Διασφάλιση κατά του Phishing στην εποχή της 4ης Βιομηχανικής Επανάστασης (CyberPhish)

A2: Κατευθυντήριες γραμμές για την εφαρμογή

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.

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

Στην εποχή της 4ης βιομηχανικής επανάστασης, η ασφάλεια στον κυβερνοχώρο αποτελεί μία από τις μεγαλύτερες προκλήσεις. Η ευρεία χρήση ψηφιακών συσκευών και συστημάτων πληροφοριών γίνεται όλο και πιο ελκυστική για τους εγκληματίες του κυβερνοχώρου. Σύμφωνα με στοιχεία της Eurostat, "...το 2019, περίπου ένας στους τρεις πολίτες της ΕΕ ηλικίας 16 έως 74 ετών ανέφερε περιστατικά που σχετίζονται με την ασφάλεια κατά τη χρήση του διαδικτύου για ιδιωτικούς σκοπούς το 2019 κατά τους τελευταίους 12 μήνες. Κατά τη διάρκεια αυτής της περιόδου το phishing ήταν το πιο συχνό περιστατικό ασφάλειας που αναφέρθηκε το 2019". Στην πράξη, κανένα πληροφοριακό σύστημα ή λογισμικό ασφαλείας δεν μπορεί να παρέχει 100% προστασία από επιθέσεις phishing. Η καταπολέμηση αυτών των απειλών δεν αφορά μόνο τις λύσεις ασφαλείας υλικού και λογισμικού, αλλά και την ανθεκτικότητα του χρήστη στις απειλές αυτές και την ικανότητά του να τις αναγνωρίζει.

Οι επιθέσεις στον κυβερνοχώρο στοχεύουν επίσης επιχειρήσεις στην Ευρώπη. Σύμφωνα με την παγκόσμια έρευνα για την κατάσταση της ασφάλειας των πληροφοριών το 2017, περίπου το 80% των ευρωπαϊκών εταιρειών αντιμετώπισαν τουλάχιστον ένα περιστατικό ασφάλειας στον κυβερνοχώρο εκείνο το έτος, ενώ οι εργαζόμενοι ήταν υπεύθυνοι για το 27% όλων των περιστατικών ασφάλειας στον κυβερνοχώρο.

Έτσι, μόνο ένας άνθρωπος - ένας χρήστης που κατανοεί πώς λειτουργεί ένας εγκληματίας στον κυβερνοχώρο και μπορεί να αναγνωρίσει τα προειδοποιητικά σημάδια κακόβουλης δραστηριότητας, μπορεί να βοηθήσει στην πρόληψη επιθέσεων στον κυβερνοχώρο, όπως το phishing.

Σύμφωνα με τον ENISA, τα θέματα που σχετίζονται με τον κυβερνοχώρο υποεκπροσωπούνται μεταξύ των φοιτητών μη τεχνικών προγραμμάτων. Ως εκ τούτου, είναι σκόπιμο να αναπτυχθεί και να προσφερθεί στο κοινό ένα ευρέως προσβάσιμο διαδικτυακό εκπαιδευτικό πρόγραμμα σχετικά με τον τρόπο αναγνώρισης του phishing.

Για τους λόγους αυτούς, ξεκίνησε και υλοποιήθηκε το διεθνές πρόγραμμα "Διασφάλιση κατά του Phishing στην εποχή της 4ης βιομηχανικής επανάστασης" (CyberPhish). Η Ευρωπαϊκή Ένωση χρηματοδότησε το έργο στο πλαίσιο του προγράμματος Erasmus+. Το έργο συντονίστηκε από τη Σχολή Κάουνας του Πανεπιστημίου του Βίλνιους, με εταίρους του έργου το Tartu Ulikool (Εσθονία), τη Dorea (Κύπρος), το MECB (Μάλτα), την Altacom (Λετονία) και το Ινστιτούτο Πληροφορικής (Λιθουανία). Η διάρκεια του έργου είναι από τον Νοέμβριο του 2020 έως τον Νοέμβριο του 2022.

