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

A1: Μεθοδολογικές κατευθυντήριες γραμμές για τους εκπαιδευτές

Διάρκεια του έργου: Νοέμβριος 2020 - Νοέμβριος 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.

Περιεχόμενα

ΣΧΕΤΙΚΑ ΜΕ ΤΟ ΕΡΓΟ

Η απάτη αποτελεί ένα από τα μεγαλύτερα προβλήματα τον τελευταίο καιρό, καθώς οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν ταχύτερες και πιο καινοτόμες τεχνολογίες για την πραγματοποίηση εκστρατειών απάτης. Η ανάπτυξη της προστασίας από το phishing με τη βοήθεια του ανθρώπου απαιτεί την εκπαίδευση των χρηστών, ώστε να μπορούν να αναγνωρίζουν και να ανταποκρίνονται κατάλληλα στις επιθέσεις phishing.

Το έργο στοχεύει στην εκπαίδευση των φοιτητών των ιδρυμάτων τριτοβάθμιας εκπαίδευσης, των εκπαιδευτικών, του πανεπιστημιακού προσωπικού (μέλη της κοινότητας), των εκπαιδευτικών κέντρων και του επιχειρηματικού τομέα (εργοδότες και εργαζόμενοι). Επιπλέον, το έργο αποσκοπεί επίσης στην ενθάρρυνση της κριτικής σκέψης της ομάδας-στόχου στον τομέα της ασφάλειας στον κυβερνοχώρο.

Η ομάδα έργου έχει αναπτύξει ένα πρόγραμμα σπουδών, υλικό ηλεκτρονικής μάθησης, ένα μικτό περιβάλλον μάθησης, τεστ αυτοαξιολόγησης, σύστημα αξιολόγησης και αξιολόγησης γνώσεων και προσομοιώσεις με βάση παιχνίδια για τους μαθητές και άλλους χρήστες για την προστασία από επιθέσεις phishing, καθώς και για την ανάπτυξη ικανοτήτων που θα τους βοηθήσουν να γνωρίζουν τις απειλές και να λαμβάνουν κατάλληλα προληπτικά μέτρα.

Τα κύρια πνευματικά αποτελέσματα είναι:

1. Ανάλυση της μελέτης και συστάσεις: Αποφυγή επιθέσεων phishing και βελτίωση της κριτικής σκέψης,

2. Πρόγραμμα σπουδών,

3. Ηλεκτρονικό εκπαιδευτικό υλικό,

4. Προσομοιώσεις για την εκπαίδευση (gamification),

5. Συστήματα αυτοαξιολόγησης και αξιολόγησης γνώσεων,

6. Μεθοδολογικές κατευθυντήριες γραμμές για τους εκπαιδευτές και την εφαρμογή της ενότητας CyberPhish.

ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΓΙΑ ΤΗΝ ΟΡΓΑΝΩΣΗ ΤΗΣ ΚΑΤΑΡΤΙΣΗΣ

Προτάσεις και καθοδήγηση για την οργάνωση της κατάρτισης των συμμετεχόντων στην ενότητα CyberPhish.

Το μάθημα Cyberphish θα μπορούσε να οργανωθεί χρησιμοποιώντας μια προσέγγιση μικτής μάθησης, συνδυάζοντας διαδικτυακές και δια ζώσης μεθόδους διδασκαλίας. Αυτό σημαίνει ότι η διαδικασία απόκτησης γνώσεων και δεξιοτήτων βασίζεται τόσο σε δια ζώσης όσο και σε διαδικτυακή διδασκαλία: σεμινάρια υπό την καθοδήγηση ενός λέκτορα, ανεξάρτητη εργασία των συμμετεχόντων με τη χρήση διαδικτυακού εκπαιδευτικού υλικού και ασκήσεις ομαδικής συνεργασίας.

Είναι σημαντικό οι συμμετέχοντες να μπορούν να έχουν την υποστήριξη του διδάσκοντα σε οποιοδήποτε σημείο της μαθησιακής διαδικασίας (εκτός από την τελική αξιολόγηση των γνώσεων), δηλαδή να μπορούν να κάνουν ερωτήσεις ενδιαφέροντος, να ζητούν βοήθεια αν αποτύχουν ή δεν καταλαβαίνουν πώς να κάνουν μια εργασία και να λαμβάνουν υποστήριξη και ανατροφοδότηση από τους διδάσκοντες.

Ομάδα-στόχος. Οι φοιτητές της τριτοβάθμιας εκπαίδευσης αποτελούν την κύρια ομάδα-στόχο του παρόντος έργου. Κατά τη διάρκεια της πιλοτικής κατάρτισης επιλέχθηκαν φοιτητές από διαφορετικά προγράμματα σπουδών. Χρησιμοποίησαν προηγμένο εκπαιδευτικό υλικό, εξασκήθηκαν σε προσομοιώσεις βασισμένες σε παιχνίδια και πραγματοποίησαν τεστ αυτοαξιολόγησης και αξιολόγησης των γνώσεων για να προσδιορίσουν το επίπεδο των γνώσεών τους πριν και μετά το μάθημα. Οι συμμετέχοντες πρέπει να διαθέτουν βασικές δεξιότητες ψηφιακού γραμματισμού. Εκτός από αυτό δεν υπάρχουν άλλες προϋποθέσεις για τις γνώσεις ή τις δεξιότητες των σπουδαστών.

Οι εκπαιδευτικοί είχαν επίσης πρόσβαση σε ένα σύγχρονο πρόγραμμα σπουδών που βασίζεται στις τελευταίες έρευνες στις χώρες εταίρους- υλικό ηλεκτρονικής μάθησης που αναπτύχθηκε από ειδικούς στον τομέα τους, εμπλουτισμένο με ασκήσεις για τους μαθητές, συνδέσμους προς πρόσθετο αναγνωστικό υλικό (πρόσφατη βιβλιογραφία) και σχετικές πηγές βίντεο. Με τον τρόπο αυτό επικαιροποιούν και βελτιώνουν τις υπάρχουσες γνώσεις τους. Οι εκπαιδευτικοί θα μπορούσαν να μάθουν για καινοτόμες μεθόδους διδασκαλίας και μάθησης, όπως οι αυτοδοκιμές και τα τεστ γνώσεων σε διαδικτυακό περιβάλλον, καθώς και οι προσομοιώσεις, οι οποίες προσομοιώνουν ελκυστικά και με παιγνιώδη τρόπο καταστάσεις της πραγματικής ζωής.

Άλλοι δικαιούχοι που επηρεάζονται από το έργο είναι οι εκπαιδευτικοί, το προσωπικό των πανεπιστημίων, τα εκπαιδευτικά κέντρα και ο επιχειρηματικός τομέας (εργοδότες και εργαζόμενοι). Θα επωφεληθούν επίσης διευρύνοντας και εμβαθύνοντας τις υπάρχουσες γνώσεις και ικανότητές τους, νιώθοντας ασφαλέστεροι στο διαδίκτυο,

αποφεύγοντας τη διαρροή ευαίσθητων/προσωπικών πληροφοριών και αποφεύγοντας οικονομικές απώλειες, τόσο προσωπικά όσο και στους οργανισμούς τους.

