσαρμοστεί εύκολα σε διαφορετικά μαθησιακά στυλ και επίπεδα γνώσεων (Bruck, Motiwalla, & Foerster, 2012).
- **Κινητικότητα και Άμεση Εφαρμογή:** Οι σύντομες μαθησιακές ενότητες της μικρο-μάθησης μπορούν να ολοκληρωθούν σε σύντομο χρονικό διάστημα και από οποιαδήποτε συσκευή με πρόσβαση στο διαδίκτυο, όπως κινητά τηλέφωνα ή tablets. Επιπλέον, η άμεση εφαρμογή των γνώσεων που αποκτήθηκαν ενισχύει τη μαθησιακή διαδικασία και την εμπέδωση (Leong, 2016).

Εφαρμογή στο συγκεκριμένο MOOC:

- **Στοχευμένη Παρουσίαση Περιεχομένου:** Το ευρύ πεδίο της ψηφιακής ασφάλειας μπορεί να αναλυθεί σε μικρότερες, πιο διαχειρίσιμες ενότητες, που εστιάζουν σε συγκεκριμένες δεξιότητες ή τομείς, όπως η δημιουργία ισχυρών κωδικών πρόσβασης, η αναγνώριση ηλεκτρονικού "ψαρέματος" ή η προστασία των προσωπικών δεδομένων (Pappas, 2016).
- **Ενίσχυση της Συμμετοχής:** Η μικρο-μάθηση μπορεί να ενσωματώσει διαδραστικά στοιχεία, όπως κουίζ, παιχνίδια και προσομοιώσεις, που ενισχύουν τη συμμετοχή των εκπαιδευόμενων και την ενεργητική μάθηση (Leong, 2016).
- **Ευελιξία για Διαφορετικά Κοινά:** Το MOOC απευθύνεται σε ένα ευρύ κοινό με διαφορετικά επίπεδα ψηφιακής παιδείας. Η μικρο-μάθηση επιτρέπει στους εκπαιδευόμενους να προσαρμόσουν τη μαθησιακή εμπειρία στις ανάγκες και τον διαθέσιμο χρόνο τους (Bruck et al., 2012).
- **Άμεση Εφαρμογή στην Πράξη:** Οι εκπαιδευόμενοι μπορούν να εφαρμόσουν άμεσα τις γνώσεις που αποκτούν σε πραγματικές καταστάσεις, ενισχύοντας την κατανόηση και την εμπέδωση των βασικών αρχών ψηφιακής ασφάλειας (Hug, 2005).

Η επιλογή της μικρο-μάθησης για τη σχεδίαση του προτεινόμενου MOOC για την ψηφιακή ασφάλεια αποτελεί μια στρατηγική απόφαση που μεγιστοποιεί την αποτελεσματικότητα της μάθησης, προάγει την ενεργή συμμετοχή των εκπαιδευόμενων και ανταποκρίνεται στις ανάγκες του σύγχρονου ψηφιακού κόσμου (Pappas, 2016).

1.5 Συνεισφορά αυτού του Online Μαθήματος

Το προτεινόμενο online μάθημα για την ψηφιακή ασφάλεια έχει τη δυνατότητα να προσφέρει σημαντική συνεισφορά στο πεδίο, καλύπτοντας ένα κρίσιμο κενό στην εκπαίδευση και την ευαισθητοποίηση του κοινού σχετικά με τους κινδύνους και τις προκλήσεις του ψηφιακού κόσμου.

- **Ενίσχυση της Ψηφιακής Παιδείας:**
  Το μάθημα αυτό μπορεί να αποτελέσει ένα πολύτιμο εργαλείο για την ενίσχυση της ψηφιακής παιδείας, παρέχοντας σε ένα ευρύ κοινό τη δυνατότητα να αποκτήσει βασικές γνώσεις και δεξιότητες για την ασφαλή και υπεύθυνη χρήση του διαδικτύου. Αυτό είναι ιδιαίτερα σημαντικό σε μια εποχή όπου η τεχνολογία εξελίσσεται ραγδαία και οι ψηφιακές απειλές γίνονται όλο και πιο περίπλοκες.

- **Προστασία από Κυβερνοεπιθέσεις:**
  Με την εκπαίδευση των χρηστών σχετικά με τους κινδύνους όπως το ηλεκτρονικό "ψάρεμα" (phishing), το κακόβουλο λογισμικό και η παραπληροφόρηση, το μάθημα

αυτό μπορεί να συμβάλει στην πρόληψη κυβερνοεπιθέσεων και στην προστασία των προσωπικών δεδομένων και των online λογαριασμών.

- **Προώθηση της Υπεύθυνης Χρήσης του Διαδικτύου:**
  Το μάθημα δίνει έμφαση στην υπεύθυνη χρήση των κοινωνικών δικτύων και στην αντιμετώπιση της διαδικτυακής παρενόχλησης, προωθώντας αξίες όπως ο σεβασμός, η ευγένεια και η ενσυναίσθηση στο διαδικτυακό περιβάλλον.

- **Ενδυνάμωση των Γονέων και των Εκπαιδευτικών:**
  Το μάθημα παρέχει στους γονείς και τους εκπαιδευτικούς τα απαραίτητα εργαλεία για να καθοδηγήσουν και να προστατεύσουν τα παιδιά από τους κινδύνους του διαδικτύου, δημιουργώντας ένα ασφαλές και υποστηρικτικό περιβάλλον για την ανάπτυξή τους.

Συνολική Κοινωνική Συνεισφορά:

Με την ευαισθητοποίηση και την εκπαίδευση του κοινού σχετικά με την ψηφιακή ασφάλεια, το μάθημα αυτό μπορεί να συμβάλει στη δημιουργία μιας πιο ασφαλούς και υπεύθυνης ψηφιακής κοινωνίας, όπου όλοι μπορούν να αξιοποιήσουν τις δυνατότητες της τεχνολογίας χωρίς να θέτουν σε κίνδυνο τον εαυτό τους ή τους άλλους.

Κεφάλαιο 2. Επισκόπηση ψηφιακών μαθημάτων για την απόκτηση ψηφιακών ικανοτήτων των ενηλίκων για την ασφαλή πλοήγηση στο διαδίκτυο.

2.1 Εισαγωγή επισκόπησης παρόμοιων ψηφιακών μαθημάτων

Στον ψηφιακό κόσμο που διαρκώς εξελίσσεται, η ανάγκη για εκπαίδευση και ενημέρωση σχετικά με την ασφαλή πλοήγηση στο διαδίκτυο καθίσταται επιτακτική. Πολλά διαδικτυακά μαθήματα έχουν αναπτυχθεί με σκοπό την ενδυνάμωση των ενηλίκων, προσφέροντας γνώσεις και δεξιότητες που είναι ζωτικής σημασίας για την προστασία τους στο ψηφιακό περιβάλλον. Αυτά τα μαθήματα ποικίλλουν από γενικές εισαγωγές στην ψηφιακή ασφάλεια μέχρι εξειδικευμένα προγράμματα που εστιάζουν σε συγκεκριμένες πτυχές, όπως η αναγνώριση phishing επιθέσεων, η χρήση εργαλείων προστασίας της ιδιωτικότητας και η διαχείριση των κοινωνικών δικτύων με ασφάλεια. Ορισμένα από αυτά τα προγράμματα προσφέρουν διαδραστικά σενάρια και πρακτικές ασκήσεις που επιτρέπουν στους συμμετέχοντες να εξασκήσουν τις δεξιότητές τους σε ρεαλιστικά περιβάλλοντα. Άλλα επικεντρώνονται στην ανάπτυξη της κριτικής σκέψης και της ψηφιακής ηθικής, αναγνωρίζοντας τη σημασία της υπευθυνότητας στη διαδικτυακή αλληλεπίδραση. Μέσα από αυτό το κεφάλαιο, θα εξετάσουμε τα χαρακτηριστικά κάποιων παρόμοιων μαθημάτων και θα τα συγκρίνουμε με την προσέγγιση του δικού μας προγράμματος.

2.2 Παρουσίαση ψηφιακών μαθημάτων

2.2.1 Μάθημα 1: Digital Literacy and Online Safety

Πίνακας 1: Digital Literacy and Online Safety

ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ	
Τίτλος Μαθήματος	**Digital Literacy and Online Safety**
Σύντομη Περιγραφή	Αυτό το MOOC εξερευνά διαδικτυακές τάσεις και ζητήματα στο πλαίσιο της νέας πραγματικότητας COVID-19. Θα παρέχει στους συμμετέχοντες στο μάθημα βασικές γνώσεις, συμβουλές και εργαλεία για να χειριστούν ένα ευρύ φάσμα θεμάτων, όπως

	παραπληροφόρηση και θεωρίες συνωμοσίας, διαδικτυακές απάτες (όπως phishing, κακόβουλο λογισμικό και ransomware), ασφάλεια λογαριασμού, ιδιωτικότητα στο διαδίκτυο, οφέλη και κίνδυνοι συνδέονται μεταξύ άλλων με τη ζωντανή ροή και τις σχέσεις υγείας στο διαδίκτυο. Συνολικά, αυτό το MOOC θα επιτρέψει στους συμμετέχοντες να κατανοήσουν καλύτερα τους κινδύνους και τις προκλήσεις που αντιμετωπίζουν οι νέοι όταν μπαίνουν στο διαδίκτυο.
Σε ποιους Απευθύνεται	Το μάθημα απευθύνεται σε εκπαιδευτικούς πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης οποιουδήποτε μαθήματος. Οι διαχειριστές ΤΠΕ, οι σχολικοί σύμβουλοι και οι γονείς μπορούν επίσης να επωφεληθούν από το μάθημα.
Μαθησιακά Αποτελέσματα	1.Να κατανοήσουν τα οφέλη και τους κινδύνους που συνδέονται με τις ψηφιακές τεχνολογίες και το διαδίκτυο στο πλαίσιο μιας πανδημίας, ειδικά σε σχέση με τα παιδιά και τους νέους. 2.Να διερευνήσουν τις ευκαιρίες που παρέχει το διαδίκτυο για πρόσβαση στη γνώση, επικοινωνία και ανάπτυξη δεξιοτήτων και δημιουργικότητας, αλλά και δεξιοτήτων κριτικής σκέψης. 3.Να ευαισθητοποιήσει σχετικά με τη σημασία των υγιών σχέσεων με την τεχνολογία και το διαδίκτυο. 4.Να αυξήσει την ευαισθητοποίηση σχετικά με τη στρατηγική για το καλύτερο Διαδίκτυο για παιδιά (BIK) και το δίκτυο Insafe, ως μέρος του δικτύου των Κέντρων Ασφαλούς Διαδικτύου (SIC) στην Ευρώπη, και των σχετικών πόρων.
Κατηγορία Μαθήματος	Διαδικτυακό
Πλατφόρμα Διάθεσης (για τα Διαδικτυακά Μαθήματα)	europeanschoolnetacademy

URL Μαθήματος	https://www.europeanschoolnetacademy.eu/courses/course-v1:BIK3+DigitalLiteracy+2021/about
Προϋποθέσεις Επιτυχούς Ολοκλήρωσης	Για να αποκτήσουν ένα πιστοποιητικό μαθήματος, οι συμμετέχοντες στο μάθημα πρέπει να περάσουν όλα τα κουίζ, να υποβάλουν ένα σχέδιο μαθήματος και να ελέγξουν 3 από τα σχέδια μαθημάτων των συνομηλίκων τους. Η συμμετοχή στα κουίζ θα μετρήσει στο 15%, και το πλάνο μαθήματος μαζί με τις αξιολογήσεις από ομοτίμους θα μετρήσει στο 85%. Ο συνολικός βαθμός επιτυχίας είναι 95%.
Είδος Πιστοποιητικού που Προσφέρει	course certificate
Διάρκεια Μαθήματος	4 εβδομάδες
Εκτιμώμενος Φόρτος Εργασίας για την Ολοκλήρωση του Μαθήματος	16 ώρες
Γλώσσα	Αγγλικά
Προαπαιτούμενα	Δεν απαιτείται προηγούμενη γνώση.
Εκπαιδευτικός Οργανισμός	Insafe and INHOPE network of Safer Internet Centres
Εκπαιδευτής	Eray Başar - COURSE COORDINATOR Gareth Cort - COURSE MODERATOR Lorcan Tuohy - COURSE MODERATOR

Το μάθημα "Digital Literacy and Online Safety" προσφέρει μια ολοκληρωμένη και επίκαιρη προσέγγιση στην εκπαίδευση σχετικά με τους κινδύνους και τις ευκαιρίες του διαδικτύου, ειδικά στο πλαίσιο της πανδημίας COVID-19. Εστιάζει στη διαχείριση θεμάτων όπως η παραπληροφόρηση, οι διαδικτυακές απάτες, και η ασφάλεια λογαριασμών, ενώ παράλληλα προάγει την κριτική σκέψη και την ψηφιακή ενδυνάμωση. Η στόχευσή του σε εκπαιδευτικούς, διαχειριστές ΤΠΕ, και γονείς το καθιστά ιδιαίτερα χρήσιμο για την ανάπτυξη ενός ασφαλούς ψηφιακού περιβάλλοντος για τα παιδιά και τους νέους.

Εντούτοις, η απαίτηση υψηλής επιτυχίας (95%) για την απόκτηση πιστοποιητικού μπορεί να λειτουργήσει αποτρεπτικά για ορισμένους συμμετέχοντες, ενώ η έλλειψη προκαθορισμένων γνώσεων το καθιστά προσιτό σε αρχάριους.

2.2.2 Μάθημα 2: Προστασία Προσωπικών δεδομένων και ιδιωτικότητα

Πίνακας 2:Προστασία Προσωπικών δεδομένων και ιδιωτικότητα

ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ	
Τίτλος Μαθήματος	**Προστασία Προσωπικών δεδομένων και ιδιωτικότητα**
Σύντομη Περιγραφή	Σκοπός του μαθήματος είναι να μάθουν οι εκπαιδευόμενοι για την αξία της προστασίας των προσωπικών δεδομένων και της ιδιωτικότητάς τους αλλά και για το ισχύον νομοθετικό πλαίσιο που τα προστατεύει. Θα μάθουν επίσης ορισμένους τρόπους και συμβουλές σχετικά με το τι μπορούν να κάνουν, ώστε να προστατεύουν τα προσωπικά δεδομένα και την ιδιωτικότητά τους.
Σε ποιους Απευθύνεται	Το μάθημα αυτό απευθύνεται σε όσους επιθυμούν να μάθουν πώς μπορούν να προστατεύουν τα προσωπικά δεδομένα και την ιδιωτικότητα τους κατά τη χρήση του Διαδικτύου.
Μαθησιακά Αποτελέσματα	Το συγκεκριμένο μάθημα αποτελείται από πέντε ενότητες και οι εκπαιδευόμενοι θα μάθουν: - Ποια είναι τα «προσωπικά δεδομένα» και τα «ευαίσθητα προσωπικά δεδομένα» , τι είναι η επεξεργασία και η «ιδιωτικότητα» των προσωπικών δεδομένων και πώς μπορείτε να τα διακρίνετε στην καθημερινότητά σας και στο διαδίκτυο. - Για το νομοθετικό πλαίσιο που προστατεύει τα προσωπικά δεδομένα και την ιδιωτικότητά σας, για το τι πρέπει να κάνετε ώστε να προστατεύετε τα προσωπικά δεδομένα που δίνετε σε τρίτους αλλά και τι πρέπει να προσέχετε ώστε να μη χρησιμοποιούν τα

	προσωπικά σας δεδομένα χωρίς εξουσιοδότηση (παραβίαση δεδομένων). - Πώς λειτουργούν τα cookies και η στοχευμένη διαφήμιση, πώς μπορείτε να διακρίνετε τις κακόβουλες διαφημίσεις και να αποφεύγετε ηλεκτρονικές απάτες, όπως το ηλεκτρονικό ψάρεμα (phishing), αλλά και πώς να αποφεύγετε να δίνετε τα προσωπικά σας δεδομένα σε τρίτους ή σε εταιρείες που δεν δικαιούνται να τα κατέχουν. - Πώς μπορείτε να δημιουργείτε ισχυρούς κωδικούς πρόσβασης για την προστασία των τραπεζικών σας λογαριασμών, του ηλεκτρονικού σας ταχυδρομείου και των λογαριασμών σας στα μέσα κοινωνικής δικτύωσης. - Τι πρέπει να κάνετε για να προστατεύσετε την ιδιωτικότητά σας από τις διάφορες εφαρμογές στο κινητό σας και ποιες ρυθμίσεις απορρήτου και ασφαλείας πρέπει να επιλέξετε στους λογαριασμούς που διατηρείτε στα κοινωνικά δίκτυα.
Κατηγορία Μαθήματος	Διαδικτυακό
Πλατφόρμα Διάθεσης (για τα Διαδικτυακά Μαθήματα)	https://nationaldigitalacademy.gov.gr
URL Μαθήματος	https://nationaldigitalacademy.gov.gr/mathimata/diadiktyo-2/prostasia-proswpikwn-dedomenwn-kai-idiwtikothta-328
Προϋποθέσεις Επιτυχούς Ολοκλήρωσης	Δεν αναφέρεται.
Είδος Πιστοποιητικού που Προσφέρει	Δεν προσφέρει κάποιο πιστοποιητικό.
Διάρκεια Μαθήματος	3 ώρες
Εκτιμώμενος Φόρτος Εργασίας για την Ολοκλήρωση του	3 ώρες

Μαθήματος	
Γλώσσα	Ελληνικά
Προαπαιτούμενα	Δεν απαιτείται προηγούμενη γνώση.
Εκπαιδευτικός Οργανισμός	Εθνική Ακαδημία ψηφιακών ικανοτήτων.

Το μάθημα "Προστασία Προσωπικών Δεδομένων και Ιδιωτικότητα" είναι ένα χρήσιμο και πρακτικό εκπαιδευτικό εργαλείο που δίνει στους συμμετέχοντες τη δυνατότητα να κατανοήσουν τις βασικές αρχές και πρακτικές της προστασίας προσωπικών δεδομένων. Με την έμφαση που δίνει στα νομοθετικά πλαίσια και τις απλές, καθημερινές πρακτικές ασφάλειας, είναι ιδιαίτερα χρήσιμο για όσους ενδιαφέρονται να βελτιώσουν τη διαδικτυακή τους ασφάλεια χωρίς να απαιτούνται προηγούμενες γνώσεις. Αν και η διάρκεια του μαθήματος είναι μικρή (3 ώρες), προσφέρει μια καλή εισαγωγή σε ένα κρίσιμο θέμα, ιδιαίτερα στο σημερινό ψηφιακό περιβάλλον όπου οι κίνδυνοι της παραβίασης δεδομένων αυξάνονται συνεχώς. Η απουσία πιστοποιητικού ίσως να περιορίζει την αναγνώριση της προσπάθειας των συμμετεχόντων σε σύγκριση με άλλα μαθήματα, αλλά παραμένει ένα αξιόλογο εργαλείο ευαισθητοποίησης.

2.2.3 Μάθημα 3: Ασφαλής Πλοήγηση στο Διαδίκτυο

Πίνακας 3:Ασφαλής Πλοήγηση στο Διαδίκτυο

ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ	
Τίτλος Μαθήματος	**Ασφαλής Πλοήγηση στο Διαδίκτυο**
Σύντομη Περιγραφή	"Εστιάζει στην ασφαλή χρήση του διαδικτύου, την προστασία προσωπικών δεδομένων και την αποφυγή διαδικτυακών κινδύνων. Οι κύριοι στόχοι της δράσης Saferinternet.gr είναι: Η προστασία των ανηλίκων από ακατάλληλο ή επιβλαβές για αυτούς περιεχόμενο, ή από ακατάλληλη ή επιβλαβή συμπεριφορά και η προώθηση της υπεύθυνης και ασφαλούς χρήσης του Διαδικτύου. Η ενδυνάμωση γονέων και εκπαιδευτικών σε θέματα

	ασφάλειας στο Διαδίκτυο μέσω ενημερώσεων, εκπαιδεύσεων και κατάλληλου online και έντυπου υλικού."
Σε ποιους Απευθύνεται	Σε εφήβους και ενήλικες, εκπαιδευτικούς ή γονείς.
Μαθησιακά Αποτελέσματα	Να αναγνωρίζουν και να αποφεύγουν διαδικτυακούς κινδύνους, να προστατεύουν τα προσωπικά τους δεδομένα και να χρησιμοποιούν το διαδίκτυο με ασφάλεια.
Κατηγορία Μαθήματος	Διαδικτυακό
Πλατφόρμα Διάθεσης (για τα Διαδικτυακά Μαθήματα)	https://www.saferinternet.gr/
URL Μαθήματος	https://www.saferinternet.gr/
Προϋποθέσεις Επιτυχούς Ολοκλήρωσης	Δεν αναφέρεται.
Είδος Πιστοποιητικού που Προσφέρει	Δεν προσφέρεται κάποιο πιστοποιητικό.
Διάρκεια Μαθήματος	Είναι χωρισμένο σε πολλές ανεξάρτητες μικρής διάρκειας ενότητες.
Εκτιμώμενος Φόρτος Εργασίας για την Ολοκλήρωση του Μαθήματος	Είναι χωρισμένο σε πολλές ανεξάρτητες μικρής διάρκειας ενότητες.
Γλώσσα	Ελληνικά
Προαπαιτούμενα	Δεν απαιτείται προηγούμενη γνώση.
Εκπαιδευτικός Οργανισμός	Πανευρωπαϊκού Δικτύου Εθνικών Κέντρων Ενημέρωσης και Επαγρύπνησης Insafe

Το μάθημα **"Ασφαλής Πλοήγηση στο Διαδίκτυο"** που προσφέρεται μέσω της πλατφόρμας

SaferInternet.gr είναι ένα σημαντικό εργαλείο για την εκπαίδευση παιδιών, εφήβων, γονέων και εκπαιδευτικών σε θέματα ασφάλειας στο διαδίκτυο. Η έμφαση του μαθήματος δίνεται στην αναγνώριση και αποφυγή διαδικτυακών κινδύνων, την προστασία προσωπικών δεδομένων, και την υπεύθυνη χρήση του διαδικτύου, γεγονός που το καθιστά πολύτιμο για όλους τους χρήστες του Διαδικτύου. Η δομή του είναι ευέλικτη, καθώς αποτελείται από ανεξάρτητες, μικρής διάρκειας ενότητες, οι οποίες επιτρέπουν στους συμμετέχοντες να επικεντρωθούν στα θέματα που τους αφορούν περισσότερο. Ωστόσο, η απουσία πιστοποιητικού ίσως να μειώνει την αξία του για όσους αναζητούν μια πιο επίσημη επιβεβαίωση των γνώσεών τους.

2.2.4 Μάθημα 4: Digital Awareness

Πίνακας 4:Digital Awareness

ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ	
Τίτλος Μαθήματος	**Digital Awareness**
Σύντομη Περιγραφή	Σχεδιασμένο με γνώμονα τον αρχάριο, αυτό το μάθημα εξοπλίζει με θεμελιώδεις γνώσεις και πρακτικές ψηφιακές δεξιότητες που μπορείτε να εφαρμόσει κάποιος στο σπίτι, στο σχολείο ή στη δουλειά. Παρουσιάζονται οι ψηφιακές δεξιότητες σαν μια εργαλειοθήκη για τον διαδικτυακό κόσμο. Δίνονται συμβουλές και κόλπα για την αναζήτηση στο διαδίκτυο, τη δημιουργία ισχυρών κωδικών πρόσβασης και την αντιμετώπιση ενοχλητικών τεχνικών προβλημάτων όπως η αργή απόδοση και τα προβλήματα Wi-Fi ή συνδεσιμότητας. Επίσης αναφέρεται στη διαχείριση των προσωπικών δεδομένων και στη προστασία από διαδικτυακές απειλές, όπως απάτες phishing και κακόβουλο λογισμικό.
Σε ποιους Απευθύνεται	Σε έφηβους, ηλικιωμένους, γονείς ή κηδεμόνες, εκπαιδευτικούς και σε οποιονδήποτε αρχάριο στην τεχνολογία που θέλει να αναπτύξει ψηφιακές δεξιότητες.

Μαθησιακά Αποτελέσματα	Βασική κατανόηση των ψηφιακών εργαλείων και τεχνολογιών και των εφαρμογών τους στην καθημερινή ζωή. Ο εκπαιδευόμενος αποκτά τις βασικές δεξιότητες για τον εντοπισμό και τη χρήση των λειτουργιών κοινών ψηφιακών συσκευών, την υπεύθυνη πλοήγηση στο ψηφιακό περιεχόμενο και τη διαχείριση της παρουσίας του στο διαδίκτυο αποτελεσματικά. Επιπλέον, ο εκπαιδευόμενος κατανοεί την εξέλιξη των ψηφιακών τεχνολογιών και τη σημασία της ηθικής και υπεύθυνης χρήσης.
Κατηγορία Μαθήματος	Διαδικτυακό
Πλατφόρμα Διάθεσης (για τα Διαδικτυακά Μαθήματα)	CISCO Networking Academy
URL Μαθήματος	https://www.netacad.com/courses/digital-awareness?courseLang=en-US
Προϋποθέσεις Επιτυχούς Ολοκλήρωσης	Η παρακολούθηση όλων των ενοτήτων, η ολοκλήρωση των δραστηριοτήτων που τους αντιστοιχούν και η παράδοση μίας τελικής εργασίας.
Είδος Πιστοποιητικού που Προσφέρει	Course Badge που εκδίδεται από τη Cisco Networking Academy
Διάρκεια Μαθήματος	6 ώρες
Εκτιμώμενος Φόρτος Εργασίας για την Ολοκλήρωση του Μαθήματος	6 ώρες
Γλώσσα	Αγγλικά, Ισπανικά
Προαπαιτούμενα	Δεν υπάρχουν προαπαιτούμενα αφού το επίπεδο των εκπαιδευόμενων είναι «αρχάριος».
Εκπαιδευτικός Οργανισμός	Έχει αναπτυχθεί από τη Cisco Network academy, σε συνεργασία με το OpenEDG.

Οτιδήποτε άλλο χρήσιμο	Είναι μέρος από μια σειρά μαθημάτων για αρχάριους που ονομάζονται Digital Literacy.

Το μάθημα **"Digital Awareness"** που προσφέρεται από τη Cisco Networking Academy έχει σχεδιαστεί για αρχάριους και στοχεύει στην ανάπτυξη βασικών ψηφιακών δεξιοτήτων που είναι χρήσιμες στο σπίτι, το σχολείο ή την εργασία. Το μάθημα επικεντρώνεται σε πρακτικά θέματα όπως η δημιουργία ισχυρών κωδικών πρόσβασης, η διαχείριση τεχνικών προβλημάτων και η προστασία από διαδικτυακές απειλές όπως το phishing και το κακόβουλο λογισμικό. Ενώ καλύπτει ένα ευρύ φάσμα θεμάτων, η περιορισμένη διάρκεια των 6 ωρών μπορεί να μην είναι επαρκής για πιο προχωρημένους εκπαιδευόμενους ή για όσους χρειάζονται σε βάθος κατανόηση. Παρά τη σύντομη διάρκεια, είναι ένα εξαιρετικό σημείο εκκίνησης για όσους θέλουν να ενισχύσουν την ψηφιακή τους αυτοπεποίθηση.

2.2.5 Μάθημα 5: Protecting Yourself Online

Πίνακας 5: Protecting Yourself Online

ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ	
Τίτλος Μαθήματος	**Protecting Yourself Online**
Σύντομη Περιγραφή	Τα μέσα κοινωνικής δικτύωσης επιτρέπουν μεγαλύτερη αλληλεπίδραση στην εκπαιδευτική κοινότητα. Μπορεί επίσης να είναι ένας προκλητικός χώρος εάν δεν γνωρίζετε πλήρως πώς να προστατεύσετε το απόρρητό σας στις δημοφιλείς πλατφόρμες κοινωνικής δικτύωσης. Αυτό το μάθημα θα διερευνήσει τα πρακτικά βήματα που μπορείτε να ακολουθήσετε για να προστατεύσετε τον εαυτό σας (και την επαγγελματική σας ταυτότητα) στο διαδικτυακό περιβάλλον.
Σε ποιους Απευθύνεται	Σε εκπαιδευτικούς πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης.
Μαθησιακά Αποτελέσματα	Οι εκπαιδευόμενοι θα μάθουν σχετικά με το

	διαδικτυακό περιβάλλον, συμπεριλαμβανομένων των κινδύνων, την έννοια της ιδιωτικότητας και τι βλέπουν τα παιδιά.
Κατηγορία Μαθήματος	Διαδικτυακό
Πλατφόρμα Διάθεσης (για τα Διαδικτυακά Μαθήματα)	Cool.org
URL Μαθήματος	https://cool.org/course/protecting-yourself-online
Προϋποθέσεις Επιτυχούς Ολοκλήρωσης	Δεν αναφέρεται.
Είδος Πιστοποιητικού που Προσφέρει	Cool.org certificate
Διάρκεια Μαθήματος	2 ώρες
Εκτιμώμενος Φόρτος Εργασίας για την Ολοκλήρωση του Μαθήματος	2 ώρες
Γλώσσα	Αγγλικά
Προαπαιτούμενα	Δεν απαιτείται προηγούμενη γνώση.
Εκπαιδευτικός Οργανισμός	cool.org
Οτιδήποτε άλλο χρήσιμο	Η πρόσβαση στο μάθημα αυτό γίνεται με δημιουργία είτε μηνιαίας είτε ετήσιας συνδρομής στο cool.org.

Το μάθημα **"Protecting Yourself Online"** που προσφέρεται από τη Cool.org εστιάζει στις βασικές πρακτικές για την προστασία της ιδιωτικότητας στις πλατφόρμες κοινωνικής δικτύωσης, κάτι που είναι ιδιαίτερα σημαντικό για εκπαιδευτικούς. Παρόλο που έχει σύντομη διάρκεια (μόλις 2 ώρες), παρέχει ουσιαστικές συμβουλές για το πώς να προστατεύουν οι συμμετέχοντες τον εαυτό τους, αλλά και την επαγγελματική τους ταυτότητα, σε ένα διαδικτυακό περιβάλλον που είναι γεμάτο προκλήσεις και κινδύνους. Το γεγονός ότι απαιτεί συνδρομή μπορεί να αποτελέσει εμπόδιο για ορισμένους χρήστες,

ωστόσο η σύντομη διάρκεια και η εστιασμένη προσέγγιση το καθιστούν ιδανικό για εκπαιδευτικούς με περιορισμένο χρόνο.

2.2.6 Μάθημα 6: Be Internet Awesome

Πίνακας 6: Be Internet Awesome

ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ	
Τίτλος Μαθήματος	**Be Internet Awesome**
Σύντομη Περιγραφή	Αυτό το διαδραστικό μάθημα, που δημιουργήθηκε από την Google, διδάσκει τις βασικές αρχές της διαδικτυακής ασφάλειας και της υπεύθυνης ψηφιακής συμπεριφοράς.
Σε ποιους Απευθύνεται	Παιδιά, εφήβους και ενήλικες που θέλουν να μάθουν πώς να είναι ασφαλείς, έξυπνοι και θετικοί στο διαδίκτυο.
Μαθησιακά Αποτελέσματα	Οι συμμετέχοντες θα μάθουν πώς να αποφεύγουν τις διαδικτυακές απάτες, να προστατεύουν τα προσωπικά τους δεδομένα, να είναι έξυπνοι κοινοποιώντας πληροφορίες στο διαδίκτυο, να είναι ευγενικοί και να σέβονται τους άλλους χρήστες, και να αναζητούν βοήθεια όταν αντιμετωπίζουν προβλήματα στο διαδίκτυο.
Κατηγορία Μαθήματος	Διαδικτυακό
Πλατφόρμα Διάθεσης (για τα Διαδικτυακά Μαθήματα)	https://beinternetawesome.withgoogle.com/el_gr
URL Μαθήματος	https://beinternetawesome.withgoogle.com/el_gr
Προϋποθέσεις Επιτυχούς Ολοκλήρωσης	Δεν αναφέρεται .
Είδος Πιστοποιητικού που Προσφέρει	Κάποια επιβράβευση ολοκλήρωσης (badges) στο λογαριασμό του google account.

Διάρκεια Μαθήματος	Αυτορρυθμιζόμενη, με διαδραστικές δραστηριότητες και κουίζ.
Γλώσσα	Επιλέγει ο χρήστης τη γλώσσα που επιθυμεί από παρά πολλές προσφερόμενες γλώσσες.
Προαπαιτούμενα	Δεν απαιτείται προηγούμενη γνώση.
Εκπαιδευτικός Οργανισμός	GOOGLE
Οτιδήποτε άλλο χρήσιμο	Το πρόγραμμα «Γίνε Ήρωας του Διαδικτύου» είναι ευθυγραμμισμένο τόσο με τα πρότυπα της ISTE (Διεθνής Εταιρία για την Τεχνολογία στην Εκπαίδευση) όσο και με τα πρότυπα της AASL (Αμερικανική Ένωση Σχολικών Βιβλιοθηκονόμων).

Το "Be Internet Awesome" παρέχει μια ευρεία γκάμα θεμάτων που καλύπτουν σημαντικές πτυχές της διαδικτυακής ασφάλειας, όπως η προστασία των προσωπικών δεδομένων, η αναγνώριση κακόβουλων περιεχομένων και η ανάπτυξη της ψηφιακής ηθικής. Το περιεχόμενο είναι διαρθρωμένο με τρόπο που διευκολύνει την κατανόηση και την αφομοίωση, κάνοντάς το κατάλληλο για νεαρούς χρήστες.

Ένα από τα πιο θετικά στοιχεία του προγράμματος είναι η διαδραστική προσέγγιση που χρησιμοποιεί. Οι συμμετέχοντες έχουν τη δυνατότητα να συμμετέχουν σε παιχνίδια και προσομοιώσεις που τους επιτρέπουν να εφαρμόσουν τις γνώσεις τους σε ρεαλιστικά σενάρια. Αυτή η προσέγγιση ενισχύει την εμπλοκή και την διασκέδαση, καθιστώντας τη διαδικασία εκμάθησης πιο ελκυστική.

Ωστόσο, υπάρχουν και ορισμένα σημεία που θα μπορούσαν να βελτιωθούν. Ορισμένοι κριτές έχουν επισημάνει ότι το πρόγραμμα μπορεί να φαίνεται περιορισμένο σε επίπεδο βάθους, καθώς επικεντρώνεται κυρίως σε βασικές έννοιες. Η προσθήκη πιο προχωρημένων θεμάτων ή σεναρίων θα μπορούσε να ενισχύσει τη συνολική εκπαιδευτική αξία του μαθήματος.

2.2.7 Μάθημα 7: Digital Empowerment: Navigating the Online World Securely

Πίνακας 7:Digital Empowerment: Navigating the Online World Securely

ΠΕΡΙΓΡΑΦΗ ΜΑΘΗΜΑΤΟΣ	
Τίτλος Μαθήματος	**Digital Empowerment: Navigating the Online World Securely**
Σύντομη Περιγραφή	Αυτό το μάθημα Ψηφιακού Αλφαβητισμού προσφέρει μια ολοκληρωμένη εξερεύνηση βασικών ψηφιακών δεξιοτήτων, εστιάζοντας στο απόρρητο, την ασφάλεια, τη διαχείριση δεδομένων και την αποτελεσματική διαδικτυακή επικοινωνία. Σε διάστημα τεσσάρων εβδομάδων, οι συμμετέχοντες θα συμμετάσχουν σε πρακτικές ασκήσεις, συνεργατικά έργα και διαδραστικά μαθήματα που έχουν σχεδιαστεί για να βελτιώσουν την ψηφιακή τους ευχέρεια, διασφαλίζοντας ότι είναι καλά εξοπλισμένοι για να πλοηγηθούν στην πολυπλοκότητα του ψηφιακού κόσμου με ασφάλεια και αποτελεσματικότητα. Σε ευθυγράμμιση με τους στόχους της ψηφιακής δεκαετίας της Ευρώπης, αυτό το μάθημα ακολουθεί μια ανθρωποκεντρική προσέγγιση για να ενδυναμώσει τις επιχειρήσεις και τα άτομα με βασικές ψηφιακές δεξιότητες και κυβερνοασφάλειας, αντιμετωπίζοντας το χάσμα ψηφιακών δεξιοτήτων και ενισχύοντας μια ασφαλή διαδικτυακή κοινωνία και οικονομία.
Σε ποιους Απευθύνεται	Αυτό το μάθημα είναι ιδανικό για οποιονδήποτε – άτομα και επαγγελματίες σε διάφορους τομείς που επιδιώκουν να βελτιώσουν τις ψηφιακές τους δεξιότητες σε ευθυγράμμιση με τις πολιτικές της Ευρώπης για την ψηφιακή δεκαετία.
Μαθησιακά Αποτελέσματα	1.Κατανόηση και διαχείριση της ψηφιακής παρουσίας:

	• Αναγνώριση της σημασίας του ψηφιακού αποτυπώματος και τρόποι διαχείρισης με ασφάλεια το διαδικτυακό προφίλ κάποιου. • Δημιουργία και χρήση λογαριασμών email αποτελεσματικά, κατανοώντας τα βασικά της ψηφιακής επικοινωνίας. 2.Ασφαλής πρόσβαση και χρήση διαδικτυακών υπηρεσιών: • Προσδιορισμός και αντιμετώπιση των κινδύνων που σχετίζονται με το δημόσιο WiFi και τις ηλεκτρονικές τραπεζικές συναλλαγές. • Χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) και των VPN για να προστασία διαδικτυακών δραστηριοτήτων. 3.Διαχείριση και αποτελεσματική προστασία των ψηφιακών δεδομένων: • Χρήση στρατηγικών για τη μεταφορά, τη διατήρηση και τη δημιουργία αντιγράφων ασφαλείας δεδομένων με ασφάλεια. • Κατανόηση του ρόλου και της σημασίας των ψηφιακών υπογραφών και της λογοδοσίας στον ψηφιακό χώρο. 4.Ασφαλής περιήγηση στο διαδίκτυο και χρησιμοποίηση των υπηρεσιών Cloud με υπευθυνότητα: • Χρησιμοποίηση αποτελεσματικά προγραμμάτων περιήγησης ιστού και υπηρεσίων cloud, ενισχύοντας την παραγωγικότητα και την ψηφιακή συνεργασία. • Υπεύθυνη συμπεριφορά στα μέσα κοινωνικής δικτύωσης, αναγνωρίζοντας και αξιολογώντας ψεύτικες ειδήσεις.

	5.Εφαρμόγη δεξιοτήτων ψηφιακού γραμματισμού σε σενάρια πραγματικού κόσμου: • Απάντηση σε μια ολοκληρωμένη άσκηση που επικυρώνει την κατανόησή και την εφαρμογή των εννοιών του ψηφιακού γραμματισμού και της ασφάλειας στον κυβερνοχώρο. • Επίδειξη ετοιμότητας για πλοήγηση στον ψηφιακό κόσμο με ασφάλεια και υπευθυνότητα, σε ευθυγράμμιση με τους στόχους της ψηφιακής δεκαετίας της Ευρώπης.
Κατηγορία Μαθήματος	Διαδικτυακό
Πλατφόρμα Διάθεσης (για τα Διαδικτυακά Μαθήματα)	https://pat.edu.eu/fintech/courses/
URL Μαθήματος	https://pat.edu.eu/fintech/product/digital-empowerment-navigating-the-online-world-securely/
Προϋποθέσεις Επιτυχούς Ολοκλήρωσης	Άσκηση επιβεβαίωσης: Μια ολοκληρωμένη άσκηση που συνδυάζει διάφορες πτυχές του περιεχομένου του μαθήματος, επικυρώνοντας τον ψηφιακό γραμματισμό και την ευαισθητοποίηση σχετικά με την ασφάλεια του συμμετέχοντα.
Είδος Πιστοποιητικού που Προσφέρει	Με την επιτυχή ολοκλήρωση, οι συμμετέχοντες θα λάβουν ένα Πιστοποιητικό Ψηφιακού Αλφαβητισμού, το οποίο θα επιβεβαιώνει την ικανότητά τους στην ασφαλή και υπεύθυνη πλοήγηση στον ψηφιακό κόσμο.
Διάρκεια Μαθήματος	4 εβδομάδων από 2 ώρες online παρακολούθησης (σύγχρονη διδασκαλία)
Εκτιμώμενος Φόρτος Εργασίας για την Ολοκλήρωση του Μαθήματος	8 ώρες
Γλώσσα	Αγγλικά

Προαπαιτούμενα	Οι συμμετέχοντες θα πρέπει να έχουν μια βασική κατανόηση των διαδικτυακών απατών, της κοινωνικής μηχανικής και της σημασίας της διαδικτυακής προστασίας. Αυτή η προϋπόθεση διασφαλίζει ότι οι μαθητές ξεκινούν με βάση την ασφάλεια και την ασφάλεια στο διαδίκτυο.
Εκπαιδευτικός Οργανισμός	PAT FINTECH PROGRAMMES
Εκπαιδευτής	Andrew Quinn- Υπεύθυνος μαθημάτων (Υπεύθυνος PAT Fintech & Financial Services στο PAT Business School) Graham Day- Υπεύθυνος μαθήματος (Ιδρυτής στο CyberGuardian.ie)
Οτιδήποτε άλλο χρήσιμο	Δίδακτρα μαθήματος 99 ευρω Επαναλαμβάνεται σε συγκεκριμένες ημερομηνίες. Αυτή η περίοδος παρακολούθησης ξεκίνησε στις 28/08/2024.

Το μάθημα "**Digital Empowerment: Navigating the Online World Securely**" παρέχει μια ολοκληρωμένη προσέγγιση στις θεμελιώδεις ψηφιακές δεξιότητες, εστιάζοντας στην ασφάλεια, το απόρρητο και τη διαχείριση δεδομένων. Μέσα σε 4 εβδομάδες, οι συμμετέχοντες θα αποκτήσουν γνώσεις για την ασφαλή χρήση διαδικτυακών υπηρεσιών και εργαλείων, τον χειρισμό των δεδομένων και την υπεύθυνη πλοήγηση στον ψηφιακό κόσμο. Το μάθημα ακολουθεί μια ανθρωποκεντρική προσέγγιση, εναρμονισμένη με τους στόχους της Ψηφιακής Δεκαετίας της Ευρώπης. Ίσως η ύπαρξη διδάκτρων και η ανάγκη για εγγραφή και σύγχρονη παρακολούθηση να είναι αποτρεπτική για κάποιους να το παρακολουθήσουν.

2.3 Ανάγκη για τη δημιουργία του MOOC «Ψηφιακή Ενδυνάμωση Ενηλίκων: Στρατηγικές για την Προαγωγή της Ασφαλούς Πλοήγησης στο Διαδίκτυο»

Παρά την πληθώρα διαδικτυακών μαθημάτων που καλύπτουν θέματα ψηφιακής ασφάλειας, το μάθημα που επέλεξα να υλοποιήσω **"Ψηφιακή Ενδυνάμωση Ενηλίκων: Στρατηγικές για την Προαγωγή της Ασφαλούς Πλοήγησης στο Διαδίκτυο"** προσφέρει μια μοναδική και ολοκληρωμένη προσέγγιση που καλύπτει τόσο βασικά όσο και πιο εξειδικευμένα ζητήματα ασφάλειας. Αυτό το μάθημα δεν περιορίζεται μόνο στην αναγνώριση απειλών, όπως το ηλεκτρονικό "ψάρεμα" (phishing), το κακόβουλο λογισμικό

και η παραπληροφόρηση, αλλά στοχεύει στην ολοκληρωμένη εκπαίδευση των συμμετεχόντων ώστε να είναι σε θέση να αξιολογούν τους κινδύνους και να αναπτύσσουν στρατηγικές για την αντιμετώπισή τους.

Μια από τις κύριες προκλήσεις που αντιμετωπίζουν σήμερα οι ενήλικες στον ψηφιακό κόσμο είναι η διαχείριση των προσωπικών τους δεδομένων. Η συνεχής εξέλιξη των μεθόδων κυβερνοεπιθέσεων, όπως η κλοπή ταυτότητας και οι απάτες ηλεκτρονικού εμπορίου, απαιτεί από τους χρήστες να είναι σε θέση να δημιουργούν ισχυρούς κωδικούς πρόσβασης, να τους διαχειρίζονται αποτελεσματικά και να αναγνωρίζουν αξιόπιστα ηλεκτρονικά καταστήματα και μεθόδους πληρωμής. Το μάθημα αυτό εξοπλίζει τους εκπαιδευόμενους με τις απαραίτητες δεξιότητες για να πλοηγούνται στο διαδίκτυο με αυτοπεποίθηση, διασφαλίζοντας την ασφάλεια των προσωπικών τους δεδομένων και των οικονομικών τους συναλλαγών.

Ένα άλλο κρίσιμο θέμα που καλύπτει το μάθημα είναι η διαδικτυακή παρουσία και η φήμη των χρηστών στα κοινωνικά δίκτυα. Οι συμμετέχοντες θα μάθουν πώς να διαχειρίζονται αποτελεσματικά τις ρυθμίσεις απορρήτου, ώστε να διατηρούν τον έλεγχο της διαδικτυακής τους ταυτότητας, καθώς και πώς να αποφεύγουν και να αντιμετωπίζουν διαδικτυακές απειλές όπως η παρενόχληση (cyberbullying). Η εστίαση στην οικογένεια και την προστασία των παιδιών στο διαδίκτυο ενισχύει τη σημασία της δημιουργίας ενός ασφαλούς και υποστηρικτικού διαδικτυακού περιβάλλοντος, με την ενσωμάτωση εργαλείων γονικού ελέγχου και ασφαλών ρυθμίσεων.

