Προστασία από το Phishing στην εποχή της 4ης Βιομηχανικής Επανάστασης (CyberPhish)

Διευρυμένο πρόγραμμα σπουδών CyberPhish

Διάρκεια του έργου: 2022

Αριθμός έργου: 2020-1-LT01-KA203-078070

Funded by the Erasmus+ Programme of the European Union

Το έργο αυτό χρηματοδοτήθηκε με την υποστήριξη της Ευρωπαϊκής Επιτροπής. Η παρούσα δημοσίευση [ανακοίνωση] αντανακλά τις απόψεις μόνο του συγγραφέα και η Επιτροπή δεν μπορεί να θεωρηθεί υπεύθυνη για οποιαδήποτε χρήση των πληροφοριών που περιέχονται σε αυτήν.

Έλεγχος εγγράφων			
Αναθεώρηση #	**Ημερομηνία αναθεώρησης**	**Περιγραφή**	**Όνομα και επώνυμο**
1Σχέδιο Έκδοση 1.0	**02/05/2021**	**Αρχικό σχέδιο**	**MECB Ltd (MT)**
2 Σχέδιο έκδοσης 2.0	**07/05/2021**	**Επικαιροποιημένο σχέδιο**	**MECB Ltd (MT)**
3 Σχέδιο έκδοσης 3.0	**09/05/2021**	**Επικαιροποιημένο σχέδιο**	**MECB Ltd (MT)**
4 Σχέδιο έκδοσης 4.0	**10/05/2021**	**Επικαιροποιημένο σχέδιο μετά από ανατροφοδότηση από τους εταίρους**	**MECB Ltd (MT)**
5 Σχέδιο έκδοσης 5.0	**31/05/2021**	**Επικαιροποιημένο σχέδιο μετά από ανατροφοδότηση από εμπειρογνώμονες**	**MECB Ltd (MT)**
6 Τελική έκδοση 1.0	**08/06/2021**	**Τελική έκδοση για διανομή**	**MECB Ltd (MT)**

ΠΕΡΙΕΧΌΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Το διευρυμένο πρόγραμμα σπουδών Cyberphish στοχεύει στην παροχή συνοπτικών αλλά εκτεταμένων ενοτήτων στην κυβερνοασφάλεια με ιδιαίτερη έμφαση στο κυβερνο-ψάρεμα. Το πρόγραμμα σπουδών χωρίζεται σε τρεις κύριες ενότητες και συγκεκριμένα σε:

- Σεμινάριο εκπαίδευσης εκπαιδευτών - εξοπλίζει τους εκπαιδευτές με τη σωστή νοοτροπία και τις δεξιότητες για την παράδοση του προγράμματος σπουδών.
- Εκπαίδευση πρόσωπο με πρόσωπο / Διαδικτυακή εκπαίδευση - καθορισμός των τρόπων με τους οποίους θα παραδίδεται η εκπαίδευση στο πρόγραμμα σπουδών.
- Η δομή του προγράμματος σπουδών (ενότητα ηλεκτρονικής μάθησης) - περιγράφει λεπτομερώς τη δομή του προγράμματος σπουδών

Είναι σημαντικό να σημειωθεί ότι, παρόλο που η παράδοση του προγράμματος σπουδών αποσκοπεί σε μια προσέγγιση μικτής μάθησης, ο τρόπος με τον οποίο είναι δομημένο, επιτρέπει ευελιξία στην εφαρμογή του.

Το Πρόγραμμα Σπουδών ασχολείται με την εισαγωγή στην κυβερνοασφάλεια με ιδιαίτερη έμφαση στο cyberphishing. Απευθύνεται σε επιχειρήσεις και ιδιώτες και έχει σχεδιαστεί για να προετοιμάσει και τους δύο για τη Βιομηχανία 4.0 και τις πιθανές προκλήσεις ασφαλείας που αυτή συνεπάγεται.

Μέσω του προγράμματος σπουδών, οι εκπαιδευόμενοι θα αποκτήσουν τις δεξιότητες αναγνώρισης και αντιμετώπισης κυβερνοεπιθέσεων και τον τρόπο προστασίας των συσκευών και των δεδομένων από επιθέσεις ωμής βίας.

1. ΕΚΠΑΊΔΕΥΣΗ ΕΚΠΑΙΔΕΥΤΩΝ

Η ακόλουθη δομή για το μάθημα εκπαίδευσης του εκπαιδευτή έχει σχεδιαστεί με τέτοιο τρόπο ώστε να μπορεί να διεξαχθεί είτε πρόσωπο με πρόσωπο είτε διαδικτυακά. Η προτεινόμενη διάρκεια μπορεί να ποικίλλει ανάλογα με τον αριθμό των συμμετεχόντων και τις απαιτήσεις παράδοσης. Λόγω της φύσης αυτού του μαθήματος εκπαίδευσης εκπαιδευτών, προτείνεται να υπάρχουν ομάδες με όχι περισσότερους από δώδεκα εκπαιδευτές ανά μάθημα.

Η διάρθρωση του προγράμματος κατάρτισης παρατίθεται στον παρακάτω πίνακα. Ο πίνακας προσφέρει τα **συνιστώμενα θέματα** για τη συνάντηση εκπαίδευσης του εκπαιδευτή και τον συνιστώμενο χρόνο. Είναι στη διακριτική ευχέρεια του οργανισμού κατάρτισης και του εκπαιδευτή να χρησιμοποιούν, να επεκτείνουν, να μειώσουν ή να αυξήσουν τη διάρκεια και το περιεχόμενο του προγράμματος εκπαίδευσης του εκπαιδευτή, όπως κρίνεται σκόπιμο και ανάλογα με την ετοιμότητα τόσο του εκπαιδευτή όσο και των εκπαιδευομένων.

Είναι σκόπιμο να σημειωθεί ότι το μάθημα Εκπαίδευσης Εκπαιδευτών απευθύνεται σε Εκπαιδευτές που έχουν ήδη γνώσεις σχετικά με το θέμα της κυβερνοασφάλειας γενικά.

Οι διοργανωτές της εκδήλωσης θα μπορούσαν να στείλουν ένα ερωτηματολόγιο στους εκπαιδευτές πριν από την εκπαιδευτική συνεδρία για να συλλέξουν το επίπεδο των εκπαιδευτών και να κατανοήσουν τι περιμένουν οι εκπαιδευτές από αυτή την εκπαιδευτική εκδήλωση. Μετά την ανατροφοδότηση από το ερωτηματολόγιο, οι διοργανωτές θα μπορούσαν να προσαρμόσουν ανάλογα την ατζέντα της εκπαιδευτικής εκδήλωσης.