Κύρια ομάδα-στόχος	ΦΟΙΤΗΤΈΣ ΤΡΙΤΟΒΆΘΜΙΑΣ ΕΚΠΑΊΔΕΥΣΗΣ

- Χρήση αναπτυγμένου υλικού
- Εξάσκηση σε προσομοιώσεις που βασίζονται σε παιχνίδια
- Εκτελέστε τεστ αυτοαξιολόγησης και αξιολόγησης γνώσεων

Δευτερεύουσα ομάδα-στόχος	ΔΆΣΚΑΛΟΙ/ΕΚΠΑΙΔΕΥΤΈΣ

- Πρόσβαση σε ένα σύγχρονο πρόγραμμα σπουδών και υλικό ηλεκτρονικής μάθησης που έχει αναπτυχθεί
- Μάθετε για καινοτόμες μεθόδους διδασκαλίας και μάθησης, όπως αυτοδοκιμές, τεστ γνώσεων και προσομοιώσεις

Άλλα	ΕΚΠΑΙΔΕΥΤΙΚΟΊ, ΠΑΝΕΠΙΣΤΗΜΙΑΚΌ ΠΡΟΣΩΠΙΚΌ, ΕΚΠΑΙΔΕΥΤΙΚΆ ΚΈΝΤΡΑ ΚΑΙ ΕΠΙΧΕΙΡΗΜΑΤΙΚΌΣ ΤΟΜΈΑΣ (ΕΡΓΟΔΌΤΕΣ ΚΑΙ ΕΡΓΑΖΌΜΕΝΟΙ)

- Πρόσβαση σε υλικό ηλεκτρονικής μάθησης που αναπτύχθηκε
- Ενίσχυση των υφιστάμενων γνώσεων και ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο

Σχήμα 1 Ομάδες-στόχοι του έργου

Διάρκεια κατάρτισης. Η συνιστώμενη διάρκεια της κατάρτισης είναι 4-6 εβδομάδες. Το σύνολο του προγράμματος σπουδών είναι 30 ώρες- ισοδυναμεί με 1 ECTS. Προτείνεται να ληφθεί υπόψη ο ίδιος αριθμός ωρών ανά ενότητα για αυτοεκπαίδευση και αξιολόγηση. Συνιστάται οι συμμετέχοντες να αφιερώνουν 2-3 ώρες την εβδομάδα κατά τη διάρκεια της εκπαίδευσης (ανάγνωση εκπαιδευτικού υλικού, επίλυση τεστ και σεναρίων).

Ο εκτιμώμενος χρόνος εκπαίδευσης μπορεί να διαφέρει ανάλογα με την εκπαίδευση. Τα θέματα και οι ασκήσεις/σενάρια που παρέχονται χωρίζονται σε μονοήμερες συνεδρίες. Ο διατιθέμενος χρόνος είναι ευέλικτος- ως εκ τούτου, δεν παρέχεται ακριβές χρονοδιάγραμμα για κάθε ημέρα.

Ο εκπαιδευτής θα πρέπει να μελετήσει το υλικό εκ των προτέρων και να προγραμματίσει το χρόνο ανάλογα με τις συγκεκριμένες εκπαιδευτικές ανάγκες.

Δομή του μαθήματος. Το πρόγραμμα σπουδών του μαθήματος είναι δομημένο σε τέσσερα μέρη:

1. Εισαγωγή στην κυβερνοασφάλεια,
2. Επισκόπηση της ασφάλειας στον κυβερνοχώρο στην ΕΕ
3. Επιθέσεις στον κυβερνοχώρο - Social Engineering και Phishing
4. Κατανόηση και χειρισμός κυβερνοεπιθέσεων

1. Εισαγωγή στην κυβερνοασφάλεια	• Στο παρόν μέρος παρουσιάζονται οι προκλήσεις κυβερνοεπιθέσεων για τις επιχειρήσεις στην εποχή της Βιομηχανίας 4.0, όπως η ευρεία χρήση των τεχνολογιών κινητής τηλεφωνίας, η υπολογιστική νέφους, το Διαδίκτυο των πραγμάτων (IoT) και τα μεγάλα δεδομένα, οι κίνδυνοι τρίτων και οι αυξανόμενες απειλές, συμπεριλαμβανομένων των απειλών από εθνικά κράτη. Σε αυτό το μέρος παρουσιάζονται επίσης ορισμοί που χρησιμοποιούνται και συναντώνται στον τομέα της κυβερνοασφάλειας.
2. Επισκόπηση της ασφάλειας στον κυβερνοχώρο στην ΕΕ	• Η ενότητα αυτή παρουσιάζει τις 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.
3. Επιθέσεις στον κυβερνοχώρο - Social Engineering και Phishing	• Αυτή η ενότητα εισάγει τις επιθέσεις στον κυβερνοχώρο με ιδιαίτερη έμφαση στο Phishing. Εμβαθύνει επίσης λεπτομερώς στην έννοια της κοινωνικής μηχανικής και της αντίστροφης κοινωνικής μηχανικής και στην ισχυρή σύνδεση της κοινωνικής μηχανικής με τις επιθέσεις στον κυβερνοχώρο. Η ενότητα παρουσιάζει επίσης διάφορους τύπους επιθέσεων και τεχνικών phishing μαζί με πραγματικά παραδείγματα μελέτης περίπτωσης..
4. Κατανόηση και χειρισμός κυβερνοεπιθέσεων	• Αυτή η ενότητα επικεντρώνεται στην έννοια της ηλεκτρονικής ασφάλειας και στη σημασία της υιοθέτησης μιας προληπτικής προσέγγισης των απειλών στον κυβερνοχώρο μέσω της έννοιας της κυβερνοϋγιεινής. Παρέχει επίσης μια λεπτομερή προσέγγιση σχετικά με τον τρόπο αναγνώρισης και χειρισμού κυβερνοεπιθέσεων, την ανάπτυξη και εφαρμογή σχεδίων αντιμετώπισης περιστατικών για την ελαχιστοποίηση των επιπτώσεων των κυβερνοεπιθέσεων.

Σχήμα 2 Δομή του μαθήματος

Το αναλυτικό πρόγραμμα σπουδών μπορεί να βρεθεί στην ιστοσελίδα του έργου www.cyberphish.eu

Σύντομη έκδοση: https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A1_EN_Cyberphish-Short-Curriculum-Final.pdf

Πλήρης έκδοση: https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EN_Cyberphish-Full-Curriculum-Final.pdf

ΚΟΙΝΕΣ ΔΙΑΔΙΚΑΣΙΕΣ ΚΑΤΑΡΤΙΣΗΣ

Αυτό το μέρος καθοδηγεί την οργάνωση της κατάρτισης. Εδώ περιλαμβάνουμε επίσης συστάσεις ορθής πρακτικής που χρησιμοποιήθηκαν κατά τη διάρκεια της πιλοτικής εκπαίδευσης CyberPhish, συμπεριλαμβανομένου ενός ερωτηματολογίου πριν από την εκπαίδευση, των απαιτήσεων για την εγγραφή των συμμετεχόντων, της μαθησιακής διαδικασίας και των όρων για ένα τεστ γνώσεων.

Πρόσκληση για κατάρτιση

Ας υποθέσουμε ότι η κατάρτιση οργανώνεται ως ξεχωριστό μάθημα που δεν περιλαμβάνεται στο πρόγραμμα σπουδών του ιδρύματος τριτοβάθμιας εκπαίδευσης. Σε αυτή την περίπτωση, συνιστάται η δημοσίευση ανακοίνωσης με πρόσκληση των συμμετεχόντων στην πιλοτική κατάρτιση στον ιστότοπο ή/και στα κοινωνικά δίκτυα ή η αποστολή προσωπικής πρόσκλησης στους δυνητικούς συμμετέχοντες μέσω ηλεκτρονικού ταχυδρομείου. Η πρόσκληση αυτή ενημερώνει τον δυνητικό συμμετέχοντα σχετικά με τον πρωταρχικό στόχο της κατάρτισης, τη διάρκεια του μαθήματος, τις αναπτυχθείσες ή αποκτηθείσες ικανότητες στην αναγνώριση επιθέσεων phishing και την πιστοποίηση μετά την ολοκλήρωση του μαθήματος. Θα μπορούσε επίσης να περιέχει τον σύνδεσμο προς τη φόρμα εγγραφής.

Παράδειγμα πρόσκλησης παρατίθεται στο παράρτημα 1. Αρχεία σε μορφή ppt και pdf είναι διαθέσιμα στη διεύθυνση https://wiki.cyberphish.eu/.

Εισαγωγική συνάντηση

Στην αρχή του μαθήματος, κατά την πρώτη συνάντηση, είναι σημαντικό να οικοδομηθεί εμπιστοσύνη μεταξύ του εκπαιδευτή και των συμμετεχόντων, να παρακινηθούν και να γνωριστούν μεταξύ τους. Παρουσιάστε τη μορφή της διαβούλευσης (δια ζώσης/ εξ αποστάσεως) και τη συχνότητα, για παράδειγμα, εβδομαδιαία, τρεις φορές ανά μάθημα (στην αρχή, στο τέλος και στη μέση). Συνιστάται να αναφέρετε τις προκλήσεις που μπορεί στη συνέχεια να προκύψουν κατά την εγγραφή στην πλατφόρμα (π.χ. το μήνυμα ηλεκτρονικού ταχυδρομείου επιβεβαίωσης να πηγαίνει στο φάκελο spam).