Ο κύριος στόχος του έργου "CyberPhish" είναι να εκπαιδεύσει τους φοιτητές της τριτοβάθμιας εκπαίδευσης, τους καθηγητές, το πανεπιστημιακό προσωπικό (μέλη της κοινότητας), τα εκπαιδευτικά κέντρα και τον επιχειρηματικό τομέα (εργοδότες και εργαζόμενους) και να προωθήσει την κριτική σκέψη στον τομέα της ασφάλειας στον κυβερνοχώρο μεταξύ της ομάδας στόχου.

Το έργο Cyberphish στοχεύει στην ανάπτυξη ενός προγράμματος σπουδών, υλικού ηλεκτρονικής μάθησης, ενός μικτού περιβάλλοντος μάθησης, προσομοιώσεων, τεστ αυτοαξιολόγησης και αξιολόγησης γνώσεων. Το αναπτυγμένο μάθημα CyberPhish δίνει τη δυνατότητα στους χρήστες να προστατεύονται από επιθέσεις phishing. Οι χρήστες αποκτούν ικανότητες που θα τους βοηθήσουν να δίνουν προσοχή στις απειλές και να λαμβάνουν τα απαραίτητα μέτρα πρόληψης.

Το έργο ανέπτυξε ένα πνευματικό προϊόν για την εκπαίδευση της κριτικής σκέψης και των δεξιοτήτων των χρηστών στον εντοπισμό του phishing. Οι χρήστες θα μάθουν να αναγνωρίζουν τα σημάδια phishing (κόκκινες σημαίες), τις τεχνικές κοινωνικής μηχανικής και τις δεξιότητες ασφάλειας στον κυβερνοχώρο. Η μικτή προσέγγιση/έννοια μάθησης θα επιτρέψει στους χρήστες να προετοιμαστούν για ένα τεστ γνώσεων και να λάβουν πιστοποιητικό ολοκλήρωσης.

Οι εταίροι του έργου χρησιμοποίησαν τη διαδικτυακή πλατφόρμα μάθησης που καλύπτει εκπαιδευτικό υλικό, προσομοιώσεις, τεστ αυτοαξιολόγησης και τεστ αξιολόγησης γνώσεων στην πιλοτική εκπαίδευση σε πέντε χώρες εταίρους. Με βάση την εμπειρία αυτή, αναπτύχθηκαν οι παρούσες κατευθυντήριες γραμμές.

Σκοπός των κατευθυντήριων γραμμών

Οι παρούσες κατευθυντήριες γραμμές έχουν ως στόχο να παρουσιάσουν τα αποτελέσματα του έργου, τις βέλτιστες πρακτικές πιλοτικής εφαρμογής και μια μεθοδολογία για την ανάπτυξη ενός εκπαιδευτικού προγράμματος CyberPhish για το κοινό-στόχο και τους ενδιαφερόμενους φορείς. Οι κατευθυντήριες γραμμές απευθύνονται σε οργανισμούς που ενδιαφέρονται να προσαρμόσουν και να χρησιμοποιήσουν το υλικό που αναπτύχθηκε για να εκπαιδεύσουν τους χρήστες του Διαδικτύου στην αναγνώριση του phishing: ιδρύματα τριτοβάθμιας εκπαίδευσης, κέντρα εκπαίδευσης/κατάρτισης ενηλίκων, επιχειρηματικός τομέας.

Στόχοι των κατευθυντήριων γραμμών

Ο κύριος στόχος των κατευθυντήριων γραμμών για την εφαρμογή του "CyberPhish" είναι να παρουσιάσει τα εργαλεία, το περιεχόμενο και τη διαδικασία οργάνωσης της κατάρτισης. Κατά τη διάρκεια αυτής της διαδικασίας, οι συμμετέχοντες αποκτούν τις γνώσεις και τις δεξιότητες που απαιτούνται για τον εντοπισμό επιθέσεων phishing στην εργασία και στην προσωπική τους ζωή και προετοιμάζονται για ένα τεστ γνώσεων. Με την επιτυχή ολοκλήρωση της εκπαίδευσης θα τους απονεμηθεί πιστοποιητικό. Η διαδικασία υλοποίησης βασίζεται στην εμπειρία των συμμετεχουσών χωρών-εταίρων.