Δομή	Εκπαίδευση των εκπαιδευτών σε ένα σύντομο πρόγραμμα 4 ημερών που αποσκοπεί στον εξοπλισμό των εκπαιδευτών με τις κατάλληλες δεξιότητες και ικανότητες.
Στόχος	Ενδυνάμωση των εκπαιδευτών με βασικές δεξιότητες διευκόλυνσης και σχεδιασμού κατάρτισης για την παροχή αποτελεσματικών εκπαιδευτικών συνεδριών στην κυβερνοασφάλεια
Πρόγραμμα	

Ημέρα 1	Μια μέρα στη ζωή ενός φοιτητή	
Στοιχείο Nº	*Στοιχείο*	*Προτεινόμενος χρόνος*
D1-01	Εισαγωγή και συνάντηση γνωριμίας • Ice Breaker ή Δραστηριότητα Οικοδόμησης Ομάδας για να γνωριστείτε μεταξύ σας - *Κοινωνικό δίκτυο χαμηλής τεχνολογίας (παγοθραύστης)* - *Πρόκληση Marshmallow (ομαδικό χτίσιμο)*	0,5 ώρα
D1-02	Κατανόηση και αντιμετώπιση των διαφορετικών μαθησιακών στυλ • Μια σύντομη εισαγωγή στα διάφορα μοντέλα μαθησιακού στυλ - *Εισαγωγή των διαφορετικών μαθησιακών στυλ (π.χ. 7 μαθησιακά στυλ, κύκλος μάθησης του Kolb) ως βάση για τις επόμενες ενότητες.*	0,5 ώρα
D1-03	Ο εκπαιδευτής ως μαθητής - Βιώνοντας τις μεθοδολογίες μάθησης (Μέρος 1) *Στόχος αυτής της συνεδρίας είναι να εμπλακούν οι εκπαιδευτές στην κατανόηση και την εμπειρία διαφορετικών παιδαγωγικών πλαισίων και μεθόδων διδασκαλίας ως φοιτητές. Θα δημιουργηθεί μια δια ζώσης ή εικονική (διαδικτυακή) τάξη με τους εκπαιδευτές να ενεργούν ως μαθητές.* • Εισαγωγή σε διαφορετικά παιδαγωγικά περιβάλλοντα και μεθόδους διδασκαλίας - *Στο πρώτο μέρος της συνεδρίας, ο κύριος εκπαιδευτής θα παρουσιάσει έναν αριθμό διαφορετικών παιδαγωγικών πλαισίων και μεθόδων διδασκαλίας. (π.χ. εργαστήρια, πρακτικές συνεδρίες, συζητήσεις, συζητήσεις, συζητήσεις, μελέτες περιπτώσεων κ.λπ.)* • Εμπειρία διαφορετικών μεθόδων διδασκαλίας - *Στο δεύτερο μέρος της συνεδρίας, οι εκπαιδευτές/εκπαιδευόμενοι θα εκτεθούν σε αυτές τις διαφορετικές μεθοδολογίες διδασκαλίας.*	3 ώρες
D1-04	Διάλειμμα δικτύωσης	0,5 ώρα
D1-05	Ο Εκπαιδευτής ως μαθητής - Βιώνοντας τις μεθοδολογίες μάθησης (Μέρος 2) • Συζήτηση, ανατροφοδότηση και ανταλλαγή βέλτιστων πρακτικών - *Ανταλλαγή συναισθημάτων, στάσεων, ανατροφοδότηση σχετικά με την εμπειρία του Μέρους 1* - *Ανταλλαγή βέλτιστων πρακτικών για τη βελτίωση της μαθησιακής εμπειρίας των μαθητών*	1 ώρα
D1-06	Ημέρα 1 - Σύνοψη και συμπέρασμα	0,5 ώρες
Ημέρα 2	Ανανέωση βασικών κοινωνικών δεξιοτήτων	
Στοιχείο Nº	*Στοιχείο*	*Προτεινόμενος χρόνος*
D2-01	Εισαγωγή στην ημέρα 2 - Η σημασία των ήπιων δεξιοτήτων • Μια σύντομη εισαγωγή στη σημασία των κοινωνικών δεξιοτήτων στην παράδοση ενός μαθήματος - *Σύντομη εισαγωγή με έμφαση κυρίως στην παρουσίαση, τη διευκόλυνση, τη διαχείριση της τάξης και την εποικοδομητική ανατροφοδότηση*	0,5 ώρα
D2-02	Απαραίτητες κοινωνικές δεξιότητες για την πραγματοποίηση εκπαιδευτικών συνεδριών (Μέρος 1) • Δεξιότητες παρουσίασης	2 ώρες

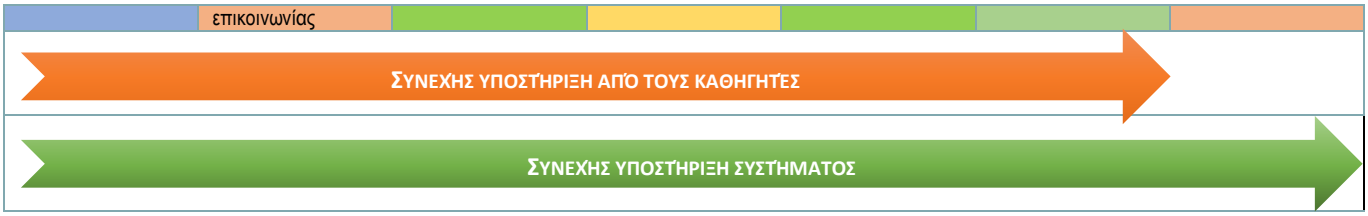
	- *Διάρθρωση παρουσιάσεων (π.χ. αριθμός και μορφή διαφανειών, χρήση διαδικτυακών εργαλείων)* - *Πτυχές της παρουσίασης (π.χ. γλώσσα του σώματος, τόνος φωνής, γλώσσα του σώματος)* - *Παρουσίαση σύντομων παρουσιάσεων (πρόσωπο με πρόσωπο ή σε απευθείας σύνδεση) με ανατροφοδότηση και αξιολόγηση από ομότιμους* • Δεξιότητες διευκόλυνσης - *Διευκόλυνση μιας ομαδικής συζήτησης (π.χ. ερωτήσεις διερεύνησης, ανακατεύθυνσης και αναδιατύπωσης)* - *Διευκόλυνση της συνεργασίας (π.χ. Brainstorming, Mind mapping, Six Thinking Hats),* • Χρήση ψηφιακών εργαλείων για την ενίσχυση των ήπιων δεξιοτήτων - *Χρήση ψηφιακών εργαλείων για τη διευκόλυνση παρουσιάσεων και συζητήσεων* - *Εισαγωγή στα ψηφιακά/διαδικτυακά εργαλεία που περιλαμβάνουν, μεταξύ άλλων, τα MS Teams, Zoom, Skype, Google Meet, Mentimeter, Kazoom κ.λπ.*	
D2-03	Διάλειμμα δικτύωσης	0,5 ώρα
D2-04	Απαραίτητες κοινωνικές δεξιότητες για την πραγματοποίηση εκπαιδευτικών συνεδριών (Μέρος 2) • Διαχείριση τάξης - *Ανταλλαγή βέλτιστων πρακτικών σχετικά με τον τρόπο ελέγχου, ενθάρρυνσης και συμμετοχής των εκπαιδευομένων τόσο δια ζώσης όσο και διαδικτυακά.* • Δίνοντας αποτελεσματική και εποικοδομητική ανατροφοδότηση - *Σύντομη ομαδική συζήτηση (πρόσωπο με πρόσωπο ή διαδικτυακό εργαστήριο) για την ανάλυση αποτελεσματικών και εποικοδομητικών τεχνικών ανατροφοδότησης*	2 ώρες
D2-05	Ημέρα 2 - Σύνοψη και συμπέρασμα	0,5 ώρες
Ημέρα 3	Εμβαθύνοντας στο πρόγραμμα σπουδών	
Στοιχείο Nº	*Στοιχείο*	*Προτεινόμενος χρόνος*
D3-01	Εισαγωγή στη δομή του προγράμματος σπουδών και στις μορφές διδασκαλίας *Μια σύντομη πρόσωπο με πρόσωπο ή διαδικτυακή συνεδρία που παρουσιάζει τη δομή του Προγράμματος Σπουδών, συμπεριλαμβανομένης της σημασίας των μαθησιακών αποτελεσμάτων μαζί με τους τρόπους διδασκαλίας.*	1 ώρα
D3-02	Λεπτομερής ανάλυση των θεμάτων του προγράμματος σπουδών (Μέρος 1) *Επεξηγηματική συνεδρία για τις δύο πρώτες εισαγωγικές ενότητες του προγράμματος σπουδών*	1 ώρα
D3-03	Διάλειμμα δικτύωσης	0,5 ώρα
D3-04	Λεπτομερής ανάλυση των θεμάτων του προγράμματος σπουδών (Μέρος 2) *Επεξηγηματική συνεδρία για τις δύο τελευταίες ενότητες του προγράμματος σπουδών*	3 ώρες
D3-05	Ημέρα 3 - Σύνοψη και συμπέρασμα	0,5 ώρες
Ημέρα 4	Τελικό εργαστήριο - Αξιολόγηση των βασικών κοινωνικών δεξιοτήτων με τη χρήση του προγράμματος σπουδών	
Στοιχείο Nº	*Στοιχείο*	*Προτεινόμενος χρόνος*
D4-01	Εισαγωγή στο εργαστήριο	0,5 ώρα