Κατά τη διάρκεια της συνάντησης, οι συμμετέχοντες εξηγούνται πώς να χρησιμοποιούν το περιβάλλον ηλεκτρονικής μάθησης, τους επιτρέπεται να το δοκιμάσουν και καλούνται να μοιραστούν τυχόν προβλήματα που μπορεί να έχουν, ώστε να μην υπάρχουν αβεβαιότητες αργότερα, όταν ξεκινήσει το μάθημα. Η συνάντηση περιλαμβάνει επίσης μια εισαγωγή στο μάθημα CyberPhish.

Ερωτηματολόγιο πριν από την κατάρτιση

Για να αξιολογηθεί ο αντίκτυπος της κατάρτισης στην πρόοδο των γνώσεων των συμμετεχόντων, συνιστάται η χρήση ερωτηματολογίου πριν από την έναρξη της κατάρτισης. Κατά τη διάρκεια της πιλοτικής κατάρτισης, οι εταίροι χρησιμοποίησαν ερωτηματολόγια που αποτελούνταν από 20 ερωτήσεις. Το ερωτηματολόγιο αναπτύχθηκε στα αγγλικά και προσαρμόστηκε στις γλώσσες των χωρών των εταίρων: Εσθονικά, ελληνικά, λετονικά και λιθουανικά.

Οι ερωτήσεις επιλέχθηκαν από τις ερωτήσεις αυτοαξιολόγησης (20 από τις 60). Σε όλους τους συμμετέχοντες δόθηκαν οι ίδιες ερωτήσεις, αλλά με διαφορετική σειρά. Αυτό το ερωτηματολόγιο δεν επηρεάζει τα αποτελέσματα του συμμετέχοντα, αλλά επιτρέπει τη μέτρηση της αλλαγής στις γνώσεις του συμμετέχοντα.

Η συμπλήρωση του ερωτηματολογίου διαρκεί 20 έως 25 λεπτά. Πριν από τη συμπλήρωση του ερωτηματολογίου, οι συμμετέχοντες πρέπει να δηλώσουν τη διεύθυνση ηλεκτρονικού ταχυδρομείου τους. Συνιστάται η χρήση της ίδιας διεύθυνσης ηλεκτρονικού ταχυδρομείου κατά την εγγραφή στο περιβάλλον μάθησης του μαθήματος (www.cyberphish.vukhf.lt). Οι συμμετέχοντες θα πρέπει να ενημερωθούν ότι πρέπει να χρησιμοποιούν έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου. Η ίδια διεύθυνση ηλεκτρονικού ταχυδρομείου πρέπει να χρησιμοποιείται στο περιβάλλον μάθησης, όπως και στο έντυπο εγγραφής του συμμετέχοντα.

Πρέπει να σημειωθεί ότι δεν είναι υποχρεωτική η διεξαγωγή ερωτηματολογίου πριν από την κατάρτιση. Αποτελεί μόνο σύσταση, αλλά η πρακτική αυτή θα μπορούσε να χρησιμοποιηθεί εάν σας ενδιαφέρει η αξιολόγηση του αντίκτυπου του εκπαιδευτικού προγράμματος στους συμμετέχοντες.

Διαδικτυακή εκπαίδευση

Μετά από μια σύντομη εισαγωγική φάση, αρχίζει η διαδικτυακή εκπαίδευση, η οποία διαρκεί περίπου ένα μήνα (4-6 εβδομάδες). Κατά τη διάρκεια της εκπαιδευτικής διαδικασίας οι συμμετέχοντες εμπλέκονται σε διάφορες μαθησιακές δραστηριότητες με τη χρήση ποικίλων μεθόδων και μορφών κατάρτισης, οι οποίες περιλαμβάνουν, μεταξύ άλλων, τη μελέτη του υλικού ηλεκτρονικής μάθησης, την ανάγνωση πρόσθετου υλικού, την παρακολούθηση βίντεο σχετικών με τα θέματα, την πραγματοποίηση τεστ αυτοαξιολόγησης και τεστ αξιολόγησης γνώσεων και την επίλυση προσομοιώσεων. Κατά τη διάρκεια αυτής της περιόδου, οι συμμετέχοντες μαθαίνουν για την κυβερνοασφάλεια, κατανοούν τις κυβερνοεπιθέσεις και την κοινωνική μηχανική, μαθαίνουν πώς να αναγνωρίζουν τα κύρια σημάδια του phishing, κατανοούν τον χειρισμό των κυβερνοεπιθέσεων, μαθαίνουν να ελαχιστοποιούν τις ζημίες μέσω της αντιμετώπισης περιστατικών. Η επιτυχής συμμετοχή στην εκπαίδευση εξαρτάται από την ικανότητα των συμμετεχόντων να προγραμματίζουν τον δικό τους χρόνο και τις δραστηριότητές τους, καθώς και από τη συνεργασία με τους εκπαιδευτές και τα άλλα μέλη της ομάδας.

Η εκπαίδευση θα πρέπει να καταλήγει στην επιτυχή ολοκλήρωση ενός τεστ αξιολόγησης γνώσεων (βαθμολογία τουλάχιστον 75%) και στην απονομή ενός πιστοποιητικού που δημιουργείται αυτόματα. Στο τέλος της κατάρτισης, οι συμμετέχοντες αποκτούν νέες γνώσεις και δεξιότητες που μπορούν να χρησιμοποιήσουν στην καθημερινή τους ζωή (όπως αναζήτηση στο διαδίκτυο, προσωπική επικοινωνία στα κοινωνικά δίκτυα, τηλεφωνική επικοινωνία με αγνώστους, σπουδές, στο χώρο εργασίας τους, κ.λπ.) Επιπλέον, ενισχύουν την αυτοπεποίθησή τους.

Δομή του περιβάλλοντος ηλεκτρονικής μάθησης

Η πλατφόρμα μάθησης Cyberphish.vuknf.lt παρέχει ανοικτή πρόσβαση σε εκπαιδευτικό υλικό. Το υλικό μπορεί να μελετηθεί ελεύθερα από όλα τα άτομα που το επιθυμούν. Δεν απαιτείται εγγραφή. Ωστόσο, για να μπορέσετε να

επιλύσετε προσομοιώσεις που διδάσκουν πώς να αναγνωρίζετε επιθέσεις phishing, να κάνετε αυτοδοκιμές, τεστ αξιολόγησης γνώσεων και να αποκτήσετε πιστοποιητικό, είναι απαραίτητο να είστε εγγεγραμμένος χρήστης.

Μαθησιακό υλικό. Κάνοντας κλικ στο κουμπί *Μαθησιακό υλικό στη* γραμμή μενού, ο χρήστης μπορεί να δει τις ενότητες μαθημάτων στα αριστερά της οθόνης. Υπάρχουν τέσσερις ενότητες: Εισαγωγή στην κυβερνοασφάλεια- Επισκόπηση της κυβερνοασφάλειας στην ΕΕ- Επιθέσεις στον κυβερνοχώρο - Κοινωνική μηχανική και ηλεκτρονικό ψάρεμα- Κατανόηση και χειρισμός επιθέσεων στον κυβερνοχώρο. Κάθε ενότητα αποτελείται από διάφορα θέματα. Μόλις επιλεγεί μια υπόθεση, το εκπαιδευτικό υλικό εμφανίζεται στο κεντρικό τμήμα της οθόνης. Ο χρήστης μπορεί να κατεβάσει το υλικό μπορεί να το κατεβάσει στον υπολογιστή του χρήστη κάνοντας κλικ στον σύνδεσμο *Λήψη διαφανειών.*

Τεστ αυτοαξιολόγησης. Οι εγγεγραμμένοι χρήστες έχουν περισσότερες επιλογές. Έχουν τη δυνατότητα να κάνουν τεστ αυτοαξιολόγησης για σκοπούς μάθησης. Το κουμπί *τεστ αυτοαξιολόγησης* εμφανίζεται όταν ένας μαθητής έχει μάθει το υλικό της ενότητας. Ως εκ τούτου, ο μαθητής πρέπει να κάνει κλικ στο κουμπί *Ολοκληρώθηκε* όταν έχει εξοικειωθεί με κάθε θέμα της ενότητας. Όταν όλα τα θέματα της ενότητας σημειωθούν ως *Ολοκληρωμένα*, πράγμα που σημαίνει ότι η ύλη της ενότητας αυτής έχει διδαχθεί, τότε είναι διαθέσιμη η δυνατότητα συμμετοχής στο τεστ αυτοαξιολόγησης κάνοντας κλικ στο κουμπί *Τεστ αυτοαξιολόγησης.* Κατά τη διάρκεια του τεστ, παρουσιάζονται στον σπουδαστή πέντε τυχαίες ερωτήσεις από τη συγκεκριμένη ενότητα.