Επιπλέον, το μάθημα αναγνωρίζει ότι η ψηφιακή ενδυνάμωση δεν αφορά μόνο την ασφάλεια, αλλά και την ανάπτυξη των δεξιοτήτων που επιτρέπουν στους χρήστες να συμμετέχουν ενεργά στον ψηφιακό κόσμο. Η χρήση προηγμένων εργαλείων ασφαλείας, όπως ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) και οι εικονικά ιδιωτικά δίκτυα (VPN), βοηθά τους εκπαιδευόμενους να προστατεύουν τις προσωπικές τους πληροφορίες και να απολαμβάνουν τις ευκαιρίες που προσφέρει το διαδίκτυο χωρίς φόβο. Σε μια εποχή που το ψηφιακό χάσμα παραμένει σημαντικό, ιδιαίτερα για τις ευάλωτες ομάδες, αυτό το μάθημα απαντά στην ανάγκη για ολιστική εκπαίδευση στις βασικές ψηφιακές δεξιότητες και την κυβερνοασφάλεια. Με την εστίαση στην πρακτική εφαρμογή των γνώσεων και την ενδυνάμωση των συμμετεχόντων, το μάθημα "Ψηφιακή Ενδυνάμωση Ενηλίκων" συμβάλλει καθοριστικά στην καλλιέργεια ενός ψηφιακά ενήμερου και ασφαλούς κοινού.

Κεφάλαιο 3. Σχεδίαση του διαδικτυακού μαθήματος Ψηφιακή Ενδυνάμωση Ενηλίκων: Στρατηγικές για την Προαγωγή της Ασφαλούς Πλοήγησης στο Διαδίκτυο

3.1 Αξιοποίηση Μαζικών Ανοικτών Διαδικτυακών Μαθημάτων (MOOC) για την Ανάπτυξη Προσωπικών Ικανοτήτων

Η αξιοποίηση των Μαζικών Ανοικτών Διαδικτυακών Μαθημάτων (MOOC) ως εκπαιδευτική μέθοδος για την ανάπτυξη προσωπικών ή επαγγελματικών ικανοτήτων έχει γνωρίσει μεγάλη απήχηση τα τελευταία χρόνια, λόγω της ευελιξίας και της προσβασιμότητας που προσφέρει (Pappas, 2016). Παρακάτω αναλύονται τα κύρια πλεονεκτήματα, καθώς και οι προκλήσεις αυτής της εκπαιδευτικής προσέγγισης.

Πλεονεκτήματα:

- Ευελιξία και Προσβασιμότητα:
  Τα MOOC προσφέρουν την ευκαιρία για μάθηση οποτεδήποτε και από οπουδήποτε, κάνοντας τα προσιτά σε άτομα με διαφορετικά προγράμματα και υποχρεώσεις. Αυτό επιτρέπει την ανάπτυξη δεξιοτήτων παράλληλα με εργασία ή άλλες υποχρεώσεις (Bruck, Motiwalla, & Foerster, 2012). Πολλοί οργανισμοί προσφέρουν MOOC σε διάφορες γλώσσες, καθιστώντας τα διαθέσιμα σε παγκόσμιο επίπεδο, ανεξαρτήτως γεωγραφικών περιορισμών (Pappas, 2016).
- Χαμηλό Κόστος ή Δωρεάν Μαθήματα:
  Πολλά MOOC προσφέρονται δωρεάν ή με πολύ χαμηλό κόστος, διευκολύνοντας την πρόσβαση στην εκπαίδευση ακόμα και για εκείνους που δεν έχουν τα οικονομικά μέσα να παρακολουθήσουν παραδοσιακά εκπαιδευτικά ιδρύματα (Pappas, 2016).
- Ποικιλία Θεματικών Πεδίων:
  Υπάρχει τεράστια ποικιλία μαθημάτων που καλύπτουν ένα ευρύ φάσμα θεμάτων, από τεχνικές δεξιότητες όπως προγραμματισμός και ανάλυση δεδομένων, μέχρι προσωπικές δεξιότητες όπως ηγεσία, διαχείριση χρόνου και επικοινωνία (Hug, 2005).
- Αυτονομία στη Μάθηση:
  Οι μαθητές μπορούν να προχωρούν με τον δικό τους ρυθμό, δίνοντάς τους τη δυνατότητα να εστιάσουν σε θέματα που τους ενδιαφέρουν περισσότερο ή να επαναλάβουν υλικό που χρειάζεται περισσότερη κατανόηση (Leong, 2016).
- Διεθνοποιημένη Μάθηση:
  Μέσω των MOOC, οι μαθητές έχουν την ευκαιρία να αλληλεπιδρούν με άτομα από διαφορετικές χώρες και πολιτισμούς, διευρύνοντας τις απόψεις και τις αντιλήψεις τους σε διεθνή ζητήματα (Pappas, 2016).
- Επαγγελματική Αναγνώριση:
  Ορισμένα MOOC προσφέρουν πιστοποιήσεις που αναγνωρίζονται από μεγάλους οργανισμούς και εταιρείες, παρέχοντας επιπλέον επαγγελματικές ευκαιρίες και ενισχύοντας τα βιογραφικά (Bruck et al., 2012).

  Προκλήσεις:

- Έλλειψη Προσωπικής Επαφής:

Ένα από τα βασικά μειονεκτήματα των MOOC είναι η έλλειψη άμεσης επικοινωνίας και αλληλεπίδρασης με τους καθηγητές και τους συμφοιτητές, κάτι που μπορεί να οδηγήσει σε περιορισμένη υποστήριξη και δυσκολίες στην επίλυση αποριών (Leong, 2016).

- Αυτοπειθαρχία και Αυτοπαρακίνηση:
  Η επιτυχής ολοκλήρωση ενός MOOC απαιτεί αυτοπειθαρχία και αυτοπαρακίνηση, καθώς η ευελιξία μπορεί να προκαλέσει αναβλητικότητα. Πολλοί μαθητές εγκαταλείπουν τα μαθήματα λόγω έλλειψης δέσμευσης ή λόγω του ότι δεν υπάρχει κάποια καθοδήγηση όπως στα παραδοσιακά εκπαιδευτικά περιβάλλοντα (Pappas, 2016).
- Ποιότητα Εκπαίδευσης:
  Παρόλο που πολλά MOOC προσφέρουν υψηλής ποιότητας υλικό, η ποιότητα μπορεί να διαφέρει σημαντικά ανάμεσα στις διαφορετικές πλατφόρμες ή εκπαιδευτές. Δεν είναι όλα τα μαθήματα κατάλληλα για κάθε επίπεδο γνώσης (Bruck et al., 2012).
- Έλλειψη Άμεσης Πρακτικής Εφαρμογής:
  Ορισμένα μαθήματα μπορεί να είναι πιο θεωρητικά και να μην προσφέρουν ευκαιρίες για άμεση πρακτική εφαρμογή, κάτι που μπορεί να είναι κρίσιμο για την ανάπτυξη συγκεκριμένων επαγγελματικών ικανοτήτων, όπως για παράδειγμα σε τεχνικά πεδία (Leong, 2016).
- Χαμηλά Ποσοστά Ολοκλήρωσης:
  Τα στατιστικά δείχνουν ότι το ποσοστό ολοκλήρωσης στα MOOC είναι συχνά χαμηλό, με πολλούς μαθητές να μην καταφέρνουν να φτάσουν μέχρι το τέλος του μαθήματος, είτε λόγω αναβλητικότητας είτε λόγω του ότι το περιεχόμενο δεν ανταποκρίνεται στις προσδοκίες τους (Hug, 2005).

Τα MOOC αποτελούν ένα ισχυρό εργαλείο για την ανάπτυξη προσωπικών και επαγγελματικών ικανοτήτων, προσφέροντας σημαντικά πλεονεκτήματα όπως ευελιξία, προσβασιμότητα, και χαμηλό κόστος. Ωστόσο, οι προκλήσεις που σχετίζονται με την έλλειψη προσωπικής καθοδήγησης και τη δέσμευση απαιτούν αυτοπειθαρχία και προσεκτική επιλογή των μαθημάτων. Εάν χρησιμοποιηθούν σωστά, τα MOOC μπορούν να αποτελέσουν ένα σημαντικό μέσο για τη συνεχή μάθηση και την επαγγελματική ανάπτυξη (Pappas, 2016).

3.2 Επιλογή της μικρο-μάθησης για την σχεδίαση του διαδικτυακού μαθήματος

Η μικρο-μάθηση (microlearning) είναι μια σύγχρονη εκπαιδευτική προσέγγιση που επικεντρώνεται στη μάθηση μέσω μικρών, συνοπτικών και εύπεπτων μονάδων γνώσης. Η επιλογή αυτής της μεθόδου για τη σχεδίαση ενός διαδικτυακού μαθήματος (MOOC) μπορεί να είναι ιδιαίτερα αποτελεσματική και να ευθυγραμμίζεται με τις ανάγκες των σύγχρονων μαθητών (Bruck, Motiwalla, & Foerster, 2012). Παρακάτω παρατίθενται οι λόγοι που υποστηρίζουν την αξιοποίηση της μικρο-μάθησης για τον σχεδιασμό ενός MOOC.

Πλεονεκτήματα της Μικρο-Μάθησης:

- Σύντομες Μονάδες Μάθησης:

Η μικρο-μάθηση προσφέρει σύντομα, στοχευμένα μαθήματα που είναι εύκολο να καταναλωθούν σε μικρό χρονικό διάστημα. Αυτό επιτρέπει στους μαθητές να ενσωματώσουν τη μάθηση στο καθημερινό τους πρόγραμμα, χωρίς να απαιτείται πολύς χρόνος ή αφοσίωση σε κάθε συνεδρία. Αυτό είναι ιδιαίτερα σημαντικό για επαγγελματίες ή πολυάσχολους μαθητές που έχουν περιορισμένο χρόνο (Leong, 2016).

- Εστίαση σε Συγκεκριμένες Δεξιότητες ή Γνώσεις:
  Η μικρο-μάθηση επιτρέπει την εστίαση σε συγκεκριμένα σημεία γνώσης ή δεξιοτήτων, κάτι που κάνει τη μάθηση πιο αποτελεσματική. Οι μαθητές μπορούν να επιλέξουν τα πιο σχετιζόμενα με αυτούς μαθήματα και να εφαρμόσουν άμεσα τις γνώσεις που αποκτούν (Hug, 2005).
- Ενίσχυση της Διατήρησης της Γνώσης:
  Μελέτες δείχνουν ότι η μάθηση σε μικρά τμήματα βοηθά στη βελτίωση της διατήρησης της γνώσης. Τα σύντομα και στοχευμένα μαθήματα ενισχύουν την επανάληψη και την εμπέδωση του υλικού, κάτι που επιτρέπει στους μαθητές να θυμούνται καλύτερα αυτά που έμαθαν (Leong, 2016).
- Ευελιξία και Προσαρμοστικότητα:
  Η μικρο-μάθηση δίνει τη δυνατότητα στους μαθητές να προσαρμόσουν το ρυθμό μάθησης στις δικές τους ανάγκες και ικανότητες. Μπορούν να προχωρήσουν γρήγορα μέσα από υλικό που ήδη γνωρίζουν ή να επαναλάβουν μονάδες που απαιτούν περισσότερη προσοχή (Pappas, 2016).
- Κατάλληλη για Κινητές Συσκευές:
  Η μικρο-μάθηση είναι απόλυτα συμβατή με την τάση χρήσης κινητών συσκευών. Οι μικρές εκπαιδευτικές μονάδες μπορούν εύκολα να παραδοθούν και να καταναλωθούν μέσω smartphones ή tablets, καθιστώντας τη διαδικασία μάθησης πιο προσβάσιμη και ευέλικτη (Bruck et al., 2012).
- Αύξηση Κινητοποίησης και Δέσμευσης:
  Τα σύντομα μαθήματα αποτρέπουν τη μονοτονία και την εξάντληση των μαθητών, αυξάνοντας τη συμμετοχή και τη δέσμευση στη μαθησιακή διαδικασία. Οι μαθητές αισθάνονται πιο κινητοποιημένοι όταν βλέπουν γρήγορα αποτελέσματα και ολοκληρώνουν μικρά βήματα προς τον στόχο τους (Pappas, 2016).

Προκλήσεις της Μικρο-Μάθησης:

- Δυσκολία Σύνθεσης Ολοκληρωμένων Ιδεών:
  Παρά τα πλεονεκτήματα της μικρο-μάθησης, υπάρχει ο κίνδυνος η κατακερματισμένη γνώση να δυσκολεύει την ολοκληρωμένη κατανόηση μεγάλων εννοιών ή περίπλοκων θεμάτων. Η μικρο-μάθηση δεν είναι ιδανική για θέματα που απαιτούν εις βάθος ανάλυση και σύνθετη σκέψη (Hug, 2005).
- Πιθανή Έλλειψη Συνέχειας:
  Επειδή οι μονάδες μικρο-μάθησης είναι ανεξάρτητες, μπορεί να υπάρχει έλλειψη συνέχειας ανάμεσα σε αυτές, κάτι που μπορεί να προκαλέσει ασυνέπεια στην εξέλιξη της γνώσης αν δεν σχεδιαστούν προσεκτικά (Leong, 2016).
- Απαιτήσεις Σχεδιασμού Υψηλής Ποιότητας:

Ο σχεδιασμός ενός μαθήματος μικρο-μάθησης απαιτεί προσοχή ώστε να παρέχει σημαντικές πληροφορίες με συνοπτικό και αποτελεσματικό τρόπο. Απαιτεί επίσης σαφή δομή και καλή οργάνωση του περιεχομένου, για να μην χαθεί η ουσία μέσα από την πολυδιάσπαση (Pappas, 2016).

Η μικρο-μάθηση είναι μια ισχυρή προσέγγιση για τη σχεδίαση διαδικτυακών μαθημάτων (MOOC), καθώς επιτρέπει τη μάθηση με τρόπο που προσαρμόζεται στις ανάγκες των μαθητών και τις σύγχρονες συνθήκες ζωής. Προσφέρει ευελιξία, αυξημένη δέσμευση και καλύτερη διατήρηση της γνώσης, ενώ είναι ιδιαίτερα κατάλληλη για επαγγελματίες και άτομα με περιορισμένο χρόνο. Ωστόσο, η προσεκτική δομή του μαθήματος είναι απαραίτητη για την αποφυγή της κατακερματισμένης και ασυνεχούς γνώσης Pappas, 2016).

3.3 Μαθησιακά Αποτελέσματα του Μαθήματος.

Τίτλος micro-MOOC : Ψηφιακή Ενδυνάμωση Ενηλίκων: Ασφαλής Πλοήγηση στο Διαδίκτυο

Το MOOC αυτό συνδέεται με την απόκτηση βασικών ικανοτήτων σε βασικές περιοχές του DigComp 2.2[1], όπως παρουσιάζονται στον πίνακα παρακάτω:

Πίνακας 8: Μαθησιακά Αποτελέσματα

Τίτλος Μικρο-μαθημάτων	**Μαθησιακό Αποτέλεσμα 1**	**Μαθησιακό Αποτέλεσμα 2**	**Σύνδεση με StandardCompetence Frameworks ή Προγράμματα Σπουδών**
Μικρο-μάθημα 1: Βασικές Αρχές Ψηφιακής Ασφάλειας	Ο εκπαιδευόμενος θα είναι σε θέση να αναγνωρίζει και να αξιολογεί τους κινδύνους και τις απειλές που σχετίζονται με τη χρήση του διαδικτύου, όπως το ηλεκτρονικό "ψάρεμα" (phishing), το κακόβουλο λογισμικό και η παραπληροφόρηση.	Ο εκπαιδευόμενος θα είναι σε θέση να δημιουργεί ισχυρούς κωδικούς πρόσβασης, να τους διαχειρίζεται με ασφάλεια και να προστατεύει τα προσωπικά του δεδομένα στο διαδίκτυο.	DigComp 2.1Αλληλοεπιδρώ μέσω ψηφιακών Τεχνολογιών DigComp 1.2Αξιολογώ δεδομένα, πληροφορίες και ψηφιακό περιεχόμενο DigComp 5.3Χρησιμοποιώ δημιουργικά τις ψηφιακές τεχνολογίες

[1] DigComp 2.2 - Το ευρωπαϊκό πλαίσιο για την ψηφιακή ικανότητα των πολιτών

Μικρο-μάθημα 2: Ασφαλείς Συναλλαγές και Αγορές	Ο εκπαιδευόμενος θα είναι σε θέση να πραγματοποιεί ασφαλείς ηλεκτρονικές συναλλαγές και αγορές, χρησιμοποιώντας αξιόπιστες μεθόδους πληρωμής και αναγνωρίζοντας αξιόπιστα ηλεκτρονικά καταστήματα.	Ο εκπαιδευόμενος θα είναι σε θέση να αναγνωρίζει και να αποφεύγει διαδικτυακές απάτες, όπως η κλοπή ταυτότητας και οι ψεύτικες προσφορές.	DigComp 2.1 Αλληλοεπιδρώ μέσω ψηφιακών τεχνολογιών DigComp 2.2 Χρησιμοποιώ από κοινού πληροφορίες και περιεχόμενο, μέσω ψηφιακών τεχνολογιών DigComp 5.4 Προσδιορίζω κενά στην ψηφιακή ικανότητα
Μικρο-μάθημα 3: Υπεύθυνη Χρήση Κοινωνικών Δικτύων	Ο εκπαιδευόμενος θα είναι σε θέση να διαχειρίζεται αποτελεσματικά την παρουσία του στα κοινωνικά δίκτυα, προσαρμόζοντας τις ρυθμίσεις απορρήτου και προστατεύοντας τη διαδικτυακή του φήμη.	Ο εκπαιδευόμενος θα είναι σε θέση να αναγνωρίζει και να αντιμετωπίζει τη διαδικτυακή παρενόχληση (cyberbullying), προωθώντας την ευγένεια και τον σεβασμό στο διαδικτυακό περιβάλλον.	DigComp 2.1 Αλληλοεπιδρώ μέσω ψηφιακών τεχνολογιών DigComp 2.2 Αξιολογώ δεδομένα, πληροφορίες και ψηφιακό περιεχόμενο DigComp 2.3 Χρησιμοποιώ δημιουργικά τις ψηφιακές τεχνολογίες
Μικρο-μάθημα 4: Προστασία Παιδιών και Οικογένειας στο Διαδίκτυο	Ο εκπαιδευόμενος θα είναι σε θέση να αναγνωρίζει τους κινδύνους που αντιμετωπίζουν τα παιδιά στο διαδίκτυο και να εφαρμόζει κατάλληλα μέτρα προστασίας, όπως εργαλεία γονικού	Ο εκπαιδευόμενος θα είναι σε θέση να δημιουργεί ένα ασφαλές και υποστηρικτικό διαδικτυακό περιβάλλον για την οικογένειά του, ενθαρρύνοντας την ανοιχτή επικοινωνία	DigComp 2.1 Αλληλοεπιδρώ μέσω ψηφιακών Τεχνολογιών DigComp 2.4Συμπράττω μέσω ψηφιακών τεχνολογιών

	ελέγχου και ασφαλείς ρυθμίσεις στις συσκευές.	και την εκπαίδευση σχετικά με την ασφαλή χρήση του διαδικτύου.	DigComp 5.2 Προσδιορίζω ανάγκες και τεχνολογικές λύσεις

3.4 Σχεδίαση του Μαζικού Ανοικτού Διαδικτυακού Μαθήματος

3.4.1 Γενικές πληροφορίες

Τίτλος micro-MOOC
Ψηφιακή Ενδυνάμωση Ενηλίκων: Ασφαλής Πλοήγηση στο Διαδίκτυο

Δημιουργός micro-MOOC
Ελένη Καλογεροπούλου

Συνοπτική Περιγραφή micro-MOOC
Το διαδίκτυο έχει μεταμορφώσει τον τρόπο που επικοινωνούμε, μαθαίνουμε, εργαζόμαστε και διασκεδάζουμε. Ωστόσο, αυτή η ψηφιακή επανάσταση συνοδεύεται και από προκλήσεις. Από την προστασία των προσωπικών μας δεδομένων μέχρι την αποφυγή διαδικτυακών απατών και την υπεύθυνη χρήση των κοινωνικών μέσων, η ασφαλής πλοήγηση στο διαδίκτυο απαιτεί γνώση και επαγρύπνηση. Το μάθημα "Ψηφιακή Ενδυνάμωση Ενηλίκων: Ασφαλής Πλοήγηση στο Διαδίκτυο" έχει σχεδιαστεί για να σας εξοπλίσει με τις απαραίτητες δεξιότητες και γνώσεις ώστε να αξιοποιήσετε στο έπακρο τις δυνατότητες του διαδικτύου, διασφαλίζοντας παράλληλα την ασφάλεια και την ιδιωτικότητά σας.
Στο τέλος αυτού του μαθήματος, θα είστε σε θέση να πλοηγήστε στο διαδίκτυο με αυτοπεποίθηση και ασφάλεια, έχοντας αποκτήσει τις απαραίτητες ψηφιακές δεξιότητες για να συμμετέχετε ενεργά στην ψηφιακή κοινωνία.

Διάρκεια micro-MOOC
Το πρόγραμμα διαρκεί 14 ώρες και μπορεί να ολοκληρωθεί σε 6 ημέρες.

Αξιολόγηση micro-MOOC
Εργαλείο Αξιολόγησης 1: Αυτοαξιολόγηση με τη χρήση εργασίας ανοιχτής απάντησης – Open Response Assessment (ORA), που βαθμολογεί ο ίδιος ο εκπαιδευόμενος με τη βοήθεια ρουμπρίκας. Στο τέλος κάθε μικρο-Μαθήματος, υπάρχει πάντα μία τέτοια εργασία ανοικτής απάντησης – Αυτοαξιολογεί ΜΑ1 , ΜΑ2 , ΜΑ3 και ΜΑ4.
Εργαλείο Αξιολόγησης 2: Αυτοαξιολόγηση – Για την αυτοαξιολόγηση έχουν επιλεγεί quizzes διαφόρων τύπων, όπως Multiple Choice Questions (MCQs)]

[Multiple Choice Questions (MCQs).Δίνονται ερωτήσεις πολλαπλών επιλογών– 2.1.4, 2.2.4, 3.1.4, 3.2.4, 4.1.4, 4.2.4, 5.1.4 και 5.2.4 για την αυτοαξιολόγηση των μαθησιακών στόχων που τους αντιστοιχούν.

Εργαλείο Αξιολόγησης 3: Τελική Αξιολόγηση - Ερωτήσεις Πολλαπλής Επιλογής (Multiple Choice Questions, MCQs) που βασίζονται σε πολύπλοκες ερωτήσεις κρίσης, έτσι ώστε να αξιολογούνται η κατανόηση και οι δεξιότητες των εκπαιδευομένων.- Αξιολογεί όλα τα ΜΑ.

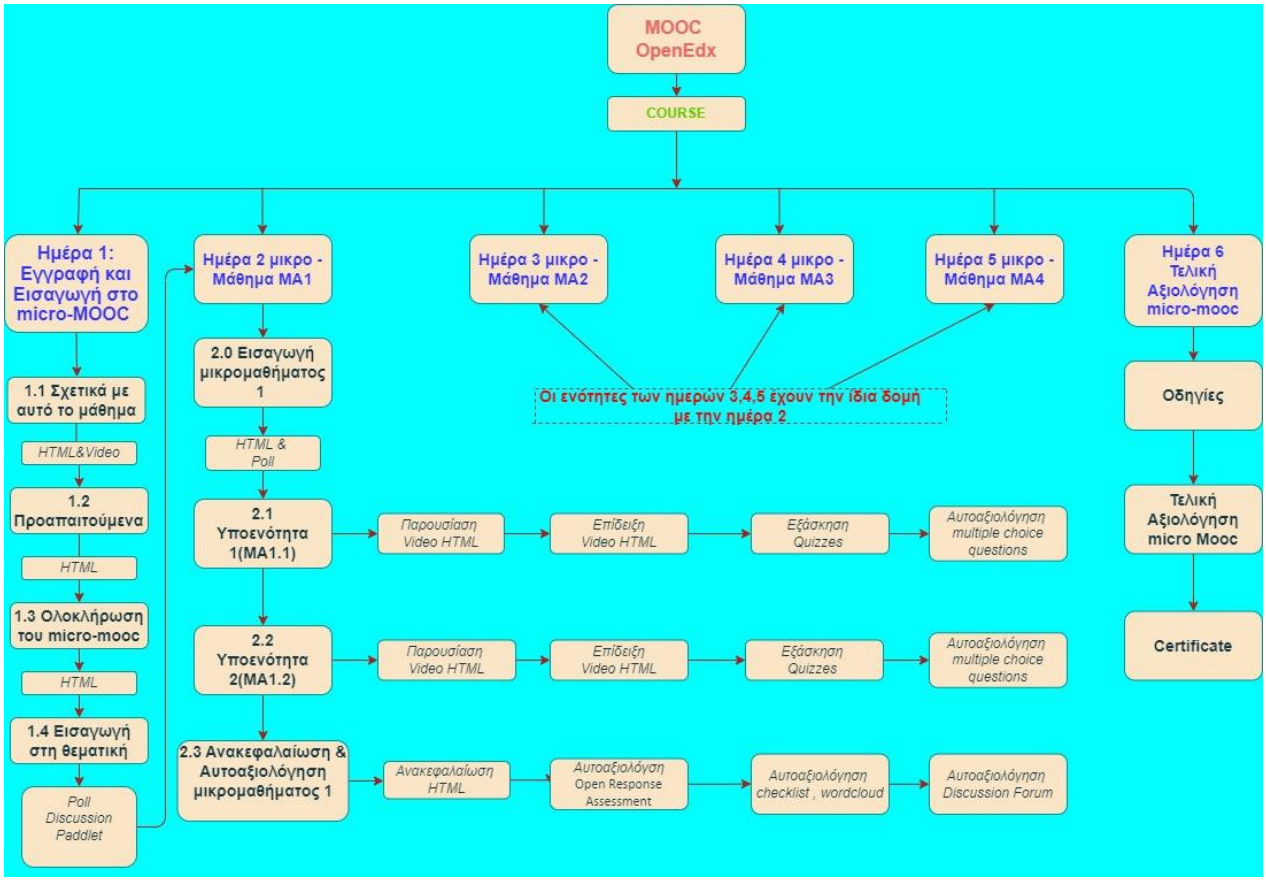
Προαπαιτούμενες Ικανότητες Εκπαιδευομένων

Η σύνδεση των μαθησιακών αποτελεσμάτων με το πλαίσιο ψηφιακών ικανοτήτων DigComp2.2 ορίζει και τις προαπαιτούμενες ικανότητες των εκπαιδευομένων ως εξής:

Ο/Η εκπαιδευόμενος/η θα πρέπει με καθοδήγηση να μπορεί στοιχειωδώς να:

- κρίνει την ακρίβεια και την καταλληλότητα των πληροφοριών. (Ψηφιακή Ικανότητα : 1.2 Αξιολόγηση δεδομένων, πληροφοριών και ψηφιακού περιεχομένου)
- χρησιμοποιεί ψηφιακές τεχνολογίες για να επικοινωνεί με άλλους. (Ψηφιακή Ικανότητα : 2.1 Αλληλεπίδραση μέσω ψηφιακών τεχνολογιών)
- κοινοποιεί δεδομένα, πληροφορίες και περιεχόμενο με άλλους μέσω ψηφιακών τεχνολογιών. (Ψηφιακή Ικανότητα : 2.2 Κοινοποίηση μέσω ψηφιακών τεχνολογιών)
- συνεργάζεται με άλλους χρησιμοποιώντας ψηφιακές τεχνολογίες και εργαλεία. (Ψηφιακή Ικανότητα : 2.3 Συνεργασία μέσω ψηφιακών τεχνολογιών)
- χρησιμοποιεί ψηφιακές υπηρεσίες για συμμετοχή στην κοινωνία (π.χ. σε δημόσιες ή κοινωνικές διαδικασίες).((Ψηφιακή Ικανότητα : 2.4 Ηλεκτρονική συμμετοχή)
- επιλέγει απλούς τρόπους ρύθμισης και προσαρμογής των ψηφιακών περιβαλλόντων στις προσωπικές του ανάγκες (Ψηφιακή Ικανότητα : 5.2 Προσδιορίζω ανάγκες και τεχνολογικές λύσεις)
- δείχνει ενδιαφέρον ατομικά και συλλογικά για συμμετοχή σε απλές γνωστικές διαδικασίες κατανόησης και αποσαφήνισης απλών εννοιολογικών προβλημάτων και προβληματικών καταστάσεων σε ψηφιακά περιβάλλοντα (Ψηφιακή Ικανότητα : 5.3 Χρησιμοποιώ δημιουργικά τις ψηφιακές τεχνολογίες)

3.4.2.Γραφική αναπαράσταση εκπαιδευτικού σχεδιασμού micro-MOOC



Εικόνα 1: Γραφική αναπαράσταση micro-MOOC

.

3.4.3 Περιγραφή του Εκπαιδευτικού σχεδιασμού του micro-MOOC

Ακολουθεί αναλυτικά η περιγραφή του εκπαιδευτικού σχεδιασμού αυτού του μαθήματος.[2]

Πίνακας 9 Περιγραφή Εκπαιδευτικού Σχεδιασμού micro-MOOC

ID Δραστηριότητας [ACT_ID]	Περιγραφή Εκπαιδευτικής Δραστηριότητας	Ψηφιακές Τεχνολογίες	Εκτίμηση Ενδεικτικής Χρονικής Διάρκειας Εκπαιδευτικής Δραστηριότητας (σε λεπτά)	Σύνδεση με Μαθησιακά Αποτελέσματα
Ημέρα 1: Εγγραφή και Εισαγωγή στο micro-MOOC (60')				
1.1	Σχετικά με αυτό το μάθημα (15')			
1.1.1	**[Παρουσίαση]** Καλωσόρισμα https://youtube.com/shorts/ZB54FE17t_A?si=30a40xDq7CtNuqCL *Εισαγωγικό βίντεο καλωσορίσματος στο μάθημα.*	βίντεο	1'	-

[2] Ο πίνακας που χρησιμοποιείται για την ανάπτυξη του εκπαιδευτικού σχεδιασμού βασίζεται στην εργασία 4 του μαθήματος ΨΣ-ΗΜ-721 του μεταπτυχιακού προγράμματος «Ηλεκτρονική Μάθηση».

1.1.2	**[Παρουσίαση]** Εισαγωγή -Σκοπός *Σελίδα κειμένου που παρουσιάζει το σκοπό του μαθήματος (το μάθημα εισάγει την έννοια/συζητά/ αναγνωρίζει/ παρουσιάζει/ τονίζει κλπ)*	Υπερκείμενο και εικόνα	2'	-
1.1.3	**[Παρουσίαση]** Μαθησιακά Αποτελέσματα micro-MOOC Συνολικά *Σελίδα κειμένου που παρουσιάζει τα Μαθησιακά Αποτελέσματα του micro-MOOC συνολικά*	Υπερκείμενο	5'	-
1.1.4	**[Παρουσίαση]** Δομή του micro-MOOC *Σελίδα κειμένου που παρουσιάζει τη δομή του micro-MOOC*	Υπερκείμενο	3'	
1.1.5	**[Παρουσίαση]** Άδεια χρήσης micro-MOOC *Σελίδα κειμένου που παρουσιάζει την άδεια χρήσης του micro-MOOC*	Υπερκείμενο και εικόνα	2'	
1.1.6	**[Παρουσίαση]** Δημιουργός του micro-MOOC *Σελίδα κειμένου που παρουσιάζει το δημιουργό με σύντομο CV και φωτογραφία*	Υπερκείμενο και εικόνα	2'	
1.2	**Προαπαιτούμενα (6')**			
1.2.1	**[Παρουσίαση]** Προαπαιτούμενες Γνώσεις και Δεξιότητες	Υπερκείμενο	5'	

	Σελίδα κειμένου που παρουσιάζει τις προαπαιτούμενες γνώσεις και δεξιότητες για την συμμετοχή στο micro-MOOC			
1.2.2	**[Παρουσίαση]** Ελάχιστες Απαραίτητες Υποδομές για την συμμετοχή στο micro-MOOC *Σελίδα κειμένου που παρουσιάζει τις Ελάχιστες Απαραίτητες Υποδομές για την συμμετοχή στο micro-MOOC*	Υπερκείμενο	1'	
1.3	**Ολοκλήρωση του μαθήματος (10')**			
1.3.1	**[Παρουσίαση]** Απαραίτητες ενέργειες *Σελίδα κειμένου που παρουσιάζει τις απαραίτητες ενέργειες για την ολοκλήρωση του micro-MOOC και παρακολούθηση της προόδου*	Υπερκείμενο	2'	
1.3.2	**[Παρουσίαση]** Εργασίες αυτοαξιολόγησης ενοτήτων του Micro-MOOC *Σελίδα κειμένου που περιγράφει τα εργαλεία αυτοαξιολόγησης του micro-MOOC*	Υπερκείμενο	3'	
1.3.3	**[Παρουσίαση]** Συμμετοχή στο forum *Σελίδα κειμένου με τους κανόνες του Netiquette για τη συμμετοχή στο forum*	Υπερκείμενο	5'	

1.3.4	**[Παρουσίαση]** Τελική εξέταση του Micro-MOOC *Σελίδα κειμένου με την περιγραφή της τελικής εξέτασης του micro-MOOC*	Υπερκείμενο	2’	
1.4	**Εισαγωγή στη θεματική του micro-MOOC (29’)**			
1.4.1	**[Poll]** Επίπεδο εξοικείωσης με την ασφάλεια στο διαδίκτυο *Poll activity* **[Discussion Forum]** Συζήτηση στο forum για το επίπεδο εξοικείωσης *Forum*	Poll & Forum	7’	
1.4.2	**[Video]** Άποψη Ειδικού *https://www.youtube.com/watch?v=XFn7iN_hrQo* [13:35] *Εξωτερικό υπάρχον video από το YouTube που παρουσιάζει έναν ειδικό για το θέμα που πραγματεύεται το micro-MOOC*	βίντεο	15’	
1.4.3	[Padlet]Δραστηριότητα γνωριμίας με χρήση padlet	Padlet	7’	

Ημέρα 2: Μικρο-μάθημα 1 – Βασικές Αρχές Ψηφιακής Ασφάλειας (≈3 ώρες)				
2.0	**Εισαγωγή Μικρο-μαθήματος 1 Βασικές Αρχές Ψηφιακής Ασφάλειας (10')**			
2.0.1	**[Παρουσίαση]** Μαθησιακά Αποτελέσματα Θεματικής Ενότητας 1 **(ΜΑ-1)** + **[Poll]** *Σελίδα κειμένου που παρουσιάζει τα επιμέρους μαθησιακά αποτελέσματα της ενότητας* *3 Polls για την αυτοαξιολόγηση της πρότερης γνώσης για τη θεματική της ενότητας.*	Υπερκείμενο, Poll	8'	
2.0.2	**[Παρουσίαση]** Δομή της ενότητας 1 *Σελίδα κειμένου που παρουσιάζει τη δομή της ενότητας 1*	Υπερκείμενο	2'	
2.1	**1η υπο-ενότητα :Κίνδυνοι και απειλές που σχετίζονται με τη χρήση του διαδικτύου (60')**			
2.1.1	**[Παρουσίαση]** Ενότητας 1.1 Cyber Threats 101: How Phishing, Malware, & Ransomware Could Be Targeting You [5:36] https://youtu.be/mcII64WbQoI?si=1Gwybx2lPcHHrt13 *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	10'	**ΜΑ1.1** Να αναγνωρίζω και να αξιολογώ τους κινδύνους και τις απειλές που σχετίζονται με τη χρήση του διαδικτύου, όπως το ηλεκτρονικό "ψάρεμα"
2.1.2	**[Επίδειξη]** Ενότητας 1.1 What is Phishing and How to Protect Yourself from it? [3:15] https://youtu.be/qdpReVgpQhc?si=ycuSkMKjb8nfLupR How to Prevent Malware[3:11] https://youtu.be/owGqhRc3AfA?si=nGUQRJrdU-dLcUtI	Υπερκείμενο και βίντεο	20'	

	Διαδίκτυο - Παραπληροφόρηση - Ψευδείς Ειδήσεις[3:06] https://youtu.be/mP4H7XAb9VA?si=DU1rXGdsoFT_cQa *Σελίδα κειμένου και βίντεο από το Youtube*			(phishing), το κακόβουλο λογισμικό και η παραπληροφόρηση.
2.1.3	**[Εξάσκηση]** Ενότητας 1.1 Δραστηριότητα εξάσκησης με 5 ερωτήσεις σωστού - λάθους.	quizzes	15’	
2.1.4	**[Αυτοαξιολόγηση]** Ενότητας 1.1 Δραστηριότητα αυτοαξιολόγησης με 5 ερωτήσεις πολλαπλής επιλογής	multiple choice questions	15’	
2.2	**2η υπο-ενότητα: Δημιουργία ισχυρών κωδικών πρόσβασης και προστασία προσωπικών δεδομένων στο διαδίκτυο. (45’)**			
2.2.1	**[Παρουσίαση]** Ενότητας 1.2 Strong Passwords [1:46] https://youtu.be/9LxdtaSvQ3I?si=eG75XurVKagQiGEh Private and Personal Information[1:36] https://youtu.be/MjPpG2e71Ec?si=VFwPmURGowc2MhDy What can happen to your personal data online?[0:55] https://youtu.be/v4IIH3sJIMc?si=_hilq8ea8OZDQNas *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	5’	**ΜΑ1.2** Να δημιουργώ ισχυρούς κωδικούς πρόσβασης, να τους διαχειρίζομαι με ασφάλεια και να προστατεύω τα προσωπικά μου
2.2.2	**[Επίδειξη]** Ενότητας 1.2	Υπερκείμενο και βίντεο	10’	

	How To Create Strong and Memorable Passwords[3:22] https://youtu.be/3fou-vw58A0?si=rft76p2-Pc44HFTq How to Protect Personal information Online [1:55] https://youtu.be/fTBVlVLNJWQ?si=krCUi7Cv26MK9qIt Think Before Your Share [1:54] https://youtu.be/2GeakIPfu54?si=DiDmUPc4Ixaf6s6A *Σελίδα κειμένου και βίντεο από το Youtube*			δεδομένα στο διαδίκτυο.
2.2.3	**[Εξάσκηση]** Ενότητας 1.2 Δραστηριότητα εξάσκησης με 5 ερωτήσεις σωστού - λάθους.	quizzes	15’	
2.2.4	**[Αυτο-Αξιολόγηση]** Ενότητας 1.2 Δραστηριότητα αυτοαξιολόγησης με 5 ερωτήσεις πολλαπλής επιλογής	multiple choice questions	15’	
2.3	**Ανακεφαλαίωση και Αυτό-Αξιολόγηση Μικρο-μαθήματος 1 (60’)**			
2.3.1	**[Παρουσίαση]** Ανακεφαλαίωση Θεματικής Ενότητας (Μικρο-Μάθημα) 1 *Σελίδα κειμένου που συνοψίζει το Μικρο-Μάθημα 1*	Υπερκείμενο	10'	MA-1
2.3.2	**[Αυτό-αξιολόγηση] Εργασία: Open Response Assessment** Εργασία αυτοαξιολόγησης της ικανότητας MA-1 με βάση	Open Response Assessment	30’	

	ρουμπρίκα			
2.3.3	**[Αυτοαξιολόγηση] Checklist: Μπορώ να το κάνω…** Checklist με : «μπορώ να το κάνω» προτάσεις WordCloud Χρήση του word cloud tool για τη συλλογή σύντομων απαντήσεων σε εύκολες ερωτήσεις που συνοψίζουν το βασικό θέμα της μικρο-μαθήματος.	Checklist, WordCloud	10’	
2.3.4	**[Discussion Forum]** Μια συζήτηση στο forum με ανάπυξη απόψεων πάνω στο θέμα της ενότητας 1.	Discussion Forum	10’	
2.4	**Προτάσεις για επιπλέον εκπαίδευση στο θέμα του Μικρο-μαθήματος 1**			
	[Προτάσεις για Επιπλέον Εκπαίδευση] https://www.getsafeonline.org/ https://www.sternsecurity.com/blog/stay-safe-online/	Υπερκείμενο		
Ημέρα 3: Μικρο-μάθημα 2 - Ασφαλείς Συναλλαγές και Αγορές (≈3 ώρες)				
3.0	**Εισαγωγή Μικρο-μαθήματος 2 Ασφαλείς Συναλλαγές και Αγορές (10’)**			
3.0.1	**[Παρουσίαση]** Μαθησιακά Αποτελέσματα Θεματικής Ενότητας 2 **(ΜΑ-1)** + **[Poll]** *Σελίδα κειμένου που παρουσιάζει τα επιμέρους μαθησιακά αποτελέσματα της ενότητας* *3 Polls για την αυτοαξιολόγηση της πρότερης γνώσης για τη θεματική της ενότητας.*	Υπερκείμενο, Poll	8'	
3.0.2	**[Παρουσίαση]** Δομή της ενότητας 2 *Σελίδα κειμένου που παρουσιάζει τη δομή της ενότητας 2*	Υπερκείμενο	2'	
3.1	**1η υπο-ενότητα: Πραγματοποίηση ασφαλών συναλλαγών και αγορών (45’)**			

3.1.1	**[Παρουσίαση]** Ενότητας 2.1 Tips for shopping online safely [1:41] https://youtu.be/cWcNQgPiqhc?si=ihec3hoImznIz9oT *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	5’	**ΜΑ2.1** Να μπορώ να πραγματοποιώ ασφαλείς ηλεκτρονικές συναλλαγές και αγορές, χρησιμοποιώντας αξιόπιστες μεθόδους πληρωμής και αναγνωρίζοντας αξιόπιστα ηλεκτρονικά καταστήματα.
3.1.2	**[Επίδειξη]** Ενότητας 2.1 Online Shopping Advice [3:20] https://youtu.be/el3N6qQjr-I?si=CX3rC4VvAtyYvl8M *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	10’	
3.1.3	**[Εξάσκηση]** Ενότητας 2.1 Δραστηριότητα εξάσκησης με 5 ερωτήσεις σωστού - λάθους.	quizzes	15’	
3.1.4	**[Αυτο-Αξιολόγηση]** Ενότητας 2.1 Δραστηριότητα αυτοαξιολόγησης με 5 ερωτήσεις πολλαπλής επιλογής	multiple choice questions	15’	
3.2	**2η υπο-ενότητα: Αποφυγή διαδικτυακών απατών (60’)**			
3.2.1	**[Παρουσίαση]** Ενότητας 2.2 8 Online ΑΠΑΤΕΣ και ΠΩΣ να τις αντιμετωπίσεις [18:28] https://youtu.be/yxSlqP8eiFc?si=W4r397fU_8-7KsFQ *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	20’	**ΜΑ2.2** Να αναγνωρίζω και να αποφεύγω διαδικτυακές απάτες, όπως η

3.2.2	**[Επίδειξη]** Ενότητας 2.2 Stop, Think and Protect Yourself against Online Scams [5:40] https://youtu.be/lkExIJ8L-GY?si=_BudVpcTyvpNrWCa *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	10’	κλοπή ταυτότητας και οι ψεύτικες προσφορές.
3.2.3	**[Εξάσκηση]** Ενότητας 2.2 Δραστηριότητα εξάσκησης με 5 ερωτήσεις σωστού - λάθους.	quizzes	15’	
3.2.4	**[Αυτο-Αξιολόγηση]** Ενότητας 2.2 Δραστηριότητα αυτοαξιολόγησης με 5 ερωτήσεις πολλαπλής επιλογής.	multiple choice questions	15’	
3.3	**Ανακεφαλαίωση και Αυτό-Αξιολόγηση Μικρο-μαθήματος 2 (50’)**			
3.3.1	**[Παρουσίαση]** Ανακεφαλαίωση Θεματικής Ενότητας (Μικρο-Μάθημα) 2 *Σελίδα κειμένου που συνοψίζει το Μικρο-Μάθημα 2*	Υπερκείμενο	5΄	MA2.1 - MA2.2
3.3.2	**[Αυτό-αξιολόγηση] Εργασία: Open Response Assessment** Εργασία αυτοαξιολόγησης της ικανότητας MA-2 με βάση ρουμπρίκα	Open Response Assessment	30’	
3.3.3	**[Αυτοαξιολόγηση] Checklist: Μπορώ να το κάνω…**	Checklist, WordCloud	5’	