	Η τελευταία ημέρα θα αποτελείται από ένα εργαστήριο όπου όλοι οι συμμετέχοντες αναμένεται να αναστοχαστούν την εμπειρία που αποκόμισαν την 1η ημέρα, να εξασκήσουν τις δεξιότητες που απέκτησαν την 2η ημέρα και να χρησιμοποιήσουν το πρόγραμμα σπουδών που εξηγήθηκε την 3η ημέρα. *Η αξιολόγηση γίνεται με τη μορφή ανατροφοδότησης από τους συμμετέχοντες εκπαιδευτές.* *Η διάρκεια του εργαστηρίου εξαρτάται από τον αριθμό των συμμετεχόντων.*	
D4-02	Αξιολόγηση των δεξιοτήτων παρουσίασης *Οι εκπαιδευτές καλούνται να προετοιμάσουν και να παρουσιάσουν μια 10λεπτη παρουσίαση επιλέγοντας οποιοδήποτε θέμα από το προτεινόμενο πρόγραμμα σπουδών. Μετά από κάθε παρουσίαση ακολουθεί αξιολόγηση από τους συναδέλφους και ανατροφοδότηση σχετικά με την παρουσίαση, συμπεριλαμβανομένων των καινοτόμων τεχνικών που χρησιμοποιήθηκαν.* Άλλες μέθοδοι αξιολόγησης μπορούν να χρησιμοποιηθούν κατά την κρίση του εκπαιδευτή.	0,25 ώρες ανά συμμετέχοντα *(μέγιστο 3 ώρες)*
D4-03	Διάλειμμα δικτύωσης	0,5 ώρα
D4-04	Αξιολόγηση των δεξιοτήτων διευκόλυνσης *Οι εκπαιδευτές καλούνται να διευκολύνουν μια 10λεπτη συνεδρία επιλέγοντας οποιοδήποτε θέμα από το προτεινόμενο πρόγραμμα σπουδών. Μετά από κάθε συνεδρία θα ακολουθεί αξιολόγηση και ανατροφοδότηση από τους συναδέλφους τόσο για τις δεξιότητες διευκόλυνσης όσο και για τη διαχείριση της τάξης.* Άλλες μέθοδοι αξιολόγησης μπορούν να χρησιμοποιηθούν κατά την κρίση του εκπαιδευτή.	0,25 ώρες ανά συμμετέχοντα *(μέγιστο 3 ώρες)*
D4-05	Ημέρα 4 - Σύνοψη και συμπέρασμα του σεμιναρίου εκπαίδευσης εκπαιδευτών	0,5 ώρες

2. ΕΚΠΑΊΔΕΥΣΗ ΠΡΌΣΩΠΟ ΜΕ ΠΡΌΣΩΠΟ / ONLINE

Για την ενσωμάτωση των μαθητών στη μαθησιακή εμπειρία υιοθετείται μια ***προσέγγιση τεσσάρων σταδίων.*** Με μια ματιά:

ONLINE ΣΥΝΕΔΡΊΑ ΠΡΟΣΑΝΑΤΟΛΙΣΜΟΎ	***ΕΚΔΉΛΩΣΗ ΚΑΛΩΣΟΡΊΣΜΑΤΟΣ ΦΟΙΤΗΤΩΝ***	***ΠΑΡΆΔΟΣΗ ΕΝΟΤΗΤΑΣ***	***ΕΡΓΑΣΤΉΡΙΟ ΕΝΣΩΜΆΤΩΣΗΣ***	***ΠΑΡΆΔΟΣΗ ΕΝΟΤΗΤΑΣ***	***ΟΛΟΚΛΉΡΩΣΗ ΜΑΘΗΜΑΤΩΝ***	***ΤΕΛΙΚΉ ΣΥΝΕΔΡΊΑ ΔΙΚΤΎΩΣΗΣ***
Πληροφορίες για το ίδρυμα κατάρτισης - *Στόχοι* - *Πολιτικές* - *Διαδικασίες* -	Εισαγωγή - Βιογραφικό του εκπαιδευτή Σύστημα διαχείρισης πληροφοριών (MIS) του εκπαιδευτικού ιδρύματος - *Πληροφορίες για το σύστημα* - *ID / Κωδικός πρόσβασης* - *Πόροι* - *Πολιτική 'Χρήσης'* - *Συχνές ερωτήσεις / Αντιμετώπιση προβλημάτων* Επίσημο πρόγραμμα μαθημάτων Μεθοδολογίες αξιολόγησης Γραμμές	Παράδοση της ενότητας ανάλογα με τον αριθμό των ωρών που ανατίθενται ανά ημέρα. Πρώτο μέρος (15 ώρες)	Διαδικτυακό έντυπο ανατροφοδότησης σχετικά με τις τρέχουσες καλές πρακτικές και άλλες πρακτικές που χρήζουν αντιμετώπισης Συζήτηση με τους μαθητές	Παράδοση της ενότητας ανάλογα με τον αριθμό των ωρών που ανατίθενται ανά ημέρα. Δεύτερο μέρος (15 ώρες)	Συγκέντρωση δεδομένων - *Από τον εκπαιδευτή: αξιολογήσεις* - *Από τους μαθητές: έντυπο αξιολόγησης ψηφιακής κατάρτισης*	Σύνοδος εστίασης - *Συζήτηση σχετικά με τα ευρήματα* - *Συμπεράσματα* - *Πορεία προς τα εμπρός*



i. Εικονική σύνοδος προσανατολισμού με αυτοκαθοδήγηση

Το πρώτο βήμα στην εμπειρία του προσανατολισμού είναι να παρακολουθήσετε μια **διαδικτυακή συνεδρία προσανατολισμού**. Αυτή η συνεδρία είναι μια αυτορυθμιζόμενη εμπειρία, που επιτρέπει στον εκπαιδευόμενο την ευελιξία να μάθει για το ίδρυμα που παρέχει την εκπαίδευση (το ίδρυμα κατάρτισης).

Οι υποψήφιοι εκπαιδευόμενοι θα έχουν την ευκαιρία να εξοικειωθούν με πληροφορίες που αφορούν (αλλά όχι μόνο) το ίδρυμα κατάρτισης στο σύνολό του και το συγκεκριμένο τμήμα. Επισημαίνονται οι στόχοι, οι πολιτικές και οι διαδικασίες του τμήματος, καθώς και οι προσδοκίες του εκπαιδευτικού ιδρύματος. Για την εξυπηρέτηση των σπουδαστών με προβλήματα όρασης και ακοής, όλο το υλικό προσανατολισμού και οι παρουσιάσεις πρέπει να είναι υπότιτλοι και προσβάσιμες για αναγνώστες οθόνης.

ii. Εκδήλωση καλωσορίσματος

Η νέα ομάδα φοιτητών καλωσορίζεται σε μια **εκδήλωση υποδοχής φοιτητών**. Η εκδήλωση αυτή μπορεί να γίνει είτε δια ζώσης είτε μέσω διαδικτύου. Αυτή η συνάντηση παρέχει μια εξαιρετική ευκαιρία στους φοιτητές να γνωρίσουν τον εκπαιδευτή και τους συμφοιτητές τους εντός της κοόρτης, να κάνουν ερωτήσεις και να εξοικειωθούν με την υλικοτεχνική υποδομή του μαθήματος.