Μετά το τεστ, το σύστημα εμφανίζει τα αποτελέσματα του τεστ, με τις απαντήσεις που επέλεξε ο μαθητής, τις σωστές και λανθασμένες απαντήσεις, το χρόνο που χρειάστηκε για την επίλυση του τεστ και τους βαθμούς που συγκέντρωσε. Ο μαθητής μπορεί να επαναλάβει το τεστ κάνοντας κλικ στο κουμπί *Do it again.* Κατά την επανάληψη του τεστ, παρουσιάζονται 5 τυχαίες ερωτήσεις. Ο μαθητής μπορεί να κάνει το τεστ αυτοαξιολόγησης απεριόριστες φορές.

Προσομοιώσεις. Οι εγγεγραμμένοι χρήστες μπορούν να επιλύουν προσομοιώσεις. Αυτές οι προσομοιώσεις είναι μακέτες πραγματικών καταστάσεων. Στην αριστερή πλευρά της οθόνης, υπάρχει ένα κουμπί *Προσομοιώσεις* πάνω από τα θέματα της ενότητας. Ο μαθητής ανά πάσα στιγμή μπορεί να τις επιλύσει. Οι προσομοιώσεις ομαδοποιούνται σε 7 ομάδες: Ενότητα, συμπάθεια, συναίνεση, συνέπεια, εξουσία, σπανιότητα και ανταπόδοση. Όταν επιλέγεται μια προσομοίωση, δίνεται μια περιγραφή της κατάστασης. Οι προσομοιώσεις μπορούν να λειτουργήσουν με δύο τρόπους: για σκοπούς μάθησης και για σκοπούς ελέγχου γνώσεων. Στον πρώτο τρόπο λειτουργίας, ο μαθητής βλέπει τις βαθμολογίες που συλλέγονται και το συνολικό συμπέρασμα στο τέλος της προσομοίωσης. Σε μια προσομοίωση για έλεγχο γνώσεων, ο μαθητής εξετάζει στο τέλος τις επιλογές που έκανε κατά τη διάρκεια της προσομοίωσης και λαμβάνει ανατροφοδότηση με σχόλια. Ο μέντορας θα πρέπει να αποφασίσει πόσες προσομοιώσεις πρέπει να λύσει ο συμμετέχων. Για παράδειγμα, κατά τη διάρκεια του πιλοτικού προγράμματος κάθε συμμετέχων έπρεπε να επιλύσει τουλάχιστον 20 προσομοιώσεις της επιλογής του.

Τεστ αξιολόγησης γνώσεων. Οι εγγεγραμμένοι χρήστες μπορούν να συμμετάσχουν στο τεστ γνώσεων και να λάβουν πιστοποιητικό. Το κουμπί *Δοκιμασία γνώσεων* εμφανίζεται στην αριστερή πλευρά της οθόνης πάνω από τις ενότητες μαθημάτων όταν ο μαθητής έχει μάθει όλο το υλικό και έχει σημειώσει όλα τα θέματα ως ολοκληρωμένα. Το τεστ θεωρείται επιτυχές αν επιτευχθεί βαθμολογία τουλάχιστον 75%. Οι συμμετέχοντες που θα περάσουν αυτό το τελικό τεστ θα λάβουν ένα πιστοποιητικό. Εάν ο συμμετέχων δεν περάσει το τεστ, μπορεί να επαναλάβει τα θέματα και, αφού αφιερώσει λίγο περισσότερο χρόνο στη μάθηση, να ξαναδώσει το τελικό τεστ Γνώσεων. Το τεστ γνώσεων μπορεί να γίνει τρεις φορές.

Αξιολογήσεις. Το σύστημα υπολογίζει βαθμολογίες για να κάνει τη διαδικασία μάθησης πιο ελκυστική για τους μαθητές. Ο συμμετέχων στο μάθημα μπορεί να δει τη βαθμολογία του και τους πόντους που συγκέντρωσε στον συνολικό πίνακα βαθμολογίας. Οι βαθμολογίες βασίζονται σε τεστ αυτοαξιολόγησης και προσομοιώσεις. Η πρόσβαση στις βαθμολογίες γίνεται μέσω του στοιχείου μενού *Βαθμολογίες* στο επάνω μέρος της οθόνης. Η βαθμολογία προσομοίωσης του μαθητή υπολογίζεται με το άθροισμα των καλύτερων αποτελεσμάτων όλων των προσομοιώσεων που επιλύθηκαν. Αντίστοιχα, η βαθμολογία των τεστ αυτοαξιολόγησης του μαθητή υπολογίζεται με την άθροιση των καλύτερων βαθμολογιών όλων των τεστ αυτοαξιολόγησης που έγιναν.

Οι μαθητές μπορούν επίσης να βλέπουν την πρόοδο της μάθησής τους. Εμφανίζεται πάνω από τις ενότητες μαθημάτων στα αριστερά της οθόνης και μέσω του μενού χρήστη στο πάνω μέρος της οθόνης. Μέσω του μενού χρήστη, ο μαθητής μπορεί να αλλάξει το όνομα χρήστη, και τον κωδικό πρόσβασης, να δει τα σήματα που έχει συλλέξει, το ιστορικό των αυτοελέγχων και το ιστορικό των προσομοιώσεων.

Πιστοποιητικά. Τα πιστοποιητικά (σε μορφή PDF) δημιουργούνται αυτόματα για όλους τους συμμετέχοντες που έχουν ολοκληρώσει το μάθημα και έχουν περάσει το τεστ αξιολόγησης γνώσεων τουλάχιστον κατά 75%. Παράδειγμα πιστοποιητικού παρατίθεται στο παράρτημα αριθ. 2.

Πιστοποιητικά θα απονεμηθούν σε όλους τους συμμετέχοντες με την ολοκλήρωση του μαθήματος. Η ολοκλήρωση του μαθήματος CyberPhish δεν αποδίδει ακαδημαϊκές μονάδες.

Η διαθεσιμότητα

Το ηλεκτρονικό μάθημα που αναπτύχθηκε είναι διαθέσιμο σε τέσσερις γλώσσες: Λετονικά και Λιθουανικά. Φιλοξενείται στη διεύθυνση https://cyberphish.vuknf.lt/. Μια εικόνα της κύριας οθόνης της πλατφόρμας μάθησης δίνεται παρακάτω.

Σχήμα 3 Η κύρια οθόνη της πλατφόρμας εκμάθησης

Συστάσεις ορθής πρακτικής από την πιλοτική εκπαίδευση. Συνιστάται η ανάπτυξη κανόνων και οδηγιών για τους σπουδαστές. Τα ερωτηματολόγια στην αρχή και στο τέλος του μαθήματος είναι προαιρετικά. Μπορούν να χρησιμοποιηθούν και άλλα εργαλεία όπως στην κανονική εκπαίδευση.

Οδηγίες για τους μαθητές

Σε αυτό το μέρος, παρέχουμε συνιστώμενα βήματα με την οργάνωση της κατάρτισης:

Βήμα 1. Ερωτηματολόγιο προ-εκπαίδευσης. Πριν από την κατάρτιση, συμπληρώστε το ερωτηματολόγιο. Δώστε μια έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου, η οποία θα χρησιμοποιηθεί και στο σύστημα ηλεκτρονικής μάθησης κατά τη συμπλήρωση αυτού του ερωτηματολογίου.

Βήμα 2. **Συνδεθείτε στο περιβάλλον ηλεκτρονικής μάθησης**. Συνδεθείτε στο περιβάλλον ηλεκτρονικής μάθησης στη διεύθυνση https://cyberphish.vuknf.lt/login με την ίδια διεύθυνση ηλεκτρονικού ταχυδρομείου που χρησιμοποιήθηκε στο ερωτηματολόγιο.