	Checklist με : «μπορώ να το κάνω» προτάσεις [WordCloud] Χρήση του wordcloud tool για τη συλλογή σύντομων απαντήσεων σε εύκολες ερωτήσεις που συνοψίζουν το βασικό θέμα της μικρο-μαθήματος.			
3.3.4	**[Discussion Forum]** Μια συζήτηση στο forum με ανάπυξη απόψεων πάνω στο θέμα της ενότητας 2.	Discussion Forum	10’	
3.4	**Προτάσεις για επιπλέον εκπαίδευση στο θέμα του Μικρο-μαθήματος 2**			
	[Προτάσεις για Επιπλέον Εκπαίδευση] https://cyberalert.gr https://safety.google	Υπερκείμενο		
Ημέρα 4: Μικρο-μάθημα 3 - Διαχείριση και προστασία της διαδικτυακής παρουσίας (≈3 ώρες)				
4.0	**Εισαγωγή Μικρο-μαθήματος 3 Διαχείριση και προστασία της διαδικτυακής παρουσίας (10’)**			
4.0.1	**[Παρουσίαση]** Μαθησιακά Αποτελέσματα Θεματικής Ενότητας 3 **(ΜΑ-1)** + **[Poll]** *Σελίδα κειμένου που παρουσιάζει τα επιμέρους μαθησιακά αποτελέσματα της ενότητας* *3 Polls για την αυτοαξιολόγηση της πρότερης γνώσης για τη θεματική της ενότητας.*	Υπερκείμενο, Poll	8'	
4.0.2	**[Παρουσίαση]** Δομή της ενότητας 3 *Σελίδα κειμένου που παρουσιάζει τη δομή της ενότητας 3*	Υπερκείμενο	2'	
4.1	**1η υπο-ενότητα: Διαχείριση και προστασία της διαδικτυακής παρουσίας (40’)**			
4.1.1	**[Παρουσίαση]** Ενότητας 3.1	Υπερκείμενο και βίντεο	5’	**ΜΑ3.1** Να μπορώ

	What is a Digital Footprint? [2:40] https://youtu.be/dmQGq_FNBpE?si=4lCER4j_oimaFnWT *Σελίδα κειμένου και βίντεο από το Youtube*			να διαχειρίζομαι αποτελεσματικά την παρουσία μου στα κοινωνικά δίκτυα, προσαρμόζοντας τις ρυθμίσεις απορρήτου και προστατεύοντας τη διαδικτυακή μου φήμη.
4.1.2	**[Επίδειξη]** Ενότητας 3.1 How to Manage Your Online Reputation [2:00] https://youtu.be/7_iVgqgXzi8?si=mRGaBYjLO5Mrgbgp *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	5’	
4.1.3	**[Εξάσκηση]** Ενότητας 3.1 Δραστηριότητα εξάσκησης με 5 ερωτήσεις σωστού - λάθους.	quizzes	15’	
4.1.4	**[Αυτο-Αξιολόγηση]** Ενότητας 3.1 Δραστηριότητα αυτοαξιολόγησης με 5 ερωτήσεις πολλαπλής επιλογής.	multiple choice questions	15’	
4.2	**2η υπο-ενότητα: Αντιμετώπιση της διαδικτυακής παρενόχλησης (50’)**			
4.2.1	**[Παρουσίαση]** Ενότητας 3.2 Καταπολεμώντας τη διαδικτυακή παρενόχληση [11:55] https://youtu.be/91dYxCMXk-4?si=gVaeQiDmUQF9rw1f *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	14’	**ΜΑ3.2** Να αναγνωρίζω και να αντιμετωπίζω τη διαδικτυακή παρενόχληση (cyberbullying), προωθώντας την ευγένεια και τον
4.2.2	**[Επίδειξη]** Ενότητας 3.2 Τι ειναι ο διαδικτυακός εκφοβισμός[2:42]	Υπερκείμενο και βίντεο	6’	

	https://youtu.be/v45sZEt_BFI?si=QT5s7ctPVZfqa_Lv Διαδικτυακός Εκφοβισμός[2:00] https://youtu.be/Fvw5tY5vgp8?si=Q8kBhZYKNaO7l1BZ *Σελίδα κειμένου και βίντεο από το Youtube*			σεβασμό στο διαδικτυακό περιβάλλον.
4.2.3	**[Εξάσκηση]** Ενότητας 3.2 Δραστηριότητα εξάσκησης με 5 ερωτήσεις σωστού - λάθους.	quizzes	15’	
4.2.4	**[Αυτο-Αξιολόγηση]** Ενότητας 3.2 Δραστηριότητα αυτοαξιολόγησης με 5 ερωτήσεις πολλαπλής επιλογής.	multiple choice questions	15’	
4.3	**Ανακεφαλαίωση και Αυτό-Αξιολόγηση Μικρο-μαθήματος 3 (50’)**			
4.3.1	**[Παρουσίαση]** Ανακεφαλαίωση Θεματικής Ενότητας (Μικρο-Μάθημα) 3 *Σελίδα κειμένου που συνοψίζει το Μικρο-Μάθημα 2*	Υπερκείμενο	5΄	ΜΑ3.1 – ΜΑ3.2
4.3.2	**[Αυτό-αξιολόγηση] Εργασία: Open Response Assessment** Εργασία αυτοαξιολόγησης της ικανότητας ΜΑ-3 με βάση ρουμπρίκα	Open Response Assessment	30’	
4.3.3	**[Αυτοαξιολόγηση] Checklist: Μπορώ να το κάνω…**	Checklist, WordCloud	5’	

	Checklist με : «μπορώ να το κάνω» προτάσεις [WordCloud] Χρήση του wordcloud tool για τη συλλογή σύντομων απαντήσεων σε εύκολες ερωτήσεις που συνοψίζουν το βασικό θέμα της μικρο-μαθήματος.			
4.3.4	**[Discussion Forum]** Μια συζήτηση στο forum με ανάπτυξη απόψεων πάνω στο θέμα της ενότητας 3.	Discussion Forum	10’	
4.4	**Προτάσεις για επιπλέον εκπαίδευση στο θέμα του Μικρο-μαθήματος 3**			
	[Προτάσεις για Επιπλέον Εκπαίδευση] https://stop-bullying.gov.gr/ https://connectsafely.org/ https://saferinternet4kids.gr/	Υπερκείμενο		
Ημέρα 5: Μικρο-μάθημα 4 Προστασία Παιδιών και Οικογένειας στο Διαδίκτυο (≈3 ώρες)				
5.0	**Εισαγωγή Μικρο-μαθήματος 4 Προστασία Παιδιών και Οικογένειας στο Διαδίκτυο (10’)**			
5.0.1	**[Παρουσίαση]** Μαθησιακά Αποτελέσματα Θεματικής Ενότητας 4 **(ΜΑ-1)** + **[Poll]** *Σελίδα κειμένου που παρουσιάζει τα επιμέρους μαθησιακά αποτελέσματα της ενότητας* *3 Polls για την αυτοαξιολόγηση της πρότερης γνώσης για τη θεματική της ενότητας.*	Υπερκείμενο, Poll	8'	
5.0.2	**[Παρουσίαση]** Δομή της ενότητας 3 *Σελίδα κειμένου που παρουσιάζει τη δομή της ενότητας 3*	Υπερκείμενο	2'	
5.1	**1η υπο-ενότητα: Προστασία των παιδιών στο διαδίκτυο και εφαρμογή κατάλληλων μέτρων(70’)**			

5.1.1	**[Παρουσίαση]** Ενότητας 4.1 Online safety guide to parental controls[6:43] https://youtu.be/c6odst87Tbo?si=Wib8O6_64Re1aZk9 Καμπάνια ενημέρωσης της Europol: «Say No!»[10:35] https://www.youtube.com/watch?v=M_2rXM3W5gQ Που είναι ο Μήτσος - (SaveMitsos.gr) [0:59] https://youtu.be/z6sIC4MXXOA?si=3nVW5UywT_WBbCjF *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	20’	**ΜΑ4.1** Να αναγνωρίζω τους κινδύνους που αντιμετωπίζουν τα παιδιά στο διαδίκτυο και να εφαρμόζω κατάλληλα μέτρα προστασίας, όπως εργαλεία γονικού ελέγχου και ασφαλείς ρυθμίσεις στις συσκευές.
5.1.2	**[Επίδειξη]** Ενότητας 4.1 Safe Web Surfing: Top Tips for Kids and Teens Online [5:01] https://youtu.be/yrln8nyVBLU?si=YtjPQbRRmeCChu6Q iPhone & iPad: Ultimate Guide for Parental Controls[11:25] https://youtu.be/eZZaQF0x4JY?si=hbk4OxRhsdUazohi *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	20’	
5.1.3	**[Εξάσκηση]** Ενότητας 4.1 Δραστηριότητα εξάσκησης με 5 ερωτήσεις σωστού - λάθους.	quizzes	15’	
5.1.4	**[Αυτο-Αξιολόγηση]** Ενότητας 4.1 Δραστηριότητα αυτοαξιολόγησης με 5 ερωτήσεις	multiple choice	15’	

	πολλαπλής επιλογής.	questions		
5.2	**2η υπο-ενότητα: Δημιουργία ασφαλούς και υποστηρικτικού διαδικτυακού περιβάλλοντος για την οικογένειά (50')**			
5.2.1	**[Παρουσίαση]** Ενότητας 4.2 Protecting children online: Κίνδυνοι διαδικτύου και τρόποι προστασίας [09:13] https://youtu.be/35nuOD3rA8I?si=1iF3zAmxfr30euaR Σε ποιο κόσμο ζεις;[1:02] https://youtu.be/8hJpgtJMNBc?si=nCGmmxZW5pvHkpt4 *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	12'	**ΜΑ4.2** Να δημιουργώ ένα ασφαλές και υποστηρικτικό διαδικτυακό περιβάλλον για την οικογένειά μου, ενθαρρύνοντας την ανοιχτή επικοινωνία και την εκπαίδευση σχετικά με την ασφαλή χρήση του διαδικτύου.
5.2.2	**[Επίδειξη]** Ενότητας 4.2 Ασφάλεια στο Διαδίκτυο συμβουλές για γονείς & παιδιά [3:00] https://youtu.be/4VAy4c1oeiI?si=tzaR1aK2m3bhywth Parental Advice and the Family Online Safety Contract [2:22] https://youtu.be/HAmbinoAyH4?si=GUaH-SY-OnlvrjR9 *Σελίδα κειμένου και βίντεο από το Youtube*	Υπερκείμενο και βίντεο	8'	
5.2.3	**[Εξάσκηση]** Ενότητας 4.2 Δραστηριότητα εξάσκησης με 5 ερωτήσεις σωστού -	quizzes	15'	

	λάθους.			
5.2.4	**[Αυτο-Αξιολόγηση]** Ενότητας 4.2 Δραστηριότητα αυτοαξιολόγησης με 5 ερωτήσεις πολλαπλής επιλογής.	multiple choice questions	15’	
5.3	**Ανακεφαλαίωση και Αυτό-Αξιολόγηση Μικρο-μαθήματος 4 (50’)**			
5.3.1	**[Παρουσίαση]** Ανακεφαλαίωση Θεματικής Ενότητας (Μικρο-Μάθημα) 4 *Σελίδα κειμένου που συνοψίζει το Μικρο-Μάθημα 2*	Υπερκείμενο	5΄	MA4.1 – MA4.2
5.3.2	**[Αυτό-αξιολόγηση] Εργασία: Open Response Assessment** Εργασία αυτοαξιολόγησης της ικανότητας MA-4 με βάση ρουμπρίκα	Open Response Assessment	30’	
5.3.3	**[Αυτοαξιολόγηση] Checklist: Μπορώ να το κάνω…** Checklist με : «μπορώ να το κάνω» προτάσεις [WordCloud] Χρήση του wordcloud tool για τη συλλογή σύντομων απαντήσεων σε εύκολες ερωτήσεις που συνοψίζουν το βασικό θέμα της μικρο-μαθήματος.	Checklist, WordCloud	5’	
5.3.4	**[Discussion Forum]** Μια συζήτηση στο forum με ανάπτυξη απόψεων πάνω στο θέμα της ενότητας 4.	Discussion Forum	10’	
5.4	**Προτάσεις για επιπλέον εκπαίδευση στο θέμα του Μικρο-μαθήματος 4**			

	[Προτάσεις για Επιπλέον Εκπαίδευση] https://www.socialworkerstoolbox.com/online-safety-agreement/	Υπερκείμενο		

Ημέρα 6: Τελική Αξιολόγηση micro-MOOC (60')				
5.0	**[Παρουσίαση] Οδηγίες για τη διεξαγωγή της τελικής εξέτασης του micro-MOOC** Σελίδα κειμένου που περιγράφει την ελάχιστη βαθμολογία που θα πρέπει να συγκεντρώσει ο εξεταζόμενος και τις προϋποθέσεις για να θεωρηθεί επιτυχής η εξέταση	Υπερκείμενο	5'	
5.1	**[Τελική Αξιολόγηση] 5 MCQs για κάθε Μαθησιακό Αποτέλεσμα Μικρο-Μαθήματος** Ερωτήσεις Σωστού-Λάθους, Πολλαπλής Επιλογής (Multiple Choice Questions, MCQs) έτσι ώστε να αξιολογούνται η κατανόηση και οι δεξιότητες των εκπαιδευομένων- αξιολογεί όλα τα ΜΑ	Quiz	50'	ΜΑ1-ΜΑ4 (5 για κάθε ΜΑ , άρα σύνολο 20)

5.2	**[Παρουσίαση] Οδηγίες για τη δημιουργία πιστοποιητικού του micro-MOOC** Σελίδα κειμένου που περιγράφει τις οδηγίες για την έκδοση και παραλαβή του πιστοποιητικού του micro-MOOC.	Υπερκείμενο	5’	

Κεφάλαιο 4. Υλοποίηση του διαδικτυακού μαθήματος «Ψηφιακή Ενδυνάμωση Ενηλίκων: Στρατηγικές για την Προαγωγή της Ασφαλούς Πλοήγησης στο Διαδίκτυο» στην πλατφόρμα OpenEdX

4.1 Παρουσίαση της πλατφόρμας OpenEdX

Το OpenEdX είναι μια ισχυρή πλατφόρμα διαχείρισης μάθησης (Learning Management System - LMS) που αναπτύχθηκε από το Πανεπιστήμιο του Harvard και το MIT για την παροχή ανοιχτών διαδικτυακών μαθημάτων (MOOCs). Η πλατφόρμα χρησιμοποιείται ευρέως από πανεπιστήμια, επιχειρήσεις και εκπαιδευτικούς οργανισμούς για τη δημιουργία και τη διαχείριση διαδικτυακών μαθημάτων, είτε πρόκειται για ανοιχτά μαθήματα είτε για ιδιωτικές εταιρικές εκπαιδεύσεις. Η OpenEdX προσφέρει στους εκπαιδευτικούς ευελιξία και προσαρμοστικότητα, ενώ στους εκπαιδευόμενους μια πλούσια, διαδραστική μαθησιακή εμπειρία (Waldrop, 2013).

4.1.1 Δυνατότητες και Λειτουργίες

Η πλατφόρμα OpenEdX διαθέτει ένα ευρύ φάσμα εργαλείων και λειτουργιών που διευκολύνουν την ανάπτυξη διαδραστικών μαθημάτων. Οι εκπαιδευτικοί μπορούν να ανεβάσουν ποικιλία ψηφιακού περιεχομένου, όπως βίντεο, παρουσιάσεις, αρχεία PDF, και να ενσωματώσουν διαδραστικά στοιχεία, όπως κουίζ, συζητήσεις και ασκήσεις κώδικα. Οι δυνατότητες δημιουργίας μαθησιακών δραστηριοτήτων είναι ευέλικτες και επιτρέπουν την εφαρμογή διαφόρων παιδαγωγικών προσεγγίσεων, όπως η ενεργητική μάθηση και η αξιολόγηση βάσει δεξιοτήτων (Ghazal et al., 2019).

Η OpenEdX υποστηρίζει την παρακολούθηση της προόδου των μαθητών μέσω αναλυτικών δεδομένων και στατιστικών αναφορών. Οι εκπαιδευτές μπορούν να δουν λεπτομερή δεδομένα για τη συμμετοχή, τις επιδόσεις και τη διάρκεια που αφιερώνουν οι μαθητές σε κάθε δραστηριότητα, διευκολύνοντας έτσι τη διαρκή ανατροφοδότηση και προσαρμογή του μαθήματος (Suparak, 2020).

Η πλατφόρμα υποστηρίζει επίσης τη συνεργασία και την επικοινωνία μεταξύ των εκπαιδευομένων, μέσω εργαλείων όπως τα forums συζητήσεων και οι δυνατότητες σχολιασμού, ενισχύοντας την κοινωνική μάθηση και την αλληλεπίδραση (Suparak, 2020). Επιπλέον, η πλατφόρμα είναι συμβατή με πολλαπλές γλώσσες και είναι σχεδιασμένη για

να υποστηρίζει μαζική κλίμακα χρηστών, γεγονός που την καθιστά κατάλληλη για μεγάλα MOOCs (Ghazal et al., 2019).

4.1.2 Κριτική και Αξιολόγηση

Παρά τις πολλές δυνατότητες της, η OpenEdX δεν είναι χωρίς προκλήσεις. Η βασική της δομή, αν και ισχυρή, μπορεί να είναι περίπλοκη για εκπαιδευτικούς που δεν έχουν μεγάλη εμπειρία με τεχνολογίες LMS (Suparak, 2020). Η διαδικασία δημιουργίας μαθημάτων απαιτεί σημαντικό χρόνο και τεχνική εξοικείωση με τη διαχείριση του περιβάλλοντος. Παράλληλα, οι προγραμματιστές έχουν τη δυνατότητα να τροποποιήσουν τον κώδικα, καθώς η πλατφόρμα είναι ανοιχτού κώδικα, αλλά αυτό απαιτεί τεχνικές γνώσεις και μπορεί να είναι δύσκολο για οργανισμούς που δεν διαθέτουν εξειδικευμένο προσωπικό (Zheng, 2018).

Μια άλλη πρόκληση της OpenEdX είναι ότι, αν και προσφέρει εργαλεία αξιολόγησης, όπως κουίζ και αυτό-αξιολογήσεις, δεν έχει τη δυνατότητα να παρέχει πολύπλοκα εργαλεία για αξιολογήσεις βάσει απόδοσης (performance-based assessments) με την ίδια ευκολία όπως άλλες πλατφόρμες. Αυτό περιορίζει σε κάποιο βαθμό τη χρήση της σε προγράμματα που απαιτούν σύνθετες αξιολογήσεις ή πολύπλοκες διαδραστικές δραστηριότητες (Ghazal et al., 2019).

Αξίζει επίσης να σημειωθεί ότι το περιβάλλον της OpenEdX, αν και φιλικό προς τον χρήστη, δεν έχει την ίδια αισθητική ομοιομορφία και την ευχρηστία που παρέχουν άλλες εμπορικές πλατφόρμες LMS, όπως το Moodle ή το Blackboard. Η εμπειρία χρήστη, κυρίως για τους εκπαιδευόμενους, μπορεί να επηρεαστεί από την ευκολία πλοήγησης, και μερικές φορές μπορεί να απαιτείται εκπαίδευση για την πλήρη κατανόηση των λειτουργιών Zheng, 2018).

4.2 Υλοποίηση του διαδικτυακού μαθήματος «Ψηφιακή Ενδυνάμωση Ενηλίκων: Στρατηγικές για την Προαγωγή της Ασφαλούς Πλοήγησης στο Διαδίκτυο»

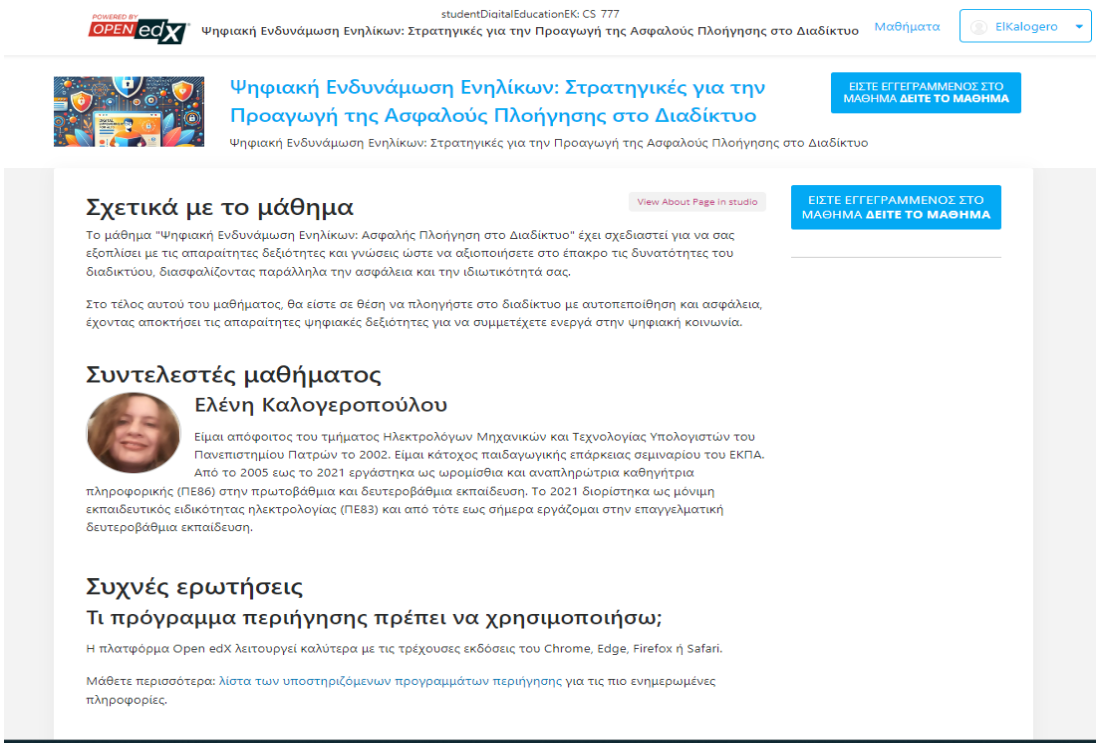
4.2.1 Αρχική σελίδα και δομή του υλικού του MOOC

Η υλοποίηση του μαθήματος αυτού βασίζεται σε πρότυπο σχεδίασης[3] που παρουσιάζεται

[3] Βασίζεται σε πρότυπο εκπαιδευτικού σχεδιασμού, όπως αυτό δόθηκε στην εργασία 4 του μαθήματος ΨΣ-ΗΜ-721 του μεταπτυχιακού προγράμματος «Ηλεκτρονική Μάθηση».

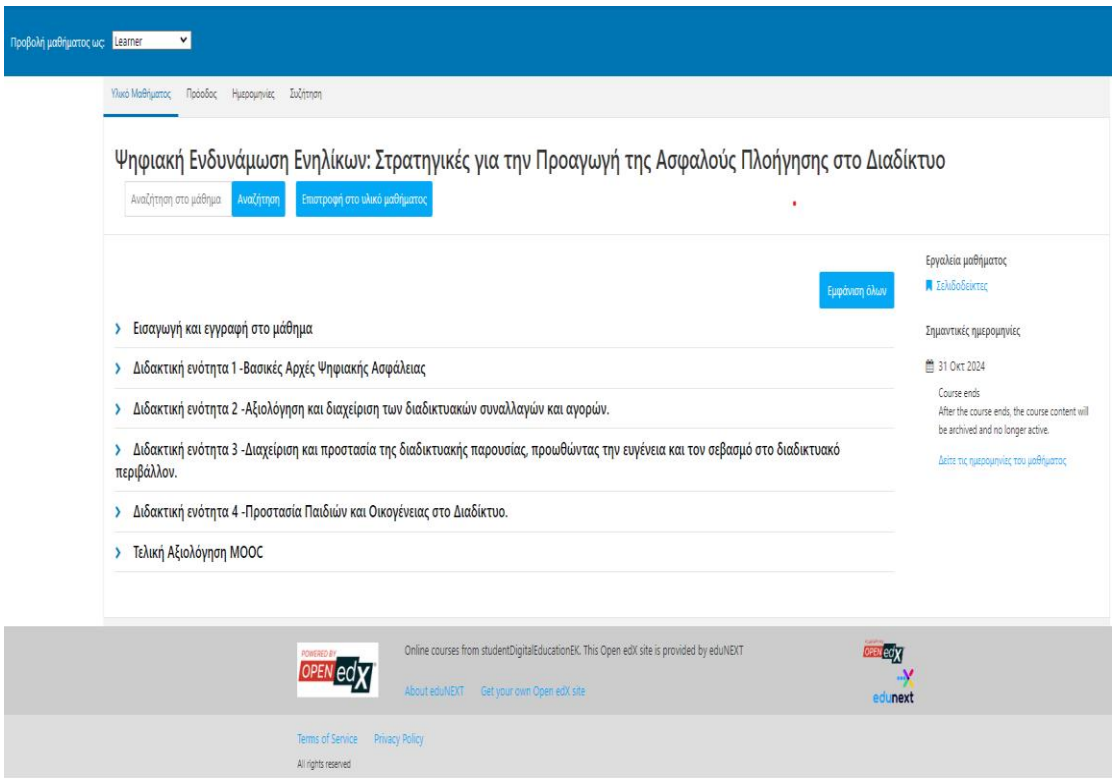
συνοπτικά στο κεφάλαιο 3 και αναλυτικά με όλο το περιεχόμενο του στο παράρτημα αυτής της εργασίας.

Ξεκινώντας, λοιπόν , έχουμε την αρχική σελίδα του μαθήματος , όπως αυτή δημιουργείται από την πλατφόρμα OpenEdX, οποία μας δίνει βασικές πληροφορίες για το MOOC και δίνει τη δυνατότητα της εγγραφής στο χρήστη.

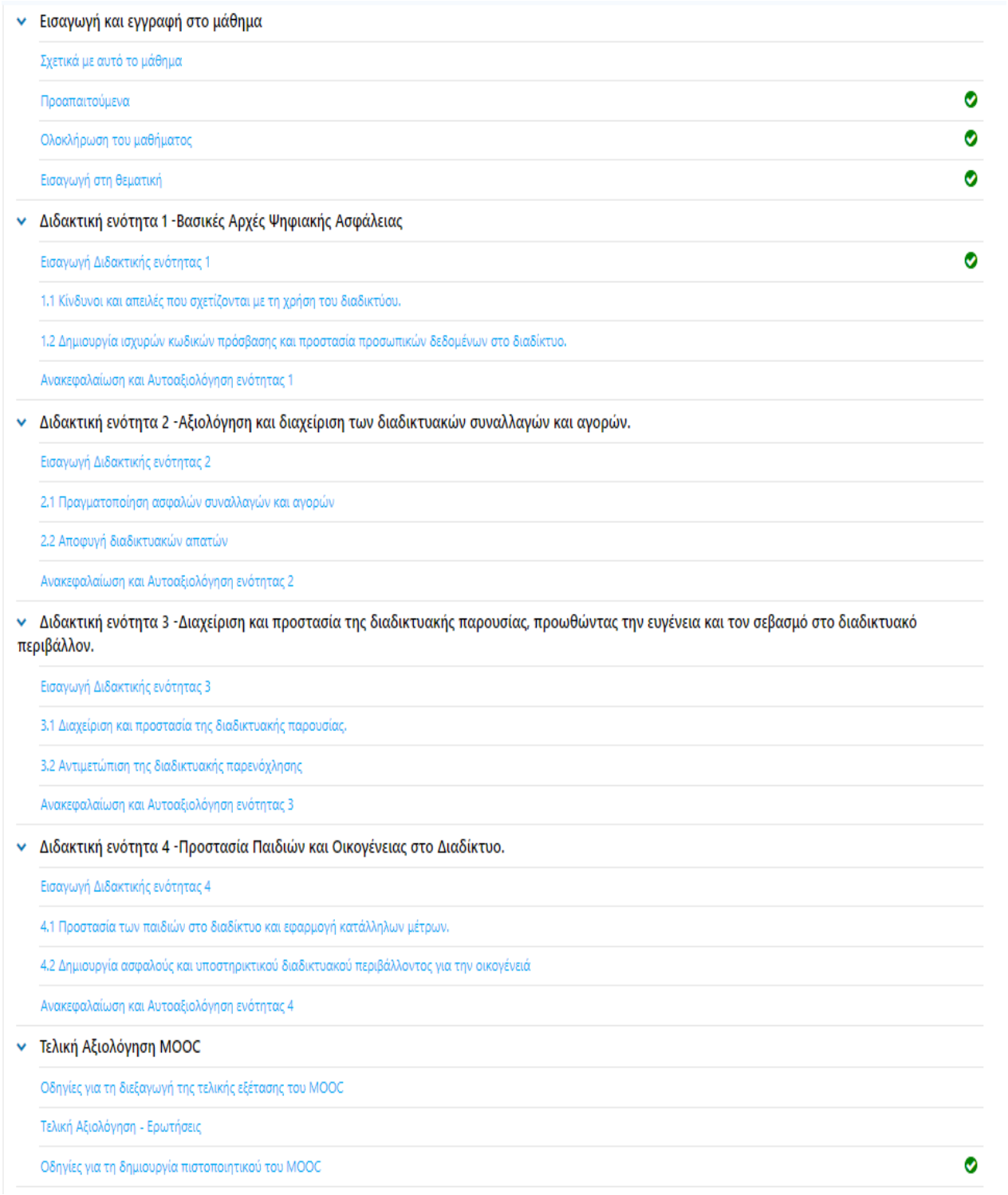


Εικόνα 2: Αρχική σελίδαMOOC

Στη συνέχεια και αφού ο χρήστης επιλέξει να εγγραφεί στο μάθημα, έχει πρόσβαση σε όλο το υλικό του μαθήματος, το οποίο φαίνεται σε συμπτυγμένη και σε αναπτυγμένη διάταξη παρακάτω.



Εικόνα 3:Συμπτυγμένη διάταξη MOOC

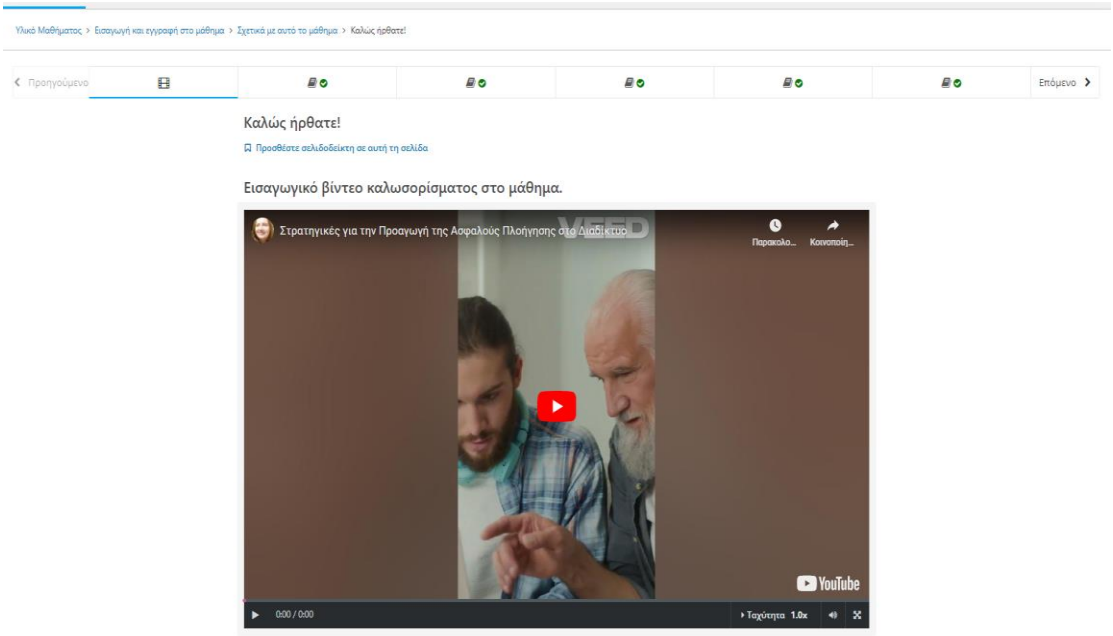


Εικόνα 4:Αναπτυγμένη διάταξη MOOC

4.2.2 Εισαγωγή και εγγραφή στο μάθημα

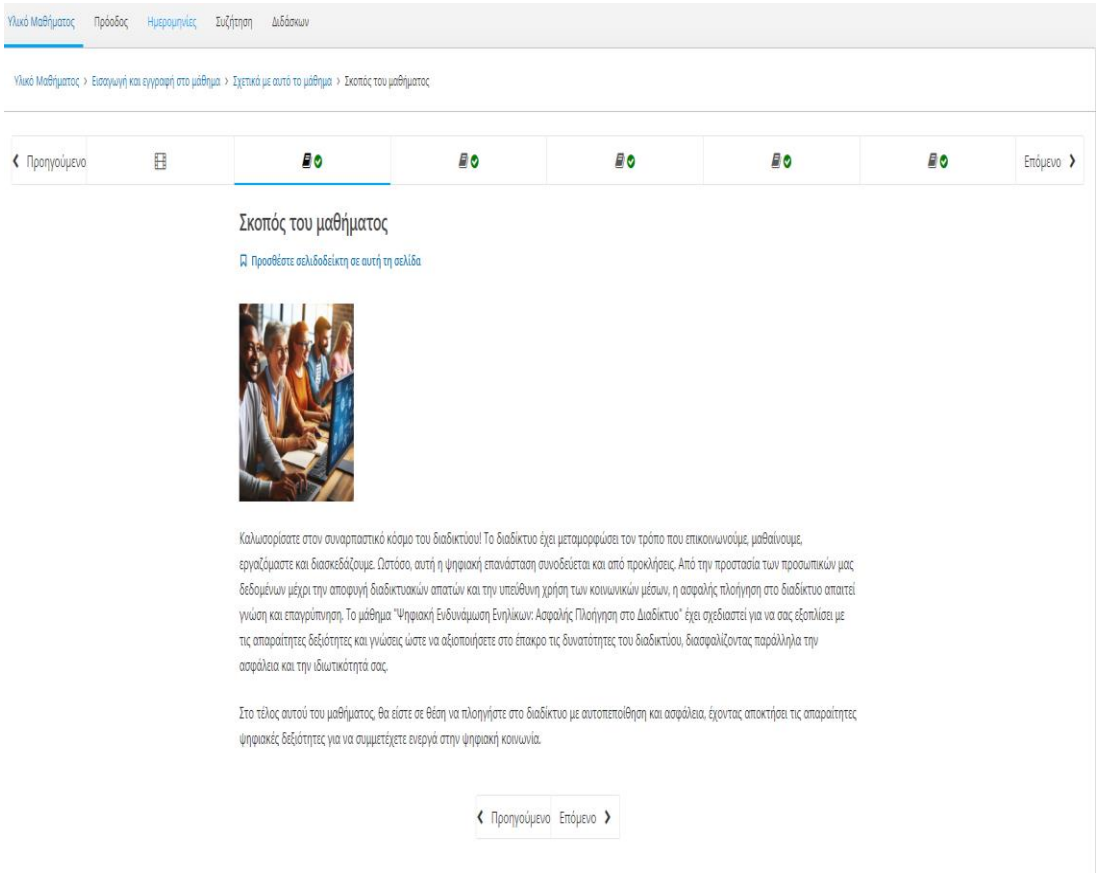
Η πρώτη ενότητα που παρουσιάζεται δίνει βασικές πληροφορίες «Σχετικά με αυτό το

μάθημα» και ξεκινάει με ένα εισαγωγικό βίντεο καλωσορίσματος.

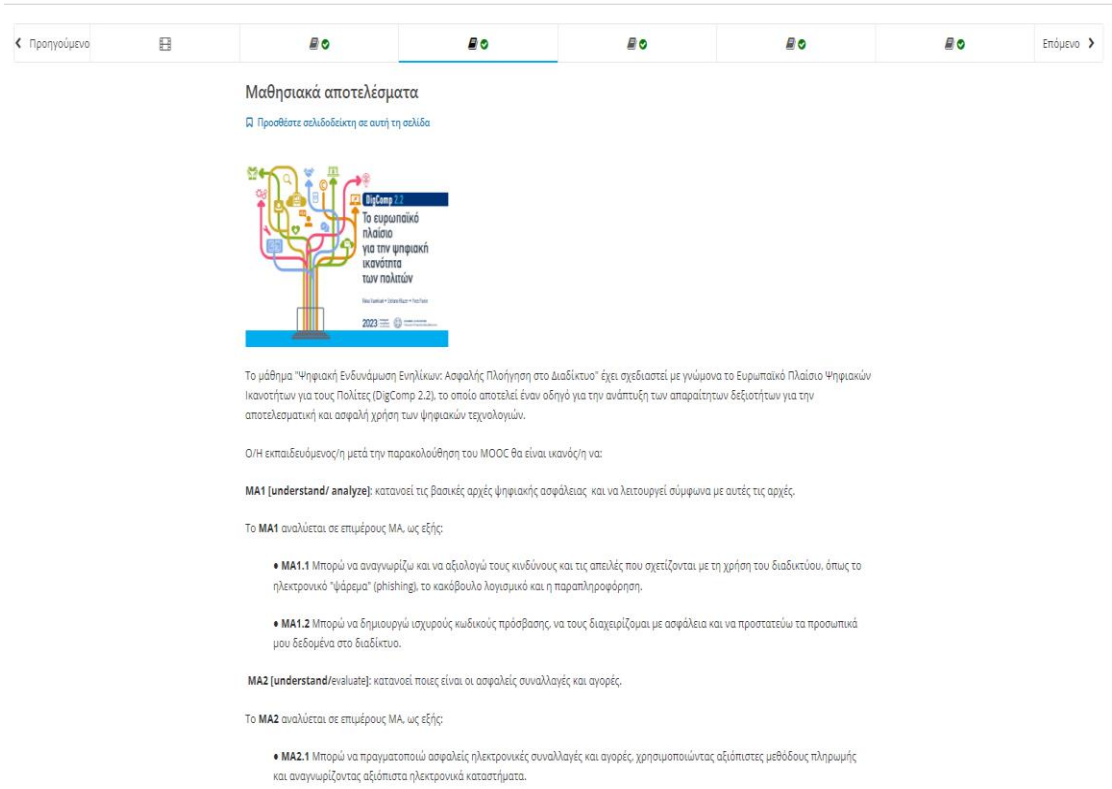


Εικόνα 5:Βίντεο Καλωσορίσματος

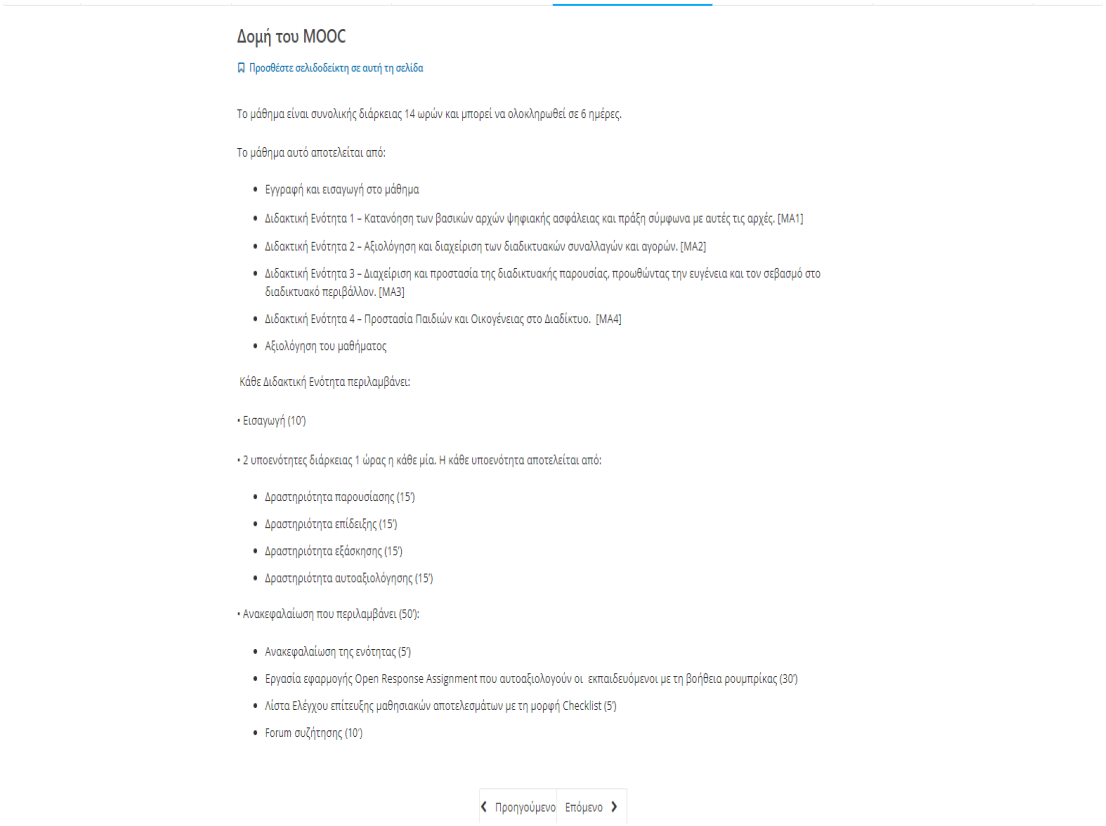
Ακολουθούν οι σελίδες με το σκοπό του μαθήματος, τα μαθησιακά αποτελέσματα, τη δομή του MOOC, την άδεια χρήσης και το δημιουργό του MOOC.



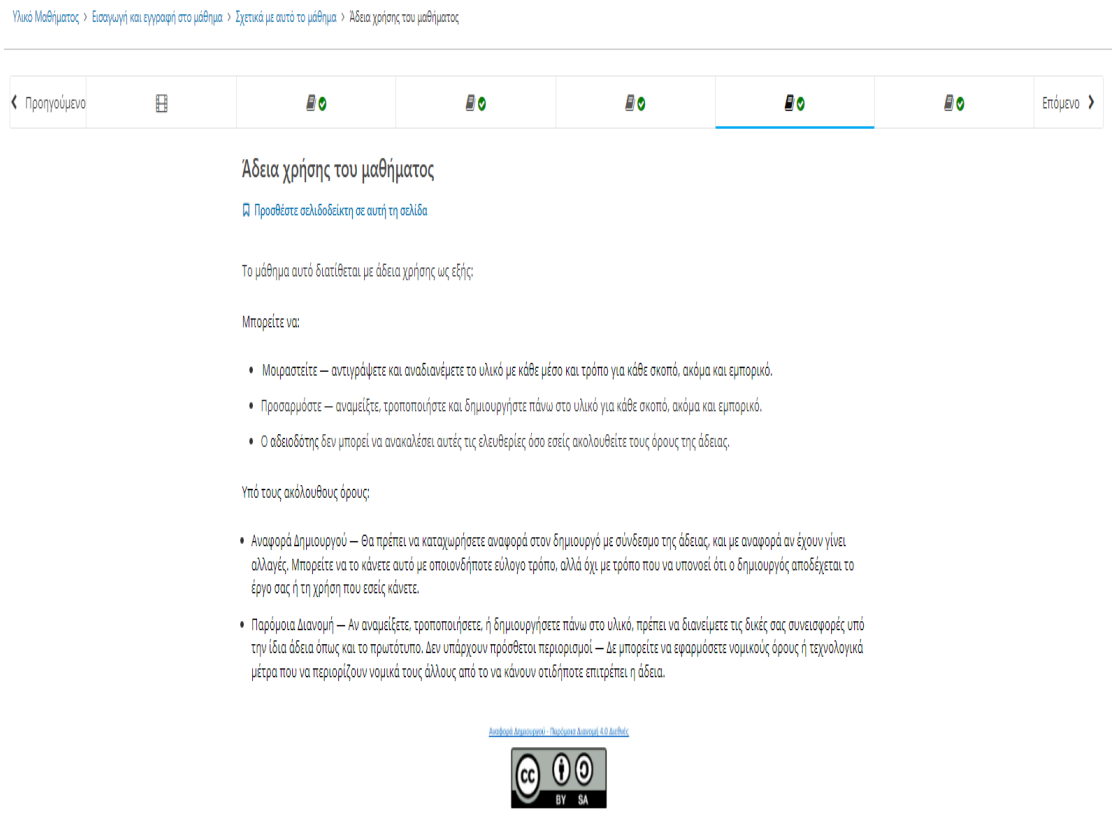
Εικόνα 6:Σκοπός του μαθήματος



Εικόνα 7:Μαθησιακά Αποτελέσματα

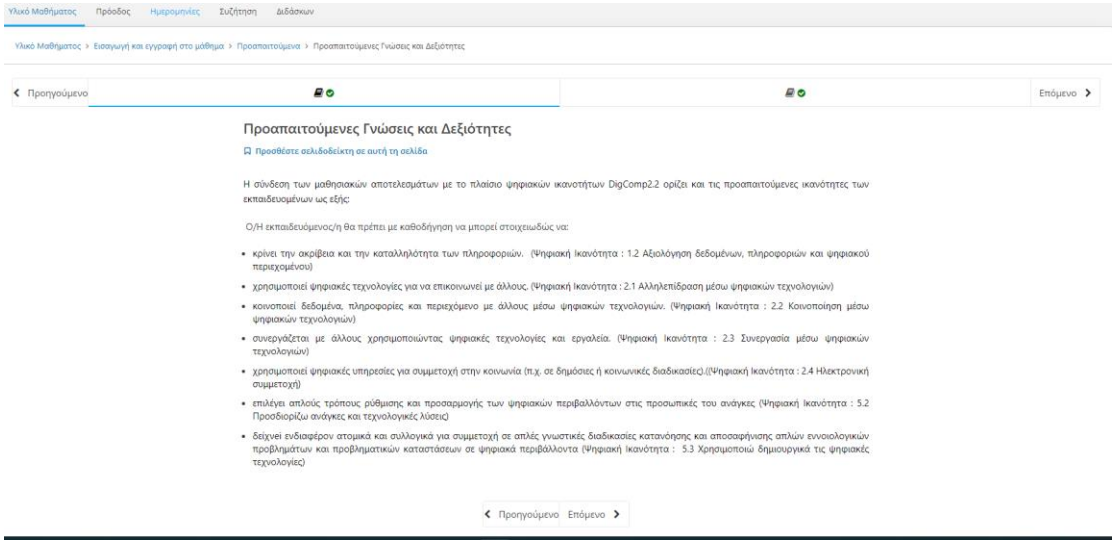


Εικόνα 8:Δομή του MOOC

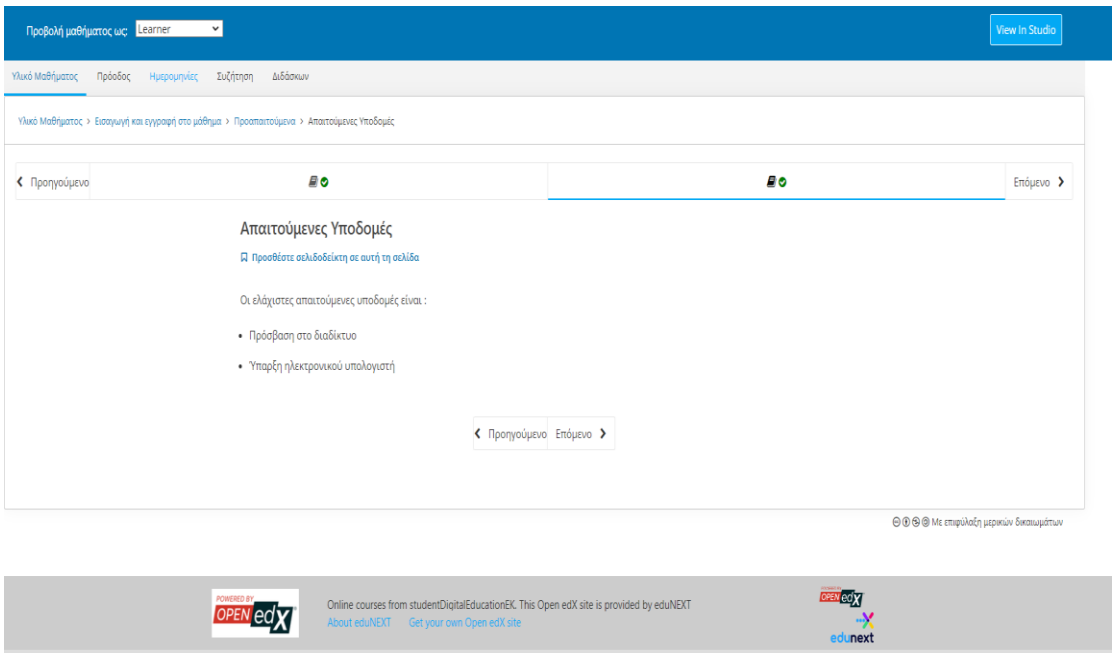


Εικόνα 9:Άδεια χρήσης

Συνεχίζουμε με τις βασικές πληροφορίες με τις σελίδες των προαπαιτούμενων γνώσεων και των ελάχιστων υποδομών.