Ειδικότερα, αφού λάβει την εξουσιοδότηση για τη χρήση του πληροφοριακού συστήματος του εκπαιδευτικού ιδρύματος, ο εκπαιδευτής θα παρέχει μια συνοπτική εισαγωγή στο σύστημα όπως έχει εγκατασταθεί. Στους εκπαιδευόμενους θα δοθούν τα αναγνωριστικά χρήστη και θα τους καθοδηγήσει στον καθορισμό των κωδικών πρόσβασης. Επιπλέον, θα δοθεί καθοδήγηση σχετικά με την πρόσβαση στους πόρους που οι εκπαιδευόμενοι έχουν εξουσιοδοτηθεί να χρησιμοποιούν. Στο πλαίσιο αυτό, διαβάζεται και υπογράφεται η "Πολιτική χρήσης". Αναγνωρίζοντας ότι αυτό μπορεί να φανεί ως πολλές τεχνικές πληροφορίες, θα διατεθεί ένα έγγραφο "Συχνές ερωτήσεις και αντιμετώπιση προβλημάτων" για μελλοντική αναφορά.

Ο εκπαιδευτής μπορεί να ολοκληρώσει τη συνεδρία σχεδιάζοντας μια ακριβή εικόνα της επίσημης διδακτέας ύλης, των μεθοδολογιών αξιολόγησης και των διαθέσιμων γραμμών επικοινωνίας.

iii. Ενδυνάμωση των μαθητών μέσω συνεχούς υποστήριξης

Εκτός από την ανάπτυξη της κατάκτησης από τους εκπαιδευόμενους γνώσεων, δεξιοτήτων και στάσεων σε σχέση με το πρόγραμμα σπουδών για την ασφάλεια στον κυβερνοχώρο, το ίδρυμα κατάρτισης αναγνωρίζει τη σημασία του εντοπισμού και της ανταπόκρισης στις μεταβαλλόμενες ανάγκες των εκπαιδευόμενων. Ως πρώτη γραμμή ανταπόκρισης, οι εκπαιδευτές θα είναι διαθέσιμοι σε τακτική βάση για θετική αλληλεπίδραση με τους σπουδαστές.

Σε πιο επίσημο επίπεδο, θα διοργανωθεί ένα **εργαστήριο ένταξης** μετά από έναν προκαθορισμένο αριθμό ολοκληρωμένων συνεδριών διδασκαλίας. Η ανατροφοδότηση των μαθητών θα συγκεντρωθεί και θα συζητηθεί για να διαπιστωθεί κατά πόσο η εξέλιξη των μαθημάτων ανταποκρίνεται στις προσδοκίες των μαθητών και στα πρότυπα του εκπαιδευτικού ιδρύματος.

Διάφορα εργαλεία αξιολόγησης της κατάρτισης μπορούν να χρησιμοποιηθούν πριν από το εργαστήριο ένταξης για να βοηθήσουν στη συλλογή δεδομένων. Οι δείκτες επιτυχίας εν προκειμένω περιλαμβάνουν, μεταξύ άλλων, την απόκτηση νέων δεξιοτήτων και γνώσεων από τους σπουδαστές, τη θετική στάση απέναντι στη μαθησιακή εμπειρία και τον αντίκτυπο στην αποτελεσματικότητα.

Με τη σειρά τους, οι πληροφορίες αυτές χρησιμοποιούνται για τη διασφάλιση της βελτίωσης της ποιότητας του προγράμματος μαθημάτων.

iv. Συμπεράσματα μαθήματος

Η **ολοκλήρωση των μαθημάτων** είναι από μόνη της μια στιγμή αναγνώρισης σημαντικών επιτευγμάτων.

Θα διεξαχθεί μια **καταληκτική συνεδρία δικτύωσης, της οποίας ο** σκοπός είναι διττός. Το σημαντικότερο είναι να δοθεί στους εκπαιδευόμενους η ευκαιρία να μοιραστούν μερικές ώρες κοινής χαράς. Ωστόσο, ο φορέας κατάρτισης θα εκμεταλλευτεί ταυτόχρονα την ευκαιρία να αξιολογήσει την επιτυχία του προγράμματος κατάρτισης. *Στο* πλαίσιο αυτό θα χρησιμοποιηθεί [1]*το μοντέλο αξιολόγησης της κατάρτισης τεσσάρων επιπέδων του Kirkpatrick.*

Πριν από τη συνάντηση δικτύωσης, ο φορέας κατάρτισης θα συλλέξει πληροφορίες:

- *από τον εκπαιδευτή σχετικά με τις αξιολογήσεις.*
  Αυτό θα χρησιμεύσει ως μέτρο για το πόσο έχουν αλλάξει οι γνώσεις και οι δεξιότητες των εκπαιδευομένων από την έναρξη του προγράμματος σπουδών.
- *από τους μαθητές.*
  Ένα ψηφιακό έντυπο αξιολόγησης της κατάρτισης, με το οποίο ζητείται ανατροφοδότηση σχετικά με τη συνολική ικανοποίηση από τη μαθησιακή εμπειρία και τη δυνατότητα (ή μη) εφαρμογής των σπουδών τους στον χώρο εργασίας.

Με αυτά τα δεδομένα στη διάθεσή σας, κατά τη διάρκεια της εκδήλωσης δικτύωσης θα διεξαχθεί μια **συνεδρία εστίασης**, όπου το ίδρυμα κατάρτισης, μέσω μιας δομημένης συζήτησης σε πάνελ, μπορεί να μετρήσει ποιοτικά τα αποτελέσματα, όπως η παραγωγικότητα, η ποιότητα και οι αξιολογήσεις αποδοτικότητας.

3. Η ΔΟΜΗ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ ΣΠΟΥΔΩΝ (ΕΝΟΤΗΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΜΑΘΗΣΗΣ)

3.1 Εισαγωγή

Το Πρόγραμμα Σπουδών απευθύνεται τόσο σε επιχειρήσεις όσο και σε ιδιώτες που βιώνουν τις αναπόφευκτες θετικές και αρνητικές επιπτώσεις που επιφέρει η Βιομηχανία 4.0 και που θέλουν να μάθουν περισσότερα και να είναι καλύτερα εξοπλισμένοι για την αντιμετώπιση των προκλήσεων ασφαλείας που επιφέρει αυτή η τέταρτη βιομηχανική επανάσταση.

Το πρόγραμμα σπουδών είναι δομημένο σε τέσσερα διακριτά μέρη, ξεκινώντας με μια εισαγωγή στον τομέα της κυβερνοασφάλειας και τις σχετικές προκλήσεις που φέρνει η έλευση της Βιομηχανίας 4.0. Εμβαθύνει στην Κυβερνοασφάλεια και τις νομικές πτυχές της σε ευρωπαϊκό επίπεδο, καθώς και στον τρόπο με τον οποίο προωθείται η Κυβερνοασφάλεια στην Ευρωπαϊκή Ένωση.

Λαμβάνοντας υπόψη τη σημασία και τις επιπτώσεις της κοινωνικής μηχανικής και τη σχέση της με τις επιθέσεις στον κυβερνοχώρο, το πρόγραμμα σπουδών αναλύει την αναγνώριση των επιθέσεων στον κυβερνοχώρο και τον τρόπο χειρισμού τους για την αποφυγή καταστροφικών και μη αναστρέψιμων επιπτώσεων.