2. ΚΥΒΕΡΝΟΑΣΦΆΛΕΙΑ, PHISHING ΚΑΙ ΚΟΙΝΩΝΙΚΉ ΜΗΧΑΝΙΚΉ

2.1 Κυβερνοασφάλεια και Phishing στα προγράμματα σπουδών

Από το 2013, η Ευρωπαϊκή Επιτροπή τονίζει τη σημασία του θέματος της ασφάλειας στον κυβερνοχώρο. Η πρώτη στρατηγική για την ασφάλεια στον κυβερνοχώρο υπογραμμίζει την ευαισθητοποίηση και την ανάπτυξη δεξιοτήτων ως βασικούς στρατηγικούς στόχους. Η έκθεση του ENISA του 2017 υπογραμμίζει επίσης τη σημασία της ασφάλειας στον κυβερνοχώρο. Συνιστά στα κράτη μέλη της ΕΕ να ενισχύσουν την εκπαίδευση και τις δεξιότητες στον τομέα της κυβερνοασφάλειας (ENISA, 2019, σ. 23). Ως αποτέλεσμα, όλα τα κράτη μέλη της ΕΕ έχουν αναπτύξει και δημοσιεύσει τις εθνικές στρατηγικές τους για την ασφάλεια στον κυβερνοχώρο (NCSS).

Τον Μάρτιο του 2021, το Ευρωπαϊκό Συμβούλιο ενέκρινε νέα συμπεράσματα σχετικά με τη στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο[1] . Τα συμπεράσματα αναγνωρίζουν την έλλειψη ψηφιακών δεξιοτήτων και δεξιοτήτων κυβερνοασφάλειας και υπογραμμίζουν την ανάγκη να καλυφθεί η ζήτηση της αγοράς με την περαιτέρω ανάπτυξη προγραμμάτων εκπαίδευσης και κατάρτισης.

Το έργο CyberPhish διερεύνησε τα υπάρχοντα προγράμματα σπουδών και κατάρτισης σε θέματα ασφάλειας στον κυβερνοχώρο και phishing στις χώρες-εταίρους Κύπρο, Εσθονία, Λετονία, Λιθουανία και Μάλτα. Επικεφαλής της μελέτης ήταν το Εκπαιδευτικό Ινστιτούτο DOREA. Τα κύρια ευρήματα της μελέτης ήταν τα εξής:

- Η ανάλυση των προγραμμάτων σπουδών των ΑΕΙ σε όλες τις χώρες εταίρους του έργου, εκτός από την Εσθονία, δεν περιλαμβάνει θέματα phishing και κοινωνικής μηχανικής ως ξεχωριστές ενότητες. Ωστόσο, μπορεί κανείς να ενσωματώσει πληροφορίες σχετικά με αυτά τα θέματα σε άλλες ενότητες μαθημάτων. Δύο προγράμματα σπουδών ΑΕΙ στην Εσθονία περιλαμβάνουν ενότητες σπουδών που επικεντρώνονται στην κοινωνική μηχανική. Η μέση διάρκεια αυτών των ενοτήτων είναι 4,5 ECTS.
- Τα αναλυθέντα προγράμματα σπουδών των ΑΕΙ στην Εσθονία, τη Λετονία και τη Μάλτα περιλαμβάνουν ενότητες μαθημάτων για κοινωνικές δεξιότητες, όπως δεξιότητες επικοινωνίας, επιχειρηματικότητα, ψυχολογία κ.λπ. Αντίθετα, τα προγράμματα σπουδών ΑΕΙ στην Κύπρο και τη Λιθουανία επικεντρώνονται κυρίως στις σκληρές δεξιότητες, δίνοντας λιγότερη έμφαση στη σημασία των κοινωνικών δεξιοτήτων.
- Σε όλες τις χώρες-εταίρους, ορισμένοι δημόσιοι και ιδιωτικοί οργανισμοί προσφέρουν μαθήματα κατάρτισης στην κυβερνοασφάλεια που απευθύνονται σε επαγγελματίες της κυβερνοασφάλειας και της πληροφορικής, σε εταιρείες, σε υπαλλήλους και στο ευρύ κοινό. Ενώ τα εκπαιδευτικά μαθήματα μικρότερης διάρκειας τείνουν να επικεντρώνονται αποκλειστικά στις απειλές, όπως το phishing, η κοινωνική μηχανική και οι τρόποι αυτοπροστασίας, τα εκπαιδευτικά μαθήματα μεγαλύτερης διάρκειας παρέχουν μια ευρύτερη προοπτική για την κυβερνοασφάλεια. Υπάρχουν επίσης ορισμένοι οργανισμοί που προσφέρουν δοκιμές διείσδυσης και κοινωνικής μηχανικής με στόχο τις εταιρείες και τους υπαλλήλους τους.