Σημείωση: Εάν ο μαθητής δεν έχει λάβει το email επιβεβαίωσης από το σύστημα, πρέπει να ελέγξει τον φάκελο ανεπιθύμητης αλληλογραφίας. Το email επιβεβαίωσης μπορεί να καταλήξει στο φάκελο spam/unk.

Βήμα 3. Συνδεθείτε στο περιβάλλον ηλεκτρονικής μάθησης.

Συνδεθείτε στο https://cyberphish.vuknf.lt με τα προσωπικά σας διαπιστευτήρια.

Βήμα 4. Μελέτη του μαθησιακού υλικού.

Αφού συνδεθείτε, μελετήστε όλο το εκπαιδευτικό υλικό, δηλαδή τα τέσσερα θέματα και τα υποθέματα (βλ. παρακάτω). Σημειώστε ως *ολοκληρωμένο* μετά την εξέταση κάθε θέματος.

Θέματα και υποθέματα:

1. Εισαγωγή στην κυβερνοασφάλεια,
1.1. Ιστορικό - Προκλήσεις της βιομηχανικής επανάστασης 4th ,
1.2. Ιστορία της κυβερνοασφάλειας,
1.3. Ορισμοί της ασφάλειας στον κυβερνοχώρο
2. Επισκόπηση της ασφάλειας στον κυβερνοχώρο στην ΕΕ,
2.1. Προώθηση της κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση,
2.2. Νομικές πτυχές της ασφάλειας στον κυβερνοχώρο,
2.3. Επισκόπηση των τάσεων του τοπίου της κυβερνοασφάλειας,

3. Επιθέσεις στον κυβερνοχώρο - Social Engineering και Phishing,
3.1. Εισαγωγή στις επιθέσεις στον κυβερνοχώρο,
3.2. Ενότητες κοινωνικής μηχανικής και χειραγώγησης,
3.3. Διαφορετικοί τύποι επιθέσεων phishing και τεχνικές,
3.4. Μελέτες περιπτώσεων,
4. Κατανόηση και χειρισμός κυβερνοεπιθέσεων.
4.1. Βασικές γνώσεις σχετικά με την ηλεκτρονική ασφάλεια,
4.2. Προληπτικές ενέργειες,
4.3. Αναγνώριση επιθέσεων phishing,
4.4. Χειρισμός επιθέσεων στον κυβερνοχώρο,
4.5. Ελαχιστοποίηση των ζημιών μέσω της αντιμετώπισης περιστατικών,

Βήμα 5. Συμπληρώστε τέσσερα τεστ αυτοαξιολόγησης. Μετά την εκμάθηση κάθε θέματος, συμπληρώστε το τεστ αυτοαξιολόγησης.

Βήμα 6. Εκτέλεση/επανεπίλυση/εκτέλεση προσομοιώσεων. Κατά τη διάρκεια της εκμάθησης, εκτελέστε προσομοιώσεις ως μέρος της διαδικασίας μελέτης.

Βήμα 7. Συμπληρώστε το τεστ αξιολόγησης γνώσεων. Τέλος, περάστε το τελικό τεστ με βαθμολογία τουλάχιστον 75%.

Βήμα 8. Αφού περάσετε το τελικό τεστ, συμπληρώστε ένα **ερωτηματολόγιο για τους συμμετέχοντες μετά το μάθημα** σχετικά με την πιλοτική εκπαίδευση.

Σημείωση: αυτό το εργαλείο χρησιμοποιήθηκε κατά τη διάρκεια της πιλοτικής κατάρτισης, αλλά μπορούν να χρησιμοποιηθούν και άλλα εργαλεία όπως στην κανονική κατάρτιση.

Τελική συνάντηση

Η τελική συνάντηση έχει διάφορους σκοπούς: πρώτον, επιτρέπει στους συμμετέχοντες να συμπληρώσουν ένα ερωτηματολόγιο μετά την κατάρτιση, δεύτερον, θα επιτρέψει στους συμμετέχοντες να εκφράσουν τις απόψεις τους σχετικά με το μάθημα. Τέλος, θα μπορούσε να συζητηθεί η διαδικασία των τεστ αξιολόγησης των γνώσεων, οι δυσκολίες και οι προκλήσεις κατά την απάντηση των ερωτήσεων και άλλα θέματα.

Ερωτηματολόγια μετά το μάθημα

Σε ένα πιλοτικό πρόγραμμα, ζητήθηκε από τους συμμετέχοντες να συμπληρώσουν ένα **ερωτηματολόγιο για τους συμμετέχοντες μετά το** πέρας του τελικού τεστ. Το ερωτηματολόγιο αποτελείται από σημεία που ζητούν την παροχή γενικών πληροφοριών, όπως email, φύλο, επάγγελμα και ερωτήσεις σχετικά με την αξιολόγηση των γνώσεων του συμμετέχοντα σε συγκεκριμένα θέματα κυβερνοασφάλειας μετά την ολοκλήρωση του εκπαιδευτικού προγράμματος CyberPhish, την εμπειρία του συμμετέχοντα στη χρήση προσομοιώσεων. Επιπλέον, τίθενται επίσης ερωτήσεις σχετικά με τους στόχους του μαθήματος, την επιλεξιμότητα της προσέγγισης της διαδικτυακής μορφής, το περιεχόμενο του μαθήματος, τη χρονική διάρκεια, την εκπαίδευση και την υποστήριξη, τη χρηστικότητα της πλατφόρμας μάθησης. Το παράδειγμα του ερωτηματολογίου παρατίθεται στο παράρτημα αριθ. 3.

Οι εκπαιδευτές και οι μέντορες κλήθηκαν να συμπληρώσουν ένα **ερωτηματολόγιο για τους εκπαιδευτές μετά το πέρας του** πιλοτικού προγράμματος. Το ερωτηματολόγιο αποτελείται από σημεία που ζητούν την παροχή γενικών πληροφοριών, όπως email, όνομα, χώρα, καθώς και από ερωτήσεις σχετικά με τη δομή και το περιεχόμενο του μαθήματος, τη χρονική διάρκεια, τη συνάφεια των θεμάτων με το κοινό-στόχο, την πληρότητα των θεμάτων του μαθήματος, το βαθμό στον οποίο το μάθημα πέτυχε το στόχο του εισάγοντας την ασφάλεια στον κυβερνοχώρο και το phishing στους μαθητές. Το παράδειγμα του ερωτηματολογίου παρατίθεται στο παράρτημα αριθ. 4.

ΠΕΡΙΓΡΑΦΕΣ ΤΟΥ ΤΡΟΠΟΥ ΕΡΓΑΣΙΑΣ ΜΕ ΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΠΛΑΤΦΟΡΜΑ

Το εκπαιδευτικό υλικό που φιλοξενείται στο περιβάλλον ηλεκτρονικής μάθησης στη διεύθυνση https://cyberphish.vuknf.lt είναι διαθέσιμο σε όλους τους επισκέπτες και είναι δωρεάν. Το εκπαιδευτικό υλικό είναι διαθέσιμο σε πέντε γλώσσες: Λετονικά και Λιθουανικά. Οι μη εγγεγραμμένοι επισκέπτες μπορούν μόνο να δουν το

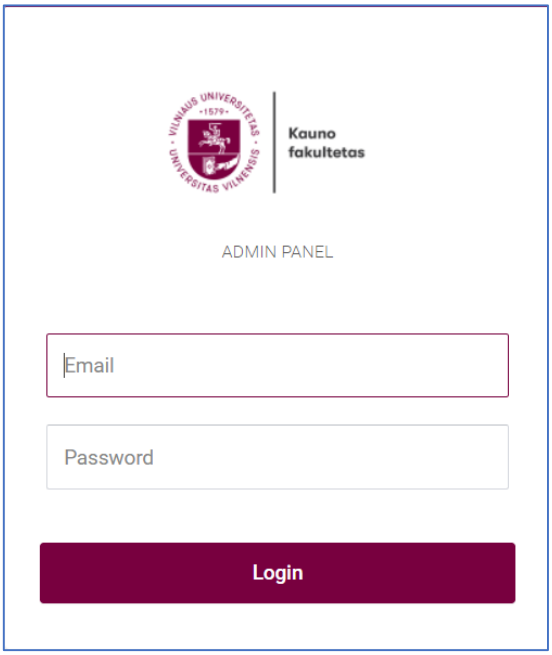
εκπαιδευτικό υλικό, αλλά δεν μπορούν να κάνουν αυτοδοκιμές, τεστ γνώσεων, να κερδίσουν και να συλλέξουν κονκάρδες, να εκτελέσουν προσομοιώσεις ή να λάβουν πιστοποιητικά. Για να γίνετε εγγεγραμμένος επισκέπτης στον ιστότοπο, πρέπει να εγγραφείτε.