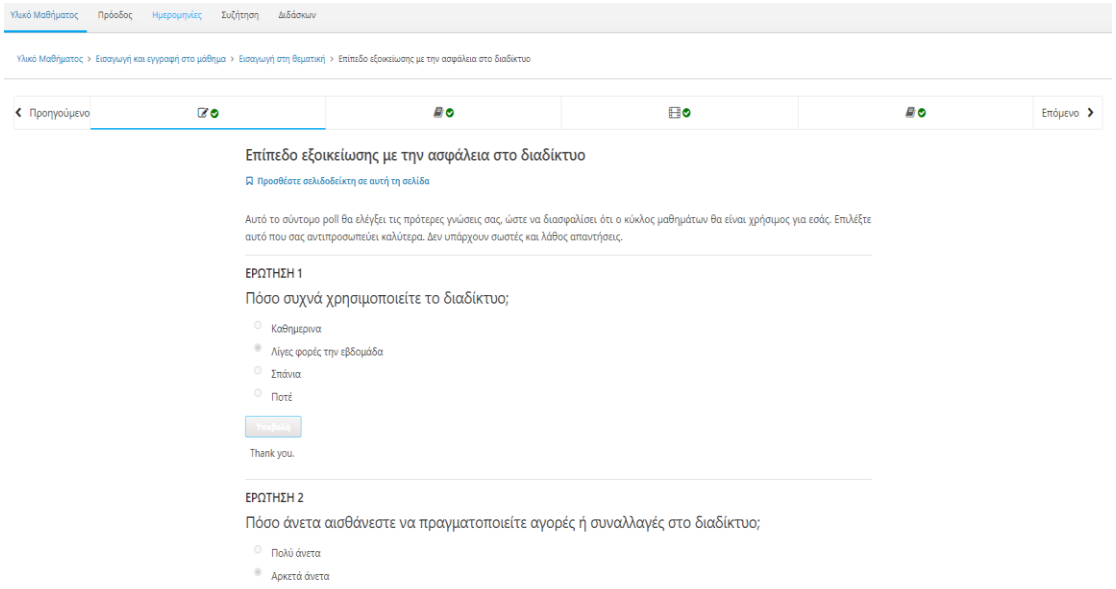
Εικόνα 10:Προαπαιτούμενες γνώσεις και δεξιότητες



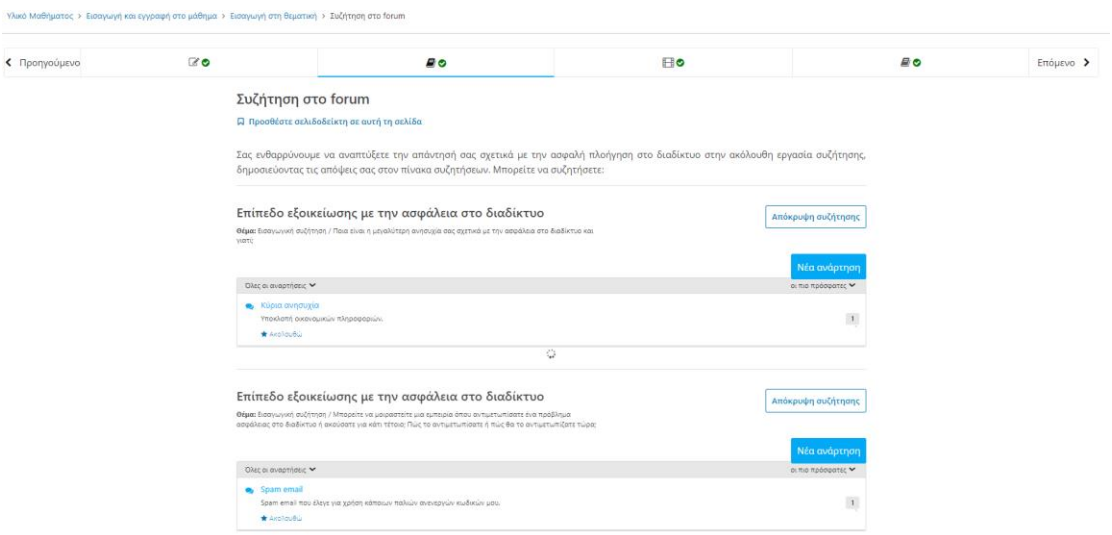
Εικόνα 11:Ελάχιστες Υποδομές

Ακολουθούν σελίδες με παρόμοια εμφάνιση μόνο με κείμενο που πληροφορούν τον εκπαιδευόμενο για τις απαραίτητες ενέργειες για την ολοκλήρωση του μαθήματος, τη μορφή των εργασιών αυτοαξιολόγησης και αξιολόγησης, τους κανόνες συμμετοχής στο forum συζητήσεων καθώς και πως γίνεται η τελική εξέταση.

Προχωράμε με την εισαγωγή στη θεματική με μία σύντομη δημοσκόπηση για το επίπεδο εξοικείωσης με την ασφάλεια στο διαδίκτυο, μία εισαγωγική συζήτηση στο forum και ένα βίντεο άποψης ειδικού.



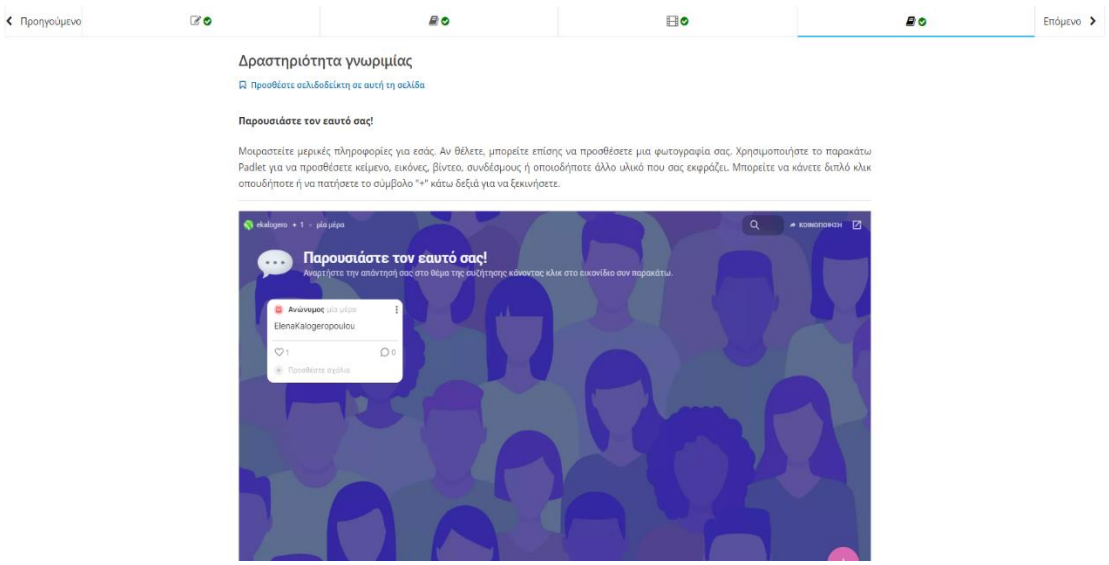
Εικόνα 12:Επίπεδο εξοικείωσης με την ασφάλεια στο διαδίκτυο



Εικόνα 13:Εισαγωγική Συζήτηση στο forum

Εικόνα 14:Άποψη Ειδικού

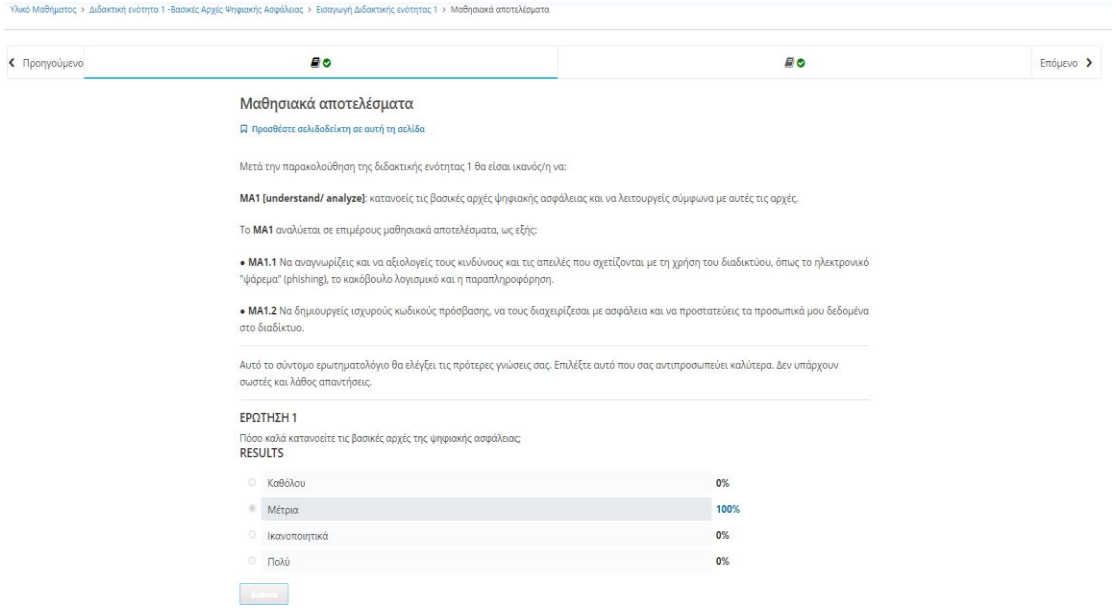
Η εισαγωγική αυτή ενότητα κλείνει με μία διαδραστική δραστηριότητα γνωριμίας με τη χρήση του εργαλείου Padlet.



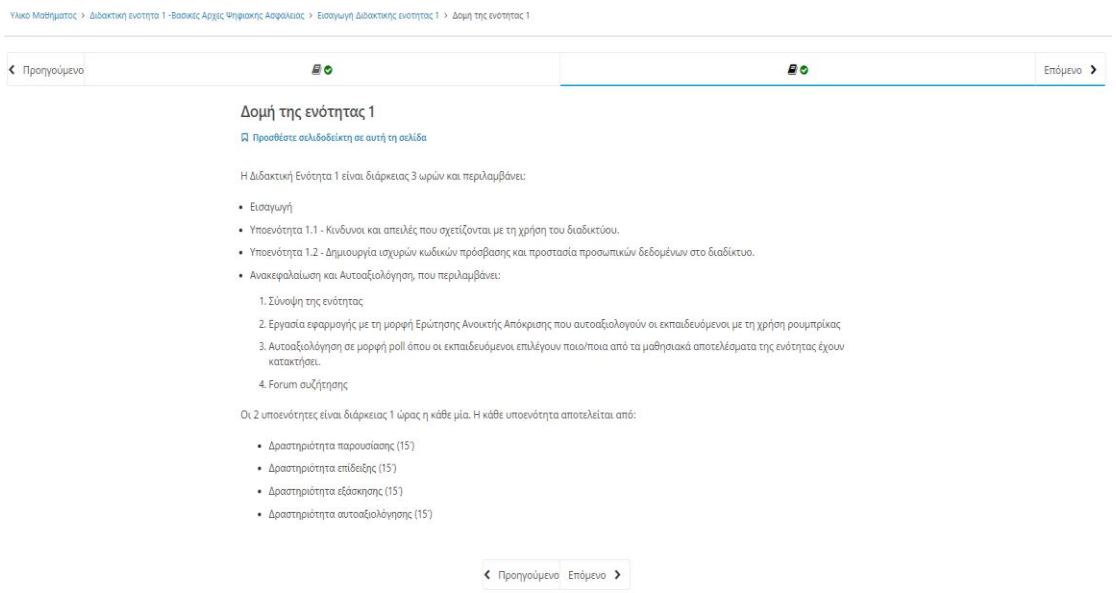
Εικόνα 15:Γνωριμία εκπαιδευομένων

4.2.3 Περιγραφή των διδακτικών ενοτήτων 1 έως 4

Όλες οι διδακτικές ενότητες έχουν ίδιο σχεδιασμό με διαφορετικό περιεχόμενο η καθεμία. Ξεκινάμε στην εισαγωγή της κάθε διδακτικής με τα μαθησιακά αποτελέσματα, μια σύντομη δημοσκόπηση «Τι γνωρίζω ήδη» και τη δομή που αντιστοιχεί στην ενότητα.



Εικόνα 16:Μαθησιακά αποτελέσματα ενότητας 1

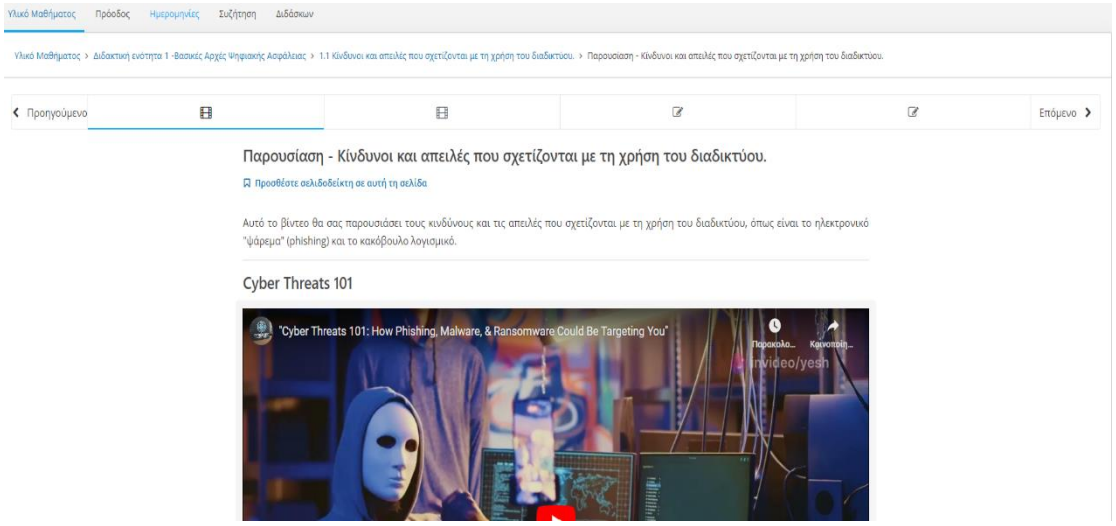


Εικόνα 17:Δομή ενότητας 1

Ακολουθεί η ανάπτυξη της κάθε υποενότητας με δραστηριότητες παρουσίασης, επίδειξης, εξάσκησης και αυτοαξιολόγησης.

Έχουν επιλεχθεί βίντεο για παρουσίαση και επίδειξη, ερωτήσεις σωστού – λάθους για εξάσκηση και ερωτήσεις πολλαπλών επιλογών για αυτοαξιολόγηση της κάθε υποενότητας.

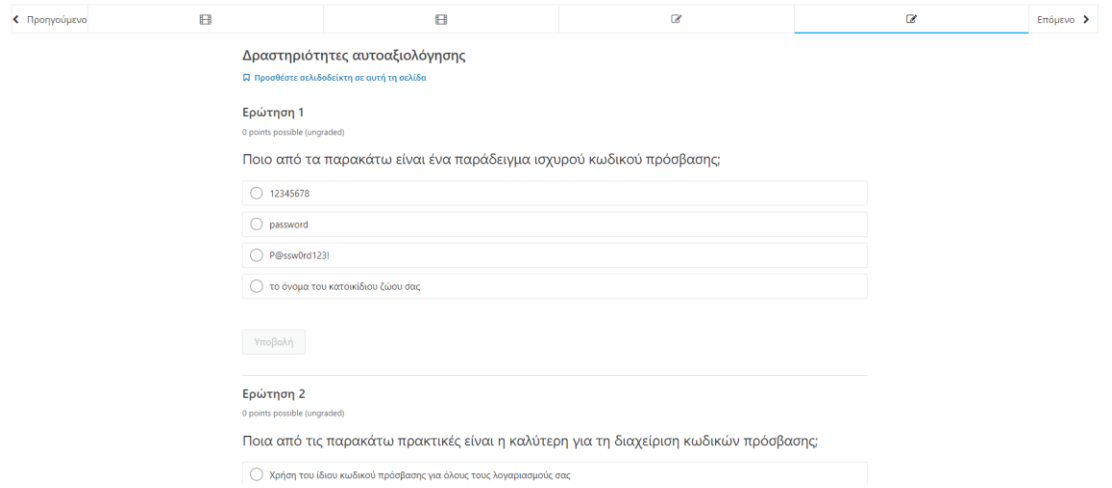
Ενδεικτικά παρουσιάζονται μερικές τέτοιες σελίδες.



Εικόνα 18:Παρουσίαση υποενότητας 1.1

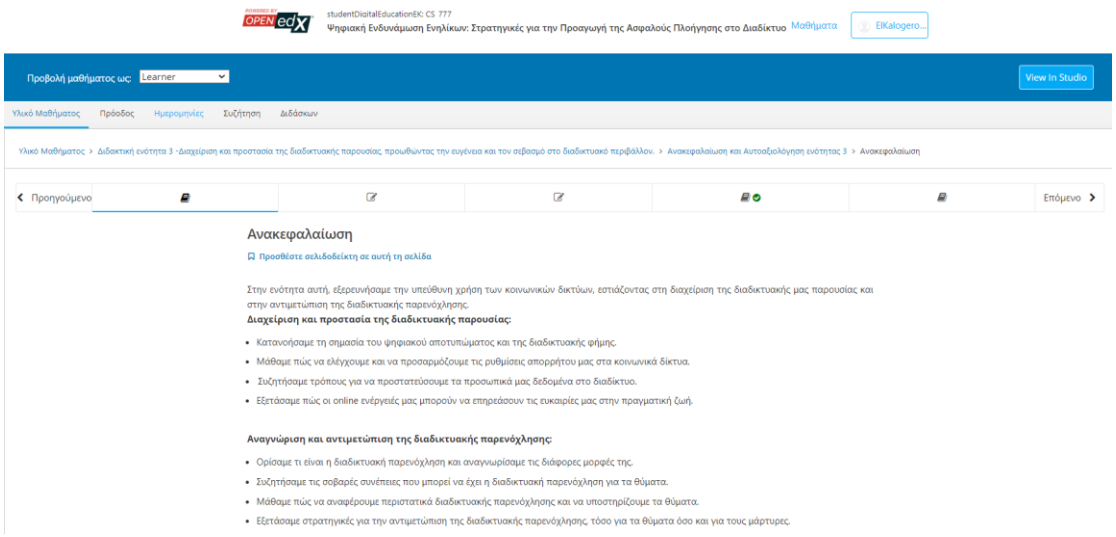
Εικόνα 19:Επίδειξη υποενότητας 1.2

Εικόνα 20:Ερωτήσεις εξάσκησης 1.2

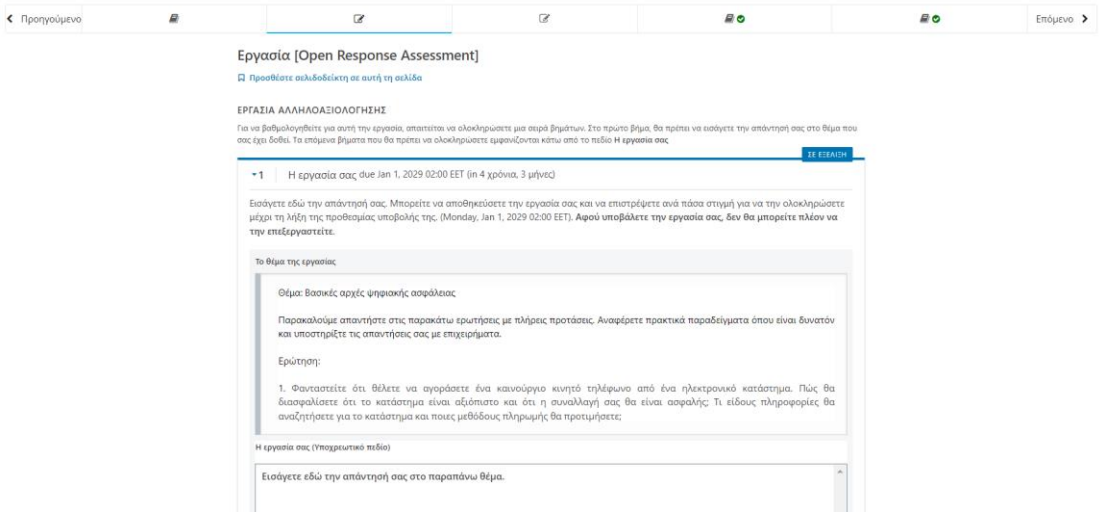


Εικόνα 21:Ερωτήσεις αυτοαξιολόγησης 1.2

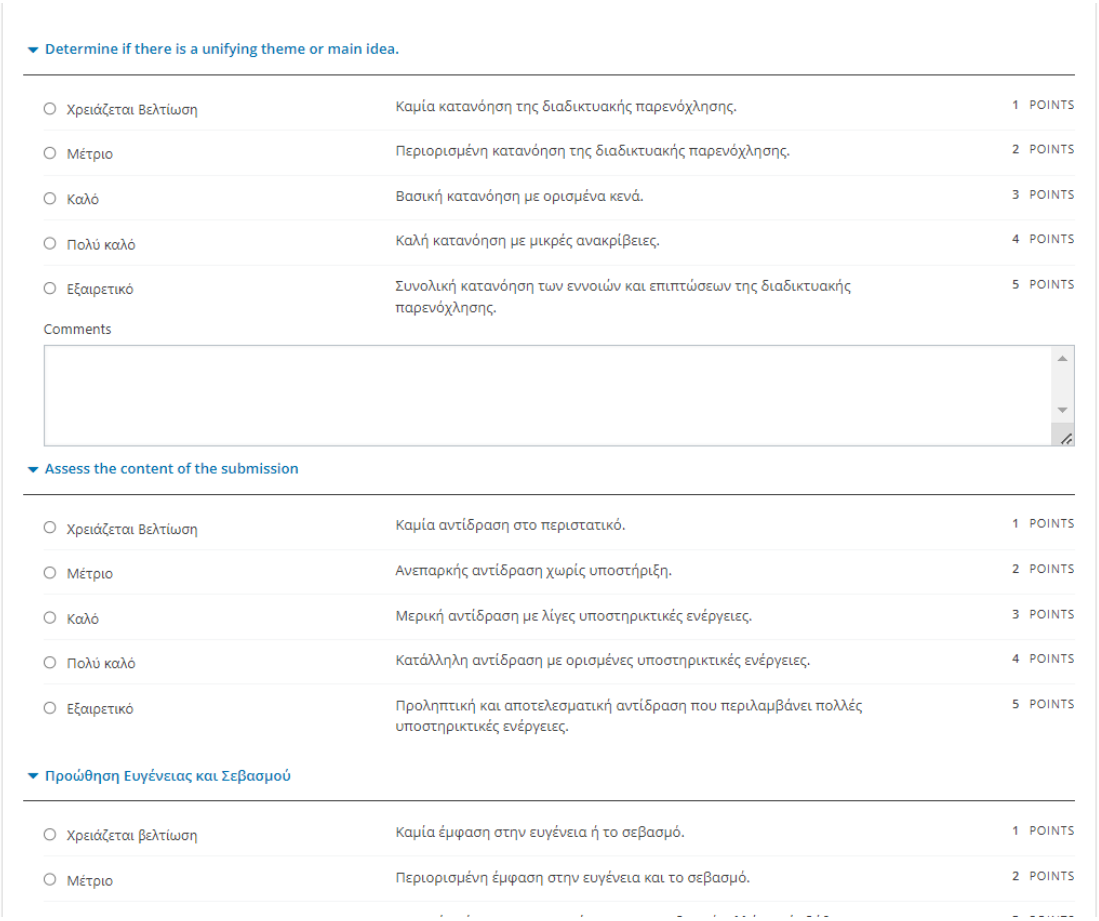
Η τρίτη υποενότητα κάθε διδακτικής ενότητας περιέχει την ανακεφαλαίωση και την αυτοαξιολόγηση. Για την αυτοαξιολόγηση χρησιμοποιείται μία εργασία ανοιχτής απόκρισης με ρουμπρίκα , λίστα με προτάσεις που συνδέονται με τα μαθησιακά αποτελέσματα όλης της διδακτικής ενότητας, ένα συνεφφόλεξο (WordCloud) με βασικές λέξεις και ερώτηση/ερωτήσεις σχετικές με το θέμα στο forum για την ενεργό συμμετοχή των εκπαιδευόμενων.



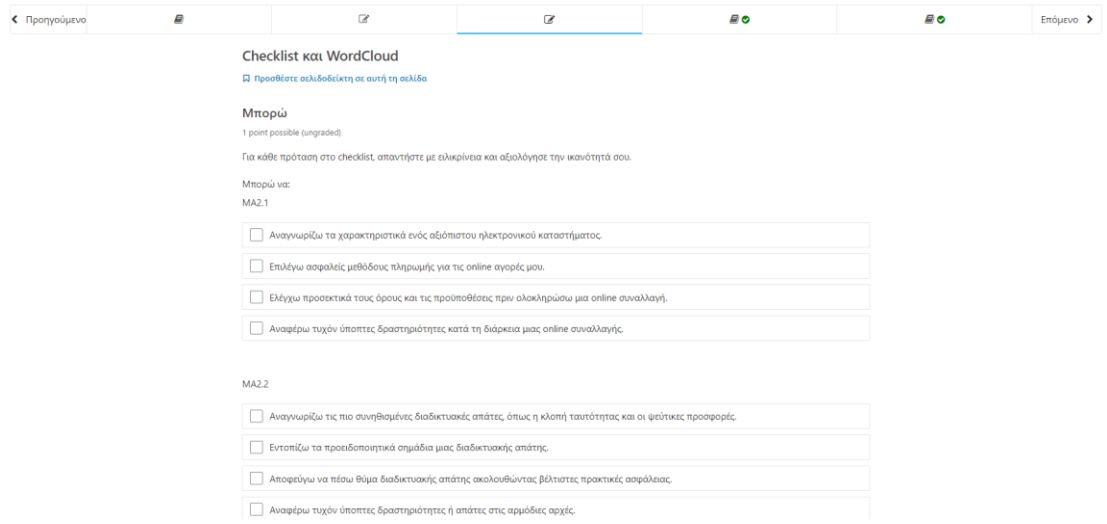
Εικόνα 22:Ανακεφαλαίωση 3.2



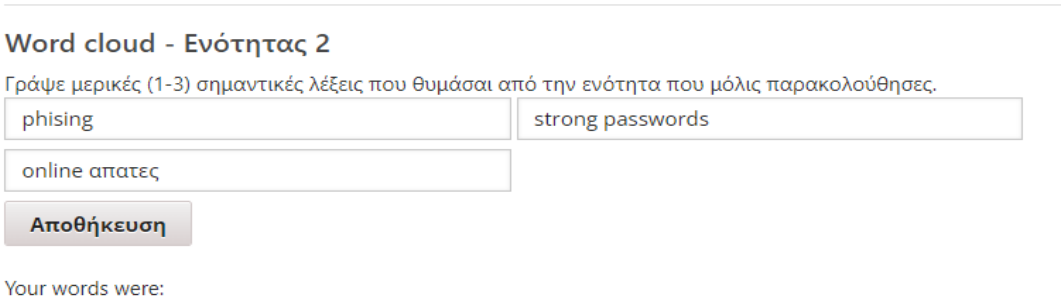
Εικόνα 23:Εργασία Ανοιχτής απόκρισης ενότητας 2



Εικόνα 24:Ενδεικτική ρουμπρίκα



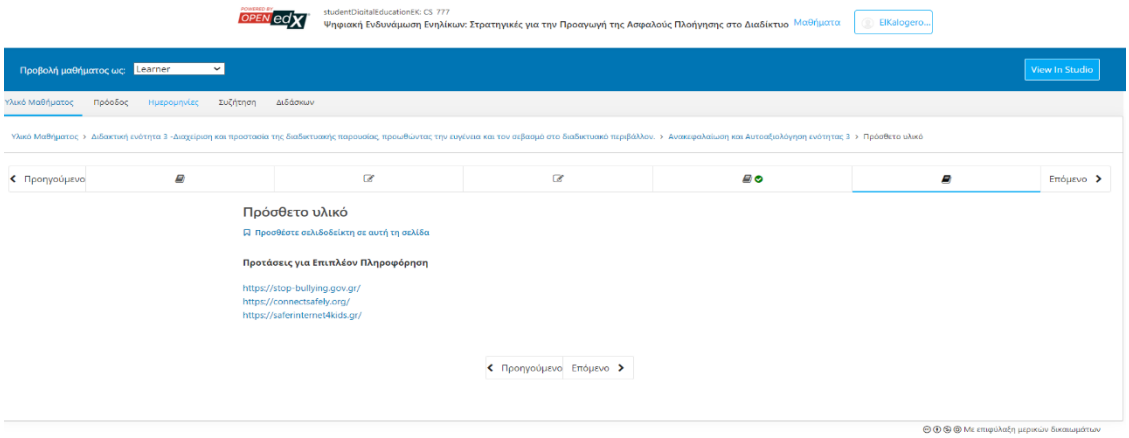
Εικόνα 25:Checklist "Μπορώ να" ενότητα 2



Εικόνα 26:Ερώτηση WordCloud

Εικόνα 27:Αποτέλεσμα WordCloud

Τέλος παρατίθενται διαδικτυακές συνδέσεις με επιπλέον πληροφορίες.



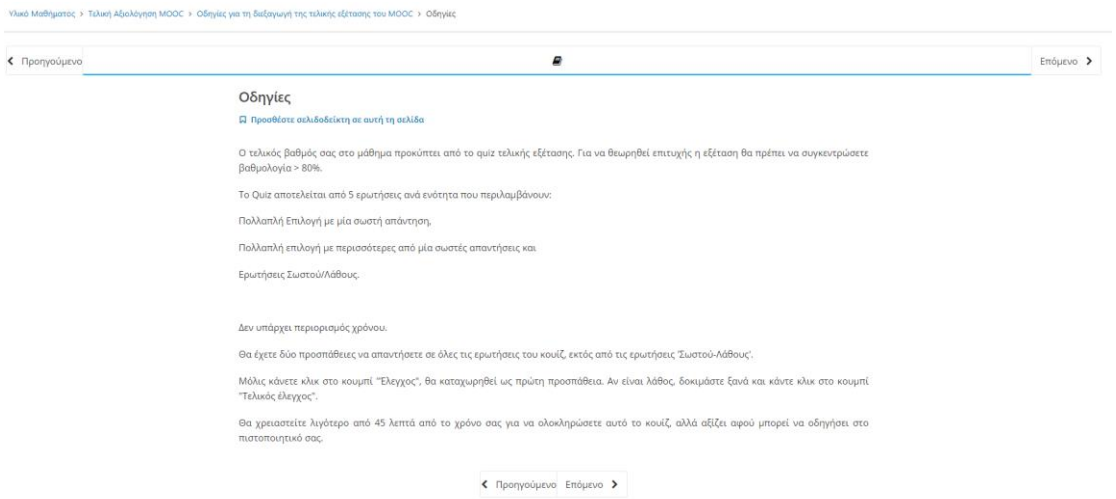
Εικόνα 28:Πρόσθετο Υλικό

4.2.4 Τελική αξιολόγηση MOOC και άλλες σημαντικές σελίδες

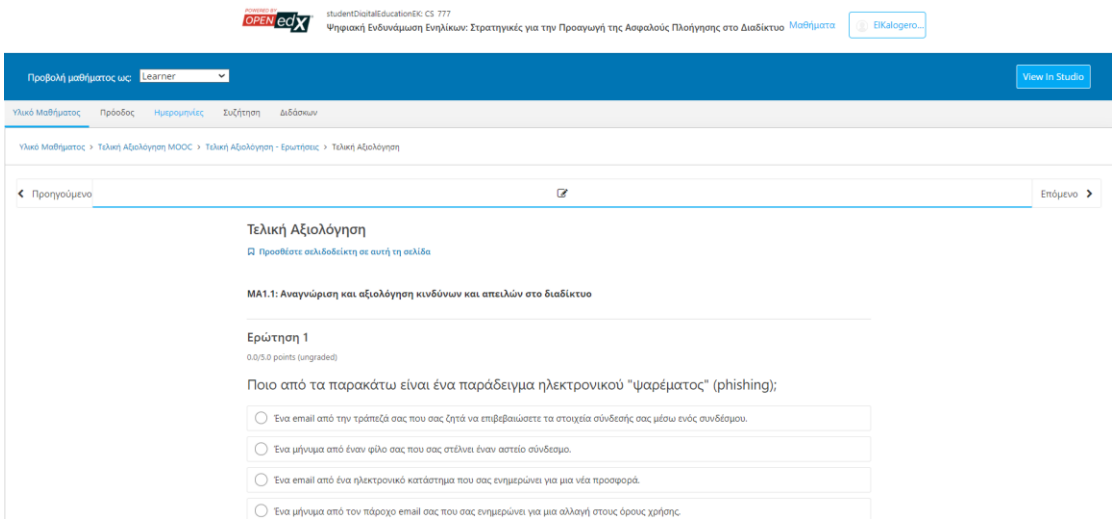
Η τελευταία ενότητα αφορά την τελική αξιολόγηση. Με την επιτυχή ολοκλήρωση της προσφέρεται πιστοποιητικό στον εκπαιδευόμενο.

Έχει όμως από την αρχική σελίδα του MOOC, πριν την εγγραφή, στις συχνές ερωτήσεις διευκρινιστεί ότι το πιστοποιητικό αυτό είναι πλασματικό.

Οι σελίδες αυτής της ενότητας είναι η σελίδα των οδηγιών, η σελίδα των ερωτήσεων της τελικής αξιολόγησης και η σελίδα με τις οδηγίες για την έκδοση του πιστοποιητικού.

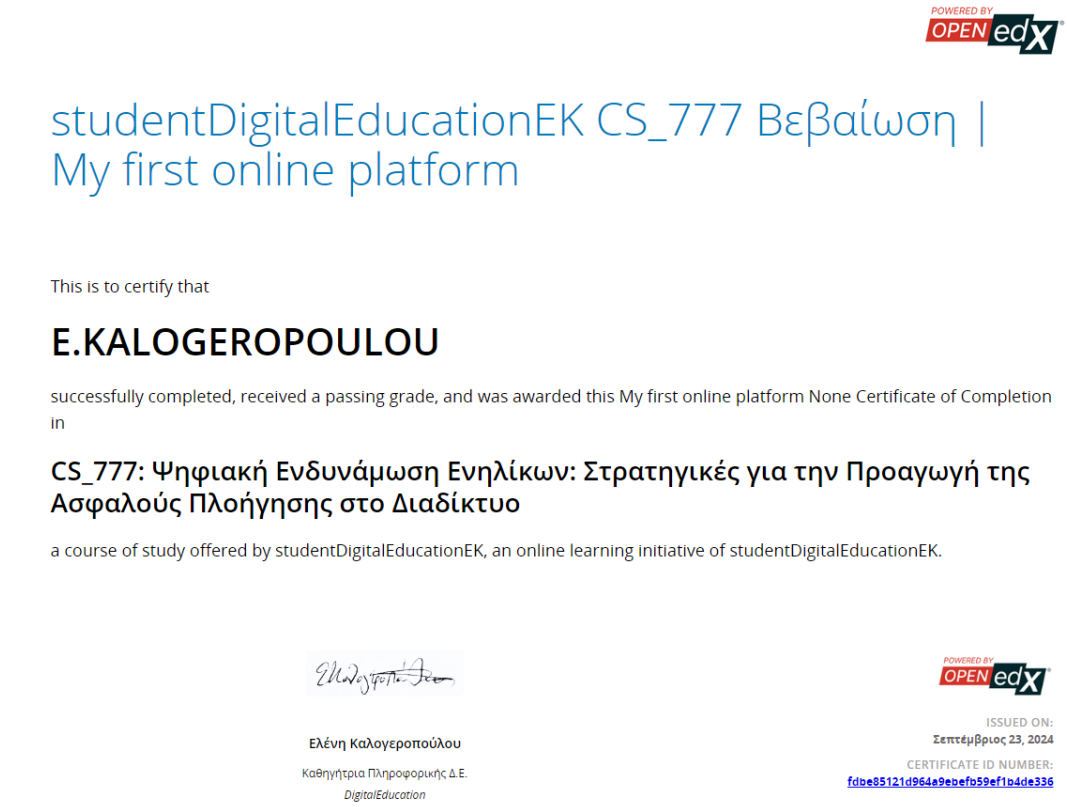


Εικόνα 29:Οδηγίες τελικής εξέτασης



Εικόνα 30:Ερωτήσεις Τελικής αξιολόγησης ενδεικτικά

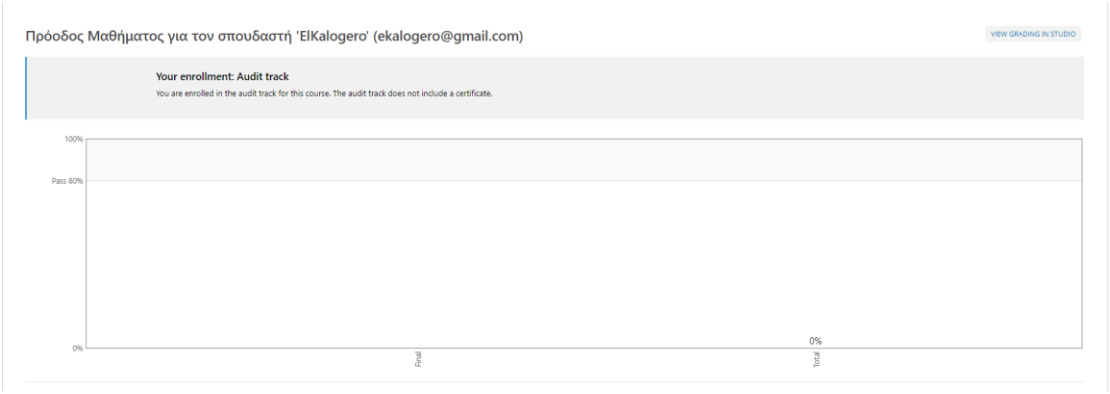
Η έκδοση του πιστοποιητικού φαίνεται στην παρακάτω εικόνα.



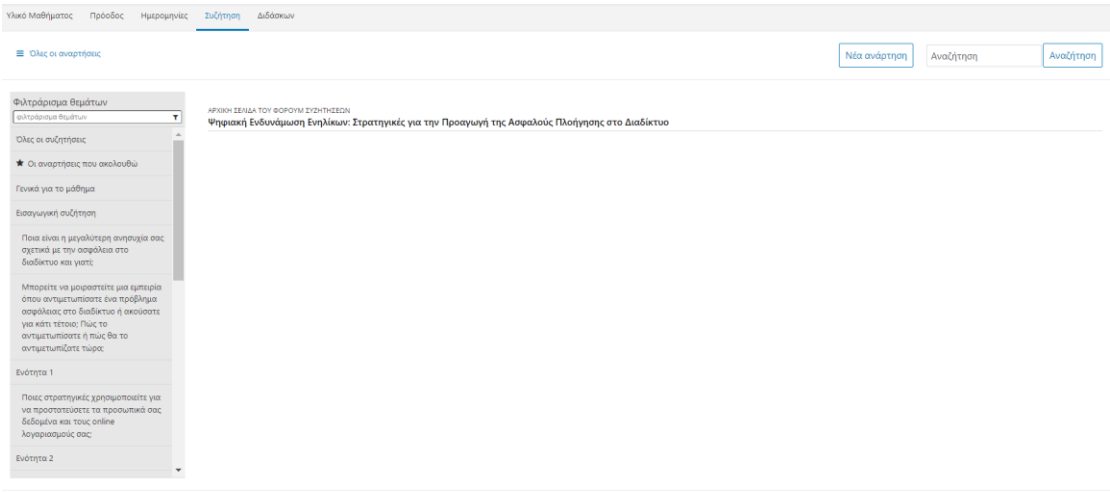
Εικόνα 31:Πιστοποιητικό επιτυχούς ολοκλήρωσης του MOOC

Είναι σημαντικές και οι σελίδες που βρίσκονται στην οριζόντια διάταξη, δίπλα από το πεδίο του υλικού του μαθήματος και δίνουν τη δυνατότητα στον εκπαιδευόμενο να

παρακολουθήσει την πορεία της προόδου του, σημαντικές ημερομηνίες για το μάθημα, το σύνολο των αναρτήσεων σε όλες τις ερωτήσεις στο forum καθώς και πληροφορίες για το διδάσκοντα.



Εικόνα 32: Πρόοδος εκπαιδευομένου



Εικόνα 33:Forum συζητήσεων

Τέλος δίνεται και ο σύνδεσμος του MOOC για εγγραφή και παρακολούθηση: https://studentdigitaleducationek.edunext.io/courses/course-v1:studentDigitalEducationEK+CS_777+2024_T3/about

Κεφάλαιο 5. Αξιολόγηση του διαδικτυακού μαθήματος

5.1 Αξιολόγηση του MOOC για την Ψηφιακή Ενδυνάμωση Ενηλίκων

Η ψηφιακή εποχή έχει αναδείξει την ανάγκη για διαρκή εκπαίδευση και ανάπτυξη ψηφιακών δεξιοτήτων, ιδίως για τους ενήλικες που συχνά αντιμετωπίζουν προκλήσεις στην πλοήγηση και τη χρήση της τεχνολογίας. Η "Ψηφιακή Ενδυνάμωση Ενηλίκων: Στρατηγικές για την Προαγωγή της Ασφαλούς Πλοήγησης στο Διαδίκτυο" αποτελεί ένα καινοτόμο MOOC (Massive Open Online Course) που στοχεύει στην προετοιμασία των ενηλίκων να περιηγούνται με ασφάλεια στο ψηφιακό περιβάλλον. Μέσω αυτού του μαθήματος, οι συμμετέχοντες αποκτούν τις απαραίτητες γνώσεις και δεξιότητες για να προστατεύουν τον εαυτό τους από τις απειλές του διαδικτύου και να αξιοποιούν τις δυνατότητες της τεχνολογίας.