Εκτός από τη συνοπτική περιγραφή των διαφόρων ενοτήτων, η δομή του προγράμματος σπουδών περιλαμβάνει τα μαθησιακά αποτελέσματα ανά ενότητα και τις προτεινόμενες ώρες και τρόπους μάθησης. Είναι σκόπιμο να σημειωθεί ότι παρόλο που το πρόγραμμα σπουδών περιλαμβάνει αριθμό ωρών ανά ενότητα, οι ώρες αυτές πρέπει

[1] Kirkpatrick, D. L. (1994). Αξιολόγηση εκπαιδευτικών προγραμμάτων: τα τέσσερα επίπεδα. Σαν Φρανσίσκο: Berrett-Koehler.

να θεωρηθούν ως ώρες επαφής. Το πλήρες πρόγραμμα σπουδών ανέρχεται σε 30 ώρες που αντιστοιχούν σε 1 ECTS. Προτείνεται ο ίδιος αριθμός ωρών ανά ενότητα να θεωρηθεί για αυτοδιδασκαλία και αξιολόγηση.

Ενότητα προγράμματος σπουδών		***Στόχος της ενότητας***
1.0	Εισαγωγή στην κυβερνοασφάλεια	Αυτή η ενότητα έχει ως στόχο να εισαγάγει το μάθημα της κυβερνοασφάλειας και τα θέματά του τόσο στους εκπαιδευτές όσο και στους φοιτητές των ιδρυμάτων τριτοβάθμιας εκπαίδευσης. Ξεκινά με μια σύντομη ιστορική αναδρομή στην ανάπτυξη του κυβερνοεγκλήματος και τους λόγους της ταχείας ανάπτυξής του, καθώς και τα ιστορικά στάδια και την τρέχουσα κατάσταση. Περιγράφει επίσης τις προκλήσεις κυβερνοεπιθέσεων που αντιμετωπίζουν οι ιδιώτες και οι επιχειρήσεις με την έλευση της Βιομηχανίας 4.0, συμπεριλαμβανομένων, μεταξύ άλλων, της μείωσης των παγκόσμιων συνόρων, της ευρείας χρήσης των κινητών τεχνολογιών, του υπολογιστικού νέφους, του Διαδικτύου των πραγμάτων (IoT) και των μεγάλων δεδομένων. Άλλες προκλήσεις περιλαμβάνουν κινδύνους από τρίτους και αυξανόμενες απειλές, συμπεριλαμβανομένων των απειλών από εθνικά κράτη. Οι εκπαιδευτές θα είναι σε θέση να βρουν το απαραίτητο υλικό για να εισαγάγουν τους εκπαιδευόμενους στην έννοια της Κυβερνοασφάλειας μαζί με τις συνήθεις προκλήσεις που αντιμετωπίζουν οι επιχειρήσεις, με πραγματικά σενάρια περιπτώσεων όπου είναι δυνατόν. Η ενότητα εξετάζει επίσης τους πολυάριθμους ορισμούς και την ορολογία που χρησιμοποιούνται και συναντώνται στον τομέα της κυβερνοασφάλειας.
2.0	Επισκόπηση της ασφάλειας στον κυβερνοχώρο στην ΕΕ	Η ενότητα αυτή εισάγει τον εκπαιδευόμενο στις υφιστάμενες πολιτικές και πρωτοβουλίες της ΕΕ που αποσκοπούν στην προώθηση της έννοιας της κυβερνοασφάλειας. Συζητά επίσης τις νομικές πτυχές της Κυβερνοασφάλειας τόσο εντός της ΕΕ όσο και παγκοσμίως, εκθέτοντας τους εκπαιδευόμενους σε πολυάριθμα σενάρια πραγματικής ζωής και μελέτες περιπτώσεων στον τομέα. Η ενότητα περιλαμβάνει μια επισκόπηση των τάσεων στο τοπίο της κυβερνοασφάλειας, συμπεριλαμβανομένων, ενδεικτικά, στατιστικών στοιχείων, τάσεων, σχετικών απειλών, νομικών κινδύνων, κινδύνων φήμης και οικονομικών κινδύνων, καθώς και ανάλυση μελετών περιπτώσεων.
3.0	Επιθέσεις στον κυβερνοχώρο - Social Engineering και Phishing	Αυτή η ενότητα εισάγει τον εκπαιδευόμενο στις επιθέσεις στον κυβερνοχώρο με ιδιαίτερη έμφαση στο Phishing. Εμβαθύνει επίσης λεπτομερώς στην έννοια της κοινωνικής μηχανικής και της αντίστροφης κοινωνικής μηχανικής μαζί με την ισχυρή σύνδεση της κοινωνικής μηχανικής με τις επιθέσεις στον κυβερνοχώρο. Στην ενότητα παρουσιάζονται επίσης διάφοροι τύποι επιθέσεων και τεχνικών phishing μαζί με ορισμένα παραδείγματα πραγματικών περιπτώσεων από τις χώρες εταίρους του έργου.

4.0	Κατανόηση και χειρισμός κυβερνοεπιθέσεων	Αυτή η ενότητα εισάγει τον εκπαιδευόμενο στην έννοια της ηλεκτρονικής ασφάλειας και στη σημασία της υιοθέτησης μιας προληπτικής προσέγγισης των απειλών στον κυβερνοχώρο μέσω της έννοιας της κυβερνοϋγιεινής. Η ενότητα παρέχει επίσης μια λεπτομερή προσέγγιση σχετικά με τον τρόπο αναγνώρισης και αντιμετώπισης επιθέσεων στον κυβερνοχώρο. Η ενότητα εισάγει την ανάπτυξη και την εφαρμογή σχεδίων αντιμετώπισης περιστατικών με σκοπό την ελαχιστοποίηση των επιπτώσεων των επιθέσεων στον κυβερνοχώρο.

3.2 Δομή της ενότητας E-Learning λεπτομερώς

3.2.1 Εισαγωγή στην κυβερνοασφάλεια

Τίτλος Ενότητας	1.0 Εισαγωγή στην κυβερνοασφάλεια
Συνολική διάρκεια *(Ώρες / Διαφάνειες)*	3 ώρες 46 - 60 διαφάνειες
Μέθοδοι παράδοσης	Πρόσωπο με πρόσωπο Online Μικτή παράδοση
Αξιολόγηση	Πρόσωπο με πρόσωπο / Διαδικτυακό κουίζ
Μαθησιακά αποτελέσματα	• να έχουν γενικό υπόβαθρο στην κυβερνοασφάλεια γενικά • Κατανόηση των προκλήσεων που επιφέρει η κυβερνοασφάλεια • Κατανοήστε πώς οι κυβερνοεπιθέσεις έχουν αλλάξει με την πάροδο του χρόνου, οδηγώντας σε αυξημένα μέτρα και, ως εκ τούτου, σε μέτρα αντιμετώπισης των κυβερνοεπιθέσεων. • Κατανοήστε γιατί είναι σημαντικό να παρακολουθείτε το τοπίο της Κυβερνοασφάλειας και γιατί είναι απαραίτητο να ενημερώνετε συνεχώς τις γνώσεις σας για την Κυβερνοασφάλεια. • Κατανόηση των διαφόρων ορισμών που σχετίζονται με την κυβερνοασφάλεια
Προαπαιτούμενα	Δεν απαιτούνται αρχικές γνώσεις
Περιγραφή ενότητας	Αυτή η ενότητα έχει ως στόχο να εισαγάγει το μάθημα της κυβερνοασφάλειας και τα θέματά του τόσο στους εκπαιδευτές όσο και στους φοιτητές των ιδρυμάτων τριτοβάθμιας εκπαίδευσης. Ξεκινά με μια σύντομη ιστορική αναδρομή στην ανάπτυξη του κυβερνοεγκλήματος και τους λόγους της ταχείας ανάπτυξής του, καθώς και τα ιστορικά στάδια και την τρέχουσα κατάσταση. Περιγράφει επίσης τις προκλήσεις κυβερνοεπιθέσεων που αντιμετωπίζουν οι