Το εγχειρίδιο χρήσης παρέχεται στο έγγραφο **User_Manual_for_training-Participants.pdf** στη διεύθυνση https://wiki.cyberphish.eu/. Το έγγραφο αυτό περιγράφει τον τρόπο χρήσης της πλατφόρμας μάθησης.

Περιβάλλον για τους εκπαιδευτικούς

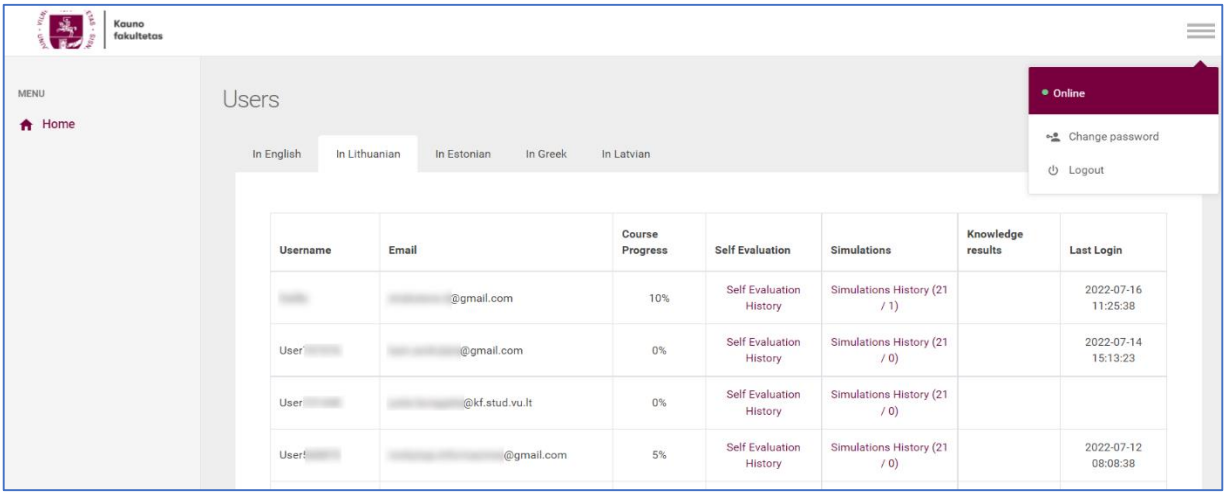
Στο περιβάλλον του καθηγητή, μπορείτε να παρακολουθείτε τους συμμετέχοντες που είναι εγγεγραμμένοι στο σύστημα μάθησης, την πρόοδο της μάθησής τους σε ποσοστά, το ιστορικό των αυτοτελών δοκιμασιών που έγιναν, το ιστορικό των προσομοιώσεων, τους βαθμούς του τεστ γνώσεων, καθώς και την ημερομηνία και την ώρα της τελευταίας σύνδεσης.

Διεύθυνση εισόδου στο περιβάλλον του εκπαιδευτικού: https://cyberphish.vuknf.lt/admin-panel. Το παράθυρο σύνδεσης δίνεται παρακάτω:



Σχήμα 4 Παράθυρο εισόδου στο περιβάλλον Teacher Environment

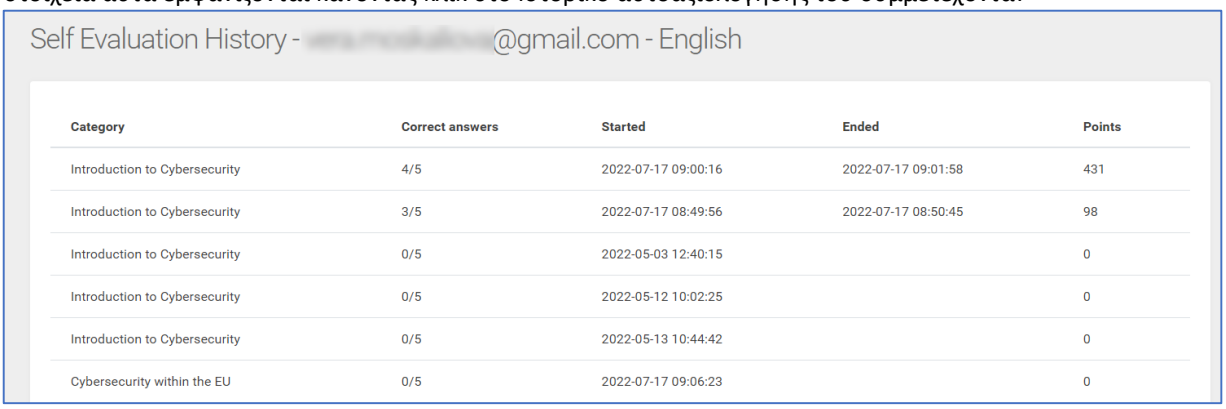
Μόλις εισαχθούν τα στοιχεία σύνδεσης, το σύστημα παρέχει στον εκπαιδευτικό έναν κατάλογο των συμμετεχόντων. Ο καθηγητής μπορεί να παρακολουθεί την πρόοδο της μάθησης των συμμετεχόντων ανά γλώσσα (αγγλικά, λιθουανικά, εσθονικά, ελληνικά και λετονικά). Η κύρια οθόνη του περιβάλλοντος του καθηγητή δίνεται παρακάτω:



Σχήμα 5 Κύρια οθόνη του περιβάλλοντος του εκπαιδευτικού

Ιστορικό δοκιμών αυτοαξιολόγησης

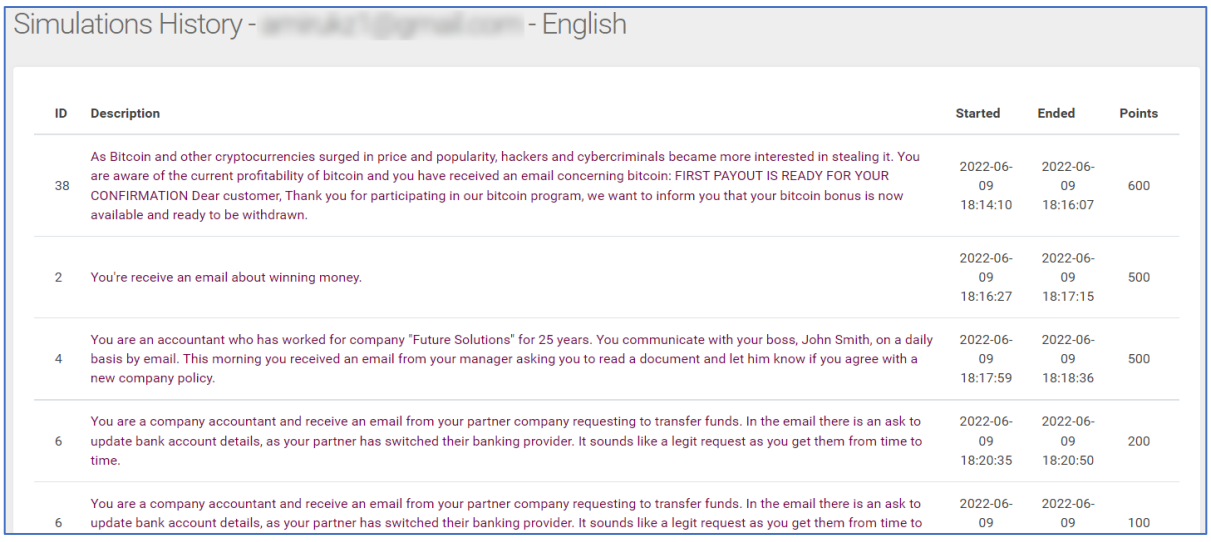
Τα στοιχεία αυτά εμφανίζονται κάνοντας κλικ στο Ιστορικό αυτοαξιολόγησης του συμμετέχοντα:



Εικόνα 6 Ιστορικό αυτοαξιολόγησης του συμμετέχοντα

Ιστορικό προσομοιώσεων

Αυτές οι λεπτομέρειες εμφανίζονται κάνοντας κλικ στο ιστορικό προσομοιώσεων του συμμετέχοντα:



Εικόνα 7 Ιστορικό προσομοιώσεων του συμμετέχοντα

ΕΡΓΑΣΙΑ ΜΕ ΚΑΙΝΟΤΟΜΕΣ ΜΕΘΟΔΟΥΣ (Π.Χ. ΜΕΘΟΔΟΙ ΠΡΟΣΟΜΟΙΩΣΗΣ, ΔΙΑΛΕΞΕΙΣ, ΣΕΜΙΝΑΡΙΑ, ΠΡΑΚΤΙΚΕΣ ΕΚΠΑΙΔΕΥΣΕΙΣ, ΧΡΗΣΗ ΕΡΓΑΛΕΙΩΝ ΔΙΑΔΙΚΤΥΟΥ Κ.ΛΠ.)