Τα δεδομένα που συγκεντρώθηκαν από την έρευνα βοήθησαν στον εντοπισμό των ελλείψεων δεξιοτήτων και στην ανάπτυξη συστάσεων για ένα νέο πρόγραμμα κατάρτισης, το CyberPhish. Το πρόγραμμα αυτό αποσκοπεί στην ενίσχυση των δεξιοτήτων και της ευαισθητοποίησης των χρηστών του διαδικτύου και στην εκπαίδευσή τους σχετικά με τα πιο πρόσφατα θέματα και απειλές της ασφάλειας στον κυβερνοχώρο, ιδίως το phishing.

[1] Συμβούλιο της Ευρωπαϊκής Ένωσης (2021): Σχέδιο συμπερασμάτων του Συμβουλίου σχετικά με τη στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο για την ψηφιακή δεκαετία, URL https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy (πρόσβαση 09/09/2022)

2.2. Αναγνώριση του Phishing και της κοινωνικής μηχανικής

Η ασφάλεια στον κυβερνοχώρο αποτελεί επίσης ζήτημα για τις ευρωπαϊκές επιχειρήσεις. Οι εταιρείες γίνονται όλο και περισσότερο στόχοι κυβερνοεπιθέσεων. Καθώς οι εγκληματίες γίνονται όλο και πιο εξελιγμένοι, οι κυβερνοεπιθέσεις καθίστανται όλο και πιο δύσκολο να εντοπιστούν και να αποτραπούν, και χρησιμοποιούνται νέες μέθοδοι και πλατφόρμες για την πραγματοποίηση τέτοιων επιθέσεων. Σύμφωνα με την παγκόσμια έρευνα για την κατάσταση της ασφάλειας των πληροφοριών το 2017, περίπου το 80% των ευρωπαϊκών επιχειρήσεων αντιμετώπισε τουλάχιστον ένα περιστατικό ασφάλειας στον κυβερνοχώρο εκείνο το έτος. Σύμφωνα με την έρευνα, οι εργαζόμενοι ευθύνονται για το 27% όλων των περιστατικών κυβερνοασφάλειας. Μόνο το πρώτο τρίμηνο του 2019, οι εταιρείες παγκοσμίως έγιναν στόχος κυβερνοεπιθέσεων 120% συχνότερα από ό,τι το 2018 και υπέστησαν τεράστιες απώλειες (22,2 δισ. ευρώ).

Όπως αναφέρει η Human Factor Report 2019, πάνω από το 99% των μηνυμάτων ηλεκτρονικού ταχυδρομείου που διανέμουν κακόβουλο λογισμικό απαιτούν ανθρώπινη παρέμβαση, δηλαδή την παρακολούθηση συνδέσμων, το άνοιγμα εγγράφων, την αποδοχή προειδοποιήσεων ασφαλείας και άλλες συμπεριφορές [5].

Επομένως, είναι απαραίτητο να εκπαιδεύσουμε και να ευαισθητοποιήσουμε τους πολίτες σε αυτόν τον τομέα. Η ανθεκτικότητα στον κυβερνοχώρο απαιτεί την εξήγηση/διδασκαλία του τρόπου αναγνώρισης του phishing με τρόπο κατανοητό και προσιτό στους περισσότερους ανθρώπους. Η γνώση των προειδοποιητικών σημάτων και η κατανόηση των μεθόδων των εγκληματιών θα κάνει πρώτον τους χρήστες του διαδικτύου inter να αισθάνονται πιο σίγουροι και ασφαλείς και δεύτερον θα τους βοηθήσει να αποτρέψουν ή τουλάχιστον να επιβραδύνουν την εξάπλωση τέτοιων επιθέσεων.