	ιδιώτες και οι επιχειρήσεις με την έλευση της Βιομηχανίας 4.0, συμπεριλαμβανομένων, μεταξύ άλλων, της μείωσης των παγκόσμιων συνόρων, της ευρείας χρήσης των κινητών τεχνολογιών, του υπολογιστικού νέφους, του Διαδικτύου των πραγμάτων (IoT) και των μεγάλων δεδομένων. Άλλες προκλήσεις περιλαμβάνουν κινδύνους από τρίτους και αυξανόμενες απειλές, συμπεριλαμβανομένων των απειλών από εθνικά κράτη. Οι εκπαιδευτές θα είναι σε θέση να βρουν το απαραίτητο υλικό για να εισαγάγουν τους εκπαιδευόμενους στην έννοια της Κυβερνοασφάλειας μαζί με τις συνήθεις προκλήσεις που αντιμετωπίζουν οι επιχειρήσεις, με πραγματικά σενάρια περιπτώσεων όπου είναι δυνατόν. Η ενότητα εξετάζει επίσης τους πολυάριθμους ορισμούς και την ορολογία που χρησιμοποιούνται και συναντώνται στον τομέα της κυβερνοασφάλειας.
ΥΠΟΘΈΜΑΤΑ ΕΝΌΤΗΤΑΣ	
1.1 Ιστορικό - Προκλήσεις της 4ης βιομηχανικής επανάστασης	• Εισαγωγή στην κυβερνοασφάλεια • Σύντομη ιστορία της ανάπτυξης του ηλεκτρονικού εγκλήματος και λόγοι για την ταχεία ανάπτυξή του, καθώς και ιστορικά στάδια και σημερινή κατάσταση • Ιστορικό του προβλήματος που περιγράφει τις προκλήσεις που αντιμετωπίζουν οι επιχειρήσεις έναντι των επιθέσεων στον κυβερνοχώρο • Προκλήσεις για τις επιχειρήσεις: - Χωρίς όρια, - Τεχνολογίες: Ευρεία χρήση τεχνολογιών (τεχνολογίες κινητής τηλεφωνίας), - Υπολογιστικό νέφος, - Προκλήσεις μεγάλων δεδομένων, - Κίνδυνοι από τρίτους, - Διαδίκτυο των πραγμάτων (IoT), • Η πρόκληση των αυξανόμενων απειλών, • Απειλές εθνικού κράτους
	Προτεινόμενες ώρες: 1.5 | *Ελάχιστες διαφάνειες*: 23 | *Μέγιστες Διαφάνειες*: 30
1.2 Ιστορία της ασφάλειας στον κυβερνοχώρο	• Σύντομο ιστορικό του τρόπου με τον οποίο οι προσεγγίσεις για τις κυβερνοεπιθέσεις έχουν αλλάξει με την πάροδο του χρόνου, οδηγώντας σε αυξημένα μέτρα και, ως εκ τούτου, σε μέτρα αντιμετώπισης των κυβερνοεπιθέσεων. • Το τμήμα αυτό μπορεί να περιλαμβάνει τοπικές / ευρωπαϊκές / διεθνείς μελέτες περίπτωσης
	Προτεινόμενες ώρες: 1.0 | *Ελάχιστες διαφάνειες*: 15 | *Μέγιστες Διαφάνειες*: 20
1.3 Ορισμοί της ασφάλειας στον	• Ενότητα σχετικά με την ορολογία/όρους και στατιστικά στοιχεία/πηγές για την κυβερνοασφάλεια
	Προτεινόμενες ώρες | *Ελάχιστες διαφάνειες* | *Μέγιστες Διαφάνειες*

κυβερνοχώρο	0.5	8	10

3.2.2 Κυβερνοασφάλεια στην Ευρωπαϊκή Ένωση (ΕΕ)

Τίτλος Ενότητας	2.0 Κυβερνοασφάλεια στην ΕΕ
Συνολική διάρκεια *(Ώρες / Διαφάνειες)*	3 ώρες 48 - 67 διαφάνειες
Μέθοδος παράδοσης	Πρόσωπο με πρόσωπο Online Μικτή μάθηση Συζητήσεις
Αξιολόγηση	Πρόσωπο με πρόσωπο / Διαδικτυακό κουίζ
Μαθησιακά αποτελέσματα	• Κατανόηση των νομικών πτυχών της κυβερνοασφάλειας • Κατανόηση των τρεχουσών πολιτικών της ΕΕ σχετικά με την κυβερνοασφάλεια • Κατανόηση της νομοθεσίας της ΕΕ σχετικά με την κυβερνοασφάλεια • Συσχέτιση και σύγκριση των τοπικών νόμων για την ασφάλεια στον κυβερνοχώρο με τους νόμους της ΕΕ
Προαπαιτούμενα	Βασικές γνώσεις πληροφορικής και επιχειρήσεων θα ήταν χρήσιμες για την καλύτερη κατανόηση της ενότητας.
Περιγραφή ενότητας	Η ενότητα αυτή εισάγει τον εκπαιδευόμενο στις υφιστάμενες πολιτικές και πρωτοβουλίες της ΕΕ που αποσκοπούν στην προώθηση της έννοιας της κυβερνοασφάλειας. Συζητά επίσης τις νομικές πτυχές της Κυβερνοασφάλειας τόσο εντός της ΕΕ όσο και παγκοσμίως, εκθέτοντας τους εκπαιδευόμενους σε πολυάριθμα σενάρια πραγματικής ζωής και μελέτες περιπτώσεων στον τομέα. Η ενότητα περιλαμβάνει μια επισκόπηση των τάσεων στο τοπίο της κυβερνοασφάλειας, συμπεριλαμβανομένων, ενδεικτικά, στατιστικών στοιχείων, τάσεων, σχετικών απειλών, νομικών κινδύνων, κινδύνων φήμης και οικονομικών κινδύνων, καθώς και ανάλυση μελετών περιπτώσεων.
ΥΠΟΘΈΜΑΤΑ ΕΝΌΤΗΤΑΣ	
2.1 Προώθηση της ασφάλειας στον κυβερνοχώρο στην Ευρωπαϊκή Ένωση	• Σύντομη εισαγωγή στις πολιτικές και τις πρωτοβουλίες της ΕΕ που αποσκοπούν στην προώθηση της έννοιας της κυβερνοασφάλειας

Προτεινόμενες ώρες	*Ελάχιστες διαφάνειες*	*Μέγιστες Διαφάνειες*
1.0	20	30

2.2	**Νομικές πτυχές της ασφάλειας στον κυβερνοχώρο**	• Νομικές πτυχές της κυβερνοασφάλειας παγκοσμίως (γενικά) και ειδικότερα στην ΕΕ, συμπεριλαμβανομένων των συνεπειών της μη συμμόρφωσης. • Η σχέση, η σύγκριση και η αντιπαράθεση των τοπικών νόμων για την ασφάλεια στον κυβερνοχώρο με τους νόμους της ΕΕ		
		Προτεινόμενες ώρες 0.5	*Ελάχιστες διαφάνειες* 5	*Μέγιστες Διαφάνειες* 7
2.3	**Επισκόπηση των τάσεων του τοπίου της κυβερνοασφάλειας**	• Η παρουσίαση πραγματικών σεναρίων και μελετών περίπτωσης, συμπεριλαμβανομένων στατιστικών στοιχείων, τάσεων, σχετικών απειλών, κινδύνων (νομικών, φήμης, οικονομικών). • Μια ματιά στις πρόσφατες επιθέσεις στον κυβερνοχώρο και συζήτηση στην τάξη σχετικά με τη σημασία της επιμόρφωσης ενόψει των πιθανών κινδύνων που επιφέρουν οι επιθέσεις στον κυβερνοχώρο. *Σημείωση: Η συζήτηση θα μπορούσε να γίνει διαδικτυακά ή πρόσωπο με πρόσωπο, με τον εκπαιδευτή να διευκολύνει και να παρέχει κατευθυντήριες γραμμές για το τι αναμένεται από τη συζήτηση.*		
		Προτεινόμενες ώρες 1.5	*Ελάχιστες διαφάνειες* 23	*Μέγιστες Διαφάνειες* 30