Η προσομοίωση μιμείται τις πραγματικές επιθέσεις phishing, παρουσιάζοντας τη διαδικασία στο χρήστη σε παιγνιώδη μορφή.

Ο κύριος στόχος της προσομοίωσης είναι να βοηθήσει τους ανθρώπους να βελτιώσουν την κριτική τους σκέψη σχετικά με την ασφάλεια στον κυβερνοχώρο και το phishing, αναγνωρίζοντας περιπτώσεις phishing, spam, κυβερνοεκφοβισμού κ.λπ. Με βάση το IO1 αναπτύχθηκαν συστάσεις για προσομοιώσεις -με επίκεντρο την προσαρμογή μελετών περιπτώσεων πραγματικής ζωής για τη διαδικασία μάθησης.

Η προσομοίωση περιλαμβάνει περιγραφή της κατάστασης, του σκοπού, των χαρακτήρων, του τύπου της επίθεσης και πολλές (3-4) επιλογές απαντήσεων για τη συμπεριφορά του χρήστη. Οι προσομοιώσεις σχεδιάστηκαν για να αξιολογήσουν την πιθανή/προφανή συμπεριφορά του χρήστη, τις πιθανές σκέψεις/προβληματισμούς και τις αποφάσεις του σε μια τέτοια κατάσταση. Οι προσομοιώσεις που παρουσιάστηκαν αποτελούνται από τρία επίπεδα βάθους. Μόλις επιλεγεί μία από τις επιλογές προβλήματος/κατάσταση, επηρεάζονται και παρουσιάζονται περαιτέρω πιθανές επιλογές για την περίπτωση που πρέπει να επιλυθεί.

Εφαρμόζονται προσομοιώσεις για σκοπούς μάθησης και για σκοπούς ελέγχου γνώσεων. Κατά την επίλυση μιας προσομοίωσης για μαθησιακούς σκοπούς, ο μαθητής βλέπει τις βαθμολογίες που συλλέγονται και το συνολικό συμπέρασμα στο τέλος της προσομοίωσης. Κατά την επίλυση προσομοίωσης για σκοπούς ελέγχου γνώσεων, ο μαθητής βλέπει τις επιλογές που έγιναν κατά τη διάρκεια της προσομοίωσης και λαμβάνει ανατροφοδότηση με σχόλια στο τέλος της προσομοίωσης. Εάν η προσομοίωση επιλύθηκε λανθασμένα, συνιστάται στον χρήστη να επιλύσει την προσομοίωση ξανά.

ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΣΥΣΤΑΣΕΙΣ

Το παρόν έγγραφο απευθύνεται σε όλους τους εκπαιδευτές και μέντορες που παρέχουν συμβουλές και κατάρτιση στους σπουδαστές. Η κοινοπραξία του έργου ελπίζει ότι θα βρουν χρήσιμες οδηγίες σχετικά με τον τρόπο χρήσης του συστήματος και τον τρόπο παροχής κατάρτισης σε άτομα που θέλουν να μάθουν για τις επιθέσεις στον κυβερνοχώρο, ιδίως για το phishing και την κοινωνική μηχανική, καθώς και για όσους θέλουν να μάθουν πώς να αναγνωρίζουν τα κύρια σημάδια τέτοιων απειλών. Οι δυνητικοί χρήστες απαιτείται να έχουν βασικές δεξιότητες ψηφιακού γραμματισμού. Δεν υπάρχουν άλλες προϋποθέσεις για τις γνώσεις ή τις δεξιότητες του χρήστη.

Οι μαθητές και οι εργαζόμενοι δεν έχουν επαρκείς γνώσεις σχετικά με το phishing, την κοινωνική μηχανική, τις επιθέσεις στον κυβερνοχώρο και την ασφάλεια των δεδομένων τους, σύμφωνα με μελέτη που διεξήχθη από εταίρους του έργου το 2020 στην Εσθονία, την Κύπρο, τη Λετονία, τη Λιθουανία και τη Μάλτα (βλ. https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EN_CYBERPHISH-REPORT_survey-results.pdf). Αυτό οδηγεί όχι μόνο σε απώλεια προσωπικών δεδομένων και προσωπικών οικονομικών σε περίπτωση phishing ή κυβερνοεπίθεσης, αλλά και σε απώλεια ευαίσθητων πληροφοριών και οικονομικών πόρων των εταιρειών/οργανισμών.

Με βάση μια μελέτη (βλ. https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A2_EN_CYBERPHISH-REPORT_study-analysis.pdf) που διεξήχθη στις χώρες εταίρους σχετικά με τα προγράμματα σπουδών της τριτοβάθμιας εκπαίδευσης που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, καθώς και με τα προγράμματα κατάρτισης για την ασφάλεια στον κυβερνοχώρο που παρέχονται από ιδιωτικές εταιρείες, αναπτύχθηκε ένα πρόγραμμα σπουδών που καλύπτει τέσσερις ενότητες:

- Εισαγωγή στην κυβερνοασφάλεια,
- Επισκόπηση της ασφάλειας στον κυβερνοχώρο στην ΕΕ,
- Επιθέσεις στον κυβερνοχώρο - Social Engineering και Phishing,
- Κατανόηση και χειρισμός κυβερνοεπιθέσεων

Για περισσότερες πληροφορίες σχετικά με τον τρόπο προετοιμασίας των εκπαιδευτών και των μεντόρων για την εκπαίδευση, δείτε το πλήρες πρόγραμμα σπουδών του CyberPhish (βλ. https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EN_Cyberphish-Full-Curriculum-Final.pdf).

Το εκπαιδευτικό πρόγραμμα CyberPhish έτυχε καλής υποδοχής από τους συμμετέχοντες στην πιλοτική εκπαίδευση. Αναγνώρισαν τη χρησιμότητά του στις καθημερινές δραστηριότητες που σχετίζονται με την πληροφορική τόσο των απλών χρηστών όσο και των υπαλλήλων της εταιρείας. Περισσότερες πληροφορίες θα παρασχεθούν στην έκθεση IO6 A2: Κατευθυντήριες γραμμές για την εφαρμογή του μαθήματος.

Το διαδικτυακό μάθημα μάθησης ενσωματώνει το εκπαιδευτικό υλικό σε μορφή PDF - με συνοπτικό και σαφή τρόπο, χωρίς να επιβαρύνει τους εκπαιδευόμενους με πολύ διάβασμα. Για όσους θέλουν να μάθουν περισσότερα για ένα συγκεκριμένο θέμα, στο τέλος κάθε εγγράφου PDF παρέχονται σύνδεσμοι προς εξωτερικές πηγές.

Τα τεστ αυτοαξιολόγησης και οι προσομοιώσεις χρησιμοποιούνται για να βοηθήσουν τους συμμετέχοντες να αφομοιώσουν καλύτερα το εκπαιδευτικό υλικό. Οι προσομοιώσεις παρέχουν ανατροφοδότηση, η οποία βοηθά είτε στην επανάληψη του εκπαιδευτικού υλικού είτε στην εκμάθηση νέων πραγμάτων. Επιπλέον, οι προσομοιώσεις μπορούν να χρησιμοποιηθούν με δύο τρόπους κατά τη διάρκεια του μαθήματος: για μάθηση και για έλεγχο γνώσεων.