Το "ψάρεμα" είναι παράνομο για την απόσπαση προσωπικών δεδομένων ενός χρήστη (στοιχεία σύνδεσης, στοιχεία πιστωτικής κάρτας κ.λπ.) με τη χρήση τεχνικών κοινωνικής μηχανικής. Οι εγκληματίες δραστηριοποιούνται στα κοινωνικά δίκτυα, στέλνοντας μηνύματα ηλεκτρονικού ταχυδρομείου και κάνοντας τηλεφωνήματα. Τα μηνύματα αυτά έχουν ως στόχο να πείσουν τον χρήστη να ανοίξει ένα κακόβουλο συνημμένο αρχείο ή να κάνει κλικ σε έναν ψεύτικο διαδικτυακό σύνδεσμο, αποκαλύπτοντας τον κωδικό πρόσβασής του. [6]

Οι πιο συνηθισμένοι τύποι phishing είναι τα εξής: Spray and pray, Cat phishing, Advanced fee scam, Spear phishing, Whaling, Vishing, Smishing, Angler Phishing, Clone Phishing και Malvertising.

Στο πλαίσιο της ασφάλειας των πληροφοριών, η κοινωνική μηχανική ορίζεται ως η ψυχολογική χειραγώγηση των ανθρώπων για την εκτέλεση ενεργειών ή την αποκάλυψη εμπιστευτικών πληροφοριών. Ο ENISA αναφέρει ότι η κοινωνική μηχανική παραμένει κορυφαία απειλή για τη διευκόλυνση άλλων τύπων εγκλημάτων στον κυβερνοχώρο, καθώς το 84% των επιθέσεων στον κυβερνοχώρο βασίζονται στην κοινωνική μηχανική. Ο αριθμός των θυμάτων phishing συνεχίζει να αυξάνεται, καθώς εκμεταλλεύεται την ανθρώπινη διάσταση που είναι ο πιο αδύναμος κρίκος [6].

Οι τεχνικές κοινωνικής μηχανικής βασίζονται σε ανθρώπινες αδυναμίες όπως η απληστία, ο φόβος, η περιέργεια, η εμπιστοσύνη, η ενσυναίσθηση και η βιασύνη. Ως εκ τούτου, ένα προσεκτικά σχεδιασμένο και εξατομικευμένο μήνυμα ηλεκτρονικού ταχυδρομείου, φωνητικό μήνυμα, τηλεφώνημα ή γραπτό μήνυμα μπορεί να επηρεάσει τους ανθρώπους να αποκαλύψουν τις εμπιστευτικές πληροφορίες τους, να κάνουν κλικ σε έναν κακόβουλο σύνδεσμο, να κατεβάσουν και να ανοίξουν ένα αρχείο που περιέχει κακόβουλο λογισμικό ή ακόμη και να μεταφέρουν χρήματα στον εγκληματία.

Ο Dr. Robert B. Cialdini στο βιβλίο του "Influence: The Psychology of Persuasion", περιέγραψε έξι αρχές της πειθούς οι οποίες υιοθετήθηκαν και χρησιμοποιήθηκαν εύκολα στην κοινωνική μηχανική και στο phishing. Αργότερα επεκτάθηκαν σε επτά: Αμοιβαιότητα, Σπανιότητα, Εξουσία, Συνέπεια, Συναίνεση, Συμπάθεια και Ενότητα. Οι απατεώνες που χρησιμοποιούν τέτοιες τεχνικές μπορούν να αναμένουν επιτυχή αποτελέσματα από τις επιθέσεις που δημιουργούν. Επομένως, είναι ιδιαίτερα σημαντικό να εκπαιδεύονται οι άνθρωποι, ώστε να γνωρίζουν πώς να αναγνωρίζουν και να αποφεύγουν τέτοιες επιθέσεις. [7; 8; 9]