3.2.3 Επιθέσεις στον κυβερνοχώρο: Ψάρεμα: Κοινωνική Μηχανική και Phishing

Τίτλος Ενότητας	3.0 Επιθέσεις στον κυβερνοχώρο: Κοινωνική Μηχανική και Ψάρεμα
Συνολική διάρκεια *(Ώρες / Διαφάνειες)*	10 ώρες 150 - 200 διαφάνειες
Μέθοδος παράδοσης	Πρόσωπο με πρόσωπο Online Μικτή μάθηση Χρήση διαδραστικών εργαλείων (π.χ. διαδικτυακά εργαλεία σεναρίων) Συζητήσεις
Αξιολόγηση	Πρόσωπο με πρόσωπο / Διαδικτυακό κουίζ
Μαθησιακά αποτελέσματα	• Να κατανοήσουν την έννοια των κυβερνοεπιθέσεων • Ορισμός της κοινωνικής μηχανικής και της αντίστροφης κοινωνικής μηχανικής • Κατανόηση των τρόπων κοινωνικής μηχανικής και της σχέσης της με τις επιθέσεις στον κυβερνοχώρο • Κατανόηση των πιο κοινών απειλών κυβερνοασφάλειας • Κατανόηση των κύριων κατηγοριών και τεχνικών κυβερνοεπιθέσεων
Προαπαιτούμενα	Βασικές γνώσεις πληροφορικής και επιχειρήσεων θα ήταν χρήσιμες για την καλύτερη κατανόηση της ενότητας.

<table>
<tr><td>Περιγραφή ενότητας</td><td colspan="3">Αυτή η ενότητα εισάγει τον εκπαιδευόμενο στις επιθέσεις στον κυβερνοχώρο με ιδιαίτερη έμφαση στο Phishing. Εμβαθύνει επίσης λεπτομερώς στην έννοια της κοινωνικής μηχανικής και της αντίστροφης κοινωνικής μηχανικής μαζί με την ισχυρή σύνδεση της κοινωνικής μηχανικής με τις επιθέσεις στον κυβερνοχώρο.

Στην ενότητα παρουσιάζονται επίσης διάφοροι τύποι επιθέσεων και τεχνικών phishing μαζί με ορισμένα παραδείγματα πραγματικών περιπτώσεων από τις χώρες εταίρους του έργου.</td></tr>
<tr><td colspan="4">ΥΠΟΘΈΜΑΤΑ ΕΝΌΤΗΤΑΣ</td></tr>
<tr><td>3.1 Εισαγωγή στις επιθέσεις στον κυβερνοχώρο</td><td colspan="3">• Σύντομη εισαγωγή στις επιθέσεις στον κυβερνοχώρο, ιδίως στις επιθέσεις Phishing</td></tr>
<tr><td></td><td>Προτεινόμενες ώρες
0.5</td><td>Ελάχιστες διαφάνειες
8</td><td>Μέγιστες Διαφάνειες
10</td></tr>
<tr><td>3.2 Ενότητες κοινωνικής μηχανικής και χειραγώγησης</td><td colspan="3">• Επισκόπηση των μοντέλων κοινωνικής μηχανικής με ιδιαίτερη έμφαση στα εξής:

α) "Τα όπλα της επιρροής" - R. Cialdini [2]
- Εμβολοφόρος
- Δέσμευση και συνέπεια
- Κοινωνική απόδειξη
- Liking
- Αρχή
- Σπανιότητα

β) Ψυχολογικές πτυχές της κοινωνικής μηχανικής
γ) Επισκόπηση της αντίστροφης κοινωνικής μηχανικής</td></tr>
<tr><td></td><td>Προτεινόμενες ώρες
4</td><td>Ελάχιστες διαφάνειες
60</td><td>Μέγιστες Διαφάνειες
80</td></tr>
<tr><td>3.3 Διαφορετικοί τύποι επιθέσεων Phishing και τεχνικές</td><td colspan="3">• Μια ενότητα για τον ορισμό των διαφόρων τύπων κυβερνοεπιθέσεων (ιδίως του Phishing) και τον τρόπο αναγνώρισής τους (επόμενο κεφάλαιο), συμπεριλαμβανομένων ενδεικτικά:

Κατηγορίες
- Επιθέσεις που σχετίζονται με τον GDPR
- Ηλεκτρονικά μηνύματα,
- Άμεση ανταλλαγή μηνυμάτων,
- Κοινωνικά δίκτυα,
- Ιστοσελίδες,
- Απάτες με λοταρίες,
- SMS,
- Τηλεφωνήματα,
- Πρόσωπο με πρόσωπο,</td></tr>
</table>

[2] Cialdini, R. B. (2016). Pre-Suasion: Σωτηρία: Ένας επαναστατικός τρόπος για να επηρεάζεις και να πείθεις. New York: Simon & Schuster. ISBN 978-1501109799.

	- Σέρφινγκ στον ώμο, **Συνδυασμός τεχνικών** - Ψεκάστε και προσευχηθείτε - Spear Phishing - Φαλαινοθηρία - Vishing - Smishing - Angler Phishing - Phishing κλώνων - Malvertising		
	Προτεινόμενες ώρες 4	*Ελάχιστες διαφάνειες* 60	*Μέγιστες Διαφάνειες* 80
3.4 Μελέτες περιπτώσεων	• Παρουσίαση ορισμένων διαφορετικών περιπτωσιολογικών μελετών από τους οργανισμούς-εταίρους • Διαδικτυακή ή δια ζώσης συζήτηση σε μικρές ομάδες (5-6 μαθητές) *Σημείωση: Η συζήτηση θα λάβει τη μορφή άσκησης με κάθε ομάδα να βρίσκει και να αναλύει μια πρόσφατη επίθεση ηλεκτρονικού "ψαρέματος", ώστε να περιλαμβάνει λεπτομέρειες όπως η ημερομηνία της επίθεσης, πληροφορίες για το θύμα, οι τρόποι της επίθεσης, οι συνέπειες, τα διδάγματα που αντλήθηκαν κ.ο.κ. Στη συνέχεια, ένας μαθητής από κάθε ομάδα παρουσιάζει τα αποτελέσματα της ανάλυσης σε όλη την τάξη. Παρέχεται επίσης εποικοδομητική ανατροφοδότηση από τον εκπαιδευτή και τους συμμαθητές του.*		
	Προτεινόμενες ώρες 1.5	*Ελάχιστες διαφάνειες* 22	*Μέγιστες Διαφάνειες* 30

3.2.4 Επισκόπηση της κατανόησης και του χειρισμού των επιθέσεων στον κυβερνοχώρο

Τίτλος Ενότητας	4.0 Κατανόηση και αντιμετώπιση κυβερνοεπιθέσεων
Συνολική διάρκεια *(Ώρες / Διαφάνειες)*	14 ώρες 210 - 255 διαφάνειες
Μέθοδος παράδοσης	Πρόσωπο με πρόσωπο Online Μικτή μάθηση
Αξιολόγηση	Πρόσωπο με πρόσωπο / Διαδικτυακό κουίζ
Μαθησιακά αποτελέσματα	• Απόκτηση βασικών γνώσεων σχετικά με την ηλεκτρονική ασφάλεια και προστασία • Κατανόηση διαφορετικού περιεχομένου πληροφοριών • Κατανόηση της ταυτότητας και διάκριση μεταξύ διαφορετικών επιθέσεων που σχετίζονται με την ταυτότητα • Κατανόηση των συνεπειών των επιθέσεων στον κυβερνοχώρο τόσο σε