Το μάθημα μπορεί να απευθύνεται στους φοιτητές ως μέρος ενός μαθήματος, ως συμπληρωματικό υλικό ή ως ξεχωριστή ενότητα/μάθημα.

ΑΝΑΦΟΡΈΣ

1. IO1 A1: Αναγνώριση του Phishing και έκθεση για τα κενά δεξιοτήτων
   https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EN_CYBERPHISH-REPORT_survey-results.pdf
2. IO1 A2: Ανάλυση των υφιστάμενων προγραμμάτων κατάρτισης για την ασφάλεια στον κυβερνοχώρο.
   https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A2_EN_CYBERPHISH-REPORT_study-analysis.pdf
3. IO2 A1: Σύντομη έκδοση των προγραμμάτων σπουδών για διάδοση
   https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A1_EN_Cyberphish-Short-Curriculum-Final.pdf
4. IO2 A2: Εκτεταμένη έκδοση των προγραμμάτων σπουδών για την ανάπτυξη εκπαιδευτικού υλικού και για εκπαιδεύσεις
   https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EN_Cyberphish-Full-Curriculum-Final.pdf
5. User_Manual_for_training-Participants.pdf [
   σύνδεσμος]

Παραρτήματα

Παράρτημα 1. Παράδειγμα ηλεκτρονικής πρόσκλησης για το μάθημα CyberPhish

Παράδειγμα έντυπης φόρμας πρόσκλησης για το μάθημα CyberPhish

We kindly invite you to participate in the online course about phishing!

Registration to online course:

Name and Surname _____

Name of education institution _____

Email _____

Duration of pilot training **4-6 week**.

You will learn about **phishing attacks** through an online training material and a scenarios in which you will have to recognise whether or not it is a phishing case and what actions you would take in such a situation.

The scenarios tool will help you **better understand fraud** and **gain knowledge interactively**.

All course participants completed the course will be **awarded certificates**.
Participants completed course with highest scores will be **awarded prizes**.

Course participants will develop competences that will help them to highlight threats and take appropriate preventive measures.

Trainings are organized in the framework of the CyberPhish (Safeguarding against Phishing in the age of 4th Industrial Revolution) project which is funded under the Erasmus+ programme.

All personal data contained in this document is collected during the implementation of the Erasmus + Program (2014-2020), according to the European Commission's regulations. These will be stored and processed by Program Beneficiary Organizations, NA, EC in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of these data and repealing Directive 95/46 / EC (General Data Protection Directive - GDPR). The beneficiary organizations of the Program, EC, NA will store and process these data according to Regulation (EC) no. No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. During the event, photographs and / or films will be taken for purposes of promoting and disseminating the results of Erasmus + funded projects. The materials will not affect your personal or institutional image. By registering to this event you consent to being filmed and / or photographed for the aforementioned reasons.

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Παράρτημα 2. Παράδειγμα πιστοποιητικού ολοκλήρωσης μαθημάτων CyberPhish

CERTIFICATE

OF COMPLETION ONLINE COURSE

Name Surname

has successfully completed the online training course

Safeguarding against Phishing in the age of 4th Industrial Revolution

This certificate was awarded on 12 May, 2022

CyberPhish

Project funding source: Erasmus+ KA2 Strategic Partnerships.
CyberPhish Project No 2020-1-LT01-KA203-078070,
https://cyberphish.eu

Funded by the
Erasmus+ Programme
of the European Union

Παράρτημα 3. Παράδειγμα ερωτηματολογίου μετά το μάθημα για τους συμμετέχοντες στο μάθημα CyberPhish

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Post-Course Questionnaire for participants

This survey is part of an EU funded CyberPhish project to design and develop e-learning materials, blended learning environment, knowledge and skills self-evaluation and knowledge evaluation system simulations for students and other users in order to prevent from phishing attacks, raise competencies in this area for identification and prevention of threats.

This survey will gather information from course participants who have completed the CyberPhish course. The data will only be used for the purpose of the project.

The survey should take approximately 10-15 minutes to complete.

Thank you for your cooperation and your time.m

[redacted]@gmail.com (nebendrinama)
Perjungti paskyrą

*Privaloma

Gender *

- ◯ Male
- ◯ Female
- ◯ Other

Occupation *

- ◯ Student
- ◯ Employee
- ◯ Self-employed
- ◯ Business owners
- ◯ Other

How would you evaluate your knowledge on these cybersecurity subjects after finishing the CyberPhish course *

	I have gained a lot of new knowledge about phishing	I have improved my knowledge about phishing	I haven't learnt anything new
Legal Aspects of Cybersecurity	○	○	○
The tendencies of Cybersecurity landscape	○	○	○
Social engineering	○	○	○
Psychological aspects of social engineering	○	○	○
Types of Phishing Attacks and Techniques	○	○	○
Recognising Phishing Attacks	○	○	○
Proactive actions of cyber incidents	○	○	○
Handling Cyber-attacks	○	○	○

How would you evaluate your knowledge on these cybersecurity subjects after finishing the CyberPhish course *

	Satisfied	Neutral	Dissatidfied	I have no opinion
Introduction to Cybersecurity	○	○	○	○
Overview of Cybersecurity within the EU	○	○	○	○
Cyber-attacks – Social Engineering and Phishing	○	○	○	○
Understanding and Handling Cyber-attacks	○	○	○	○

Your experience using simulations *

	Strongly helped	Helped	Not helped	I have no opinion
Did the simulations help to improve your skills recognising phishing?	○	○	○	○

Please rate your experience of the following elements of the CyberPhish course? *

	Strongly agree	Agree	Disagree	Strongly disagree
I had a clear understanding of the course objectives	○	○	○	○
I found the online approach to learning was suitable for the course	○	○	○	○
I found the course content covered the course objectives	○	○	○	○
I found the amount of time given to complete the course to be ample	○	○	○	○
I found the training and support throughout the course to be appropriate	○	○	○	○

I would recommend this course to other people	○	○	○	○
The online learning platform was easy to use	○	○	○	○

What are the main benefits you gained from completing the CyberPhish course? (Please provide one or two sentences)

Jūsų atsakymas

Was there anything missing from the course or anything that could have been improved? (Please provide one or two sentences)

Jūsų atsakymas

Thank you for your participation in this survey and for completing the CyberPhish course!

Pateikti Puslapis 1 iš 1 Valyti formą

Παράρτημα 4. Παράδειγμα ερωτηματολογίου μετά το μάθημα για τους εκπαιδευτές, τους συμβούλους και τους μέντορες των μαθημάτων CyberPhish

CyberPhish
Safeguarding your digital future

Funded by the
Erasmus+ Programme
of the European Union

Post-Course Questionnaire for trainers/ consultants/ mentors

This survey is part of an EU funded project to design and develop e-learning materials, blended learning environment, knowledge and skills self-evaluation and knowledge evaluation system simulations for students and other users in order to prevent from phishing attacks, raise competencies in this area for identification and prevention of threats.

This survey will gather information from CyberPhish course teachers/consultants/mentors. This survey will help to evaluate the project's pilot trainings.

The survey should take approximately 10-15 minutes to complete.

Thank you for your cooperation and your time.

[redacted]@gmail.com (nebendrinama)
Perjungti paskyrą

*Privaloma

Name *

Jūsų atsakymas

Country *

- ◯ Lithuania
- ◯ Latvia
- ◯ Estonia
- ◯ Malta
- ◯ Cyprus

Please indicate how strongly you agree or disagree with the following statements *

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
The structure and content of the course motivated participants to complete it.	○	○	○	○	○
The time provided for participants to complete the pilot course was sufficient.	○	○	○	○	○
Areas of topics covered by the course were appropriate for the target audience.	○	○	○	○	○
The appropriate amount of detail was provided for the topics covered by the programme.	○	○	○	○	○

What other additional support or resources could have helped to organise the course

Jūsų atsakymas

Please indicate how much you agree or disagree with the following statement *

	Fully achieved	Achieved to a high extent	Achieved to a low extent	Not achieved
To what extent has CyberPhish achieved its goal of introducing cybersecurity and phishing to students	○	○	○	○

Other comments, suggestions

Jūsų atsakymas

Thank you for your participation in this survey and for completing the CyberPhish course!