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

CyberPhish Σύντομο πρόγραμμα σπουδών

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	**02/04/2021**	**Αρχικό σχέδιο**	**MECB Ltd (MT)**
2 Σχέδιο έκδοσης 2.0	**07/04/2021**	**Επικαιροποιημένο σχέδιο**	**MECB Ltd (MT)**
4 Σχέδιο έκδοσης 3.0	**10/04/2021**	**Επικαιροποιημένο σχέδιο μετά την ανατροφοδότηση από τους εταίρους**	**MECB Ltd (MT)**
4 Σχέδιο έκδοσης 4.0	**31/05/2021**	**Τελική έκδοση μετά από ανατροφοδότηση από εταίρους και εμπειρογνώμονες**	**MECB Ltd (MT)**
5 Τελική έκδοση 1.0	**08/06/2021**	**Τελική έκδοση για διανομή**	**MECB Ltd (MT)**

ΠΕΡΙΕΧΌΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Το σύντομο πρόγραμμα σπουδών Cyberphish περιγράφει λεπτομερώς τη δομή του προγράμματος σπουδών και αποσκοπεί στην παροχή συνοπτικών αλλά εκτεταμένων ενοτήτων στην κυβερνοασφάλεια με ιδιαίτερη έμφαση στο κυβερνο-ψάρεμα. Θα χρησιμοποιηθεί για την εφαρμογή σε ενότητες σπουδών σε Ανώτατα Εκπαιδευτικά Ιδρύματα (ΑΕΙ) και για σκοπούς διάδοσης προκειμένου να προσελκύσει συμμετέχοντες στο μάθημα.

Αυτή η σύντομη έκδοση αποτελείται από τρία επίπεδα θεμάτων: κύρια θέματα, υποθέματα και στοιχεία υποθεμάτων με κύριο στόχο τους μαθητές, τους άλλους συμμετέχοντες στα μαθήματα και τους εκπαιδευτικούς. Αυτοί μπορούν να χρησιμοποιήσουν αυτό το πρόγραμμα σπουδών προκειμένου να κατανοήσουν τους κύριους στόχους και σκοπούς αυτού του μαθήματος.

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. Η ΔΟΜΗ ΤΟΥ ΠΡΟΓΡΑΜΜΑΤΟΣ ΣΠΟΥΔΩΝ (ΕΝΟΤΗΤΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΜΑΘΗΣΗΣ)

1.1 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 εξοπλιστούν καλύτερα 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 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	***Στόχος της ενότητας***

σπουδών		
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.

1.2 Δομή της ενότητας E-Learning λεπτομερώς

1.2.1 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 κυβερνοχώρο	• Ενότητα σχετικά με την ορολογία/όρους και στατιστικά στοιχεία/πηγές για την κυβερνοασφάλεια
	Προτεινόμενες ώρες: 0.5 | *Ελάχιστες διαφάνειες*: 8 | *Μέγιστες Διαφάνειες*: 10

1.2.2 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	*Ελάχιστες διαφάνειες*	*Μέγιστες Διαφάνειες*
0.5	5	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	*Ελάχιστες διαφάνειες*	*Μέγιστες Διαφάνειες*
1.5	23	30

1.2.3 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.
Περιγραφή ενότητας	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

<table>
<tr><td></td><td colspan="3">phishing μαζί με ορισμένα παραδείγματα πραγματικών περιπτώσεων από τις χώρες εταίρους του έργου.</td></tr>
<tr><td colspan="4">ΥΠΟΘΕΜΑΤΑ ΕΝΟΤΗΤΑΣ</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
<table><tr><td>Προτεινόμενες ώρες
0.5</td><td>Ελάχιστες διαφάνειες
8</td><td>Μέγιστες Διαφάνειες
10</td></tr></table></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 [1]
- Εμβολοφόρος
- Δέσμευση και συνέπεια
- Κοινωνική απόδειξη
- Liking
- Αρχή
- Σπανιότητα
β) Ψυχολογικές πτυχές της κοινωνικής μηχανικής
γ) Επισκόπηση της αντίστροφης κοινωνικής μηχανικής
<table><tr><td>Προτεινόμενες ώρες
4</td><td>Ελάχιστες διαφάνειες
60</td><td>Μέγιστες Διαφάνειες
80</td></tr></table></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,
- Σέρφινγκ στον ώμο,
Συνδυασμός τεχνικών
- Ψεκάστε και προσευχηθείτε
- Spear Phishing
- Φαλαινοθηρία
- Vishing</td></tr>
</table>

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

	- 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 προσωπό με πρόσωπο 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	*Μέγιστο Διαφάνειες* 30

1.2.4 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: 2 | *Ελάχιστες διαφάνειες*: 30 | *Μέγιστες Διαφάνειες*: 35

<table>
<tr><td>4.3</td><td>Αναγνώριση επιθέσεων phishing</td><td>

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

<table>
<tr><td>Προτεινόμενες ώρες
5</td><td>Ελάχιστες διαφάνειες
75</td><td>Μέγιστο Διαφάνειες
90</td></tr>
</table>
</td></tr>
<tr><td>4.4</td><td>Χειρισμός κυβερνοεπιθέσεων</td><td>

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.

<table>
<tr><td>Προτεινόμενες ώρες
5</td><td>Ελάχιστες διαφάνειες
75</td><td>Μέγιστες Διαφάνειες
90</td></tr>
</table>
</td></tr>
<tr><td>4.5</td><td>Ελαχιστοποίηση των ζημιών μέσω της αντιμετώπισης περιστατικών</td><td>

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 συγκεκριμένες χώρες.
</td></tr>
</table>

	Προτεινόμενες ώρες	*Ελάχιστες διαφάνειες*	*Μέγιστο Διαφάνειες*
	1.5	22	30