Η αξιολόγηση της αποτελεσματικότητας του MOOC είναι κρίσιμη για τη διασφάλιση ότι πληροί τις εκπαιδευτικές ανάγκες των συμμετεχόντων και τις απαιτήσεις της σύγχρονης ψηφιακής κοινωνίας. Στο πλαίσιο αυτό, θα χρησιμοποιηθεί μια πρότυπη ρούμπρικα αυτοαξιολόγησης που περιλαμβάνει σημαντικά κριτήρια για την αποτίμηση του μαθήματος. Τα κριτήρια αυτά εστιάζουν σε διάφορες πτυχές του MOOC, όπως τα μαθησιακά αποτελέσματα, η εφαρμογή της εκπαιδευτικής προσέγγισης, η καταλληλότητα των ψηφιακών μέσων, η διάρκεια και ο φόρτος εργασίας, καθώς και η σαφήνεια παρουσίασης.

5.2 Αξιολόγηση με Ρούμπρικα

Η αξιολόγηση της αποτελεσματικότητας του MOOC θα γίνει με τη χρήση μιας ρουμπρίκας[4] που περιλαμβάνει τα εξής σημαντικά κριτήρια, όπως αναλύονται στις παρακάτω ενότητες.

5.2.1. Α μέρος: Σχεδίαση του MOOC

Α1. Μαθησιακά Αποτελέσματα

Τα μαθησιακά αποτελέσματα του MOOC θα αξιολογηθούν με βάση την κάλυψη της Ψηφιακής Ικανότητας που έχει επιλεγεί, καθώς και τη συμβατότητά τους με τα αντίστοιχα

[4] Η ρούμπρικα που χρησιμοποιείται για την αυτοαξιολόγηση του μαθήματος βασίζεται στην εργασία 4 του μαθήματος ΨΣ-ΗΜ-721 του μεταπτυχιακού προγράμματος «Ηλεκτρονική Μάθηση».

επίπεδα επάρκειας όπως ορίζονται στο DigiComp 2.2. Αυτό θα περιλαμβάνει την εξέταση της δυνατότητας του μαθήματος να εκπληρώσει τις προσδοκίες των συμμετεχόντων και να καλύψει τις ανάγκες τους.

Α2. Εφαρμογή Constructive Alignment

Η ικανότητα του MOOC να εφαρμόζει την αρχή του Constructive Alignment, δηλαδή τη συμφωνία μεταξύ μαθησιακών αποτελεσμάτων και εργαλείων αξιολόγησης, είναι κρίσιμη για την επιτυχία του. Θα αξιολογηθεί κατά πόσο οι εκπαιδευτικές δραστηριότητες και οι μέθοδοι αξιολόγησης είναι ευθυγραμμισμένες με τους στόχους μάθησης.

Α3. Καταλληλότητα Επιλογής Ψηφιακών Μέσων

Η καταλληλότητα των ψηφιακών μέσων και εργαλείων που χρησιμοποιούνται για τις εκπαιδευτικές δραστηριότητες είναι καθοριστική. Η αξιολόγηση θα περιλάβει την εξέταση της ποιότητας και της ευχρηστίας των ψηφιακών μέσων στις δραστηριότητες παρουσίασης, επίδειξης, εξάσκησης και αξιολόγησης.

Α4. Διάρκεια και Φόρτος Εργασίας

Η διάρκεια των εκπαιδευτικών δραστηριοτήτων και ο φόρτος εργασίας που απαιτείται από τους συμμετέχοντες θα αξιολογηθούν ως προς την επάρκεια, την ελλιπή ή υπερβολική κατανομή χρόνου. Αυτό θα διασφαλίσει ότι οι συμμετέχοντες μπορούν να ολοκληρώσουν τις δραστηριότητες εντός των προβλεπόμενων χρονικών πλαισίων.

Α5. Σαφήνεια Γραφικής Αναπαράστασης

Η σαφήνεια της γραφικής αναπαράστασης του περιεχομένου και η συμβατότητα με το επιδειχθέν πρότυπο είναι επίσης σημαντικά κριτήρια. Η αποτελεσματική παρουσίαση του υλικού μπορεί να επηρεάσει την κατανόηση και τη συμμετοχή των εκπαιδευομένων.

5.2.2 Β Μέρος: Υλοποίηση και Αποτελεσματικότητα της Πλατφόρμας OpenEdX

Η υλοποίηση του MOOC στο περιβάλλον OpenEdX προσφέρει πολλές δυνατότητες για την ενίσχυση της μαθησιακής εμπειρίας. Η αξιολόγηση θα εξετάσει τις εξής πτυχές:

Β1. Αποτελεσματική Χρήση Λειτουργιών OpenEdX

Η πληρότητα της ολοκλήρωσης θα κριθεί με βάση τη συνεπή υλοποίηση του περιεχομένου του μαθήματος, την αισθητική ομοιομορφία, και την ευκολία πλοήγησης στην πλατφόρμα. Η ποικιλία των ψηφιακών μέσων και εργαλείων εκπαιδευτικής τεχνολογίας θα εξεταστεί ως προς την καταλληλότητα και την ευχρηστία τους.

Β2. Περιεχόμενο του Micro-MOOC

Η αξιολόγηση του περιεχομένου θα εξετάσει την πληρότητα και την παρουσίαση των απαιτούμενων πληροφοριών, την εγκυρότητα και την επίκαιρη διατύπωση, καθώς και τη συμμόρφωση με τους κανόνες ακαδημαϊκής ηθικής. Οι μαθησιακές δραστηριότητες θα πρέπει να στοχεύουν στην επίτευξη των μαθησιακών αποτελεσμάτων και να ενθαρρύνουν την ενεργό συμμετοχή.

Β3. Πληροφορίες και Υποστήριξη για τον Εκπαιδευόμενο

Η διαθεσιμότητα πληροφοριών σχετικά με την χρονική διαθεσιμότητα του μαθήματος, τις απαιτήσεις πιστοποίησης και τις δραστηριότητες αξιολόγησης είναι κρίσιμη για την εμπειρία του εκπαιδευόμενου. Οι καθαρές οδηγίες και η ανατροφοδότηση είναι απαραίτητες για την υποστήριξη των συμμετεχόντων.

Πίνακας 10: Κριτήρια αυτοαξιολόγησης MOOC

<table>
<tr><th colspan="4">ΚΡΙΤΗΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ</th></tr>
<tr><td colspan="4">Μέρος Α: Σχεδίαση [Μονάδες 2.5]</td></tr>
<tr><td colspan="4">1. Μαθησιακά Αποτελέσματα (καλύπτουν τις Ψηφιακές Ικανότητες που έχει επιλεγεί;)
Ναι, η σχεδίαση έχει βασιστεί έχοντας ως βάση τα μαθησιακά αποτελέσματα.</td></tr>
<tr><td colspan="4">2. Εφαρμογή Constructive Alignment (Μαθησιακά Αποτελέσματα - Εργαλεία Αξιολόγησης)
Υπάρχει αντιστοιχία των εργαλείων αξιολόγησης με τα μαθησιακά αποτελέσματα.</td></tr>
<tr><td colspan="4">3. Καταλληλότητα της Επιλογής των Ψηφιακών Μέσων / Εργαλείων για τις Εκπαιδευτικές Δραστηριότητες</td></tr>
<tr><td>3α Παρουσίασης</td><td>3β Επίδειξης</td><td>3γ Εξάσκησης</td><td>3δ Αξιολόγησης</td></tr>
<tr><td colspan="4">Τα ψηφιακά μέσα/εργαλεία που έχουν επιλεχθεί είναι κατάλληλα (βίντεο, κείμενο, εικόνες , ερωτήσεις πολλαπλής επιλογής και σωστού - λάθους). Δεν υπάρχει μεγάλη ποικιλία όμως.</td></tr>
<tr><td colspan="4">4. Διάρκεια και φόρτος εργασίας (κατά πόσο οι σχεδιαζόμενες εκπαιδευτικές δραστηριότητες ανταποκρίνονται στον προβλεπόμενο χρόνο – επαρκείς, ελλιπείς ή υπερβολικές;)
Κάποιες δραστηριότητες χρειάζονται λίγο περισσότερο χρόνο από τον προβλεπόμενο, αλλά δεν είναι τόσο σημαντική η διαφορά αυτή (μερικά λεπτά).</td></tr>
</table>

5. **Σαφήνεια γραφικής αναπαράστασης** και **συμβατότητα** με το επιδειχθέν πρότυπο.

   Απόλυτη συμβατότητα με το πρότυπο το οποίο λειτούργησε ως σκελετός της σχεδίασης του μαθήματος αυτού.

Μέρος Β: Υλοποίηση [Μονάδες 7.5]

Β1. Αποτελεσματική χρήση λειτουργιών Open edX για την παροχή μαθησιακής εμπειρίας [2.0]

1. **Πληρότητα ολοκλήρωσης:** Η υλοποίηση του μαθήματος στο περιβάλλον του OpenEdX είναι συνεπής ως προς το περιεχόμενο του μαθήματος, όπως έχει καταγραφεί στο αντίστοιχο έγγραφο.

   Ναι η υλοποίηση έχει γίνει βασισμένη επακριβώς στο έγγραφο της αναλυτικής περιγραφής του περιεχομένου.

2. **Συνολικό αισθητικό αποτέλεσμα και εμπειρία** μάθησης. Ευκολία πλοήγησης, αισθητική ομοιομορφία κλπ

   Σε γενικές γραμμές είναι καλαίσθητο και η ίδια η πλατφόρμα δημιουργεί ένα περιβάλλον ελκυστικό και εύκολο στην πλοήγηση.

3. **Αξιοποίηση ποικιλίας ψηφιακών μέσων/ εργαλείων εκπαιδευτικής τεχνολογίας** με έμφαση στην **καταλληλότητα** και **ευχρηστία** για τις δραστηριότητες α) παρουσίασης, β)επίδειξης, γ) εξάσκησης, δ) αυτό-αξιολόγησης.

   Σε αυτό το σημείο ενώ τα ψηφιακά μέσα/ εργαλεία είναι κατάλληλα και εύχρηστα δεν υπάρχει μεγάλη ποικιλία και επαναλαμβάνονται ανά ενότητα.

4. **Οι ερωτήσεις αυτό-αξιολόγησης** παρέχουν **ανατροφοδότηση** στον εκπαιδευόμενο.

   Η ανατροφοδότηση στις ερωτήσεις αυτοαξιολόγησης χρειάζεται καλύτερο σχεδιασμό.

5. Ύπαρξη **δραστηριοτήτων αλληλεπίδρασης** μεταξύ των εκπαιδευομένων π.χ. μέσω forum συζήτησης.

   *Υπάρχουν αρκετές δραστηριότητες **αλληλεπίδρασης** μεταξύ των εκπαιδευομένων (γνωριμίας και συζητήσεων στο forum ανά διδακτική ενότητα).*

Β2. Περιεχόμενο του micro-MOOC [4.5]

6. **Αποτίμηση γενικής επισκόπησης micro-MOOC** (ως προς την πληρότητα και την παρουσίαση των απαιτούμενων πληροφοριών)

   Σε μεγάλο βαθμό παρουσιάζεται το υλικό του μαθήματος πλήρες. Ίσως κάποια θέματα να αγγίζονται επιφανειακά , αλλά για αρχάριο κοινό και για τη διάρκεια που υλοποιείται φαίνεται ικανοποιητικό.

7. **Το περιεχόμενο του μαθήματος** είναι έγκυρο και επίκαιρο και διατυπώνεται με σαφήνεια.

Το περιεχόμενο είναι έγκυρο και επίκαιρο στο χρόνο που παρουσιάζεται. Κι αυτό γιατί σχετίζεται με τη ψηφιακή τεχνολογία, η οποία μεταβάλλεται με ραγδαίους ρυθμούς, οπότε αναγκαστικά πρέπει να υπάρχει επικαιροποίηση σε τακτά χρονικά διαστήματα.

8. Έχουν τηρηθεί οι κανόνες ακαδημαϊκής ηθικής και δεοντολογίας με έμφαση στη διαχείριση των πνευματικών δικαιωμάτων.

Ναι , όπου χρειάζεται γίνεται η σχετική αναφορά .

9. Οι μαθησιακές δραστηριότητες στοχεύουν στην επίτευξη των μαθησιακών αποτελεσμάτων.

Ναι οι μαθησιακές δραστηριότητες έχουν σχεδιαστεί με γνώμονα τα μαθησιακά αποτελέσματα.

10. Περιλαμβάνονται διαδραστικές μαθησιακές δραστηριότητες που ευνοούν την ενεργό συμμετοχή **.**

Ναι υπάρχουν τέτοιες δραστηριότητες (Padlet, wordcloud, forum)

11. Η **λίστα αναφορών** είναι ενημερωμένη και οι **πρόσθετοι πόροι** είναι σε άμεση σύνδεση με το μάθημα (σαφήνεια, ποιότητα). Έχει γίνει χρήση **ανοικτού περιεχομένου** με κατάλληλη αναφορά στο δημιουργό και όλοι οι **υπερσύνδεσμοι** είναι ενεργοί.

Ναι , αν και χρειάζεται συνεχής έλεγχος για την εμφάνιση του ανοιχτού υλικού τρίτων , γιατί συχνά υπάρχουν αλλάγες.

12. Συνοχή του micro-MOOC. Οι διαφορετικοί δημιουργοί των ενοτήτων του micro-MOOC να έχουν συνεργαστεί για να διασφαλίσουν ότι οι ενότητες, που έχουν σχεδιαστεί, είναι συνεκτικές ως προς τη δομή και τις μεθόδους διδασκαλίας και αξιολόγησης, ώστε να διατηρήσουν τη συνοχή και την ενότητα του εκπαιδευτικού περιεχομένου, αποφεύγοντας τις περιττές επαναλήψεις.

Το συγκεκριμένο MOOC έχει σχεδιαστεί από ένα μόνο πρόσωπο.

Β3. Ο εκπαιδευόμενος έχει στη διάθεσή του: [1.0]

13. Πληροφορίες για τη χρονική διαθεσιμότητα του μαθήματος (ημερολόγιο μαθημάτων, προγραμματισμένη πρόσβαση στις ενότητες των μαθημάτων και σημαντικές ημερομηνίες, συμπεριλαμβανομένων των εξετάσεων), την αναμενόμενη **χρονική δέσμευση, τα μαθησιακά αποτελέσματα, τα προαπαιτούμενα.**

Όλες οι απαραίτητες αυτές πληροφορίες είναι διαθέσιμες στους εκπαιδευομένους σε κατάλληλες ενότητες.

14. Τα **κριτήρια βαθμολόγησης** και οι **απαιτήσεις πιστοποιητικού** έχουν αναρτηθεί στο μάθημα.

Ναι, από την εισαγωγή του μαθήματος οι εκπαιδευόμενοι ενημερώνονται για αυτά τα θέματα.
15. Οδηγίες για τις δραστηριότητες εξάσκησης και (αυτο) αξιολόγησης καθώς και για τη χρήση των φόρουμ, την εθιμοτυπία του φόρουμ. *Υπάρχουν οδηγίες για όλες τις δραστηριότητες εξάσκησης και (αυτο) αξιολόγησης.*

Η αυτοαξιολόγηση του MOOC για την Ψηφιακή Ενδυνάμωση Ενηλίκων μέσω της πρότυπης ρουμπρίκας συμβάλλει στην αναγνώριση των δυνατών σημείων και των αδυναμιών του προγράμματος, καθώς και στη συνεχή βελτίωσή του. Με τη σωστή αξιολόγηση των μαθησιακών αποτελεσμάτων, την εφαρμογή των εκπαιδευτικών εργαλείων και τη συνολική ποιότητα του περιεχομένου, το MOOC μπορεί να διασφαλίσει ότι οι ενήλικες συμμετέχοντες θα αποκτήσουν τις απαραίτητες δεξιότητες για να κινηθούν με ασφάλεια στο ψηφιακό περιβάλλον. Η διαδικασία αυτοαξιολόγησης δεν είναι μόνο ένα εργαλείο για τη βελτίωση της εκπαιδευτικής διαδικασίας, αλλά και μια ευκαιρία για τους εκπαιδευτές να αναστοχαστούν πάνω στις εκπαιδευτικές τους προσεγγίσεις και στρατηγικές.

Κεφάλαιο 6. Συμπεράσματα και Μελλοντικές Προτάσεις για την Ψηφιακή Ενδυνάμωση Ενηλίκων και την Ασφαλή Πλοήγηση στο Διαδίκτυο

6.1 Συμπεράσματα για την Ψηφιακή Ενδυνάμωση Ενηλίκων και την Ασφαλή Πλοήγηση στο Διαδίκτυο

Η ψηφιακή ενδυνάμωση ενηλίκων αποτελεί κρίσιμο παράγοντα για την ανάπτυξη της ικανότητάς τους να προσαρμόζονται στις απαιτήσεις της σύγχρονης κοινωνίας και να χρησιμοποιούν αποτελεσματικά τις ψηφιακές τεχνολογίες (García-Martín & García-Sánchez, 2020). Η ενδυνάμωση αυτή δεν περιορίζεται στην τεχνολογική εκπαίδευση, αλλά επεκτείνεται και στην καλλιέργεια των δεξιοτήτων για την ασφαλή πλοήγηση στο διαδίκτυο. Οι προκλήσεις της ψηφιακής εποχής, όπως οι απειλές για την ασφάλεια και την προστασία των προσωπικών δεδομένων, καθιστούν επιτακτική την ανάγκη για εκπαίδευση σε ζητήματα ψηφιακής ασφάλειας (Livingstone et al., 2017).

Η μελέτη του θέματος της ψηφιακής ενδυνάμωσης ενηλίκων υποδεικνύει ότι η πρόσβαση στις ψηφιακές τεχνολογίες δεν είναι από μόνη της αρκετή για την πλήρη συμμετοχή στην ψηφιακή κοινωνία. Οι ενήλικες χρειάζονται ουσιαστική εκπαίδευση και κατανόηση τόσο των δυνατοτήτων όσο και των κινδύνων που συνεπάγεται η χρήση των ψηφιακών τεχνολογιών (Van Deursen & Van Dijk, 2019). Ειδικότερα, η ασφαλής πλοήγηση στο διαδίκτυο αποτελεί μια κρίσιμη δεξιότητα, καθώς οι ψηφιακοί κίνδυνοι εξελίσσονται διαρκώς. Από τις απλές απειλές όπως τα κακόβουλα προγράμματα μέχρι πιο σύνθετες απειλές όπως η παραπληροφόρηση και η διαδικτυακή εκμετάλλευση, οι ενήλικες πρέπει να είναι σε θέση να προστατεύουν τα προσωπικά τους δεδομένα και την ιδιωτικότητά τους (Helsper & Eynon, 2013).

6.1.1 Ανάγκη για Ψηφιακή Ενδυνάμωση

Ένα από τα βασικά ευρήματα της ανάλυσης είναι ότι η ψηφιακή ενδυνάμωση πρέπει να είναι ολιστική και διαρκής. Η ανάπτυξη δεξιοτήτων ψηφιακής ασφάλειας δεν είναι μια διαδικασία που ολοκληρώνεται άμεσα, αλλά απαιτεί συνεχή προσαρμογή και ενημέρωση (García-Martín & García-Sánchez, 2020). Οι τεχνολογικές εξελίξεις είναι ραγδαίες και οι απειλές εξελίσσονται συνεχώς, γεγονός που καθιστά απαραίτητη την καλλιέργεια μιας νοοτροπίας δια βίου μάθησης στην ψηφιακή ασφάλεια.

Η έρευνα καταδεικνύει ότι οι ενήλικες, ιδίως εκείνοι που δεν είναι εξοικειωμένοι με τις νέες τεχνολογίες, διατρέχουν μεγαλύτερο κίνδυνο να πέσουν θύματα διαδικτυακών απειλών

(Livingstone et al., 2017). Η ελλιπής γνώση για την ασφάλεια των δεδομένων τους και η έλλειψη συνειδητοποίησης για τους κινδύνους που εγκυμονεί η χρήση του διαδικτύου μπορούν να οδηγήσουν σε σημαντικά προβλήματα, όπως η παραβίαση της ιδιωτικότητας και η κλοπή ταυτότητας (Helsper & Eynon, 2013). Η εκπαίδευση γύρω από τις βασικές αρχές της ασφάλειας στο διαδίκτυο, όπως η χρήση ισχυρών κωδικών πρόσβασης, η προσεκτική διαχείριση των προσωπικών δεδομένων και η γνώση των κακόβουλων πρακτικών, αποτελεί τον ακρογωνιαίο λίθο της προστασίας (Van Deursen & Van Dijk, 2019).

Στρατηγικές για την Ασφαλή Πλοήγηση

Οι στρατηγικές για την ασφαλή πλοήγηση στο διαδίκτυο που εξετάστηκαν περιλαμβάνουν την εκπαίδευση σε τεχνικές αυτοπροστασίας, τη χρήση εργαλείων ασφάλειας, όπως προγράμματα antivirus και VPN, καθώς και τη διάδοση της γνώσης για την ασφαλή χρήση κοινωνικών δικτύων (Helsper & Eynon, 2013). Παράλληλα, η ανάπτυξη της κριτικής σκέψης είναι εξίσου σημαντική, καθώς βοηθά τους ενήλικες να διακρίνουν αξιόπιστες από αναξιόπιστες πηγές πληροφοριών και να αποφεύγουν την παραπληροφόρηση και τα fake news (Livingstone et al., 2017).

Η στρατηγική αυτή ενισχύεται με την υιοθέτηση πολιτικών που ενθαρρύνουν την υπεύθυνη χρήση του διαδικτύου. Παράδειγμα τέτοιων πολιτικών είναι η προώθηση των δικαιωμάτων ψηφιακής ασφάλειας και ιδιωτικότητας, καθώς και η επιβολή κανονισμών που επιβάλλουν στις εταιρείες να ενημερώνουν τους χρήστες για τις πολιτικές διαχείρισης των δεδομένων τους (García-Martín & García-Sánchez, 2020).

6.2 Μελλοντικές Προτάσεις για Βελτίωση

Η ανάλυση καταδεικνύει ότι η ψηφιακή ενδυνάμωση ενηλίκων στον τομέα της ασφάλειας στο διαδίκτυο μπορεί να βελτιωθεί μέσω μιας σειράς στρατηγικών που ενσωματώνουν τόσο την τεχνολογική εκπαίδευση όσο και την ανάπτυξη δεξιοτήτων ψηφιακής ασφάλειας (Van Deursen & Van Dijk, 2019). Μερικές προτάσεις για μελλοντικές βελτιώσεις περιλαμβάνουν:

1. Δημιουργία Εξειδικευμένων Εκπαιδευτικών Προγραμμάτων:

Η ανάπτυξη προγραμμάτων ψηφιακής εκπαίδευσης που εστιάζουν αποκλειστικά στην ασφάλεια στο διαδίκτυο για ενήλικες θα πρέπει να αποτελεί βασικό στόχο των κυβερνήσεων και των εκπαιδευτικών οργανισμών. Τα προγράμματα αυτά θα πρέπει να

καλύπτουν ένα ευρύ φάσμα θεμάτων, από βασικά θέματα ασφάλειας μέχρι προηγμένες τεχνικές προστασίας προσωπικών δεδομένων (García-Martín & García-Sánchez, 2020).

2. Δια βίου Μάθηση και Ενημέρωση:

Όπως ήδη αναφέρθηκε, οι γνώσεις και οι τεχνολογίες στον τομέα της ψηφιακής ασφάλειας εξελίσσονται διαρκώς. Προγράμματα δια βίου μάθησης και τακτικής ενημέρωσης των ενηλίκων σχετικά με νέες απειλές και τρόπους αντιμετώπισης είναι απαραίτητα για τη διατήρηση της ψηφιακής ασφάλειας (Helsper & Eynon, 2013).

3. Δημιουργία Ψηφιακών Κοινοτήτων Υποστήριξης:

Μια από τις πιο αποτελεσματικές στρατηγικές είναι η δημιουργία διαδικτυακών κοινοτήτων μάθησης, όπου οι ενήλικες θα μπορούν να ανταλλάσσουν εμπειρίες και να μαθαίνουν από ειδικούς και ομότιμους. Οι κοινότητες αυτές μπορούν να υποστηρίζουν τη συνεχή ενημέρωση και την κοινή χρήση εργαλείων και στρατηγικών ασφαλείας (Livingstone et al., 2017).

4.Ενσωμάτωση της Ψηφιακής Ασφάλειας στα Εκπαιδευτικά Συστήματα:

Η ψηφιακή ασφάλεια θα πρέπει να ενσωματωθεί πιο ουσιαστικά στα τυπικά εκπαιδευτικά προγράμματα, προκειμένου οι νέες γενιές ενηλίκων να είναι καλύτερα προετοιμασμένες για τους κινδύνους της ψηφιακής εποχής. Οι κυβερνήσεις και οι εκπαιδευτικοί οργανισμοί πρέπει να ενσωματώσουν μαθήματα ψηφιακής ασφάλειας στις διάφορες βαθμίδες εκπαίδευσης (Van Deursen & Van Dijk, 2019).

5. Διεθνής Συνεργασία και Ρυθμιστικά Πλαίσια:

Η προστασία της ιδιωτικότητας και της ασφάλειας των δεδομένων είναι παγκόσμιο ζήτημα. Η συνεργασία μεταξύ χωρών για την ανάπτυξη κοινών κανονισμών και ρυθμιστικών πλαισίων μπορεί να συμβάλει στη βελτίωση της ασφάλειας στο διαδίκτυο. Διεθνείς οργανισμοί θα πρέπει να συνεχίσουν να διαμορφώνουν και να προωθούν πρότυπα ασφαλείας (García-Martín & García-Sánchez, 2020).

6. Χρήση Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης:

Η τεχνητή νοημοσύνη και η μηχανική μάθηση μπορούν να χρησιμοποιηθούν για την αυτόματη ανίχνευση και πρόληψη διαδικτυακών απειλών. Τα συστήματα αυτά μπορούν να ενισχύσουν την ασφάλεια του διαδικτύου μέσω πιο εξελιγμένων και αυτόματων μηχανισμών προστασίας (Helsper & Eynon, 2013).

Συνοψίζοντας, η ψηφιακή ενδυνάμωση ενηλίκων και η ανάπτυξη δεξιοτήτων ασφαλούς

πλοήγησης στο διαδίκτυο είναι ζωτικής σημασίας για τη σύγχρονη κοινωνία. Η εκπαίδευση στις ψηφιακές τεχνολογίες πρέπει να επικεντρώνεται όχι μόνο στην παροχή πρόσβασης αλλά και στην προστασία των χρηστών από τις απειλές της ψηφιακής εποχής. Οι στρατηγικές που προτάθηκαν για την ενδυνάμωση των ενηλίκων στην ασφαλή πλοήγηση μπορούν να συμβάλουν στη δημιουργία μιας πιο προστατευμένης και ενημερωμένης ψηφιακής κοινωνίας. Οι προτάσεις για μελλοντικές βελτιώσεις μπορούν να υποστηρίξουν την ανάπτυξη μιας ασφαλούς και υπεύθυνης διαδικτυακής παρουσίας για όλους τους πολίτες.

Βιβλιογραφικές Αναφορές (APA)

Bruck, P. A., Motiwalla, L., & Foerster, F. (2012). Mobile learning with micro-content: A framework and evaluation. BLED 2012 Proceedings.

Chuang, I., & Ho, A. (2016). HarvardX and MITx: Four Years of Open Online Courses.

García-Martín, J., & García-Sánchez, J. N. (2020). The digital competence of university students: A systematic literature review. Aloma: Revista de Psicologia, Ciències de l'Educació i de l'Esport, 38(1), 63-74.

Ghazal, S., Samsudin, M. A., & Al-Qahtani, S. A. (2019). Open edX: The revolution of e-learning. Journal of Advanced Research in Dynamical and Control Systems, 11(7), 1821-1828.

Helsper, E. J., & Eynon, R. (2013). Distinct skill pathways to digital engagement. New Media & Society, 15(5), 769-785.

Hug, T. (2005). Micro Learning and Narration: Exploring possibilities of utilization of narrations and storytelling for the design of "micro units" and didactical micro-learning arrangements. Proceedings of Media in Transition.

Kizilcec, R., & Schneider, E. (2015). Motivations for Learning in Massive Open Online Courses. ACM Learning at Scale.

Leong, P. (2016). Mobile Microlearning: A New Way to Learn in the Mobile Age.

Li, K. C. (2019). The Future of MOOCs: Exploring Opportunities for the Future of Digital Learning. International Journal of Education and Management Engineering, 9(2), 25-34. https://doi.org/10.5815/ijeme.2019.02.03

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2017). EU Kids Online. London: LSE.

Pappas, C. (2016). Microlearning: A Powerful Way To Measure Learning Effectiveness. eLearning Industry.

Shah, D. (2020). By The Numbers: MOOCs in 2020. Class Central.

Siemens, G. (2013). Massive Open Online Courses: Innovation in Education? Open Educational Resources: Innovation, Research and Practice.

Suparak, R. (2020). Adoption of OpenEdX in higher education institutions. International Journal of Technology in Education, 3(2), 98-104.

Van Deursen, A. J., & Van Dijk, J. A. (2019). The first-level digital divide shifts to differences in usage. New Media & Society, 21(2), 354-375.

Waldrop, M. M. (2013). Campus 2.0. Nature, 495(7440), 160-163.

Zheng, Y. (2018). A comparative study of OpenEdX and Moodle. Journal of Educational Technology & Society, 21(4), 12-19.

Παράρτημα :Ολοκληρωμένη έκδοση του μαθήματος σε μορφή κειμένου «Ψηφιακή Ενδυνάμωση Ενηλίκων: Στρατηγικές για την Προαγωγή της Ασφαλούς Πλοήγησης στο Διαδίκτυο»

Ημέρα 1: Εγγραφή και Εισαγωγή στο MOOC (1 ώρα)

1.1 Σχετικά με αυτό το μάθημα

Act_ID#1.1.1 Καλωσόρισμα [Βίντεο]

Εισαγωγικό βίντεο καλωσορίσματος στο μάθημα.

https://www.youtube.com/shorts/ZB54FE17t_A

[End_of_Page]

Act_ID#1.1.2 Εισαγωγή – Σκοπός [Υπερκείμενο και εικόνα]

Καλωσορίσατε στον συναρπαστικό κόσμο του διαδικτύου! Το διαδίκτυο έχει μεταμορφώσει τον τρόπο που επικοινωνούμε, μαθαίνουμε, εργαζόμαστε και διασκεδάζουμε. Ωστόσο, αυτή η ψηφιακή επανάσταση συνοδεύεται και από προκλήσεις. Από την προστασία των προσωπικών μας δεδομένων μέχρι την αποφυγή διαδικτυακών απατών και την υπεύθυνη χρήση των κοινωνικών μέσων, η ασφαλής πλοήγηση στο διαδίκτυο απαιτεί γνώση και επαγρύπνηση. Το μάθημα "Ψηφιακή Ενδυνάμωση Ενηλίκων: Ασφαλής Πλοήγηση στο Διαδίκτυο" έχει σχεδιαστεί για να σας εξοπλίσει με τις απαραίτητες δεξιότητες και γνώσεις ώστε να αξιοποιήσετε στο έπακρο τις δυνατότητες του διαδικτύου, διασφαλίζοντας παράλληλα την ασφάλεια και την ιδιωτικότητά σας.

Στο τέλος αυτού του μαθήματος, θα είστε σε θέση να πλοηγήστε στο διαδίκτυο με αυτοπεποίθηση και ασφάλεια, έχοντας αποκτήσει τις απαραίτητες ψηφιακές δεξιότητες για να συμμετέχετε ενεργά στην ψηφιακή κοινωνία.

[End_of_Page]

Act_ID#1.1.3 Μαθησιακά Αποτελέσματα [Υπερκείμενο]

Το μάθημα "Ψηφιακή Ενδυνάμωση Ενηλίκων: Ασφαλής Πλοήγηση στο Διαδίκτυο" έχει σχεδιαστεί με γνώμονα το Ευρωπαϊκό Πλαίσιο Ψηφιακών Ικανοτήτων για τους Πολίτες (DigComp 2.2), το οποίο αποτελεί έναν οδηγό για την ανάπτυξη των απαραίτητων δεξιοτήτων για την αποτελεσματική και ασφαλή χρήση των ψηφιακών τεχνολογιών.

Ο/Η εκπαιδευόμενος/η μετά την παρακολούθηση του MOOC θα είναι ικανός/η να:

MA1 [understand/ analyze]: κατανοεί τις βασικές αρχές ψηφιακής ασφάλειας και να λειτουργεί σύμφωνα με αυτές τις αρχές.

Το **MA1** αναλύεται σε επιμέρους MA, ως εξής:

- **ΜΑ1.1** Μπορώ να αναγνωρίζω και να αξιολογώ τους κινδύνους και τις απειλές που σχετίζονται με τη χρήση του διαδικτύου, όπως το ηλεκτρονικό "ψάρεμα" (phishing), το κακόβουλο λογισμικό και η παραπληροφόρηση.
- **ΜΑ1.2** Μπορώ να δημιουργώ ισχυρούς κωδικούς πρόσβασης, να τους διαχειρίζομαι με ασφάλεια και να προστατεύω τα προσωπικά μου δεδομένα στο διαδίκτυο.

ΜΑ2 [understand/evaluate]: κατανοεί ποιες είναι οι ασφαλείς συναλλαγές και αγορές.

Το **ΜΑ2** αναλύεται σε επιμέρους ΜΑ, ως εξής:

- **ΜΑ2.1** Μπορώ να πραγματοποιώ ασφαλείς ηλεκτρονικές συναλλαγές και αγορές, χρησιμοποιώντας αξιόπιστες μεθόδους πληρωμής και αναγνωρίζοντας αξιόπιστα ηλεκτρονικά καταστήματα.
- **ΜΑ2.2** Μπορώ να αναγνωρίζω και να αποφεύγω διαδικτυακές απάτες, όπως η κλοπή ταυτότητας και οι ψεύτικες προσφορές.

ΜΑ3 [understand/evaluate] κατανοεί τι σημαίνει υπεύθυνη χρήση κοινωνικών δικτύων.

Το **ΜΑ3** αναλύεται σε επιμέρους ΜΑ, ως εξής:

- **ΜΑ3.1** Μπορώ να διαχειρίζομαι αποτελεσματικά την παρουσία μου στα κοινωνικά δίκτυα, προσαρμόζοντας τις ρυθμίσεις απορρήτου και προστατεύοντας τη διαδικτυακή μου φήμη.
- **ΜΑ3.2** Μπορώ να αναγνωρίζω και να αντιμετωπίζω τη διαδικτυακή παρενόχληση (cyberbullying), προωθώντας την ευγένεια και τον σεβασμό στο διαδικτυακό περιβάλλον.

ΜΑ4 [understand/evaluate/create]: κατανοεί και να εφαρμόζει τους τρόπους προστασίας των παιδιών και της οικογένειας στο διαδίκτυο.

Το **ΜΑ4** αναλύεται σε επιμέρους ΜΑ, ως εξής:

- **ΜΑ4.1** Μπορώ να αναγνωρίζω τους κινδύνους που αντιμετωπίζουν τα παιδιά στο διαδίκτυο και να εφαρμόζω κατάλληλα μέτρα προστασίας, όπως εργαλεία γονικού ελέγχου και ασφαλείς ρυθμίσεις στις συσκευές.
- **ΜΑ4.2** Μπορώ να δημιουργώ ένα ασφαλές και υποστηρικτικό διαδικτυακό περιβάλλον για την οικογένειά μου, ενθαρρύνοντας την ανοιχτή επικοινωνία και την εκπαίδευση σχετικά με την ασφαλή χρήση του διαδικτύου.

[End_of_Page]

Act_ID#1.1.4 Δομή του MOOC [Υπερκείμενο]

Το μάθημα είναι συνολικής διάρκειας 14 ωρών και μπορεί να ολοκληρωθεί σε 6 ημέρες.

Το μάθημα αυτό αποτελείται από:

- Εισαγωγή
- Διδακτική Ενότητα 1 – Κατανόηση των βασικών αρχών ψηφιακής ασφάλειας και πράξη σύμφωνα με αυτές τις αρχές. [MA1]
- Διδακτική Ενότητα 2 – Αξιολόγηση και διαχείριση των διαδικτυακών συναλλαγών και αγορών. [MA2]
- Διδακτική Ενότητα 3 – Διαχείριση και προστασία της διαδικτυακής παρουσίας, προωθώντας την ευγένεια και τον σεβασμό στο διαδικτυακό περιβάλλον. [MA3]
- Διδακτική Ενότητα 4 – Προστασία Παιδιών και Οικογένειας στο Διαδίκτυο. [MA4]
- Αξιολόγηση του μαθήματος

Κάθε Διδακτική Ενότητα περιλαμβάνει:

- Εισαγωγή (10')
- 2 υποενότητες διάρκειας 1 ώρας η κάθε μία. Η κάθε υποενότητα αποτελείται από:
    - ο Δραστηριότητα παρουσίασης (15')
    - ο Δραστηριότητα επίδειξης (15')
    - ο Δραστηριότητα εξάσκησης (15')
    - ο Δραστηριότητα αυτοαξιολόγησης (15')
- Ανακεφαλαίωση που περιλαμβάνει (50'):
    - ο Ανακεφαλαίωση της ενότητας (5')
    - ο Εργασία εφαρμογής Open Response Assignment που αυτοαξιολογούν οι εκπαιδευόμενοι με τη βοήθεια ρουμπρίκας (30')
    - ο Λίστα Ελέγχου επίτευξης μαθησιακών αποτελεσμάτων με τη μορφή Checklist (5')
    - ο Forum συζήτησης (10')

[End_of_Page]

Act_ID#1.1.5 Άδεια χρήσης [Υπερκείμενο]

Το μάθημα αυτό διατίθεται με άδεια χρήσης ως εξής:

Μπορείτε να:

- Μοιραστείτε — αντιγράψετε και αναδιανέμετε το υλικό με κάθε μέσο και τρόπο για κάθε σκοπό, ακόμα και εμπορικό.
- Προσαρμόστε — αναμείξτε, τροποποιήστε και δημιουργήστε πάνω στο υλικό για κάθε σκοπό, ακόμα και εμπορικό.
- Ο αδειοδότης δεν μπορεί να ανακαλέσει αυτές τις ελευθερίες όσο εσείς ακολουθείτε τους όρους της άδειας.

Υπό τους ακόλουθους όρους:

- Αναφορά Δημιουργού — Θα πρέπει να καταχωρήσετε αναφορά στον δημιουργό με σύνδεσμο της άδειας, και με αναφορά αν έχουν γίνει αλλαγές. Μπορείτε να το κάνετε αυτό με οποιονδήποτε εύλογο τρόπο, αλλά όχι με τρόπο που να υπονοεί ότι ο δημιουργός αποδέχεται το έργο σας ή τη χρήση που εσείς κάνετε.
- Παρόμοια Διανομή — Αν αναμείξετε, τροποποιήσετε, ή δημιουργήσετε πάνω στο υλικό, πρέπει να διανείμετε τις δικές σας συνεισφορές υπό την ίδια άδεια όπως και το πρωτότυπο. Δεν υπάρχουν πρόσθετοι περιορισμοί — Δε μπορείτε να εφαρμόσετε νομικούς όρους ή τεχνολογικά μέτρα που να περιορίζουν νομικά τους άλλους από το να κάνουν οτιδήποτε επιτρέπει η άδεια.

[End_of_Page]

Act_ID#1.1.6 Δημιουργός του MOOC [Υπερκείμενο]

Ελένη Καλογεροπούλου:

Είμαι απόφοιτος του τμήματος Ηλεκτρολόγων Μηχανικών και Τεχνολογίας Υπολογιστών του Πανεπιστημίου Πατρών το 2002. Είμαι κάτοχος παιδαγωγικής επάρκειας σεμιναρίου του ΕΚΠΑ. Από το 2005 εως το 2021 εργάστηκα ως ωρομίσθια και αναπληρώτρια καθηγήτρια πληροφορικής (ΠΕ86) στην πρωτοβάθμια και δευτεροβάθμια εκπαίδευση. Το 2021 διορίστηκα ως μόνιμη εκπαιδευτικός ειδικότητας ηλεκτρολογίας (ΠΕ83) και από τότε εως σήμερα εργάζομαι στην επαγγελματική δευτεροβάθμια εκπαίδευση.

[End_of_Page]

1.2 Προαπαιτούμενα

Act_ID#1.2.1 Προαπαιτούμενες Γνώσεις και Δεξιότητες [Υπερκείμενο]

Η σύνδεση των μαθησιακών αποτελεσμάτων με το πλαίσιο ψηφιακών ικανοτήτων DigComp2.2 ορίζει και τις προαπαιτούμενες ικανότητες των εκπαιδευομένων ως εξής:

Ο/Η εκπαιδευόμενος/η θα πρέπει με καθοδήγηση να μπορεί στοιχειωδώς να:

- κρίνει την ακρίβεια και την καταλληλότητα των πληροφοριών. (Ψηφιακή Ικανότητα : 1.2 Αξιολόγηση δεδομένων, πληροφοριών και ψηφιακού περιεχομένου)
- χρησιμοποιεί ψηφιακές τεχνολογίες για να επικοινωνεί με άλλους. (Ψηφιακή Ικανότητα : 2.1 Αλληλεπίδραση μέσω ψηφιακών τεχνολογιών)
- κοινοποιεί δεδομένα, πληροφορίες και περιεχόμενο με άλλους μέσω ψηφιακών τεχνολογιών. (Ψηφιακή Ικανότητα : 2.2 Κοινοποίηση μέσω ψηφιακών τεχνολογιών)
- συνεργάζεται με άλλους χρησιμοποιώντας ψηφιακές τεχνολογίες και εργαλεία. (Ψηφιακή Ικανότητα : 2.3 Συνεργασία μέσω ψηφιακών τεχνολογιών)
- χρησιμοποιεί ψηφιακές υπηρεσίες για συμμετοχή στην κοινωνία (π.χ. σε δημόσιες ή κοινωνικές διαδικασίες).((Ψηφιακή Ικανότητα : 2.4 Ηλεκτρονική συμμετοχή)
- επιλέγει απλούς τρόπους ρύθμισης και προσαρμογής των ψηφιακών περιβαλλόντων στις προσωπικές του ανάγκες (Ψηφιακή Ικανότητα : 5.2 Προσδιορίζω ανάγκες και τεχνολογικές λύσεις)
- δείχνει ενδιαφέρον ατομικά και συλλογικά για συμμετοχή σε απλές γνωστικές διαδικασίες κατανόησης και αποσαφήνισης απλών εννοιολογικών προβλημάτων και προβληματικών καταστάσεων σε ψηφιακά περιβάλλοντα (Ψηφιακή Ικανότητα : 5.3 Χρησιμοποιώ δημιουργικά τις ψηφιακές τεχνολογίες)

[End_of_Page]

Act_ID#1.2.2 Απαιτούμενες Υποδομές [Υπερκείμενο]

Οι ελάχιστες απαιτούμενες υποδομές είναι :

- Πρόσβαση στο διαδίκτυο
- Ύπαρξη ηλεκτρονικού υπολογιστή

[End_of_Page]

1.3 Ολοκλήρωση του μαθήματος

Act_ID#1.3.1 Απαραίτητες ενέργειες [Υπερκείμενο]

Για την ολοκλήρωση του μαθήματος αυτού θα πρέπει:

- να παρακολουθήσετε το εκπαιδευτικό υλικό των ενοτήτων 1-4
- να υλοποιήσετε τις δραστηριότητες που περιλαμβάνονται στις ενότητες 1-4 και συγκεκριμένα να ολοκληρώσετε:
    - τις δραστηριότητες εξάσκησης
    - τις δραστηριότητες αυτοαξιολόγησης

- να υλοποιήσετε τις εργασίες ανοικτής απόκρισης (Open Response Assignments – ORA) και να τις αυτοαξιολογήσετε με βάση τη ρουμπρίκα
- να συμμετέχετε στο forum υποβάλλοντας τουλάχιστον μία απάντηση και σχολιάζοντας τουλάχιστον μία ανάρτηση
- να απαντήσετε στο poll αυτοαξιολόγησης των ενοτήτων 1-4
- να επιτύχετε βαθμό > 80% στο τελικό quiz Αξιολόγησης του μαθήματος

Μπορείτε να παρακολουθείτε την πρόοδό σας ανά πάσα στιγμή από το tab Progress (Πρόοδος).

[End_of_Page]

Act_ID#1.3.2 Εργασίες αξιολόγησης [Υπερκείμενο]

Εργαλείο Αξιολόγησης 1: Αυτοαξιολόγηση ενότητας με τη χρήση εργασίας ανοιχτής απάντησης – Open Response Assessment (ORA), που βαθμολογεί ο ίδιος ο εκπαιδευόμενος με τη βοήθεια ρουμπρίκας. Στο τέλος κάθε ενότητας, υπάρχει μία τέτοια εργασία ανοικτής απάντησης] – Αυτοαξιολογεί MA1, MA2, MA3 και MA4.

Εργαλείο Αξιολόγησης 2: Αυτοαξιολόγηση υποενότητας – Για την αυτοαξιολόγηση κάθε υποενότητας έχουν επιλεγεί quizzes Multiple Choice Questions (MCQs) μίας σωστής απάντησης. Αυτοαξιολογεί MA1.1 -MA1.2, MA2.1 -MA2.2, MA3.1 -MA3.2 και MA4.1 -MA4.2.