	άτομα όσο και σε οργανισμούς • Ορισμός και κατανόηση της σημασίας της κυβερνοϋγιεινής ως προληπτικής δράσης έναντι των κυβερνοεπιθέσεων • Κατανόηση και εφαρμογή διαφορετικών μεθόδων προστασίας από κυβερνοεπιθέσεις • Σχεδιασμός και εφαρμογή σχεδίου αντιμετώπισης περιστατικών επιθέσεων στον κυβερνοχώρο
Προαπαιτούμενα	Προηγούμενες ενότητες
Περιγραφή ενότητας	Αυτή η ενότητα εισάγει τον εκπαιδευόμενο στην έννοια της ηλεκτρονικής ασφάλειας και στη σημασία της υιοθέτησης μιας προληπτικής προσέγγισης των απειλών στον κυβερνοχώρο μέσω της έννοιας της κυβερνοϋγιεινής. Η ενότητα παρέχει επίσης μια λεπτομερή προσέγγιση σχετικά με τον τρόπο αναγνώρισης και αντιμετώπισης επιθέσεων στον κυβερνοχώρο. Η ενότητα εισάγει την ανάπτυξη και την εφαρμογή σχεδίων αντιμετώπισης περιστατικών με σκοπό την ελαχιστοποίηση των επιπτώσεων των επιθέσεων στον κυβερνοχώρο.
ΥΠΟΘΈΜΑΤΑ ΕΝΌΤΗΤΑΣ	
4.1 Βασικές γνώσεις για την ηλεκτρονική ασφάλεια	• Διαφορές του περιεχομένου των πληροφοριών (ανοικτό, ιδιωτικό, επιχειρηματικό κ.λπ.)- Πνευματική ιδιοκτησία- Πνευματικά δικαιώματα, • Κατανοήστε τον όρο ταυτότητα- να γνωρίζετε για την κλοπή ταυτότητας και τις μεθόδους κλοπής. Να γνωρίζουν για το spyware, τον κατασκοπευτή πληκτρολογίου, τη διαφήμιση απάτης, τα Trojans. Να γνωρίζετε διάφορους τρόπους με τους οποίους κακόβουλο λογισμικό μπορεί να εισέλθει στη συσκευή. • Να γνωρίζουν τους λόγους και τις συνέπειες της κλοπής ταυτότητας και προσωπικών δεδομένων στο χώρο εργασίας και στο διαδίκτυο (δόλια χρήση πληροφοριών, απειλή απώλειας πληροφοριών, δολιοφθορά). • Γνωρίστε τις απειλές που σχετίζονται με την αποκάλυψη προσωπικών δεδομένων. • Μια σύντομη εισαγωγή στις επιπτώσεις των επιθέσεων στον κυβερνοχώρο τόσο στο άτομο όσο και στον οργανισμό. Περισσότερες λεπτομέρειες θα εξεταστούν στην ενότητα 4.4.
	Προτεινόμενες ώρες: 0.5 | *Ελάχιστες διαφάνειες*: 8 | *Μέγιστες Διαφάνειες*: 10
4.2 Προληπτικές ενέργειες	• Υγιεινή στον κυβερνοχώρο στο Διαδίκτυο (ελαχιστοποίηση των πληροφοριών σχετικά με πρόσωπα, συμπεριλαμβανομένων των προσωπικών λογαριασμών στα μέσα κοινωνικής δικτύωσης, οι οποίες θα μπορούσαν να χρησιμοποιηθούν από επιτιθέμενους). • Υγιεινή στον κυβερνοχώρο στο χώρο εργασίας • Τεχνολογικά εργαλεία και μέτρα (φίλτρα και αποκλεισμός ηλεκτρονικών μηνυμάτων ηλεκτρονικού "ψαρέματος")
	Προτεινόμενες ώρες | *Ελάχιστες διαφάνειες* | *Μέγιστες Διαφάνειες*

		2	30	35
4.3	**Αναγνώριση επιθέσεων phishing**	• Ανάλυση μελετών περίπτωσης με τη χρήση τεχνικών από την ενότητα *3.3 - Διαφορετικοί τύποι επιθέσεων phishing και τεχνικές* • Ένα τμήμα για την αναγνώριση των κυβερνοεπιθέσεων (με αναφορά στα στοιχεία του προηγούμενου κεφαλαίου), συμπεριλαμβανομένων ενδεικτικά: - Κριτική σκέψη - Μάθετε να μετακινείτε τους συνδέσμους - Κατανόηση της διεύθυνσης URL - Ανάλυση μηνυμάτων - Αναγνώριση των κόκκινων σημαιών		
		Προτεινόμενες ώρες 5	*Ελάχιστες διαφάνειες* 75	*Μέγιστες Διαφάνειες* 90
4.4	**Χειρισμός κυβερνοεπιθέσεων**	• Οδηγός για την κυβερνοασφάλεια, συμπεριλαμβανομένου ενός τμήματος σχετικά με τις ζημιές που προκαλούν οι κυβερνοεπιθέσεις τόσο στο **άτομο** όσο και στους **οργανισμούς** και τον τρόπο αντιμετώπισης των κυβερνοεπιθέσεων με βάση το προηγούμενο κεφάλαιο. Αυτό θα πρέπει να περιλαμβάνει, μεταξύ άλλων, τα εξής: - Ασφαλής πλοήγηση - Δημιουργία ισχυρών κωδικών πρόσβασης - Αποφυγή επιθέσεων - Ασφαλείς ηλεκτρονικές αγορές - Εγκατάσταση λογισμικού κατά των επιθέσεων στον κυβερνοχώρο - Αντιμετώπιση των Cookies - Λήψη κατάλληλων αντιγράφων ασφαλείας - Κρυπτογράφηση αρχείων - Έλεγχος ταυτότητας δύο παραγόντων - Κακόβουλο λογισμικό - Ασφαλής περιήγηση • Η ενότητα αυτή περιλαμβάνει επίσης τοπικές / ευρωπαϊκές / διεθνείς μελέτες περίπτωσης ως παραδείγματα που αναφέρονται σε προηγούμενες ενότητες. • Το τμήμα αυτό περιλαμβάνει εύκολες οδηγίες βήμα προς βήμα και εικόνες κατά περίπτωση. • Το τμήμα αυτό περιλαμβάνει επίσης την αντιδραστική δράση σε περίπτωση κυβερνοεπίθεσης, συμπεριλαμβανομένων των διαδικασιών αποκατάστασης σε περίπτωση που ένας οργανισμός ή/και ένας χρήστης πέσει θύμα κυβερνοεπίθεσης.		
		Προτεινόμενες ώρες 5	*Ελάχιστες διαφάνειες* 75	*Μέγιστες Διαφάνειες* 90
4.5	**Ελαχιστοποίηση των ζημιών μέσω της αντιμετώπισης**	• Σχεδιασμός, ανάπτυξη και εφαρμογή σχεδίων αντιμετώπισης περιστατικών που υποδεικνύουν τις προτεινόμενες και βέλτιστες πρακτικές τεχνικές που πρέπει να εφαρμοστούν σε περίπτωση περιστατικού παραβίασης δεδομένων. *Σημείωση: Μέρος της ενότητας μπορεί να προσαρμοστεί ανάλογα με τις*		

περιστατικών	*συγκεκριμένες χώρες.*		
	Προτεινόμενες ώρες 1.5	*Ελάχιστες διαφάνειες* 22	*Μέγιστες Διαφάνειες* 30