Εργαλείο Αξιολόγησης 3: Τελική Αξιολόγηση -Γίνεται με τη χρήση ερωτήσεων πολλαπλής επιλογής (Multiple Choice Questions, MCQs) μίας σωστής απάντησης, ερωτήσεων πολλαπλής επιλογής πολλών σωστών απαντήσεων και ερωτήσεις σωστού – λάθους, που βασίζονται σε πολύπλοκες ερωτήσεις κρίσης, έτσι ώστε να αξιολογούνται η κατανόηση και οι δεξιότητες των εκπαιδευομένων.- Αξιολογεί (τελικά) όλα τα MA

Act_ID#1.3.3 Συμμετοχή στο forum [Υπερκείμενο]

Σε κάθε ενότητα υπάρχει forum συζήτησης στο οποίο μπορείτε να μοιραστείτε τις απόψεις σχετικά με το αντικείμενο της ενότητας, όπως και να ρωτήσετε απορίες σχετικά με τις εργασίες. Υπάρχουν επίσης κάποια θέματα συζήτησης που έχουν ξεκινήσει οι εκπαιδευτές σας, στα οποία καλείστε να υποβάλετε τουλάχιστον μία απάντηση καθώς και να σχολιάσετε τουλάχιστον μία ανάρτηση.

Netiquette

Ας ρίξουμε πρώτα μια ματιά στους κανόνες της επικοινωνίας που θα εφαρμοστούν στο

μάθημα, προκειμένου να προωθηθούν ευχάριστες, φιλικές συζητήσεις που είναι πλούσιες σε περιεχόμενο και διευκολύνουν τη μάθηση και τη διαχείριση της γνώσης μεταξύ των συμμετεχόντων:

1. Μείνετε στο θέμα: Τα μηνύματα που ξεφεύγουν από το θέμα δυσκολεύουν τους άλλους συμμετέχοντες να βρουν τις πληροφορίες που χρειάζονται. Βρείτε το καταλληλότερο φόρουμ για το θέμα που θέλετε να μοιραστείτε και μην το δημοσιεύετε πάνω από μία φορά. Εάν θέλετε να αλλάξετε το θέμα, ξεκινήστε μια νέα δημοσίευση.

2. Να δείχνετε σεβασμό: αν διαφωνείτε με μια δημοσίευση, δείξτε την άποψή σας με σεβασμό και αποφύγετε κάθε προσωπική επίθεση.

3. Χρησιμοποιήστε τη δύναμη της ψήφου σας: ψηφίστε τις καλύτερες αναρτήσεις και απαντήσεις χρησιμοποιώντας τα εργαλεία που παρέχει η πλατφόρμα. Επίσης, αν δείτε ότι μια δημοσίευση παραβιάζει τους κανόνες, αναφέρετε την πατώντας το εικονίδιο της σημαίας. Με αυτόν τον τρόπο, μας βοηθάτε να διατηρήσουμε έναν χώρο συζήτησης στον οποίο όλοι αισθάνονται άνετα.

4. Να είστε σαφείς: γράψτε τις ιδέες σας με πληρότητα, προσπαθώντας να κάνετε όλους να καταλάβουν τι θέλετε να πείτε. Χρησιμοποιήστε το χιούμορ και τον σαρκασμό με μεγάλη σύνεση, στη γραπτή γλώσσα συχνά παρερμηνεύονται.

5. Δώστε το πλαίσιο των ερωτήσεων σας: όταν κάνετε ερωτήσεις, δώστε όσες περισσότερες πληροφορίες μπορείτε για την πλαισίωσή τους, π.χ. θέματα που έχετε διαβάσει, ιδέες που είχατε στο παρελθόν για το θέμα, απόψεις που έχετε εξετάσει κ.λπ. Αυτό θα βοηθήσει τους συναδέλφους σας που έχουν παρόμοιες ερωτήσεις και τους συντονιστές να σας δώσουν την ακριβέστερη δυνατή απάντηση.

6. Κάντε αναφορές: Όταν παρουσιάζετε ιδέες, λόγια ή σκέψεις άλλων ανθρώπων, να κάνετε την κατάλληλη αναφορά.

7. Μη χρησιμοποιείτε το φόρουμ για προσωπικούς σκοπούς: τα φόρουμ μαθημάτων δεν είναι εργαλεία για την προώθηση των προϊόντων ή των υπηρεσιών σας. Αν δείτε κάποιον να το χρησιμοποιεί για αυτούς τους σκοπούς, αναφέρετε το πατώντας το εικονίδιο της σημαίας.

8. Προσκαλέστε να συμμετάσχουν στη συζήτηση: στο τέλος μιας δημοσίευσης, ζητήστε από τους συμμετέχοντες να σας πουν τη γνώμη τους, προσκαλέστε τους να συμμετάσχουν στη συζήτηση. Κάτι σαν "Θα ήθελα πολύ να μάθω τι σκέφτεστε εσείς γι' αυτό" είναι ένας καλός τρόπος για να το κάνετε.

Πηγή:

https://courses.edx.org/assetv1:IDBx+IDB20.1x+1T2021+type@asset+block@Discussion_forum_guide_CCE_2021.pdf

Περισσότερες πληροφορίες σχετικά με τη χρήση του forum μπορείτε να βρείτε στον ακόλουθο σύνδεσμο:

https://support.edx.org/hc/en-us/articles/360002095553-How-do-I-add-a-post-in-thediscussion-forum

[End_of_Page]

Act_ID#1.3.4 Τελική εξέταση [Υπερκείμενο]

Ο τελικός βαθμός σας στο μάθημα προκύπτει από τις ερωτήσεις της τελικής εξέτασης. Για να θεωρηθεί επιτυχής η εξέταση θα πρέπει να συγκεντρώσετε βαθμολογία > 80%.

Αυτή η τελική εξέταση αποτελείται από 5 ερωτήσεις ανά ενότητα που περιλαμβάνουν:

- Πολλαπλή Επιλογή με μία σωστή απάντηση,
- Πολλαπλή επιλογή με περισσότερες από μία σωστές απαντήσεις και
- Ερωτήσεις Σωστού-Λάθους.

Δεν υπάρχει περιορισμός χρόνου.

Θα έχετε δύο προσπάθειες να απαντήσετε σε όλες τις ερωτήσεις, εκτός από τις ερωτήσεις 'Σωστού-Λάθους'.

Μόλις κάνετε κλικ στο κουμπί "Έλεγχος", θα καταχωρηθεί ως πρώτη προσπάθεια. Αν είναι λάθος, δοκιμάστε ξανά και κάντε κλικ στο κουμπί "Τελικός έλεγχος".

Θα χρειαστείτε περίπου 50 λεπτά από το χρόνο σας για να ολοκληρώσετε αυτό την εξέταση.

[End_of_Page]

1.4 Εισαγωγή στη θεματική

Act_ID#1.4.1 Επίπεδο εξοικείωσης με την ασφάλεια στο διαδίκτυο[Poll & Discussion]

Αυτό το σύντομο poll θα ελέγξει τις πρότερες γνώσεις σας, ώστε να διασφαλίσει ότι ο κύκλος μαθημάτων θα είναι χρήσιμος για εσάς. Επιλέξτε αυτό που σας αντιπροσωπεύει καλύτερα. Δεν υπάρχουν σωστές και λάθος απαντήσεις.

Πόσο συχνά χρησιμοποιείτε το διαδίκτυο;

- Καθημερινά
- Λίγες φορές την εβδομάδα
- Σπάνια
- Ποτέ

Πόσο άνετα αισθάνεστε να πραγματοποιείτε αγορές ή συναλλαγές στο διαδίκτυο;

- Πολύ άνετα
- Αρκετά άνετα
- Λίγο άνετα
- Καθόλου άνετα

Ποια από τις παρακάτω ενέργειες θεωρείτε ότι συμβάλλει στην προστασία των προσωπικών σας δεδομένων στο διαδίκτυο; (Επιλέξτε όσες ισχύουν)

- Χρήση ισχυρών και μοναδικών κωδικών πρόσβασης για κάθε λογαριασμό
- Ενεργοποίηση του ελέγχου ταυτότητας δύο παραγόντων (2FA)
- Προσοχή στις πληροφορίες που κοινοποιείτε στα κοινωνικά δίκτυα
- Αποφυγή σύνδεσης σε δημόσια δίκτυα Wi-Fi
- Τακτική ενημέρωση του λογισμικού και του λειτουργικού συστήματος των συσκευών σας

Συζήτηση στο forum

Σας ενθαρρύνουμε να αναπτύξετε την απάντησή σας σχετικά με την ασφαλή πλοήγηση στο διαδίκτυο στην ακόλουθη εργασία συζήτησης, δημοσιεύοντας τις απόψεις σας στον πίνακα συζητήσεων. Μπορείτε να συζητήσετε:

1.Ποια είναι η μεγαλύτερη ανησυχία σας σχετικά με την ασφάλεια στο διαδίκτυο και γιατί;

2.Μπορείτε να μοιραστείτε μια εμπειρία όπου αντιμετωπίσατε ένα πρόβλημα ασφάλειας στο διαδίκτυο ή ακούσατε για κάτι τέτοιο; Πώς το αντιμετωπίσατε ή πώς θα το αντιμετωπίζατε τώρα;

[End_of_Page]

Act_ID#1.4.2 Άποψη Ειδικού [Video]

Βασικές συμβουλές για την ασφαλή χρήση του Διαδικτύου και του κινητού τηλεφώνου

OnlineSafety – Part1

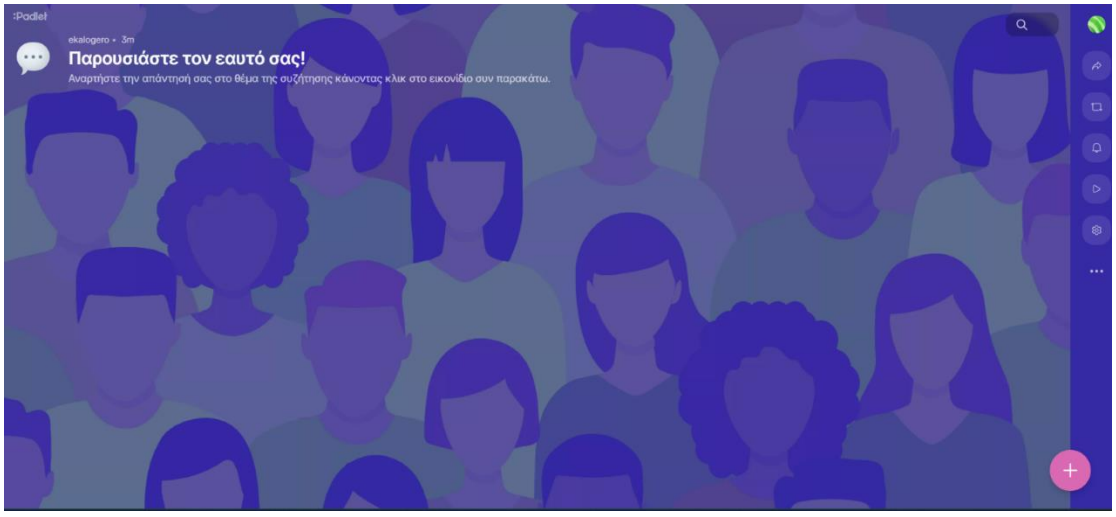
https://www.youtube.com/watch?v=9Uj4REm2nKE

[End_of_Page]

Act_ID#1.4.3 Δραστηριότητα γνωριμίας [εξωτ. εργ. Padlet]

Παρουσιάστε τον εαυτό σας!

Μοιραστείτε μερικές πληροφορίες για εσάς. Αν θέλετε, μπορείτε επίσης να προσθέσετε μια φωτογραφία σας. Χρησιμοποιήστε το παρακάτω Padlet για να προσθέσετε κείμενο, εικόνες, βίντεο, συνδέσμους ή οποιοδήποτε άλλο υλικό που σας εκφράζει. Μπορείτε να κάνετε διπλό κλικ οπουδήποτε ή να πατήσετε το σύμβολο "+" κάτω δεξιά για να ξεκινήσετε.



https://padlet.com/ekalogero/padlet-mg2qri80u92fpp94

[End_of_Page]

[End_of_Topic]

Ημέρα 2: Διδακτική Ενότητα 1 – Βασικές Αρχές Ψηφιακής Ασφάλειας (3 ώρες)

2.0 Εισαγωγή Διδακτικής ενότητας 1

Act_ID#2.0.1 Μαθησιακά αποτελέσματα [Υπερκείμενο & Poll]

Μετά την παρακολούθηση της διδακτικής ενότητας 1 θα είσαι ικανός/η να:

MA1 [understand/ analyze]: κατανοείς τις βασικές αρχές ψηφιακής ασφάλειας και να λειτουργείς σύμφωνα με αυτές τις αρχές.

Το **MA1** αναλύεται σε επιμέρους μαθησιακά αποτελέσματα, ως εξής:

● **MA1.1** Να αναγνωρίζεις και να αξιολογείς τους κινδύνους και τις απειλές που σχετίζονται με τη χρήση του διαδικτύου, όπως το ηλεκτρονικό "ψάρεμα" (phishing), το κακόβουλο λογισμικό και η παραπληροφόρηση.

● **MA1.2** Να δημιουργείς ισχυρούς κωδικούς πρόσβασης, να τους διαχειρίζεσαι με ασφάλεια και να προστατεύεις τα προσωπικά μου δεδομένα στο διαδίκτυο.

Poll

Αυτό το σύντομο ερωτηματολόγιο θα ελέγξει τις πρότερες γνώσεις σας. Επιλέξτε αυτό που σας αντιπροσωπεύει καλύτερα. Δεν υπάρχουν σωστές και λάθος απαντήσεις.

1.Πόσο καλά κατανοείτε τις βασικές αρχές της ψηφιακής ασφάλειας;

- Καθόλου
- Μέτρια
- Ικανοποιητικά
- Πολύ

2. Πόσο συχνά εφαρμόζετε πρακτικές ψηφιακής ασφάλειας στην καθημερινή σας χρήση του διαδικτύου (π.χ., ισχυροί κωδικοί πρόσβασης, ενημερώσεις λογισμικού, προσοχή σε συνδέσμους);

- Καθόλου
- Μέτρια
- Ικανοποιητικά
- Πολύ

3. Πόσο άνετα αισθάνεστε να αναγνωρίζετε και να αποφεύγετε πιθανούς κινδύνους στο διαδίκτυο (π.χ., phishing, κακόβουλο λογισμικό);

- Καθόλου

- Μέτρια
- Ικανοποιητικά
- Πολύ

[End_of_Page]

Act_ID#2.0.2 Δομή της ενότητας 1 [Υπερκείμενο]

Η Διδακτική Ενότητα 1 είναι διάρκειας 3 ωρών και περιλαμβάνει:

- Εισαγωγή
- Υποενότητα 1 - Κίνδυνοι και απειλές που σχετίζονται με τη χρήση του διαδικτύου.
- Υποενότητα 2 - Δημιουργία ισχυρών κωδικών πρόσβασης και προστασία προσωπικών δεδομένων στο διαδίκτυο.
- Ανακεφαλαίωση και Αυτοαξιολόγηση, που περιλαμβάνει:
  - Σύνοψη της ενότητας
  - Εργασία εφαρμογής με τη μορφή Ερώτησης Ανοικτής Απόκρισης που αυτοαξιολογούν οι εκπαιδευόμενοι με τη χρήση ρουμπρίκας
  - Αυτοαξιολόγηση σε μορφή poll όπου οι εκπαιδευόμενοι επιλέγουν ποιο/ποια από τα μαθησιακά αποτελέσματα της ενότητας έχουν κατακτήσει.
  - Forum συζήτησης

Οι 2 υποενότητες είναι διάρκειας 1 ώρας η κάθε μία. Η κάθε υποενότητα αποτελείται από:

- Δραστηριότητα παρουσίασης (15')
- Δραστηριότητα επίδειξης (15')
- Δραστηριότητα εξάσκησης (15')
- Δραστηριότητα αυτοαξιολόγησης (15')

2.1 Βασικές Αρχές Ψηφιακής Ασφάλειας

Act_ID#2.1.1 Παρουσίαση - Κίνδυνοι και απειλές που σχετίζονται με τη χρήση του διαδικτύου. [Υπερκείμενο & Video]

Αυτό το βίντεο θα σας παρουσιάσει τους κινδύνους και τις απειλές που σχετίζονται με τη χρήση του διαδικτύου, όπως είναι το ηλεκτρονικό "ψάρεμα" (phishing) και το κακόβουλο λογισμικό.

https://youtu.be/mcII64WbQoI?si=1Gwybx2lPcHHrt13

[End_of_Page]

Act_ID#2.1.2 Επίδειξη - Ηλεκτρονικό "ψάρεμα" (phishing), κακόβουλο λογισμικό (malware) και παραπληροφόρηση (misinformation) [Υπερκείμενο & Video]

Παρακολουθήστε τα παρακάτω βίντεο για να μάθετε πώς να προστατεύετε από τις διαδικτυακές απειλές .

Για το ηλεκτρονικό "ψάρεμα":

https://youtu.be/qdpReVgpQhc?si=ycuSkMKjb8nfLupR

Για το κακόβουλο λογισμικό:

https://youtu.be/owGqhRc3AfA?si=nGUQRJrdU-dLcUtI

Για την παραπληροφόρηση:

https://youtu.be/mP4H7XAb9VA?si=DU1rXGdsoFT_cQae

[End_of_Page]

Act_ID#2.1.3 Δραστηριότητες εξάσκησης [quizzes]

1.Το phishing είναι μια τεχνική που χρησιμοποιείται από τους απατεώνες για να κλέψουν προσωπικά δεδομένα, όπως κωδικούς πρόσβασης και στοιχεία πιστωτικών καρτών, μέσω παραπλανητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου ή ιστότοπων που μοιάζουν με νόμιμους. (Σωστό)

2.Το malware είναι ένα είδος λογισμικού που έχει σχεδιαστεί για να βλάψει ή να εκμεταλλευτεί ένα υπολογιστικό σύστημα χωρίς τη γνώση ή τη συγκατάθεση του χρήστη. (Σωστό)

3.Η παραπληροφόρηση είναι η διάδοση ψευδών ή παραπλανητικών πληροφοριών, συχνά με σκοπό να επηρεάσει τη κοινή γνώμη ή να προκαλέσει σύγχυση. (Σωστό)

4.Είναι ασφαλές να κάνετε κλικ σε συνδέσμους ή να ανοίγετε συνημμένα σε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς. (Λάθος)

5.Οι αξιόπιστες πηγές πληροφοριών, όπως οι επίσημοι κυβερνητικοί ιστότοποι και οι αναγνωρισμένοι ειδησεογραφικοί οργανισμοί, είναι λιγότερο πιθανό να διαδίδουν παραπληροφόρηση. (Σωστό)

[End_of_Page]

Act_ID#2.1.4 Δραστηριότητα αυτοαξιολόγησης [multiple choice questions]

1.Ποια από τις παρακάτω ενέργειες είναι ένα παράδειγμα phishing; a)

a) Λήψη ενός email που φαίνεται να προέρχεται από την τράπεζά σας και σας ζητά να επιβεβαιώσετε τα στοιχεία σύνδεσής σας.
b) Εγκατάσταση ενός προγράμματος προστασίας από ιούς στον υπολογιστή σας.
c) Δημιουργία ενός ισχυρού κωδικού πρόσβασης.
d) Αναφορά ενός ύποπτου email στον πάροχο email σας.

2.Ποιος είναι ο κύριος σκοπός του malware; c)

a) Να βελτιώσει την απόδοση του υπολογιστή σας.
b) Να προστατεύσει τον υπολογιστή σας από ιούς.
c) Να βλάψει ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στον υπολογιστή σας.
d) Να σας βοηθήσει να οργανώσετε τα αρχεία σας.

3.Ποια από τις παρακάτω πηγές είναι πιο πιθανό να διαδίδει παραπληροφόρηση; c)

a) Ένας επίσημος κυβερνητικός ιστότοπος.
b) Ένας αναγνωρισμένος ειδησεογραφικός οργανισμός.
c) Ένας ιστότοπος που ειδικεύεται σε θεωρίες συνωμοσίας.
d) Μια ακαδημαϊκή ερευνητική δημοσίευση.

4.Πώς μπορείτε να προστατευτείτε από το malware; c)

a) Κάνοντας κλικ σε συνδέσμους από άγνωστους αποστολείς.
b) Ανοίγοντας συνημμένα σε email από άγνωστους αποστολείς.
c) Εγκαθιστώντας και ενημερώνοντας τακτικά ένα πρόγραμμα προστασίας από ιούς.
d) Μοιράζοντας τους κωδικούς πρόσβασής σας με άλλους.

5. Ποια από τις παρακάτω ενέργειες μπορεί να βοηθήσει στην καταπολέμηση της παραπληροφόρησης; a)

a) Έλεγχος των γεγονότων πριν από την κοινοποίηση πληροφοριών.
b) Κοινοποίηση πληροφοριών από αναξιόπιστες πηγές.
c) Αποφυγή κριτικής σκέψης.
d) Εμπιστοσύνη σε όλα όσα διαβάζετε στο διαδίκτυο.

[End_of_Page]

2.2 Δημιουργία ισχυρών κωδικών πρόσβασης και προστασία προσωπικών δεδομένων στο διαδίκτυο.

Act_ID#2.2.1 Παρουσίαση- Δημιουργία ισχυρών κωδικών πρόσβασης και προστασία προσωπικών δεδομένων στο διαδίκτυο. [Υπερκείμενο & Video]

Η δημιουργία ισχυρών κωδικών πρόσβασης είναι απαραίτητη για την προστασία των online λογαριασμών σας.

https://youtu.be/9LxdtaSvQ3I?si=eG75XurVKagQiGEh

Η προστασία των προσωπικών σας δεδομένων είναι σημαντική. Αυτά τα βίντεο θα σας βοηθήσουν να κατανοήσετε πώς συλλέγονται, χρησιμοποιούνται και μοιράζονται τα προσωπικά σας δεδομένα.

https://youtu.be/MjPpG2e71Ec?si=VFwPmURGowc2MhDy

https://youtu.be/v4IIH3sJIMc?si=_hilq8ea8OZDQNas

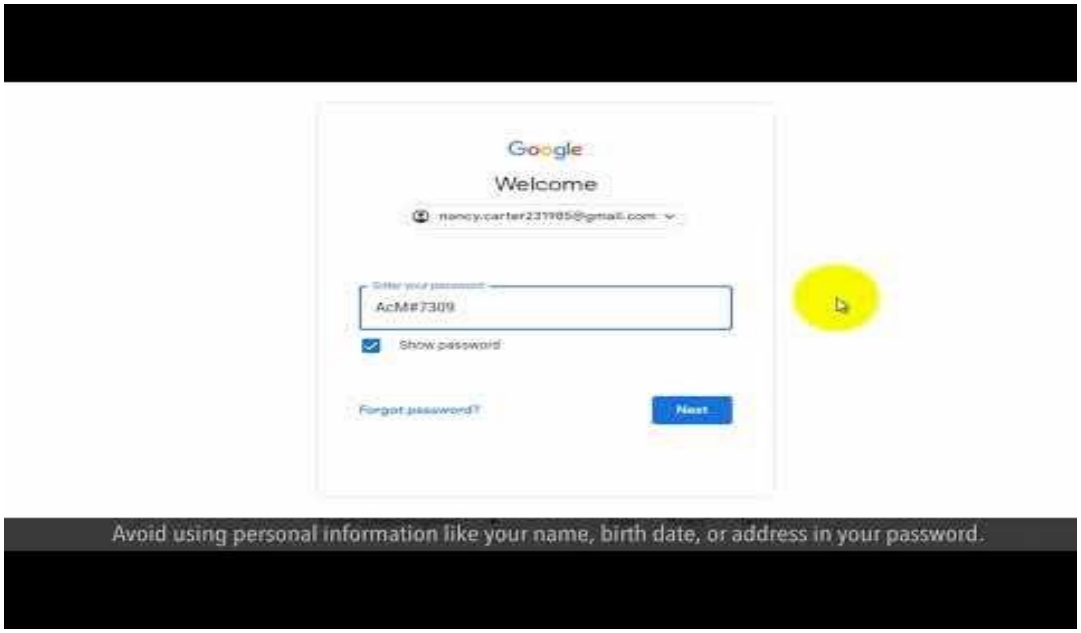
[End_of_Page]

Act_ID#2.2.2 Επίδειξη - Δημιουργία ισχυρών κωδικών πρόσβασης και προστασία προσωπικών δεδομένων στο διαδίκτυο [Υπερκείμενο & Video]

Παρακολουθήστε τα βίντεο για να μάθετε πώς να δημιουργείτε ισχυρούς κωδικούς πρόσβασης και πως να προστατεύτε τα προσωπικά σας δεδομένα.

https://youtu.be/3f0u-vw58A0?si=rft76p2-Pc44HFTq

https://youtu.be/fTBVlVLNJWQ?si=krCUi7Cv26MK9qIt



https://youtu.be/2GeakIPfu54?si=DiDmUPc4Ixaf6s6A

[End_of_Page]

Act_ID#2.2.3 Δραστηριότητες εξάσκησης [quizzes]

Ισχυροί κωδικοί πρόσβασης:

1.Ένας ισχυρός κωδικός πρόσβασης πρέπει να περιέχει τουλάχιστον 8 χαρακτήρες, συμπεριλαμβανομένων κεφαλαίων και μικρών γραμμάτων, αριθμών και συμβόλων. (Σωστό)

2.Είναι ασφαλές να χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για όλους τους online λογαριασμούς σας. (Λάθος)

3.Η χρήση προσωπικών πληροφοριών, όπως η ημερομηνία γέννησής σας ή το όνομα του κατοικίδιου ζώου σας, σε έναν κωδικό πρόσβασης είναι μια καλή πρακτική. (Λάθος)

Προσωπικά δεδομένα:

4.Τα προσωπικά δεδομένα περιλαμβάνουν πληροφορίες όπως το όνομα, η διεύθυνση, ο αριθμός τηλεφώνου, η διεύθυνση ηλεκτρονικού ταχυδρομείου και ο αριθμός κοινωνικής ασφάλισης. (Σωστό)

5.Είναι ασφαλές να μοιράζεστε τα προσωπικά σας δεδομένα με οποιονδήποτε σας τα ζητήσει. (Λάθος)

[End_of_Page]

Act_ID#2.2.4 Δραστηριότητα αυτοαξιολόγησης [multiple choice questions]

Ισχυροί κωδικοί πρόσβασης:

1.Ποιο από τα παρακάτω είναι ένα παράδειγμα ισχυρού κωδικού πρόσβασης;

a) 12345678
b) password
c) P@ssword123!
d) το όνομα του κατοικίδιου ζώου σας

2.Ποια από τις παρακάτω πρακτικές είναι η καλύτερη για τη διαχείριση κωδικών πρόσβασης;

a) Χρήση του ίδιου κωδικού πρόσβασης για όλους τους λογαριασμούς σας
b) Χρήση ενός διαχειριστή κωδικών πρόσβασης
c) Γραφή των κωδικών πρόσβασης σε ένα χαρτί και φύλαξή τους σε ένα συρτάρι
d) Κοινοποίηση των κωδικών πρόσβασης με φίλους και συγγενείς

Προσωπικά δεδομένα:

3.Ποια από τις παρακάτω πληροφορίες ΔΕΝ θεωρείται προσωπικό δεδομένο;

a) Ημερομηνία γέννησης
b) Αριθμός τηλεφώνου
c) Χρώμα ματιών
d) Διεύθυνση ηλεκτρονικού ταχυδρομείου

4.Ποιος είναι ο καλύτερος τρόπος για να προστατεύσετε τα προσωπικά σας δεδομένα online;

a) Κοινοποίηση των προσωπικών σας δεδομένων σε ιστότοπους κοινωνικής δικτύωσης
b) Χρήση ισχυρών κωδικών πρόσβασης και ενεργοποίηση του ελέγχου ταυτότητας δύο παραγόντων
c) Κλικ σε συνδέσμους σε email από άγνωστους αποστολείς
d) Λήψη λογισμικού από μη αξιόπιστες πηγές

5.Εάν πιστεύετε ότι τα προσωπικά σας δεδομένα έχουν παραβιαστεί, τι πρέπει να κάνετε;

a) Να μην κάνετε τίποτα

b) Να αλλάξετε τους κωδικούς πρόσβασής σας και να ενημερώσετε τις σχετικές εταιρείες ή οργανισμούς
c) Να διαγράψετε όλους τους online λογαριασμούς σας
d) Να πληρώσετε τα λύτρα που ζητούν οι χάκερ

[End_of_Page]

2.3 Ανακεφαλαίωση και Αυτοαξιολόγηση ενότητας 1

Act_ID#2.3.1 Ανακεφαλαίωση [Υπερκείμενο]

Βασικές αρχές ψηφιακής ασφάλειας

Η ψηφιακή ασφάλεια είναι απαραίτητη για την προστασία των προσωπικών σας δεδομένων και λογαριασμών online. Ακολουθούν μερικές βασικές αρχές που θα σας βοηθήσουν να διατηρήσετε ασφαλή την ψηφιακή σας παρουσία:

Ισχυροί κωδικοί πρόσβασης:

- Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης για όλους τους online λογαριασμούς σας. Ένας ισχυρός κωδικός πρόσβασης πρέπει να περιέχει τουλάχιστον 8 χαρακτήρες, συμπεριλαμβανομένων κεφαλαίων και μικρών γραμμάτων, αριθμών και συμβόλων.
- Μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για πολλούς λογαριασμούς.
- Μην μοιράζεστε τους κωδικούς πρόσβασής σας με άλλους.

Προστασία προσωπικών δεδομένων:

- Να είστε προσεκτικοί με τα προσωπικά σας δεδομένα που μοιράζεστε online. Μην μοιράζεστε ευαίσθητες πληροφορίες, όπως η διεύθυνση του σπιτιού σας ή ο αριθμός κοινωνικής ασφάλισης, με άγνωστους ή σε ιστότοπους που δεν εμπιστεύεστε.
- Να γνωρίζετε πώς συλλέγονται, χρησιμοποιούνται και μοιράζονται τα προσωπικά σας δεδομένα από τους ιστότοπους και τις εφαρμογές που χρησιμοποιείτε. Διαβάστε τους όρους χρήσης και τις πολιτικές απορρήτου πριν από τη χρήση οποιασδήποτε υπηρεσίας.

Προστασία από malware:

- Εγκαταστήστε και ενημερώστε τακτικά ένα πρόγραμμα προστασίας από ιούς στον υπολογιστή σας.
- Να είστε προσεκτικοί με τα email και τα συνημμένα που λαμβάνετε από άγνωστους αποστολείς. Μην κάνετε κλικ σε συνδέσμους ή ανοίγετε συνημμένα από άγνωστους αποστολείς.
- Λήψη λογισμικού από αξιόπιστες πηγές.

Ενημέρωση:

- Ενημερώστε το λειτουργικό σύστημα του υπολογιστή σας και τις εφαρμογές που χρησιμοποιείτε τακτικά. Οι ενημερώσεις συχνά περιλαμβάνουν επιδιορθώσεις ασφαλείας που μπορούν να προστατέψουν τον υπολογιστή σας από γνωστά κενά ασφαλείας.

Ακολουθώντας αυτές τις βασικές αρχές, μπορείτε να μειώσετε σημαντικά τον κίνδυνο hacking και κλοπής προσωπικών δεδομένων.

[End_of_Page]

Act_ID#2.3.2 Εργασία [Open Response Assessment]

Θέμα: Βασικές αρχές ψηφιακής ασφάλειας

Παρακαλούμε απαντήστε στις παρακάτω ερωτήσεις με πλήρεις προτάσεις. Αναφέρετε πρακτικά παραδείγματα όπου είναι δυνατόν και υποστηρίξτε τις απαντήσεις σας με επιχειρήματα.

Ερώτηση:

1.Πώς μπορείς να αναγνωρίσεις ένα ύποπτο email ή μήνυμα που μπορεί να είναι προσπάθεια ηλεκτρονικού "ψαρέματος" (phishing); Ποιες είναι οι συνέπειες αν κάποιος πέσει θύμα phishing και τι μπορεί να κάνει για να προστατευτεί;

Απάντηση:

Ρουμπρίκα

Κριτήρια	**1 - Χρειάζεται Βελτίωση**	**2 - Μέτριο**	**3 - Καλό**	**4 - Πολύ Καλό**	**5 - Εξαιρετικό**
Αναγνώριση Στοιχείων	Αδυνατώ να αναγνωρίσω	Αναγνωρίζω 1-2 σημάδια	Αναγνωρίζω αρκετά	Αναγνωρίζω τα	Αναγνωρίζω και εξηγώ

Phishing	οποιαδήποτε σημάδια phishing.	αλλά χωρίς λεπτομέρειες.	σημάδια με κάποια εξήγηση.	περισσότερα σημάδια καθαρά και παρέχει καλές εξηγήσεις.	λεπτομερώς όλα τα σημάδια του phishing.
Κατανόηση Συνεπειών	Καμία κατανόηση των συνεπειών.	Περιορισμένη κατανόηση των συνεπειών.	Κάποια επίγνωση των συνεπειών αλλά χωρίς βάθος.	Καλή κατανόηση των συνεπειών με σχετικά παραδείγματα.	Συνολική κατανόηση των συνεπειών με διεισδυτικά παραδείγματα.
Προστατευτικά Μέτρα	Καμία πρόταση προστατευτικών μέτρων.	Προτείνει 1-2 βασικά μέτρα με λίγες λεπτομέρειες.	Προτείνει αρκετά μέτρα με κάποια εξήγηση.	Προτείνει πολλά αποτελεσματικά μέτρα με σαφείς εξηγήσεις.	Προτείνει λεπτομερή και αποτελεσματικά προστατευτικά μέτρα με αναλυτικές εξηγήσεις.

Οδηγίες Αυτοαξιολόγησης

- **Απαντήστε με:**
    - *Πληρότητα και σαφήνεια*
    - *Πρακτικά παραδείγματα*
    - *Υποστήριξη με επιχειρήματα*
- **Ανατρέξτε στις σημειώσεις σας:** Αναλογιστείτε τα μαθησιακά αποτελέσματα και την πρόοδό σας σε κάθε θεματική ενότητα.

- **Αξιολογήστε τις γνώσεις σας:** Χρησιμοποιήστε την παραπάνω ρουμπρίκα για να αξιολογήσετε την επίτευξη κάθε μαθησιακού αποτελέσματος. Δώστε στον εαυτό σας μια βαθμολογία για κάθε κριτήριο από 1 έως 5.
- **Συνολική Βαθμολογία:** Υπολογίστε το άθροισμα των βαθμολογιών σας για όλα τα κριτήρια.

Αυτή η διαδικασία αυτοαξιολόγησης θα σας βοηθήσει να αναγνωρίσετε τις δυνατές και αδύναμες πλευρές της μάθησής σας και να κατανοήσετε καλύτερα πώς μπορείτε να βελτιωθείτε στο μέλλον.

[End_of_Page]

Act_ID#2.3.3 Checklist: Μπορώ να το κάνω… [Checklist & WordCloud]

Για κάθε πρόταση στο checklist, απαντήστε με ειλικρίνεια και αξιολόγησε την ικανότητά σου.

Μπορώ να:

- Αναγνωρίζω τα βασικά χαρακτηριστικά ενός email ή μηνύματος ηλεκτρονικού "ψαρέματος" (phishing).
- Εξηγήσω τις πιθανές συνέπειες αν κάποιος πέσει θύμα ηλεκτρονικού "ψαρέματος".
- Αναφέρω τουλάχιστον τρεις τρόπους για να προστατεύσω τον υπολογιστή μου από κακόβουλο λογισμικό.
- Διακρίνω την αξιόπιστη πληροφόρηση από την παραπληροφόρηση στο διαδίκτυο, χρησιμοποιώντας κριτική σκέψη και ελέγχοντας τις πηγές.
- Εξηγήσω τις πιθανές συνέπειες της διάδοσης παραπληροφόρησης.
- Δημιουργήσω έναν ισχυρό κωδικό πρόσβασης που πληροί τα κριτήρια ασφαλείας.
- Εξηγήσω γιατί είναι σημαντικό να χρησιμοποιώ διαφορετικούς κωδικούς πρόσβασης για διαφορετικούς λογαριασμούς.
- Περιγράψω ασφαλείς μεθόδους για τη διαχείριση πολλών κωδικών πρόσβασης.
- Εφαρμόσω βέλτιστες πρακτικές για την προστασία των προσωπικών μου δεδομένων στο διαδίκτυο, όπως η χρήση ισχυρών κωδικών πρόσβασης και η προσοχή στις πληροφορίες που κοινοποιώ.

WordCloud

Γράψε μερικές (1-3) σημαντικές λέξεις που θυμάσαι από την ενότητα που μόλις παρακολούθησες.

[End_of_Page]

Act_ID#2.3.4 [Discussion Forum]

Θέμα συζήτησης: Προστατεύοντας τον εαυτό μας στον ψηφιακό κόσμο

Σας προσκαλούμε να μοιραστείτε τις σκέψεις και τις εμπειρίες σας σχετικά με την ψηφιακή ασφάλεια.

Ερώτηση για συζήτηση:

1.Ποιες στρατηγικές χρησιμοποιείτε για να προστατεύσετε τα προσωπικά σας δεδομένα και τους online λογαριασμούς σας;

[End_of_Page]

2.4 Πρόσθετο υλικό

Act_ID#2.4.1 Προτάσεις για Επιπλέον Πληροφόρηση

https://www.getsafeonline.org/

https://www.sternsecurity.com/blog/stay-safe-online/

[End_of_Page]

[End_of_Topic]

Ημέρα 3 : Διδακτική Ενότητα 2 – Ασφαλείς Συναλλαγές και Αγορές (3 ώρες)

3.0 Εισαγωγή Διδακτικής ενότητας 2

Act_ID#3.0.1 Μαθησιακά αποτελέσματα [Υπερκείμενο &Poll]

Μετά την παρακολούθηση της διδακτικής ενότητας 2 θα είσαι ικανός/η να:

MA2 [understand/evaluate]: κατανοείς ποιες είναι οι ασφαλείς συναλλαγές και αγορές.

Το **MA2** αναλύεται σε επιμέρους μαθησιακά αποτελέσματα, ως εξής:

- **MA2.1** Να μπορείς να πραγματοποιείς ασφαλείς ηλεκτρονικές συναλλαγές και αγορές, χρησιμοποιώντας αξιόπιστες μεθόδους πληρωμής και αναγνωρίζοντας αξιόπιστα ηλεκτρονικά καταστήματα.

- **ΜΑ2.2** Να αναγνωρίζεις και να αποφεύγεις διαδικτυακές απάτες, όπως η κλοπή ταυτότητας και οι ψεύτικες προσφορές.

Poll

Αυτό το σύντομο poll θα ελέγξει τις προγενέστερες γνώσεις σας. Επιλέξτε αυτό που σας αντιπροσωπεύει καλύτερα. Δεν υπάρχουν σωστές και λάθος απαντήσεις.

1.Πόσο καλά γνωρίζετε τις διάφορες μεθόδους πληρωμής που χρησιμοποιούνται για online αγορές (π.χ., πιστωτικές κάρτες, PayPal, κλπ.);

- Καθόλου
- Μέτρια
- Ικανοποιητικά
- Πολύ

2. Πόσο σίγουροι αισθάνεστε ότι μπορείτε να αναγνωρίσετε ένα αξιόπιστο ηλεκτρονικό κατάστημα από ένα μη αξιόπιστο;

- Καθόλου
- Μέτρια
- Ικανοποιητικά
- Πολύ

3. Έχετε ποτέ πέσει θύμα διαδικτυακής απάτης ή γνωρίζετε κάποιον που έχει πέσει;

- Καθόλου
- Μέτρια (Έχω ακούσει για περιπτώσεις, αλλά δεν μου έχει συμβεί προσωπικά)
- Ικανοποιητικά (Μου έχει συμβεί ή γνωρίζω κάποιον που έχει πέσει θύμα)
- Πολύ (Έχω πέσει θύμα πολλές φορές ή γνωρίζω πολλούς που έχουν πέσει θύμα)

[End_of_Page]

Act_ID#3.0.2 Δομή της ενότητας 2 [Υπερκείμενο]

Η Διδακτική Ενότητα 2 είναι διάρκειας 3 ωρών και περιλαμβάνει:

- Εισαγωγή
- Υποενότητα 1 - Πραγματοποίηση ασφαλών συναλλαγών και αγορών
- Υποενότητα 2 - Αποφυγή διαδικτυακών απατών
- Ανακεφαλαίωση και Αυτοαξιολόγηση, που περιλαμβάνει:
    - Σύνοψη της ενότητας
    - Εργασία εφαρμογής με τη μορφή Ερώτησης Ανοικτής Απόκρισης που αυτοαξιολογούν οι εκπαιδευόμενοι με τη χρήση ρουμπρίκας
    - Αυτοαξιολόγηση σε μορφή poll όπου οι εκπαιδευόμενοι επιλέγουν ποιο/ποια από τα μαθησιακά αποτελέσματα της ενότητας έχουν κατακτήσει.
    - Forum συζήτησης

Οι 2 υποενότητες είναι διάρκειας 1 ώρας η κάθε μία. Η κάθε υποενότητα αποτελείται από:

- Δραστηριότητα παρουσίασης (15')
- Δραστηριότητα επίδειξης (15')
- Δραστηριότητα εξάσκησης (15')
- Δραστηριότητα αυτοαξιολόγησης (15')

3.1 Πραγματοποίηση ασφαλών συναλλαγών και αγορών

Act_ID#3.1.1 Παρουσίαση -Πραγματοποίηση ασφαλών συναλλαγών και αγορών [Υπερκείμενο & Video]

Αυτό το βίντεο θα σας παρουσιάσει μερικές χρήσιμες συμβουλές για το πως να κάνετε αγορές από το διαδίκτυο με ασφάλεια.

https://youtu.be/cWcNQgPiqhc?si=ihec3hoImznIz9oT

End_of_Page]

Act_ID#3.1.2 Επίδειξη - Πραγματοποίηση ασφαλών συναλλαγών και αγορών [Υπερκείμενο & Video]

Σε αυτό το βίντεο θα δείτε παραδείγματα από σελίδες για πραγματοποίηση ηλεκτρονικών αγορών και σε ποια στοιχεία πρέπει να δώσουμε παραπάνω προσοχή.

https://youtu.be/el3N6qQjr-I?si=CX3rC4VvAtyYvl8M

[End_of_Page]

Act_ID#3.1.3 Δραστηριότητα εξάσκησης [quizzes]

1. Είναι ασφαλές να χρησιμοποιείτε δημόσια δίκτυα Wi-Fi για να πραγματοποιείτε online αγορές. (Λάθος)
2. Πρέπει πάντα να ελέγχετε αν ένας ιστότοπος χρησιμοποιεί ασφαλή σύνδεση (https) πριν εισάγετε τα στοιχεία της πιστωτικής σας κάρτας. (Σωστό)
3. Οι πιστωτικές κάρτες προσφέρουν γενικά καλύτερη προστασία από τις χρεωστικές κάρτες σε περίπτωση απάτης. (Σωστό)
4. Είναι καλή ιδέα να αποθηκεύετε τα στοιχεία της πιστωτικής σας κάρτας σε έναν ιστότοπο για μελλοντικές αγορές, ώστε να μην χρειάζεται να τα εισάγετε ξανά. (Λάθος)
5. Πρέπει πάντα να διαβάζετε τις κριτικές άλλων πελατών πριν κάνετε μια αγορά από ένα ηλεκτρονικό κατάστημα. (Σωστό)

[End_of_Page]

Act_ID#3.1.4 Δραστηριότητα αυτοαξιολόγησης [multiple choice questions]

1.Ποιο από τα παρακάτω είναι ένα σημάδι ότι ένα ηλεκτρονικό κατάστημα είναι πιθανώς αξιόπιστο; a)

a) Έχει επαγγελματική εμφάνιση και παρέχει σαφείς πληροφορίες επικοινωνίας.
b) Ζητάει τον αριθμό κοινωνικής ασφάλισής σας για να ολοκληρώσετε μια αγορά.
c) Έχει πολλές αναδυόμενες διαφημίσεις και ανακατευθύνσεις σε άλλους ιστότοπους.
d) Δεν έχει πολιτική επιστροφών ή εγγυήσεις προϊόντων.

2.Ποια από τις παρακάτω μεθόδους πληρωμής θεωρείται γενικά η πιο ασφαλής για online αγορές; b)

a) Πιστωτική κάρτα
b) Χρεωστική κάρτα
c) Μετρητά κατά την παράδοση
d) Τραπεζική μεταφορά

3.Ποιο από τα παρακάτω ΔΕΝ είναι ένα βήμα που πρέπει να ακολουθήσετε για να διασφαλίσετε μια ασφαλή online συναλλαγή; c)

a) Χρήση ισχυρού κωδικού πρόσβασης για τον λογαριασμό σας στο ηλεκτρονικό κατάστημα
b) Έλεγχος των κριτικών άλλων πελατών για το ηλεκτρονικό κατάστημα
c) Κοινοποίηση των στοιχείων της πιστωτικής σας κάρτας σε φίλους και συγγενείς
d) Αποφυγή χρήσης δημόσιων δικτύων Wi-Fi για online αγορές

4.Τι πρέπει να κάνετε εάν αντιμετωπίσετε κάποιο πρόβλημα κατά τη διάρκεια μιας online συναλλαγής, όπως μια μη εξουσιοδοτημένη χρέωση στην πιστωτική σας κάρτα; b)

a) Να μην κάνετε τίποτα και να ελπίζετε ότι το πρόβλημα θα λυθεί από μόνο του
b) Να επικοινωνήσετε αμέσως με την τράπεζα ή τον εκδότη της πιστωτικής σας κάρτας
c) Να διαγράψετε όλους τους online λογαριασμούς σας
d) Να αλλάξετε τον κωδικό πρόσβασης του email σας

5.Ποιο από τα παρακάτω είναι ένα παράδειγμα ασφαλούς πρακτικής κατά την πραγματοποίηση online αγορών; c)

a) Αποθήκευση των στοιχείων της πιστωτικής σας κάρτας σε πολλούς ιστότοπους για ευκολία
b) Χρήση της ίδιας πιστωτικής κάρτας για όλες τις online αγορές σας
c) Έλεγχος τακτικά των κινήσεων της πιστωτικής σας κάρτας για τυχόν ύποπτες χρεώσεις
d) Κλικ σε συνδέσμους σε email που υπόσχονται απίστευτες προσφορές

[End_of_Page]

3.2 Αποφυγή διαδικτυακών απατών

Act_ID#3.2.1 Παρουσίαση - Αποφυγή διαδικτυακών απατών [Υπερκείμενο & Video]

Αυτό το βίντεο θα σας παρουσιάσει μερικά αληθινά παραδείγματα διαδικτυακών απατών. Είναι λίγο μεγαλύτερο σε διάρκεια αλλά αξίζει να δώσετε την πλήρη προσοχή σας!

https://youtu.be/yxSlqP8eiFc?si=W4r397fU_8-7KsFQ

[End_of_Page]

Act_ID#3.2.2 Επίδειξη - Αποφυγή διαδικτυακών απατών [Υπερκείμενο & Video]

Σταμάτα, σκέψου και προστάτεψε τον εαυτό σου από τις διαδικτυακές απάτες!

https://youtu.be/lkExIJ8L-GY?si=_BudVpcTyvpNrWCa

[End_of_Page]

Act_ID# 3.2.3 Δραστηριότητα εξάσκησης [quizzes]

1. Είναι ασφαλές να δίνετε τα προσωπικά σας στοιχεία σε οποιονδήποτε σας τα ζητάει μέσω email ή τηλεφώνου, ακόμα και αν ισχυρίζεται ότι είναι από μια αξιόπιστη εταιρεία ή οργανισμό. (Λάθος)
2. Οι ψεύτικες προσφορές συχνά υπόσχονται απίστευτα δώρα ή εκπτώσεις για να σας δελεάσουν να κάνετε κλικ σε έναν σύνδεσμο ή να δώσετε τα προσωπικά σας στοιχεία. (Σωστό)
3. Η κλοπή ταυτότητας μπορεί να συμβεί μόνο εάν κάποιος κλέψει το πορτοφόλι ή την τσάντα σας. (Λάθος)
4. Είναι σημαντικό να είστε επιφυλακτικοί με τα email ή τα μηνύματα που σας ζητούν να ενεργήσετε επειγόντως ή να κάνετε κλικ σε έναν σύνδεσμο χωρίς να το σκεφτείτε καλά. (Σωστό)
5. Αν υποψιάζεστε ότι έχετε πέσει θύμα διαδικτυακής απάτης, πρέπει να το αναφέρετε αμέσως στις αρμόδιες αρχές. (Σωστό)

[End_of_Page]

Act_ID#3.2.4 Δραστηριότητα αυτοαξιολόγησης [multiple choice questions]

1.Ποιο από τα παρακάτω είναι ένα σημάδι ότι ένα ηλεκτρονικό κατάστημα είναι πιθανώς αξιόπιστο;

a) Έχει επαγγελματική εμφάνιση και παρέχει σαφείς πληροφορίες επικοινωνίας.
b) Ζητάει τον αριθμό κοινωνικής ασφάλισής σας για να ολοκληρώσετε μια αγορά.
c) Έχει πολλές αναδυόμενες διαφημίσεις και ανακατευθύνσεις σε άλλους ιστότοπους.
d) Δεν έχει πολιτική επιστροφών ή εγγυήσεις προϊόντων.

2. Ποια από τις παρακάτω ενέργειες είναι η πιο πιθανή να οδηγήσει σε κλοπή ταυτότητας;

a) Χρήση του ίδιου κωδικού πρόσβασης για όλους τους online λογαριασμούς σας.
b) Κοινοποίηση των προσωπικών σας στοιχείων σε δημόσια δίκτυα Wi-Fi.
c) Απάντηση σε ένα email που σας ζητά να επιβεβαιώσετε τα στοιχεία σύνδεσής σας για έναν λογαριασμό που δεν αναγνωρίζετε.
d) Εγκατάσταση ενός προγράμματος προστασίας από ιούς στον υπολογιστή σας.

3.Ποιο από τα παρακάτω ΔΕΝ είναι ένα βήμα που πρέπει να ακολουθήσετε για να διασφαλίσετε μια ασφαλή online συναλλαγή;

a) Χρήση ισχυρού κωδικού πρόσβασης για τον λογαριασμό σας στο ηλεκτρονικό κατάστημα

b) Έλεγχος των κριτικών άλλων πελατών για το ηλεκτρονικό κατάστημα
c) Κοινοποίηση των στοιχείων της πιστωτικής σας κάρτας σε φίλους και συγγενείς
d) Αποφυγή χρήσης δημόσιων δικτύων Wi-Fi για online αγορές

4.Τι πρέπει να κάνετε εάν αντιμετωπίσετε κάποιο πρόβλημα κατά τη διάρκεια μιας online συναλλαγής, όπως μια μη εξουσιοδοτημένη χρέωση στην πιστωτική σας κάρτα;

a) Να μην κάνετε τίποτα και να ελπίζετε ότι το πρόβλημα θα λυθεί από μόνο του
b) Να επικοινωνήσετε αμέσως με την τράπεζα ή τον εκδότη της πιστωτικής σας κάρτας
c) Να διαγράψετε όλους τους online λογαριασμούς σας
d) Να αλλάξετε τον κωδικό πρόσβασης του email σας

5.Ποιο από τα παρακάτω είναι ένα παράδειγμα ασφαλούς πρακτικής κατά την πραγματοποίηση online αγορών;

a) Αποθήκευση των στοιχείων της πιστωτικής σας κάρτας σε πολλούς ιστότοπους για ευκολία
b) Χρήση της ίδιας πιστωτικής κάρτας για όλες τις online αγορές σας
c) Έλεγχος τακτικά των κινήσεων της πιστωτικής σας κάρτας για τυχόν ύποπτες χρεώσεις
d) Κλικ σε συνδέσμους σε email που υπόσχονται απίστευτες προσφορές

[End_of_Page]

3.3 Ανακεφαλαίωση και Αυτοαξιολόγηση ενότητας 2

Act_ID#3.3.1 Ανακεφαλαίωση [Υπερκείμενο]

Στην ενότητα αυτή, εξερευνήσαμε πώς να πραγματοποιούμε ασφαλείς συναλλαγές και αγορές στο διαδίκτυο, καθώς και πώς να αναγνωρίζουμε και να αποφεύγουμε τις διαδικτυακές απάτες.

- **Ασφαλείς Ηλεκτρονικές Συναλλαγές και Αγορές:**

- Επιλέγουμε αξιόπιστα ηλεκτρονικά καταστήματα, ελέγχοντας την ασφάλεια της ιστοσελίδας (https), τις κριτικές πελατών και τις πληροφορίες επικοινωνίας.
- Χρησιμοποιούμε ασφαλείς μεθόδους πληρωμής, όπως πιστωτικές κάρτες, που προσφέρουν προστασία σε περίπτωση απάτης.
- Διαβάζουμε προσεκτικά τους όρους και τις προϋποθέσεις πριν ολοκληρώσουμε μια συναλλαγή.
- Αποφεύγουμε τη χρήση δημόσιων Wi-Fi για online αγορές και συναλλαγές.

- **Αναγνώριση και Αποφυγή Διαδικτυακών Απατών:**
  - Είμαστε επιφυλακτικοί με προσφορές που φαίνονται πολύ καλές για να είναι αληθινές.
  - Δεν κοινοποιούμε προσωπικά δεδομένα σε αγνώστους ή μη αξιόπιστες πηγές.
  - Ελέγχουμε προσεκτικά τα email και τα μηνύματα για ύποπτους συνδέσμους ή συνημμένα.
  - Αναφέρουμε τυχόν ύποπτες δραστηριότητες ή απάτες στις αρμόδιες αρχές.

Συμπέρασμα:

Η ασφάλεια στις online συναλλαγές και αγορές απαιτεί προσοχή και ενημέρωση. Με την εφαρμογή των βέλτιστων πρακτικών που συζητήθηκαν σε αυτήν την ενότητα, μπορούμε να ελαχιστοποιήσουμε τους κινδύνους και να απολαύσουμε τα οφέλη του ηλεκτρονικού εμπορίου με ασφάλεια και σιγουριά.

[End_of_Page]

Act_ID#3.3.2 Εργασία [Open Response Assessment]

Θέμα: Βασικές αρχές ψηφιακής ασφάλειας

Παρακαλούμε απαντήστε στις παρακάτω ερωτήσεις με πλήρεις προτάσεις. Αναφέρετε πρακτικά παραδείγματα όπου είναι δυνατόν και υποστηρίξτε τις απαντήσεις σας με επιχειρήματα.

Ερώτηση:

1. Φανταστείτε ότι θέλετε να αγοράσετε ένα καινούργιο κινητό τηλέφωνο από ένα

ηλεκτρονικό κατάστημα. Πώς θα διασφαλίσετε ότι το κατάστημα είναι αξιόπιστο και ότι η συναλλαγή σας θα είναι ασφαλής; Τι είδους πληροφορίες θα αναζητήσετε για το κατάστημα και ποιες μεθόδους πληρωμής θα προτιμήσετε;

Απάντηση:

Ρουμπρίκα

Κριτήρια	**1 - Χρειάζεται Βελτίωση**	**2 - Μέτριο**	**3 - Καλό**	**4 - Πολύ Καλό**	**5 - Εξαιρετικό**
Ταυτοποίηση Αξιοπιστων Καταστημάτων	Αποτυχία στην ταυτοποίηση αξιόπιστων καταστημάτων.	Ταυτοποίηση ενός καταστήματος αλλά χωρίς λεπτομέρειες.	ταυτοποίηση 2-3 καταστημάτων με ελάχιστες λεπτομέρειες.	ταυτοποίηση πολλαπλών καταστημάτων με καλές λεπτομέρειες.	Εξαιρετική ταυτοποίηση πολλών αξιόπιστων καταστημάτων με εκτενή λεπτομέρεια.
Μέτρα Ασφαλείας για Συναλλαγές	Καμία αναφορά σε μέτρα ασφαλείας.	Αναφέρω ένα μέτρο ασφαλείας.	Αναφέρω 2-3 μέτρα ασφαλείας.	Αναφέρω πολλά μέτρα ασφαλείας με εξηγήσεις.	Εκτενής συζήτηση για τα μέτρα ασφαλείας και τη σημασία τους.
Προτιμώμενες Μέθοδοι Πληρωμής	Καμία προτιμώμενη μέθοδος δεν αναφέρεται.	Αναφορά σε μία μέθοδο πληρωμής.	Αναφορά σε 2-3 μεθόδους πληρωμής.	Αναφορά σε πολλές μεθόδους πληρωμής και την αξιοπιστία τους.	Εκτενής ανάλυση μεθόδων πληρωμής με σαφή αιτιολόγηση για τις προτιμήσεις.
Έρευνα και Συλλογή	Καμία έρευνα ή	Ελάχιστη έρευνα	Κάποιες σχετικές	Καλή έρευνα με σχετικές	Εκτενής έρευνα με

Πληροφοριών	πληροφορία δεν αναφέρεται.	υποδεικνύεται.	πληροφορίες συλλέγονται.	πληροφορίες.	λεπτομερή ανάλυση πληροφοριών.

Οδηγίες Αυτοαξιολόγησης

- **Απαντήστε με:**
    - *Πληρότητα και σαφήνεια*
    - *Πρακτικά παραδείγματα*
    - *Υποστήριξη με επιχειρήματα*
- **Ανατρέξτε στις σημειώσεις σας:** Αναλογιστείτε τα μαθησιακά αποτελέσματα και την πρόοδό σας σε κάθε θεματική ενότητα.
- **Αξιολογήστε τις γνώσεις σας:** Χρησιμοποιήστε την παραπάνω ρουμπρίκα για να αξιολογήσετε την επίτευξη κάθε μαθησιακού αποτελέσματος. Δώστε στον εαυτό σας μια βαθμολογία για κάθε κριτήριο από 1 έως 5.
- **Συνολική Βαθμολογία:** Υπολογίστε το άθροισμα των βαθμολογιών σας για όλα τα κριτήρια.

Αυτή η διαδικασία αυτοαξιολόγησης θα σας βοηθήσει να αναγνωρίσετε τις δυνατές και αδύναμες πλευρές της μάθησής σας και να κατανοήσετε καλύτερα πώς μπορείτε να βελτιωθείτε στο μέλλον.

[End_of_Page]

Act_ID#3.3.3 Checklist: Μπορώ να το κάνω… [Checklist & WordCloud]

Για κάθε πρόταση στο checklist, απαντήστε με ειλικρίνεια και αξιολόγησε την ικανότητά σου.

Μπορώ να:

MA2.1

- Αναγνωρίζω τα χαρακτηριστικά ενός αξιόπιστου ηλεκτρονικού καταστήματος.
- Επιλέγω ασφαλείς μεθόδους πληρωμής για τις online αγορές μου.
- Ελέγχω προσεκτικά τους όρους και τις προϋποθέσεις πριν ολοκληρώσω μια online συναλλαγή.

- Αναφέρω τυχόν ύποπτες δραστηριότητες κατά τη διάρκεια μιας online συναλλαγής.

ΜΑ2.2

- Αναγνωρίζω τις πιο συνηθισμένες διαδικτυακές απάτες, όπως η κλοπή ταυτότητας και οι ψεύτικες προσφορές.
- Εντοπίζω τα προειδοποιητικά σημάδια μιας διαδικτυακής απάτης.
- Αποφεύγω να πέσω θύμα διαδικτυακής απάτης ακολουθώντας βέλτιστες πρακτικές ασφάλειας.
- Αναφέρω τυχόν ύποπτες δραστηριότητες ή απάτες στις αρμόδιες αρχές.

WordCloud

Γράψε μερικές (1-3) σημαντικές λέξεις που θυμάσαι από την ενότητα που μόλις παρακολούθησες

[End_of_Page]

Act_ID#3.3.4 [Discussion Forum]

Θέμα συζήτησης: Πραγματοποίηση ασφαλών συναλλαγών και αγορών

Σας προσκαλούμε να μοιραστείτε τις σκέψεις και τις εμπειρίες σας σχετικά με τις ασφαλείς διαδικτυακές συναλλαγές και αγορές.

Ερωτήσεις για συζήτηση:

1. Ποιες είναι οι πιο συνηθισμένες μέθοδοι ηλεκτρονικής πληρωμής και ποια είναι τα πλεονεκτήματα και τα μειονεκτήματά τους όσον αφορά την ασφάλεια;

2. Ποιες είναι οι ενδείξεις ότι ένας ιστότοπος ή μια προσφορά μπορεί να είναι ψεύτικη; Τι μπορείτε να κάνετε για να προστατευτείτε από τέτοιου είδους απάτες;

[End_of_Page]

3.4 Πρόσθετο υλικό

Act_ID#3.4.1 Προτάσεις για Επιπλέον Πληροφόρηση

https://cyberalert.gr

https://safety.google

[End_of_Page]

[End_of_Topic]

Ημέρα 4 : Διδακτική Ενότητα 3 – Διαχείριση και προστασία της διαδικτυακής παρουσίας (3 ώρες)

4.0 Εισαγωγή Διδακτικής ενότητας 3

Act_ID#4.0.1 Μαθησιακά αποτελέσματα [Υπερκείμενο+Poll]

Μετά την παρακολούθηση της διδακτικής ενότητας 3 θα είσαι ικανός/η να:

MA3 [understand/evaluate]: κατανοείς τι σημαίνει υπεύθυνη χρήση κοινωνικών δικτύων.

Το **MA3** αναλύεται σε επιμέρους μαθησιακά αποτελέσματα, ως εξής:

- **MA3.1** Να μπορείς να διαχειρίζεσαι αποτελεσματικά την παρουσία σου στα κοινωνικά δίκτυα, προσαρμόζοντας τις ρυθμίσεις απορρήτου και προστατεύοντας τη διαδικτυακή σου φήμη.
- **MA3.2** να αναγνωρίζεις και να αντιμετωπίζεις τη διαδικτυακή παρενόχληση (cyberbullying), προωθώντας την ευγένεια και τον σεβασμό στο διαδικτυακό περιβάλλον.

Poll

Αυτό το σύντομο poll θα ελέγξει τις πρότερες γνώσεις σας. Επιλέξτε αυτό που σας αντιπροσωπεύει καλύτερα. Δεν υπάρχουν σωστές και λάθος απαντήσεις.

1.Πόσο καλά γνωρίζετε τους βασικούς κανόνες συμπεριφοράς και επικοινωνίας στα κοινωνικά δίκτυα (π.χ., σεβασμός στην ιδιωτικότητα των άλλων, αποφυγή προσβλητικής γλώσσας);

- Καθόλου
- Μέτρια
- Ικανοποιητικά
- Πολύ

2.Πόσο συχνά ελέγχετε τις ρυθμίσεις απορρήτου σας στα κοινωνικά δίκτυα και κατανοείτε πώς αυτές επηρεάζουν το ποιος μπορεί να δει τις πληροφορίες και τις αναρτήσεις σας;

- Καθόλου
- Μέτρια
- Ικανοποιητικά

- Πολύ

3.Πόσο άνετα αισθάνεστε να αναγνωρίζετε και να αποφεύγετε την παραπληροφόρηση και τις ψεύτικες ειδήσεις που κυκλοφορούν στα κοινωνικά δίκτυα;

- Καθόλου
- Μέτρια
- Ικανοποιητικά
- Πολύ

[End_of_Page]

Act_ID#3.0.2 Δομή της ενότητας [Υπερκείμενο]

Η Διδακτική Ενότητα 3 είναι διάρκειας 3 ωρών και περιλαμβάνει:

- Εισαγωγή
- Υποενότητα 1 - Διαχείριση και προστασία της διαδικτυακής παρουσίας.
- Υποενότητα 2 - Αντιμετώπιση της διαδικτυακής παρενόχλησης
- Ανακεφαλαίωση και Αυτοαξιολόγηση, που περιλαμβάνει:
  - Σύνοψη της ενότητας
  - Εργασία εφαρμογής με τη μορφή Ερώτησης Ανοικτής Απόκρισης που αυτοαξιολογούν οι εκπαιδευόμενοι με τη χρήση ρουμπρίκας
  - Αυτοαξιολόγηση σε μορφή poll όπου οι εκπαιδευόμενοι επιλέγουν ποιο/ποια από τα μαθησιακά αποτελέσματα της ενότητας έχουν κατακτήσει.
  - Forum συζήτησης

Οι 2 υποενότητες είναι διάρκειας 1 ώρας η κάθε μία. Η κάθε υποενότητα αποτελείται από:

- Δραστηριότητα παρουσίασης (15')
- Δραστηριότητα επίδειξης (15')
- Δραστηριότητα εξάσκησης (15')
- Δραστηριότητα αυτοαξιολόγησης (15')

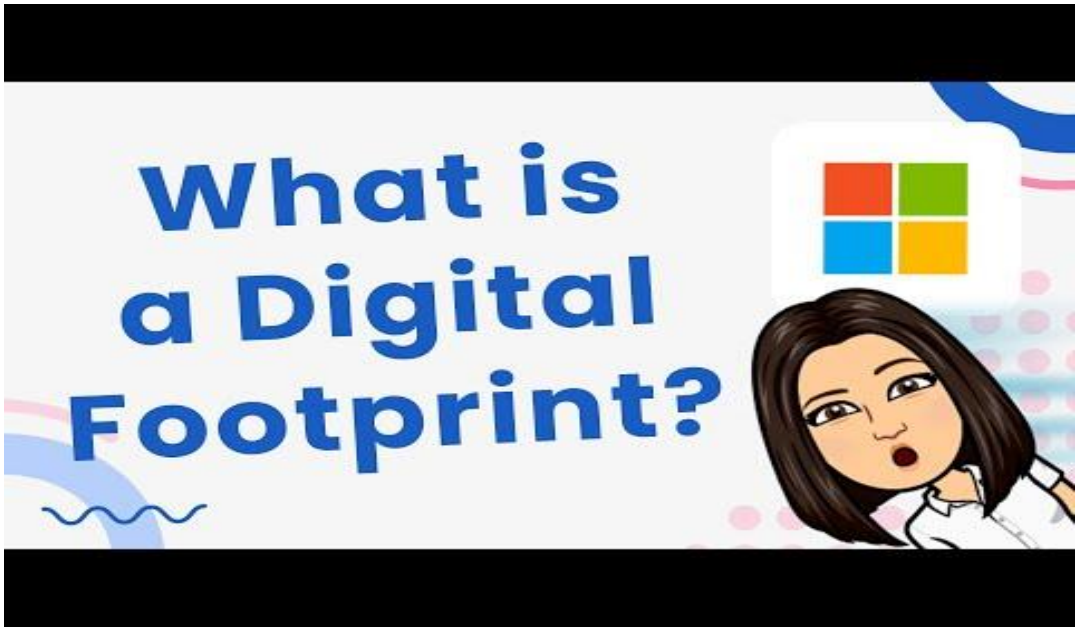
[End_of_Page]

4.1 Διαχείριση και προστασία της διαδικτυακής παρουσίας

Act_ID#4.1.1 Παρουσίαση - Διαχείριση και προστασία της διαδικτυακής παρουσίας [Υπερκείμενο & Video]

Παρακολουθήστε το παρακάτω βίντεο που αναφέρεται στο διαδικτυακό μας αποτύπωμα και πως μπορούμε να το διαχειριστούμε.

https://youtu.be/dmQGq_FNBpE?si=4lCER4j_oimaFnWT



[End_of_Page]

Act_ID#3.1.2 Επίδειξη - Διαχείριση και προστασία της διαδικτυακής παρουσίας [Υπερκείμενο & Video]

Dos and don'ts σχετικά με τη διαδικτυακή παρουσία.

https://youtu.be/7_iVgqgXzi8?si=mRGaBYjLO5Mrgbgp

[End_of_Page]

Act_ID#3.1.3 Δραστηριότητα εξάσκησης [quizzes]

1. Οι πληροφορίες που δημοσιεύουμε στο διαδίκτυο μπορούν να παραμείνουν εκεί για πάντα, ακόμα και αν τις διαγράψουμε. (Σωστό)
2. Είναι ασφαλές να κοινοποιούμε προσωπικές πληροφορίες, όπως τη διεύθυνση ή τον αριθμό τηλεφώνου μας, σε δημόσια προφίλ στα κοινωνικά δίκτυα. (Λάθος)
3. Οι ρυθμίσεις απορρήτου στα κοινωνικά δίκτυα μας επιτρέπουν να ελέγχουμε ποιος μπορεί να δει τις αναρτήσεις και τις πληροφορίες μας. (Σωστό)
4. Το ψηφιακό αποτύπωμα περιλαμβάνει μόνο τις πληροφορίες που δημοσιεύουμε εμείς οι ίδιοι στο διαδίκτυο. (Λάθος)
5. Η διαδικτυακή μας φήμη μπορεί να επηρεάσει τις ευκαιρίες μας για εργασία ή σπουδές. (Σωστό)

[End_of_Page]

Act_ID#3.1.4 Δραστηριότητα αυτοαξιολόγησης [multiple choice questions]

1.Ποιο από τα παρακάτω ΔΕΝ αποτελεί μέρος του ψηφιακού σας αποτυπώματος;

a) Οι αναρτήσεις σας στα κοινωνικά δίκτυα.
b) Τα σχόλιά σας σε ιστοσελίδες και blogs.
c) Οι φωτογραφίες που σας έχουν τραβήξει άλλοι και έχουν αναρτήσει στο διαδίκτυο.
d) Οι σκέψεις σας που δεν έχετε μοιραστεί με κανέναν.

2.Ποιος είναι ο καλύτερος τρόπος για να προστατεύσετε τα προσωπικά σας δεδομένα στα κοινωνικά δίκτυα;

a) Να κοινοποιείτε όσο το δυνατόν περισσότερες πληροφορίες για τον εαυτό σας.
b) Να αποδέχεστε αιτήματα φιλίας από αγνώστους.
c) Να ελέγχετε και να προσαρμόζετε τις ρυθμίσεις απορρήτου σας.
d) Να μην χρησιμοποιείτε καθόλου τα κοινωνικά δίκτυα.

3.Τι μπορεί να επηρεάσει η διαδικτυακή σας φήμη;

a) Τις ευκαιρίες σας για εργασία ή σπουδές
b) Τις σχέσεις σας με φίλους και συγγενείς
c) Την αυτοεκτίμησή σας
d) Όλα τα παραπάνω

4.Ποια από τις παρακάτω ενέργειες μπορεί να βλάψει τη διαδικτυακή σας φήμη;

a) Δημοσίευση προσβλητικών ή ακατάλληλων σχολίων.
b) Κοινοποίηση ψευδών πληροφοριών.
c) Συμμετοχή σε διαδικτυακό εκφοβισμό (cyberbullying).
d) Όλα τα παραπάνω

5.Ποιο από τα παρακάτω είναι ένα παράδειγμα καλής διαχείρισης της διαδικτυακής σας παρουσίας;

a) Δημιουργία ενός επαγγελματικού προφίλ σε ένα κοινωνικό δίκτυο που αναδεικνύει τις δεξιότητες και τα επιτεύγματά σας
b) Συμμετοχή σε online συζητήσεις με σεβασμό και ευγένεια

c) Τακτικός έλεγχος και ενημέρωση των προσωπικών σας πληροφοριών στο διαδίκτυο

d) Όλα τα παραπάνω

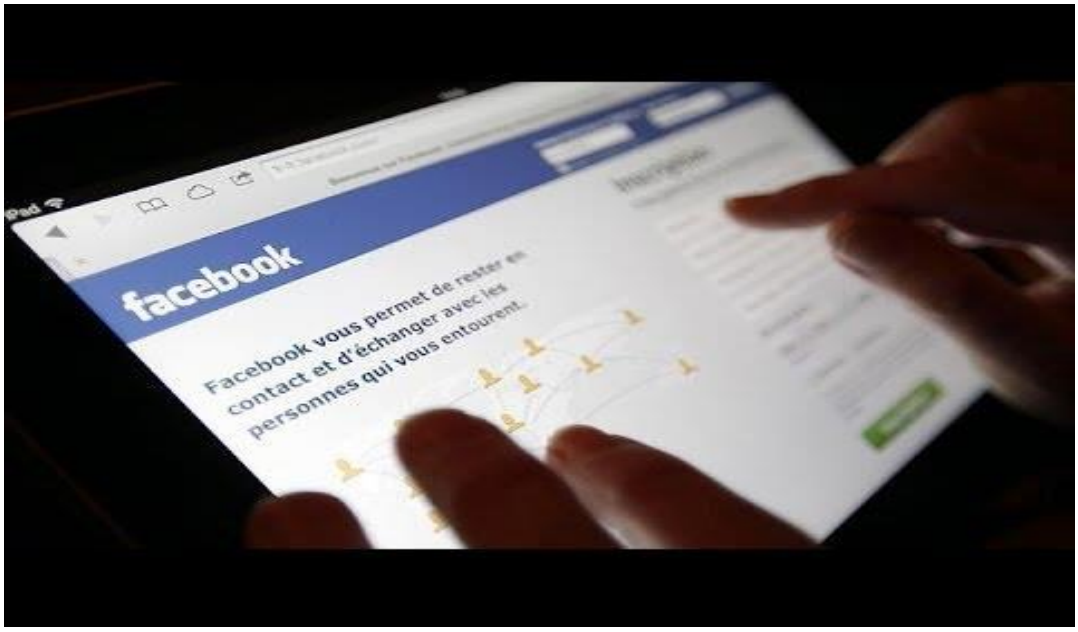
[End_of_Page]

3.2 Αντιμετώπιση της διαδικτυακής παρενόχλησης

Act_ID#3.2.1 Παρουσίαση - Αντιμετώπιση της διαδικτυακής παρενόχλησης [Υπερκείμενο & Video]

Συζήτηση από ειδικούς για την καταπολέμηση της διαδικτυακής παρενόχλησης

https://youtu.be/91dYxCMXk-4?si=gVaeQiDmUQF9rw1f



[End_of_Page]

Act_ID#3.2.2 Επίδειξη - Αντιμετώπιση της διαδικτυακής παρενόχλησης [Υπερκείμενο & Video]

Πως ορίζεται ο διαδικτυακός εκφοβισμός και ποια είναι τα κύρια στοιχεία για την αναγνώριση και αντιμετώπιση του.

https://youtu.be/v45sZEt_BFI?si=QT5s7ctPVZfqa_Lv

https://youtu.be/Fvw5tY5vgp8?si=Q8kBhZYKNaO7l1BZ

[End_of_Page]

Act_ID# 3.2.3 Δραστηριότητα εξάσκησης [quizzes]

1. Η διαδικτυακή παρενόχληση μπορεί να περιλαμβάνει την αποστολή προσβλητικών μηνυμάτων, τη διάδοση φημών ή την κοινοποίηση εξευτελιστικών φωτογραφιών ή βίντεο. (Σωστό)
2. Η διαδικτυακή παρενόχληση είναι απλώς ένα αστείο και δεν έχει σοβαρές συνέπειες για τα θύματα. (Λάθος)
3. Αν κάποιος σας παρενοχλεί στο διαδίκτυο, είναι καλύτερο να το αγνοήσετε και να ελπίζετε ότι θα σταματήσει από μόνο του. (Λάθος)
4. Είναι σημαντικό να αποθηκεύετε αποδεικτικά στοιχεία της διαδικτυακής παρενόχλησης, όπως μηνύματα ή στιγμιότυπα οθόνης. (Σωστό)
5. Αν είστε μάρτυρας διαδικτυακής παρενόχλησης, δεν πρέπει να παρέμβετε, καθώς αυτό μπορεί να σας κάνει στόχο. (Λάθος)

[End_of_Page]

Act_ID#3.2.4 Δραστηριότητα αυτοαξιολόγησης [multiple choice questions]

1.Ποια από τις παρακάτω ενέργειες ΔΕΝ αποτελεί μορφή διαδικτυακής παρενόχλησης;

a) Αποστολή απειλητικών μηνυμάτων
b) Διάδοση ψευδών φημών
c) Κοινοποίηση προσωπικών πληροφοριών χωρίς την άδεια του ατόμου
d) Αποστολή ενός μηνύματος υποστήριξης σε ένα φίλο που έχει πέσει θύμα διαδικτυακής παρενόχλησης

2.Ποιες μπορεί να είναι οι συνέπειες της διαδικτυακής παρενόχλησης για τα θύματα;

a) Χαμηλή αυτοεκτίμηση και κατάθλιψη
b) Άγχος και κοινωνική απομόνωση
c) Προβλήματα στο σχολείο ή την εργασία
d) Όλα τα παραπάνω

3.Αν κάποιος σας παρενοχλεί στο διαδίκτυο, ποια είναι η καλύτερη πρώτη σας ενέργεια;

a) Να απαντήσετε με τον ίδιο τρόπο και να ξεκινήσετε έναν διαδικτυακό καυγά
b) Να αποκλείσετε τον χρήστη και να αναφέρετε την παρενόχληση στην πλατφόρμα κοινωνικής δικτύωσης ή στις αρμόδιες αρχές
c) Να διαγράψετε όλους τους λογαριασμούς σας στα κοινωνικά δίκτυα
d) Να μην πείτε τίποτα σε κανέναν και να ελπίζετε ότι θα σταματήσει

4.Αν είστε μάρτυρας διαδικτυακής παρενόχλησης, τι μπορείτε να κάνετε για να βοηθήσετε;

a) Να υποστηρίξετε το θύμα και να του πείτε ότι δεν είναι μόνο του
b) Να αναφέρετε την παρενόχληση στην πλατφόρμα κοινωνικής δικτύωσης ή στις αρμόδιες αρχές
c) Να μην συμμετέχετε στην παρενόχληση και να μην την ενθαρρύνετε
d) Όλα τα παραπάνω

5.Ποιο από τα παρακάτω ΔΕΝ είναι ένας αποτελεσματικός τρόπος για να αντιμετωπίσετε τη διαδικτυακή παρενόχληση;

a) Να αναφέρετε την παρενόχληση στις αρμόδιες αρχές
b) Να αποκλείσετε τον χρήστη που σας παρενοχλεί
c) Να αλλάξετε τους κωδικούς πρόσβασής σας
d) Να απαντήσετε με προσβλητικά σχόλια

[End_of_Page]

3.3 Ανακεφαλαίωση και Αυτοαξιολόγηση ενότητας 3

Act_ID#3.3.1 Ανακεφαλαίωση [Υπερκείμενο]

Στην ενότητα αυτή, εξερευνήσαμε την υπεύθυνη χρήση των κοινωνικών δικτύων, εστιάζοντας στη διαχείριση της διαδικτυακής μας παρουσίας και στην αντιμετώπιση της διαδικτυακής παρενόχλησης.

Διαχείριση και προστασία της διαδικτυακής παρουσίας:

- Κατανοήσαμε τη σημασία του ψηφιακού αποτυπώματος και της διαδικτυακής φήμης.
- Μάθαμε πώς να ελέγχουμε και να προσαρμόζουμε τις ρυθμίσεις απορρήτου μας στα κοινωνικά δίκτυα.

- Συζητήσαμε τρόπους για να προστατεύσουμε τα προσωπικά μας δεδομένα στο διαδίκτυο.
- Εξετάσαμε πώς οι online ενέργειές μας μπορούν να επηρεάσουν τις ευκαιρίες μας στην πραγματική ζωή.

Αναγνώριση και αντιμετώπιση της διαδικτυακής παρενόχλησης:

- Ορίσαμε τι είναι η διαδικτυακή παρενόχληση και αναγνωρίσαμε τις διάφορες μορφές της.
- Συζητήσαμε τις σοβαρές συνέπειες που μπορεί να έχει η διαδικτυακή παρενόχληση για τα θύματα.
- Μάθαμε πώς να αναφέρουμε περιστατικά διαδικτυακής παρενόχλησης και να υποστηρίζουμε τα θύματα.
- Εξετάσαμε στρατηγικές για την αντιμετώπιση της διαδικτυακής παρενόχλησης, τόσο για τα θύματα όσο και για τους μάρτυρες.

Συμπέρασμα:

Η υπεύθυνη χρήση των κοινωνικών δικτύων απαιτεί να είμαστε συνειδητοί για τις online ενέργειές μας και τις επιπτώσεις τους. Με την εφαρμογή των βέλτιστων πρακτικών που συζητήθηκαν σε αυτήν την ενότητα, μπορούμε να δημιουργήσουμε μια θετική διαδικτυακή παρουσία, να προστατεύσουμε τα προσωπικά μας δεδομένα και να συμβάλλουμε στη δημιουργία ενός ασφαλέστερου και πιο σεβαστού διαδικτυακού περιβάλλοντος για όλους.

[End_of_Page]

Act_ID#3.3.2 Εργασία [Open Response Assessment]

Θέμα: Βασικές αρχές ψηφιακής ασφάλειας

Παρακαλούμε απαντήστε στις παρακάτω ερωτήσεις με πλήρεις προτάσεις. Αναφέρετε πρακτικά παραδείγματα όπου είναι δυνατόν και υποστηρίξτε τις απαντήσεις σας με επιχειρήματα.

Ερώτηση:

*1.*Φανταστείτε ότι είστε μάρτυρας ενός περιστατικού διαδικτυακής παρενόχλησης σε μια πλατφόρμα κοινωνικής δικτύωσης. Πώς θα αντιδρούσατε σε αυτήν την κατάσταση; Ποιες ενέργειες θα αναλαμβάνατε για να υποστηρίξετε το θύμα και να προωθήσετε ένα πιο θετικό και ασφαλές διαδικτυακό περιβάλλον;

Απάντηση:

Ρουμπρίκα

Κριτήρια	**5 - Εξαιρετικό**	**4 - Καλό**	**3 - Ικανοποιητικό**	**2 - Χρειάζεται Βελτίωση**	**1 - Μη Ικανοποιητικό**
Κατανόηση της Διαδικτυακής Παρενόχλησης	Συνολική κατανόηση των εννοιών και επιπτώσεων της διαδικτυακής παρενόχλησης.	Καλή κατανόηση με μικρές ανακρίβειες.	Βασική κατανόηση με ορισμένα κενά.	Περιορισμένη κατανόηση της διαδικτυακής παρενόχλησης.	Καμία κατανόηση της διαδικτυακής παρενόχλησης.
Αντίκτυπος στο Περιστατικό	Προληπτική και αποτελεσματική αντίκρουση που περιλαμβάνει πολλές υποστηρικτικές ενέργειες.	Κατάλληλη αντίκρουση με ορισμένες υποστηρικτικές ενέργειες.	Ελάχιστη αντίκρουση με λίγες υποστηρικτικές ενέργειες.	Ανεπαρκής αντίκρουση χωρίς υποστήριξη.	Καμία αντίκρουση στο περιστατικό.

Προώθηση Ευγένειας και Σεβασμού	Ισχυρή έμφαση στην προώθηση της ευγένειας και του σεβασμού, με σαφή παραδείγματα.	Καλή έμφαση στην ευγένεια και το σεβασμό, με ορισμένα παραδείγματα.	Ορισμένη έμφαση στην ευγένεια και το σεβασμό, αλλά χωρίς βάθος.	Περιορισμένη έμφαση στην ευγένεια και το σεβασμό.	Καμία έμφαση στην ευγένεια ή το σεβασμό.

Οδηγίες Αυτοαξιολόγησης

- **Απαντήστε με:**
    - *Πληρότητα και σαφήνεια*
    - *Πρακτικά παραδείγματα*
    - *Υποστήριξη με επιχειρήματα*
- **Ανατρέξτε στις σημειώσεις σας:** Αναλογιστείτε τα μαθησιακά αποτελέσματα και την πρόοδό σας σε κάθε θεματική ενότητα.
- **Αξιολογήστε τις γνώσεις σας:** Χρησιμοποιήστε την παραπάνω ρουμπρίκα για να αξιολογήσετε την επίτευξη κάθε μαθησιακού αποτελέσματος. Δώστε στον εαυτό σας μια βαθμολογία για κάθε κριτήριο από 1 έως 5.
- **Συνολική Βαθμολογία:** Υπολογίστε το άθροισμα των βαθμολογιών σας για όλα τα κριτήρια.

Αυτή η διαδικασία αυτοαξιολόγησης θα σας βοηθήσει να αναγνωρίσετε τις δυνατές και αδύναμες πλευρές της μάθησής σας και να κατανοήσετε καλύτερα πώς μπορείτε να βελτιωθείτε στο μέλλον.

[End_of_Page]

Act_ID#3.3.3 Checklist: Μπορώ να το κάνω… [Checklist & WordCloud]

Για κάθε πρόταση στο checklist, απαντήστε με ειλικρίνεια και αξιολόγησε την ικανότητά σου.

Μπορώ να:

- **Διαχείριση και προστασία της διαδικτυακής παρουσίας:**
  - Εξηγήσω τι είναι το ψηφιακό αποτύπωμα και η διαδικτυακή φήμη.
  - Περιγράψω πώς οι online ενέργειές μου μπορούν να επηρεάσουν τη ζωή μου εκτός διαδικτύου (π.χ., στην εργασία, στις σπουδές, στις σχέσεις).
  - Ελέγξω και προσαρμόσω τις ρυθμίσεις απορρήτου μου στα κοινωνικά δίκτυα.
  - Αναφέρω τουλάχιστον τρεις τρόπους για να προστατεύσω τα προσωπικά μου δεδομένα στο διαδίκτυο.
  - Δημιουργήσω μια θετική διαδικτυακή παρουσία που αντικατοπτρίζει την καλύτερη εκδοχή του εαυτού μου.
- **Αναγνώριση και αντιμετώπιση της διαδικτυακής παρενόχλησης:**
  - Ορίσω τι είναι η διαδικτυακή παρενόχληση και να αναγνωρίσω τις διάφορες μορφές της (π.χ., προσβλητικά μηνύματα, διάδοση φημών, αποκλεισμός από ομάδες).
  - Περιγράψω τις συνέπειες που μπορεί να έχει η διαδικτυακή παρενόχληση για τα θύματα (π.χ., χαμηλή αυτοεκτίμηση, άγχος, κατάθλιψη).
  - Αναφέρω περιστατικά διαδικτυακής παρενόχλησης στις αρμόδιες αρχές ή στην πλατφόρμα κοινωνικής δικτύωσης.
  - Υποστηρίξω ένα θύμα διαδικτυακής παρενόχλησης με ενσυναίσθηση και σεβασμό.
  - Εφαρμόσω στρατηγικές για την αντιμετώπιση της διαδικτυακής παρενόχλησης, όπως ο αποκλεισμός του χρήστη και η αποθήκευση αποδεικτικών στοιχείων.
  - Προωθήσω την ευγένεια και τον σεβασμό στο διαδικτυακό περιβάλλον μέσω των δικών μου αναρτήσεων και σχολίων.

WordCloud

Γράψε μερικές (1-3) σημαντικές λέξεις που θυμάσαι από την ενότητα που μόλις παρακολούθησες.

[End_of_Page]

Act_ID#3.3.4 [Discussion Forum]

Θέμα συζήτησης: Υπεύθυνη Χρήση Κοινωνικών Δικτύων

Σας προσκαλούμε να μοιραστείτε τις σκέψεις και τις εμπειρίες σας σχετικά με τη διαδικτυακή παρουσία και την αντιμετώπιση τη διαδικτυακής παρενόχλησης (cyberbullying), προωθώντας την ευγένεια και τον σεβασμό στο διαδικτυακό περιβάλλον.

Ερωτήσεις για συζήτηση:

1. Έχετε ποτέ ανησυχήσει για το πώς χρησιμοποιούνται τα προσωπικά σας δεδομένα από τις εταιρείες τεχνολογίας;
2. Πώς μπορούμε να δημιουργήσουμε ένα πιο ασφαλές και υποστηρικτικό διαδικτυακό περιβάλλον για όλους;
3. Ποιοι είναι οι βασικοί κανόνες συμπεριφοράς που πρέπει να ακολουθούμε στα κοινωνικά δίκτυα;

[End_of_Page]

3.4 Πρόσθετο υλικό

Act_ID#3.4.1 Προτάσεις για Επιπλέον Πληροφόρηση

https://stop-bullying.gov.gr/

https://connectsafely.org/

https://saferinternet4kids.gr/

https://www.cyberkid.gov.gr/

https://www.commonsensemedia.org/

[End_of_Page]

[End_of_Topic]

Ημέρα 5 : Διδακτική Ενότητα 4 – Προστασία Παιδιών και Οικογένειας στο Διαδίκτυο (3 ώρες)

4.0 Εισαγωγή Διδακτικής ενότητας 4

Act_ID#4.0.1 Μαθησιακά αποτελέσματα [Υπερκείμενο & Poll]

Μετά την παρακολούθηση της διδακτικής ενότητας 4 θα είσαι ικανός/η να:

MA4 [understand/evaluate/create]: κατανοείς και να εφαρμόζεις τους τρόπους προστασίας των παιδιών και της οικογένειας στο διαδίκτυο..

Το **MA4** αναλύεται σε επιμέρους μαθησιακά αποτελέσματα, ως εξής:

- **MA4.1** Να αναγνωρίζεις τους κινδύνους που αντιμετωπίζουν τα παιδιά στο διαδίκτυο και να εφαρμόζεις κατάλληλα μέτρα προστασίας, όπως εργαλεία γονικού ελέγχου και ασφαλείς ρυθμίσεις στις συσκευές.
- **MA4.2** Να δημιουργείς ένα ασφαλές και υποστηρικτικό διαδικτυακό περιβάλλον για την οικογένειά σου, ενθαρρύνοντας την ανοιχτή επικοινωνία και την εκπαίδευση σχετικά με την ασφαλή χρήση του διαδικτύου.

Poll

Αυτό το σύντομο poll θα ελέγξει τις πρότερες γνώσεις σας. Επιλέξτε αυτό που σας αντιπροσωπεύει καλύτερα. Δεν υπάρχουν σωστές και λάθος απαντήσεις.

1. Πόσο εξοικειωμένοι είστε με τους κινδύνους που μπορεί να αντιμετωπίσουν τα παιδιά στο διαδίκτυο (π.χ., διαδικτυακή παρενόχληση, ακατάλληλο περιεχόμενο, διαδικτυακοί θηρευτές);

- Καθόλου
- Μέτρια
- Ικανοποιητικά
- Πολύ

2. Έχετε χρησιμοποιήσει ποτέ εργαλεία γονικού ελέγχου ή ρυθμίσεις ασφαλείας σε συσκευές που χρησιμοποιούν παιδιά;

- Καθόλου
- Μέτρια
- Ικανοποιητικά
- Πολύ

3. Πόσο συχνά συζητάτε με τα παιδιά σας (ή με παιδιά που γνωρίζετε) για την ασφαλή και υπεύθυνη χρήση του διαδικτύου;

- Καθόλου
- Μέτρια
- Ικανοποιητικά
- Πολύ

[End_of_Page]

Act_ID#4.0.2 Δομή της ενότητας [Υπερκείμενο]

Η Διδακτική Ενότητα 4 είναι διάρκειας 3 ωρών και περιλαμβάνει:

- Εισαγωγή
- Υποενότητα 1 – Προστασία των παιδιών στο διαδίκτυο και εφαρμογή κατάλληλων μέτρων.
- Υποενότητα 2 – Δημιουργία ασφαλούς και υποστηρικτικού διαδικτυακού περιβάλλοντος για την οικογένειά
- Ανακεφαλαίωση και Αυτοαξιολόγηση, που περιλαμβάνει:
  - Σύνοψη της ενότητας
  - Εργασία εφαρμογής με τη μορφή Ερώτησης Ανοικτής Απόκρισης που αυτοαξιολογούν οι εκπαιδευόμενοι με τη χρήση ρουμπρίκας
  - Αυτοαξιολόγηση σε μορφή poll όπου οι εκπαιδευόμενοι επιλέγουν ποιο/ποια από τα μαθησιακά αποτελέσματα της ενότητας έχουν κατακτήσει.
  - Forum συζήτησης

Οι 2 υποενότητες είναι διάρκειας 1 ώρας η κάθε μία. Η κάθε υποενότητα αποτελείται από:

- Δραστηριότητα παρουσίασης (15')
- Δραστηριότητα επίδειξης (15')
- Δραστηριότητα εξάσκησης (15')
- Δραστηριότητα αυτοαξιολόγησης (15')

[End_of_Page]

4.1 Προστασία των παιδιών στο διαδίκτυο και εφαρμογή κατάλληλων μέτρων.

Act_ID#4.1.1 Παρουσίαση - Προστασία των παιδιών στο διαδίκτυο και εφαρμογή κατάλληλων μέτρων [Υπερκείμενο & Video]

Σύντομος οδηγός για γονείς.

https://youtu.be/c6odst87Tbo?si=Wib8O6_64Re1aZk9

Βίντεο που παρουσιάζουν περιπτώσεις διαδικτυακών κινδύνων για παιδιά και εφήβους.

https://youtu.be/M_2rXM3W5gQ?si=Rk4pisMwoSSmymFx

https://youtu.be/z6sIC4MXXOA?si=3nVW5UywT_WBbCjF

[End_of_Page]

Act_ID#4.1.2 Επίδειξη - Προστασία των παιδιών στο διαδίκτυο και εφαρμογή κατάλληλων μέτρων. **[Υπερκείμενο & Video]**

Οδηγίες για τα ίδια τα παιδιά.

https://youtu.be/yrln8nyVBLU?si=YtjPQbRRmeCChu6Q

Εφαρμογή γονικού ελέγχου σε συγκεκριμένες συσκευές

https://youtu.be/eZZaQFox4JY?si=hbk4OxRhsdUazohi

[End_of_Page]

Act_ID#4.1.3 Δραστηριότητα εξάσκησης [quizzes]

1. Η διαδικτυακή παρενόχληση (cyberbullying) είναι ένας από τους κινδύνους που αντιμετωπίζουν τα παιδιά στο διαδίκτυο. (Σωστό)
2. Τα εργαλεία γονικού ελέγχου μπορούν να εμποδίσουν εντελώς την πρόσβαση των παιδιών σε ακατάλληλο περιεχόμενο. (Λάθος)
3. Είναι σημαντικό να συζητάτε με τα παιδιά σας για τους κινδύνους του διαδικτύου και να τα ενθαρρύνετε να σας μιλούν αν αντιμετωπίσουν κάποιο πρόβλημα. (Σωστό)
4. Οι ασφαλείς ρυθμίσεις στις συσκευές, όπως η ενεργοποίηση του απορρήτου και η απενεργοποίηση της τοποθεσίας, μπορούν να βοηθήσουν στην προστασία των παιδιών. (Σωστό)
5. Τα παιδιά δεν πρέπει ποτέ να χρησιμοποιούν το διαδίκτυο χωρίς την επίβλεψη ενός ενήλικα. (Λάθος)

[End_of_Page]

Act_ID#4.1.4 Δραστηριότητα αυτοαξιολόγησης [multiple choice questions]

1.Ποιος από τους παρακάτω ΔΕΝ είναι ένας κίνδυνος που αντιμετωπίζουν τα παιδιά στο

διαδίκτυο;

a) Διαδικτυακή παρενόχληση (cyberbullying)
b) Έκθεση σε ακατάλληλο περιεχόμενο
c) Διαδικτυακοί θηρευτές
d) Χρήση εκπαιδευτικών εφαρμογών

2.Ποιος είναι ο κύριος σκοπός των εργαλείων γονικού ελέγχου;

a) Να εμποδίσουν εντελώς την πρόσβαση των παιδιών στο διαδίκτυο
b) Να περιορίσουν την πρόσβαση των παιδιών σε ακατάλληλο περιεχόμενο και να παρακολουθούν τη διαδικτυακή τους δραστηριότητα
c) Να επιτρέψουν στα παιδιά να έχουν απεριόριστη πρόσβαση στο διαδίκτυο
d) Να αντικαταστήσουν την ανάγκη για επικοινωνία και επίβλεψη από τους γονείς

3.Ποια από τις παρακάτω ρυθμίσεις ασφαλείας είναι σημαντικό να ενεργοποιήσετε στις συσκευές που χρησιμοποιούν τα παιδιά;

a) Απενεργοποίηση της τοποθεσίας
b) Ενεργοποίηση του απορρήτου
c) Χρήση ισχυρών κωδικών πρόσβασης
d) Όλα τα παραπάνω

4.Ποια είναι η καλύτερη προσέγγιση για να μιλήσετε στα παιδιά σας για τους κινδύνους του διαδικτύου;

a) Να τα τρομάξετε με ιστορίες για διαδικτυακούς κινδύνους
b) Να τους απαγορεύσετε να χρησιμοποιούν το διαδίκτυο
c) Να έχετε ανοιχτές και ειλικρινείς συζητήσεις μαζί τους, εξηγώντας τους κινδύνους και πώς να τους αποφεύγουν
d) Να τους δώσετε πλήρη ελευθερία στο διαδίκτυο χωρίς καμία επίβλεψη

5.Ποια είναι η σημασία της συνεργασίας μεταξύ γονέων και σχολείου για την ασφάλεια των παιδιών στο διαδίκτυο;

a) Το σχολείο μπορεί να παρέχει εκπαιδευτικά προγράμματα και πόρους για την ψηφιακή ασφάλεια
b) Οι γονείς μπορούν να ενημερώνουν το σχολείο για τυχόν προβλήματα που αντιμετωπίζουν τα παιδιά τους στο διαδίκτυο

c) Η συνεργασία μπορεί να βοηθήσει στη δημιουργία ενός ασφαλούς και υποστηρικτικού περιβάλλοντος για τα παιδιά τόσο στο σχολείο όσο και στο σπίτι
d) Όλα τα παραπάνω

[End_of_Page]

4.2 Δημιουργία ασφαλούς και υποστηρικτικού διαδικτυακού περιβάλλοντος για την οικογένειά

Act_ID#4.2.1 Παρουσίαση - Δημιουργία ασφαλούς και υποστηρικτικού διαδικτυακο περιβάλλοντος για την οικογένειά [Υπερκείμενο & Video]

Κίνδυνοι διαδικτύου και τρόποι προστασίας.

https://youtu.be/35nuOD3rA8I?si=1iF3zAmxfr30euaR

Ένα βίντεο που αναφέρεται στο διαδικτυακό εθισμό των εφήβων.

https://youtu.be/8hJpgtJMNBc?si=nCGmmxZW5pvHkpt4

[End_of_Page]

Act_ID#4.2.2 Επίδειξη - Δημιουργία ασφαλούς και υποστηρικτικού διαδικτυακού περιβάλλοντος για την οικογένειά [Υπερκείμενο & Video]

Παρακολουθήστε τα παρακάτω βίντεο για τη χρήση των οικογενειακών συσκευών(υπολογιστές, κινητα, tablet) και τους κανόνες που μπορεί να συμφωνήσει όλη η οικογένεια.

https://youtu.be/4VAy4c1oeiI?si=tzaR1aK2m3bhywth

https://youtu.be/HAmbinoAyH4?si=GUaH-SY-OnlvrjR9

[End_of_Page]

Act_ID# 4.2.3 Δραστηριότητα εξάσκησης [quizzes]

1. Η δημιουργία ενός ασφαλούς διαδικτυακού περιβάλλοντος για την οικογένεια περιλαμβάνει μόνο την εγκατάσταση εργαλείων γονικού ελέγχου. (Λάθος)

2. Η ανοιχτή επικοινωνία με τα παιδιά σχετικά με τη χρήση του διαδικτύου μπορεί να τα βοηθήσει να αισθάνονται άνετα να μιλούν για τυχόν προβλήματα ή ανησυχίες που αντιμετωπίζουν online. (Σωστό)
3. Οι γονείς δεν χρειάζεται να εκπαιδεύονται σχετικά με την ασφαλή χρήση του διαδικτύου, καθώς τα παιδιά τους είναι πιο εξοικειωμένα με την τεχνολογία. (Λάθος)
4. Η δημιουργία κανόνων για τη χρήση του διαδικτύου στην οικογένεια μπορεί να βοηθήσει στην προώθηση της υπεύθυνης και ασφαλούς συμπεριφοράς online. (Σωστό)
5. Είναι σημαντικό να δείχνετε ενδιαφέρον για τις online δραστηριότητες των παιδιών σας και να τα ενθαρρύνετε να μοιράζονται τις εμπειρίες τους μαζί σας. (Σωστό

[End_of_Page]

Act_ID#4.2.4 Δραστηριότητα αυτοαξιολόγησης [multiple choice questions]

1.Ποιος από τους παρακάτω τρόπους ΔΕΝ συμβάλλει στη δημιουργία ενός ασφαλούς διαδικτυακού περιβάλλοντος για την οικογένεια;

a) Εγκατάσταση εργαλείων γονικού ελέγχου.
b) Ανοιχτή επικοινωνία με τα παιδιά σχετικά με τη χρήση του διαδικτύου.
c) Εκπαίδευση των παιδιών σχετικά με την ασφαλή χρήση του διαδικτύου.
d) Αποφυγή κάθε συζήτησης σχετικά με τους κινδύνους του διαδικτύου για να μην τρομάξουν τα παιδιά.

2.Ποιος είναι ο ρόλος της ανοιχτής επικοινωνίας στη δημιουργία ενός ασφαλούς διαδικτυακού περιβάλλοντος για την οικογένεια;

a) Επιτρέπει στα παιδιά να μοιράζονται τις εμπειρίες τους και να εκφράζουν τυχόν ανησυχίες τους σχετικά με το διαδίκτυο.
b) Βοηθά τους γονείς να κατανοήσουν καλύτερα τις online δραστηριότητες των παιδιών τους.
c) Ενισχύει την εμπιστοσύνη μεταξύ γονέων και παιδιών.
d) Όλα τα παραπάνω.

3.Γιατί είναι σημαντικό οι γονείς να εκπαιδεύονται σχετικά με την ασφαλή χρήση του

διαδικτύου;

a) Για να μπορούν να καθοδηγήσουν τα παιδιά τους και να τα προστατεύσουν από τους κινδύνους.
b) Για να είναι σε θέση να χρησιμοποιούν αποτελεσματικά τα εργαλεία γονικού ελέγχου.
c) Για να είναι ενήμεροι για τις τελευταίες εξελίξεις στον τομέα της ψηφιακής ασφάλειας.
d) Όλα τα παραπάνω.

4.Πώς μπορούν οι γονείς να ενθαρρύνουν τα παιδιά τους να μιλούν για τυχόν προβλήματα που αντιμετωπίζουν στο διαδίκτυο;

a) Δημιουργώντας ένα κλίμα εμπιστοσύνης και κατανόησης.
b) Ακούγοντας προσεκτικά τα παιδιά τους χωρίς να τα κρίνουν.
c) Διαβεβαιώνοντας τα παιδιά τους ότι δεν θα τιμωρηθούν αν μιλήσουν για κάποιο πρόβλημα
d) Όλα τα παραπάνω.

5.Ποιος είναι ο ρόλος του σχολείου στην προώθηση της ασφαλούς χρήσης του διαδικτύου από τα παιδιά;

a) Να παρέχει εκπαιδευτικά προγράμματα και δραστηριότητες για την ψηφιακή ασφάλεια.
b) Να συνεργάζεται με τους γονείς για την αντιμετώπιση τυχόν προβλημάτων που σχετίζονται με το διαδίκτυο
c) Να δημιουργεί ένα ασφαλές διαδικτυακό περιβάλλον στο σχολείο.
d) Όλα τα παραπάνω.

[End_of_Page]

4.3 Ανακεφαλαίωση και Αυτοαξιολόγηση ενότητας 4

Act_ID#4.3.1 Ανακεφαλαίωση [Υπερκείμενο]

Σε αυτήν την ενότητα, εξερευνήσαμε τη σημασία της δημιουργίας ενός ασφαλούς διαδικτυακού περιβάλλοντος για τα παιδιά και τις οικογένειες.

Κίνδυνοι στο Διαδίκτυο για τα παιδιά:

- Αναγνωρίσαμε τους κυριότερους κινδύνους που αντιμετωπίζουν τα παιδιά στο διαδίκτυο, όπως η διαδικτυακή παρενόχληση, η έκθεση σε ακατάλληλο περιεχόμενο και οι διαδικτυακοί θηρευτές.
- Συζητήσαμε τη σημασία της ενημέρωσης και της εγρήγορσης για την προστασία των παιδιών από αυτές τις απειλές.
- Εργαλεία και Ρυθμίσεις Ασφαλείας:
- Εξετάσαμε τη χρήση εργαλείων γονικού ελέγχου για τον περιορισμό της πρόσβασης σε ακατάλληλο περιεχόμενο και την παρακολούθηση της online δραστηριότητας των παιδιών.
- Μάθαμε για τις σημαντικότερες ρυθμίσεις ασφαλείας που πρέπει να εφαρμόζονται στις συσκευές που χρησιμοποιούν τα παιδιά.

Δημιουργία Ασφαλούς Οικογενειακού Περιβάλλοντος:

- Τονίσαμε τη σημασία της ανοιχτής επικοινωνίας και της εκπαίδευσης για την προώθηση της ασφαλούς χρήσης του διαδικτύου από τα παιδιά.
- Συζητήσαμε πώς οι γονείς μπορούν να ενθαρρύνουν τα παιδιά τους να μιλούν για τυχόν προβλήματα ή ανησυχίες που αντιμετωπίζουν στο διαδίκτυο.
- Επισημάναμε τη σημασία της συνεργασίας μεταξύ γονέων και σχολείου για την προστασία των παιδιών στο διαδίκτυο.

Συμπέρασμα:

Η ασφάλεια των παιδιών στο διαδίκτυο είναι μια κοινή ευθύνη που απαιτεί τη συνεργασία γονέων, εκπαιδευτικών και της κοινωνίας στο σύνολό της. Με την εφαρμογή των κατάλληλων μέτρων προστασίας και την προώθηση της ανοιχτής επικοινωνίας, μπορούμε να βοηθήσουμε τα παιδιά να αξιοποιήσουν τις δυνατότητες του διαδικτύου με ασφάλεια και υπευθυνότητα.

[End_of_Page]

Act_ID#4.3.2 Εργασία [Open Response Assessment]

Θέμα: Προστασία Παιδιών και Οικογένειας στο Διαδίκτυο

Παρακαλούμε απαντήστε στις παρακάτω ερωτήσεις με πλήρεις προτάσεις. Αναφέρετε πρακτικά παραδείγματα όπου είναι δυνατόν και υποστηρίξτε τις απαντήσεις σας με επιχειρήματα.

Ερώτηση:

1.Πώς μπορούν οι γονείς να ενθαρρύνουν τα παιδιά τους να μιλήσουν για τυχόν προβλήματα ή ανησυχίες που αντιμετωπίζουν στο διαδίκτυο;

Απάντηση:

Ρουμπρίκα

Κριτήρια	**1 - Χρειάζεται Βελτίωση**	**2 - Μέτριο**	**3 - Καλό**	**4 - Πολύ Καλό**	**5 - Εξαιρετικό**
Κατανόηση Θεμάτων Ασφάλειας στο Διαδίκτυο	Περιορισμένη κατανόηση των θεμάτων ασφάλειας στο διαδίκτυο; έλλειψη λεπτομέρειας.	Βασική κατανόηση-μερικά σχετικά σημεία αλλά λείπει βάθος.	Καλή κατανόηση-καλύπτει τα περισσότερα βασικά θέματα.	Πολύ καλή κατανόηση-καλύπτει όλα τα κύρια θέματα με σαφήνεια.	Εξαιρετική κατανόηση-περιεκτική και διορατική ανάλυση των θεμάτων ασφάλειας στο διαδίκτυο.
Ενθάρρυνση Ανοιχτής Επικοινωνίας	Δεν παρέχει στρατηγικές για την επικοινωνία.	Λίγες στρατηγικές αναφέρονται, έλλειψη αποτελεσματικότητας.	Παρέχει κάποιες αποτελεσματικές στρατηγικές για την επικοινωνία.	Προσφέρει πολλές αποτελεσματικές στρατηγικές; ενθαρρύνει τον διάλογο.	Παρέχει μια ποικιλία εξαιρετικά αποτελεσματικών στρατηγικών, προάγει ένα υποστηρικτικό

					περιβάλλον για ανοιχτό διάλογο.
Πρακτικά Παραδείγματα	Δεν παρέχονται παραδείγματα.	Λίγα παραδείγματα που δεν είναι σχετικά ή αποτελεσματικά.	Ορισμένα σχετικά παραδείγματα παρέχονται; κάπως αποτελεσματικά.	Πολλαπλά σχετικά παραδείγματα που εικονογραφούν καλά τα σημεία.	Πολλά και εξαιρετικά σχετικά παραδείγματα που ενισχύουν την κατανόηση και τη συμμετοχή.

Οδηγίες Αυτοαξιολόγησης

- **Απαντήστε με:**
    - Πληρότητα και σαφήνεια
    - Πρακτικά παραδείγματα
    - Υποστήριξη με επιχειρήματα
- **Ανατρέξτε στις σημειώσεις σας:** Αναλογιστείτε τα μαθησιακά αποτελέσματα και την πρόοδό σας σε κάθε θεματική ενότητα.
- **Αξιολογήστε τις γνώσεις σας:** Χρησιμοποιήστε την παραπάνω ρουμπρίκα για να αξιολογήσετε την επίτευξη κάθε μαθησιακού αποτελέσματος. Δώστε στον εαυτό σας μια βαθμολογία για κάθε κριτήριο από 1 έως 5.
- **Συνολική Βαθμολογία:** Υπολογίστε το άθροισμα των βαθμολογιών σας για όλα τα κριτήρια.

Αυτή η διαδικασία αυτοαξιολόγησης θα σας βοηθήσει να αναγνωρίσετε τις δυνατές και αδύναμες πλευρές της μάθησής σας και να κατανοήσετε καλύτερα πώς μπορείτε να βελτιωθείτε στο μέλλον.

[End_of_Page]

Act_ID#4.3.3 Checklist: Μπορώ να το κάνω… [Checklist & WordCloud]

Για κάθε πρόταση στο checklist, απαντήστε με ειλικρίνεια και αξιολόγησε την ικανότητά σου.

MA4.1

- Αναγνωρίζω τους κυριότερους κινδύνους που αντιμετωπίζουν τα παιδιά στο διαδίκτυο (π.χ., διαδικτυακή παρενόχληση, έκθεση σε ακατάλληλο περιεχόμενο, διαδικτυακοί θηρευτές).
- Εξηγώ πώς λειτουργούν τα εργαλεία γονικού ελέγχου και πώς μπορούν να χρησιμοποιηθούν για την προστασία των παιδιών.
- Εφαρμόζω κατάλληλες ρυθμίσεις ασφαλείας στις συσκευές που χρησιμοποιούν τα παιδιά.
- Ενημερώνομαι για τις τελευταίες εξελίξεις στον τομέα της ασφάλειας στο διαδίκτυο για παιδιά.

MA4.2

- Δημιουργώ ένα κλίμα εμπιστοσύνης και ανοιχτής επικοινωνίας με τα παιδιά μου σχετικά με τη χρήση του διαδικτύου.
- Εκπαιδεύω τα παιδιά μου σχετικά με την ασφαλή και υπεύθυνη χρήση του διαδικτύου.
- Ενθαρρύνω τα παιδιά μου να μου μιλούν για τυχόν προβλήματα ή ανησυχίες που αντιμετωπίζουν στο διαδίκτυο.
- Συνεργάζομαι με το σχολείο για την προώθηση της ασφαλούς χρήσης του διαδικτύου από τα παιδιά.

WordCloud

Γράψε μερικές (1-3) σημαντικές λέξεις που θυμάσαι από την ενότητα που μόλις παρακολούθησες.

[End_of_Page]

Act_ID#4.3.4 [Discussion Forum]

Θέμα συζήτησης: Ασφαλές Διαδίκτυο για τα παιδιά μας: Προκλήσεις και Λύσεις

Τα παιδιά σήμερα μεγαλώνουν σε έναν κόσμο όπου το διαδίκτυο είναι πανταχού παρόν. Ενώ το διαδίκτυο προσφέρει πολλές ευκαιρίες για μάθηση και επικοινωνία, εγκυμονεί και κινδύνους για τα παιδιά.

Σας προσκαλούμε να μοιραστείτε τις σκέψεις και τις εμπειρίες σας σχετικά με την ασφάλεια των παιδιών στο διαδίκτυο.

Ερωτήσεις για Συζήτηση:

1.Ποιες είναι οι μεγαλύτερες ανησυχίες σας ως γονείς σχετικά με τη χρήση του διαδικτύου από τα παιδιά σας;

2.Πώς μπορούμε να βοηθήσουμε τα παιδιά να αναπτύξουν κριτική σκέψη και να λαμβάνουν υπεύθυνες αποφάσεις στο διαδίκτυο;

[End_of_Page]

4.4 Πρόσθετο υλικό

Act_ID#4.4.1 Προτάσεις για Επιπλέον Πληροφόρηση

https://www.socialworkerstoolbox.com/online-safety-agreement/

[End_of_Page]

[End_of_Topic]

Ημέρα 6: Τελική Αξιολόγηση MOOC (1 ώρα)

5.0 Οδηγίες για τη διεξαγωγή της τελικής εξέτασης του MOOC

Act_ID#5.0.1 Οδηγίες για τη διεξαγωγή της τελικής εξέτασης του MOOC [Υπερκείμενο]

Ο τελικός βαθμός σας στο μάθημα προκύπτει από το quiz τελικής εξέτασης. Για να θεωρηθεί επιτυχής η εξέταση θα πρέπει να συγκεντρώσετε βαθμολογία > 80%.

Το Quiz αποτελείται από 5 ερωτήσεις ανά ενότητα που περιλαμβάνουν:

Πολλαπλή Επιλογή με μία σωστή απάντηση,

Πολλαπλή επιλογή με περισσότερες από μία σωστές απαντήσεις και

Ερωτήσεις Σωστού/Λάθους.

Δεν υπάρχει περιορισμός χρόνου.

Θα έχετε δύο προσπάθειες να απαντήσετε σε όλες τις ερωτήσεις του κουίζ, εκτός από τις ερωτήσεις 'Σωστού-Λάθους'.
Μόλις κάνετε κλικ στο κουμπί "Έλεγχος", θα καταχωρηθεί ως πρώτη προσπάθεια. Αν είναι λάθος, δοκιμάστε ξανά και κάντε κλικ στο κουμπί "Τελικός έλεγχος".
Θα χρειαστείτε λιγότερο από 45 λεπτά από το χρόνο σας για να ολοκληρώσετε αυτό το κουίζ, αλλά αξίζει αφού μπορεί να οδηγήσει στο πιστοποιητικό σας.
[End_of_Page]

5.1 Τελική Αξιολόγηση

Act_ID#5.1.1 Τελική Αξιολόγηση [Quiz]

Ενότητα 1: Βασικές Αρχές Ψηφιακής Ασφάλειας

ΜΑ1.1: Αναγνώριση και αξιολόγηση κινδύνων και απειλών στο διαδίκτυο

1.Ποιο από τα παρακάτω είναι ένα παράδειγμα ηλεκτρονικού "ψαρέματος" (phishing);

(α) Ένα email από την τράπεζά σας που σας ζητά να επιβεβαιώσετε τα στοιχεία σύνδεσής σας μέσω ενός συνδέσμου.
(β) Ένα μήνυμα από έναν φίλο σας που σας στέλνει έναν αστείο σύνδεσμο.
(γ) Ένα email από ένα ηλεκτρονικό κατάστημα που σας ενημερώνει για μια νέα προσφορά.
(δ) Ένα μήνυμα από τον πάροχο email σας που σας ενημερώνει για μια αλλαγή στους όρους χρήσης.

2.Ποια από τις παρακάτω ενέργειες μπορεί να βοηθήσει στην προστασία από το κακόβουλο λογισμικό (malware);

(α) Ανοίγω συνημμένα από άγνωστους αποστολείς.
(β) Κάνω κλικ σε αναδυόμενες διαφημίσεις.
(γ) Εγκαθιστώ ένα πρόγραμμα προστασίας από ιούς και το ενημερώνω τακτικά
(δ) Χρησιμοποιώ τον ίδιο κωδικό πρόσβασης για όλους τους λογαριασμούς μου

3.Ποια από τις παρακάτω πηγές είναι πιο πιθανό να παρέχει αξιόπιστες πληροφορίες;

(α)Ένας ιστότοπος με πολλές αναδυόμενες διαφημίσεις.

(β)Ένα blog που γράφεται από έναν ανώνυμο χρήστη.

(γ)Ένας επίσημος κυβερνητικός ιστότοπος.

(δ)Ένα μήνυμα που κοινοποιήθηκε ευρέως στα μέσα κοινωνικής δικτύωσης χωρίς να έχει επαληθευτεί η πηγή του.

4.Η παραπληροφόρηση μπορεί να έχει σοβαρές συνέπειες, όπως η διάδοση πανικού ή η πρόκληση βλάβης στη φήμη κάποιου. (Σωστό ή Λάθος)(Απάντηση: Σωστό)

5.Ποιες από τις παρακάτω ενέργειες μπορούν να βοηθήσουν στην καταπολέμηση της παραπληροφόρησης; (Πολλαπλής επιλογής - περισσότερες από μία σωστές απαντήσεις)

(α) Έλεγχος των γεγονότων πριν από την κοινοποίηση πληροφοριών
(β) Κριτική σκέψη και αξιολόγηση των πηγών
(γ) Αναφορά ύποπτου περιεχομένου στις πλατφόρμες κοινωνικής δικτύωσης
(δ) Κοινοποίηση πληροφοριών από μη επαληθευμένες πηγές

ΜΑ1.2: Δημιουργία και διαχείριση ισχυρών κωδικών πρόσβασης και προστασία προσωπικών δεδομένων

1.Ποιο από τα παρακάτω είναι ένα παράδειγμα ισχυρού κωδικού πρόσβασης;

(α) 12345678
(β) Το όνομά σας
(γ) Pa$$word123!
(δ) Η ημερομηνία γέννησής σας

2.Είναι ασφαλές να χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για όλους τους online λογαριασμούς σας. (**Σωστό ή Λάθος**)(Απάντηση: Λάθος)

3.Ποια από τις παρακάτω ενέργειες μπορεί να βοηθήσει στην προστασία των προσωπικών σας δεδομένων στο διαδίκτυο;

(α) Κοινοποίηση των κωδικών πρόσβασής σας με φίλους.
(β) Χρήση δημόσιων υπολογιστών για να συνδεθείτε σε ευαίσθητους λογαριασμούς.

(γ) Έλεγχος των ρυθμίσεων απορρήτου στις εφαρμογές και τους ιστότοπους που χρησιμοποιείτε

(δ) Αποθήκευση των κωδικών πρόσβασής σας σε ένα σημειωματάριο

4.Ποιες από τις παρακάτω πληροφορίες θεωρούνται προσωπικά δεδομένα; (Πολλαπλής επιλογής -περισσότερες από μία σωστές απαντήσεις)

(α) Όνομα

(β) Διεύθυνση

(γ) Αριθμός τηλεφώνου

(δ) Χρώμα ματιών

5.Ποια είναι η σημασία του ελέγχου ταυτότητας δύο παραγόντων (2FA);

(α) Παρέχει ένα επιπλέον επίπεδο ασφάλειας στους online λογαριασμούς σας

(β) Κάνει πιο εύκολη την ανάκτηση του κωδικού πρόσβασής σας σε περίπτωση που τον ξεχάσετε

(γ) Σας επιτρέπει να χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για όλους τους λογαριασμούς σας

(δ) Δεν είναι απαραίτητος για την προστασία των προσωπικών σας δεδομένων

Ενότητα 2: Ασφαλείς Συναλλαγές και Αγορές στο Διαδίκτυο

ΜΑ2.1: Πραγματοποίηση ασφαλών ηλεκτρονικών συναλλαγών και αγορών

1.Ποιο από τα παρακάτω είναι ένα σημάδι ότι ένα ηλεκτρονικό κατάστημα είναι πιθανώς αξιόπιστο;

(α) Έχει επαγγελματική εμφάνιση και παρέχει σαφείς πληροφορίες επικοινωνίας

(β) Ζητάει τον αριθμό κοινωνικής ασφάλισής σας για να ολοκληρώσετε μια αγορά

(γ) Έχει πολλές αναδυόμενες διαφημίσεις και ανακατευθύνσεις σε άλλους ιστότοπους

(δ) Δεν έχει πολιτική επιστροφών ή εγγυήσεις προϊόντων

2.Ποια από τις παρακάτω μεθόδους πληρωμής θεωρείται γενικά η πιο ασφαλής για online αγορές;

(α) Πιστωτική κάρτα

(β) Χρεωστική κάρτα

(γ) Μετρητά κατά την παράδοση

(δ) Τραπεζική μεταφορά

3.Είναι ασφαλές να χρησιμοποιείτε δημόσια δίκτυα Wi-Fi για να πραγματοποιείτε online αγορές. (Σωστό ή Λάθος)(Απάντηση: Λάθος)

4.Ποιες από τις παρακάτω ενέργειες πρέπει να αποφεύγετε κατά την πραγματοποίηση online αγορών; (Πολλαπλής επιλογής -περισσότερες από μία σωστές απαντήσεις)

(α) Χρήση ισχυρού κωδικού πρόσβασης για τον λογαριασμό σας στο ηλεκτρονικό κατάστημα

(β) Αποθήκευση των στοιχείων της πιστωτικής σας κάρτας σε πολλούς ιστότοπους

(γ) Κλικ σε συνδέσμους σε email που υπόσχονται απίστευτες προσφορές

(δ) Έλεγχος τακτικά των κινήσεων της πιστωτικής σας κάρτας

5.Τι πρέπει να κάνετε εάν αντιμετωπίσετε κάποιο πρόβλημα κατά τη διάρκεια μιας online συναλλαγής, όπως μια μη εξουσιοδοτημένη χρέωση;

(α) Να μην κάνετε τίποτα

(β) Να επικοινωνήσετε αμέσως με την τράπεζα ή τον εκδότη της πιστωτικής σας κάρτας

(γ) Να αλλάξετε τον κωδικό πρόσβασης του email σας

(δ) Να ενημερώσετε αμέσως τον πιστωτικό σας φορέα

Ενότητα 2: Ασφαλείς Συναλλαγές και Αγορές στο Διαδίκτυο
ΜΑ2.2: Αποφυγή διαδικτυακών απατών

1.Οι ψεύτικες προσφορές συχνά υπόσχονται απίστευτα δώρα ή εκπτώσεις για να σας δελεάσουν να κάνετε κλικ σε έναν σύνδεσμο ή να δώσετε τα προσωπικά σας στοιχεία. (Σωστό ή Λάθος)(Απάντηση: Σωστό)

2.Ποια από τις παρακάτω ενέργειες είναι πιθανό να εμποδίσει την κλοπή ταυτότητας;

(α) Χρήση του ίδιου κωδικού πρόσβασης για όλους τους online λογαριασμούς σας.

(β) Κοινοποίηση των προσωπικών σας στοιχείων σε δημόσια δίκτυα Wi-Fi.

(γ) Απάντηση σε ένα email που σας ζητά να επιβεβαιώσετε τα στοιχεία σύνδεσής σας για έναν λογαριασμό που δεν αναγνωρίζετε.

(δ) Εγκατάσταση ενός προγράμματος προστασίας από ιούς στον υπολογιστή σας.

3.Ποια από τα παρακάτω είναι ένα παράδειγμα ασφαλούς πρακτικής κατά την πραγματοποίηση online αγορών;

(α)Αποθήκευση των στοιχείων της πιστωτικής σας κάρτας σε πολλούς ιστότοπους για ευκολία

(β)Χρήση της ίδιας πιστωτικής κάρτας για όλες τις online αγορές σας

(γ)Έλεγχος τακτικά των κινήσεων της πιστωτικής σας κάρτας για τυχόν ύποπτες χρεώσεις

(δ)Κλικ σε συνδέσμους σε email που υπόσχονται απίστευτες προσφορές

4. Είναι ασφαλές να δίνετε τα προσωπικά σας στοιχεία σε οποιονδήποτε σας τα ζητάει μέσω email ή τηλεφώνου, ακόμα και αν ισχυρίζεται ότι είναι από μια αξιόπιστη εταιρεία ή οργανισμό. (Σωστό ή Λάθος)(Απάντηση: Λάθος)

5.Ποιες από τις παρακάτω ενέργειες πρέπει να ακολουθήσετε για να διασφαλίσετε μια ασφαλή online συναλλαγή; (Πολλαπλής επιλογής - περισσότερες από μία σωστές απαντήσεις)

(α) Χρήση ισχυρού κωδικού πρόσβασης για τον λογαριασμό σας στο ηλεκτρονικό κατάστημα

(β) Έλεγχος των κριτικών άλλων πελατών για το ηλεκτρονικό κατάστημα

(γ) Κοινοποίηση των στοιχείων της πιστωτικής σας κάρτας σε φίλους και συγγενείς

(δ) Αποφυγή χρήσης δημόσιων δικτύων Wi-Fi για online αγορές

Ενότητα 3: Υπεύθυνη χρήση των κοινωνικών δικτύων

ΜΑ3.1: Διαχείριση και προστασία της διαδικτυακής παρουσίας

1.Ποιο από τα παρακάτω ΔΕΝ αποτελεί μέρος του ψηφιακού σας αποτυπώματος;

(α) Οι αναρτήσεις σας στα κοινωνικά δίκτυα

(β) Τα σχόλιά σας σε ιστοσελίδες και blogs

(γ) Οι σκέψεις σας που δεν έχετε μοιραστεί με κανέναν

(δ) Οι φωτογραφίες που σας έχουν τραβήξει άλλοι και έχουν αναρτήσει στο διαδίκτυο

2.Ποιος είναι ο καλύτερος τρόπος για να προστατεύσετε τα προσωπικά σας δεδομένα στα κοινωνικά δίκτυα;

(α) Να κοινοποιείτε όσο το δυνατόν περισσότερες πληροφορίες για τον εαυτό σας

(β) Να αποδέχεστε αιτήματα φιλίας από αγνώστους

(γ) Να ελέγχετε και να προσαρμόζετε τις ρυθμίσεις απορρήτου σας

(δ) Να μην χρησιμοποιείτε καθόλου τα κοινωνικά δίκτυα

3.Η διαδικτυακή μας φήμη μπορεί να επηρεάσει τις ευκαιρίες μας για εργασία ή σπουδές. (**Σωστό ή Λάθος**)(Απάντηση: Σωστό)

4.Ποιες από τις παρακάτω ενέργειες μπορούν να βλάψουν τη διαδικτυακή σας φήμη; (Πολλαπλής επιλογής - περισσότερες από μία σωστές απαντήσεις)

(α) Δημοσίευση προσβλητικών ή ακατάλληλων σχολίων

(β) Κοινοποίηση ψευδών πληροφοριών

(γ) Συμμετοχή σε διαδικτυακό εκφοβισμό (cyberbullying)

(δ) Δημιουργία ενός επαγγελματικού προφίλ που αναδεικνύει τις δεξιότητες και τα επιτεύγματά σας

5.Ποιο από τα παρακάτω είναι ένα παράδειγμα καλής διαχείρισης της διαδικτυακής σας παρουσίας;

(α) Δημιουργία ενός επαγγελματικού προφίλ σε ένα κοινωνικό δίκτυο που αναδεικνύει τις δεξιότητες και τα επιτεύγματά σας

(β) Συμμετοχή σε online συζητήσεις με σεβασμό και ευγένεια

(γ) Τακτικός έλεγχος και ενημέρωση των προσωπικών σας πληροφοριών στο

διαδίκτυο

(δ) Όλα τα παραπάνω

ΜΑ3.2: Αναγνώριση και Αντιμετώπιση της διαδικτυακής παρενόχλησης

1.Ποια από τις παρακάτω ενέργειες ΔΕΝ αποτελεί μορφή διαδικτυακής παρενόχλησης;

(α) Αποστολή απειλητικών μηνυμάτων

(β) Διάδοση ψευδών φημών

(γ) Κοινοποίηση προσωπικών πληροφοριών χωρίς την άδεια του ατόμου

(δ) Αποστολή ενός μηνύματος υποστήριξης σε ένα φίλο που έχει πέσει θύμα διαδικτυακής παρενόχλησης

2. Ποιες μπορεί να είναι οι συνέπειες της διαδικτυακής παρενόχλησης για τα θύματα; (Πολλαπλής επιλογής - περισσότερες από μία σωστές απαντήσεις)

(α) Χαμηλή αυτοεκτίμηση και κατάθλιψη

(β) Άγχος και κοινωνική απομόνωση

(γ) Προβλήματα στο σχολείο ή την εργασία

(δ) Αυξημένη αυτοπεποίθηση

3.Αν κάποιος σας παρενοχλεί στο διαδίκτυο, ποια είναι η καλύτερη πρώτη σας ενέργεια;

(α) Να απαντήσετε με τον ίδιο τρόπο και να ξεκινήσετε έναν διαδικτυακό καυγά

(β) Να αποκλείσετε τον χρήστη και να αναφέρετε την παρενόχληση στην πλατφόρμα κοινωνικής δικτύωσης ή στις αρμόδιες αρχές

(γ) Να διαγράψετε όλους τους λογαριασμούς σας στα κοινωνικά δίκτυα

(δ) Να μην πείτε τίποτα σε κανέναν και να ελπίζετε ότι θα σταματήσει

4.Αν είστε μάρτυρας διαδικτυακής παρενόχλησης, δεν πρέπει να παρέμβετε, καθώς αυτό μπορεί να σας κάνει στόχο. (Σωστό ή Λάθος)(Απάντηση: Λάθος)

5.Ποιες από τις παρακάτω ενέργειες είναι αποτελεσματικοί τρόποι για να αντιμετωπίσετε τη διαδικτυακή παρενόχληση; (Πολλαπλής επιλογής - περισσότερες από μία σωστές απαντήσεις)

(α) Να αναφέρετε την παρενόχληση στις αρμόδιες αρχές

(β) Να αποκλείσετε τον χρήστη που σας παρενοχλεί

(γ) Να αλλάξετε τους κωδικούς πρόσβασής σας

(δ) Να απαντήσετε με προσβλητικά σχόλια

Ενότητα 4: Ασφαλές Διαδίκτυο για Παιδιά και Οικογένειες

ΜΑ4.1: Αναγνώριση κινδύνων για παιδιά στο διαδίκτυο και εφαρμογή μέτρων προστασίας

1.Ποιοι από τους παρακάτω είναι κίνδυνοι που αντιμετωπίζουν τα παιδιά στο διαδίκτυο; (Πολλαπλής επιλογής - περισσότερες από μία σωστές απαντήσεις)

(α) Διαδικτυακή παρενόχληση (cyberbullying)

(β) Έκθεση σε ακατάλληλο περιεχόμενο

(γ) Διαδικτυακοί θηρευτές

(δ) Χρήση εκπαιδευτικών εφαρμογών

2.Ποιος είναι ο κύριος σκοπός των εργαλείων γονικού ελέγχου;

(α) Να εμποδίσουν εντελώς την πρόσβαση των παιδιών στο διαδίκτυο

(β) Να περιορίσουν την πρόσβαση των παιδιών σε ακατάλληλο περιεχόμενο και να παρακολουθούν τη διαδικτυακή τους δραστηριότητα

(γ) Να επιτρέψουν στα παιδιά να έχουν απεριόριστη πρόσβαση στο διαδίκτυο

(δ) Να αντικαταστήσουν την ανάγκη για επικοινωνία και επίβλεψη από τους γονείς

3.Τα παιδιά δεν πρέπει ποτέ να χρησιμοποιούν το διαδίκτυο χωρίς την επίβλεψη ενός ενήλικα. (Σωστό ή Λάθος)(Απάντηση: Λάθος)

4.Ποιες από τις παρακάτω ρυθμίσεις ασφαλείας είναι σημαντικό να ενεργοποιήσετε στις συσκευές που χρησιμοποιούν τα παιδιά; (Πολλαπλής επιλογής - περισσότερες από μία σωστές απαντήσεις)

(α) Απενεργοποίηση της τοποθεσίας

(β) Ενεργοποίηση του απορρήτου

(γ) Χρήση ισχυρών κωδικών πρόσβασης

(δ) Απενεργοποίηση του antivirus

5.Ποια είναι η καλύτερη προσέγγιση για να μιλήσετε στα παιδιά σας για τους κινδύνους του διαδικτύου;

(α) Να τα τρομάξετε με ιστορίες για διαδικτυακούς κινδύνους

(β) Να τους απαγορεύσετε να χρησιμοποιούν το διαδίκτυο

(γ) Να έχετε ανοιχτές και ειλικρινείς συζητήσεις μαζί τους, εξηγώντας τους κινδύνους και πώς να τους αποφεύγουν

(δ) Να τους δώσετε πλήρη ελευθερία στο διαδίκτυο χωρίς καμία επίβλεψη

ΜΑ4.2: Δημιουργία ασφαλούς και υποστηρικτικού διαδικτυακού περιβάλλοντος για την οικογένεια

1.Η δημιουργία ενός ασφαλούς διαδικτυακού περιβάλλοντος για την οικογένεια περιλαμβάνει μόνο την εγκατάσταση εργαλείων γονικού ελέγχου. (Σωστό ή Λάθος)(Απάντηση: Λάθος)

2.Ποιος είναι ο ρόλος της ανοιχτής επικοινωνίας στη δημιουργία ενός ασφαλούς διαδικτυακού περιβάλλοντος για την οικογένεια;

(α) Επιτρέπει στα παιδιά να μοιράζονται τις εμπειρίες τους και να εκφράζουν τυχόν ανησυχίες τους σχετικά με το διαδίκτυο

(β) Βοηθά τους γονείς να κατανοήσουν καλύτερα τις online δραστηριότητες των παιδιών τους

(γ) Ενισχύει την εμπιστοσύνη μεταξύ γονέων και παιδιών

(δ) Όλα τα παραπάνω

3.Γιατί είναι σημαντικό οι γονείς να εκπαιδεύονται σχετικά με την ασφαλή χρήση του διαδικτύου;

(α) Για να μπορούν να καθοδηγήσουν τα παιδιά τους και να τα προστατεύσουν από τους κινδύνους

(β) Για να είναι σε θέση να χρησιμοποιούν αποτελεσματικά τα εργαλεία γονικού ελέγχου

(γ) Για να είναι ενήμεροι για τις τελευταίες εξελίξεις στον τομέα της ψηφιακής ασφάλειας

(δ) Όλα τα παραπάνω

4.Πώς μπορούν οι γονείς να ενθαρρύνουν τα παιδιά τους να μιλούν για τυχόν προβλήματα που αντιμετωπίζουν στο διαδίκτυο; (Πολλαπλής επιλογής - περισσότερες από μία σωστές απαντήσεις)

(α) Δημιουργώντας ένα κλίμα εμπιστοσύνης και κατανόησης

(β) Ακούγοντας προσεκτικά τα παιδιά τους χωρίς να τα κρίνουν

(γ) Διαβεβαιώνοντας τα παιδιά τους ότι δεν θα τιμωρηθούν αν μιλήσουν για κάποιο πρόβλημα

(δ) Αγνοώντας τα παιδιά όταν προσπαθούν να μιλήσουν για το διαδίκτυο

5. Ποιος είναι ο ρόλος του σχολείου στην προώθηση της ασφαλούς χρήσης του διαδικτύου από τα παιδιά;

(α) Να παρέχει εκπαιδευτικά προγράμματα και δραστηριότητες για την ψηφιακή ασφάλεια

(β) Να συνεργάζεται με τους γονείς για την αντιμετώπιση τυχόν προβλημάτων που σχετίζονται με το διαδίκτυο

(γ) Να δημιουργεί ένα ασφαλές διαδικτυακό περιβάλλον στο σχολείο

(δ) Όλα τα παραπάνω

[End_of_Page]

5.2 Οδηγίες για τη δημιουργία πιστοποιητικού του MOOC

Act_ID#5.2 Οδηγίες για τη δημιουργία πιστοποιητικού του MOOC [Υπερκείμενο]

Όταν ολοκληρώσετε επιτυχώς το μάθημα τότε από την καρτέλα Progress μπορείτε να κατεβάσετε το πιστοποιητικό σας.

[End_of_Page]

[End_of_Topic]

[End_of_MOOC]