Οι εταίροι του έργου διεξήγαγαν έρευνα για να διαπιστώσουν πώς οι άνθρωποι αναγνωρίζουν τις επιθέσεις phishing, να προσδιορίσουν την ευαισθητοποίηση των ανθρώπων σχετικά με το phishing και τους διάφορους τύπους phishing και να εντοπίσουν τα κενά δεξιοτήτων στις χώρες εταίρους Κύπρο, Εσθονία, Λετονία, Λιθουανία και Μάλτα. Τα αποτελέσματα της μελέτης είναι διαθέσιμα στην έκθεση μελέτης "Αναγνώριση του phishing και κενά δεξιοτήτων". [7]

Πεντακόσια δεκατέσσερα άτομα έλαβαν μέρος στην έρευνα, εκ των οποίων 259 ήταν γυναίκες, 248 άνδρες και 7 άτομα προτίμησαν να μην προσδιορίσουν το φύλο τους. Οι περισσότεροι ερωτηθέντες είναι φοιτητές (304), ακολουθούμενοι από εργαζόμενους (139), ιδιοκτήτες επιχειρήσεων (53), ανέργους (10) και αυτοαπασχολούμενους (8). Οι περισσότεροι από τους ερωτηθέντες στην έρευνα είναι υψηλά μορφωμένοι - με την πλειοψηφία των ερωτηθέντων (38%) να έχουν πτυχίο, ακολουθούμενο από μεταπτυχιακό (23%) και διδακτορικό (6%).

Είναι ενδιαφέρον ότι σχεδόν ένας στους πέντε ερωτηθέντες ανέφερε ότι έχει πέσει θύμα επίθεσης phishing στο παρελθόν. Οι πιο συνηθισμένες επιθέσεις phishing συνέβησαν κατά το κλικ σε συνδέσμους σε μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα, το άνοιγμα συνημμένων αρχείων ή την απάντηση σε μηνύματα ηλεκτρονικού ταχυδρομείου και την παροχή εμπιστευτικών δεδομένων. Οι συνηθέστεροι λόγοι για αυτές τις επιθέσεις ήταν η απόσπαση της προσοχής, η περιέργεια ή η βιασύνη. Οι περισσότεροι ερωτηθέντες (74%) δεν έχουν παρακολουθήσει καμία εκπαίδευση ή σεμινάριο για την ασφάλεια στον κυβερνοχώρο. Περισσότεροι από τους μισούς ερωτηθέντες (54%) δήλωσαν ότι είχαν αναπτύξει ενδιαφέρον για τον τομέα αυτό ανεξάρτητα. Όλα αυτά δείχνουν μια αυξανόμενη ανάγκη για γνώση σχετικά με το phishing και την ασφάλεια στον κυβερνοχώρο.

3. ΠΡΌΓΡΑΜΜΑ ΣΠΟΥΔΏΝ ΓΙΑ ΤΟ CYBERPHISH

Με βάση μια ανάλυση αναγκών, η κοινοπραξία εταίρων ανέπτυξε ένα πρόγραμμα κατάρτισης σχετικά με την ασφάλεια στον κυβερνοχώρο, τις κυβερνοεπιθέσεις, την κοινωνική μηχανική, με ιδιαίτερη έμφαση στον εντοπισμό και την πρόληψη του phishing.

Στόχος του προγράμματος σπουδών είναι να προσφέρει μια εισαγωγή στην ασφάλεια στον κυβερνοχώρο, με έμφαση στις επιθέσεις phishing. Το πρόγραμμα μαθημάτων απευθύνεται σε ιδιώτες, φοιτητές, επιχειρηματίες, υπαλλήλους οργανισμών και θα τους προετοιμάσει για τις απειλές ασφάλειας της εποχής της τέταρτης βιομηχανικής επανάστασης. Το μάθημα θα παρέχει στους εκπαιδευόμενους τις δεξιότητες για τον εντοπισμό και τη διαχείριση κυβερνοεπιθέσεων και την προστασία συσκευών και δεδομένων.

Το πρόγραμμα σπουδών έχει σχεδιαστεί για μικτή μάθηση, αλλά η δομή του το καθιστά ευέλικτο και μπορεί να χρησιμοποιηθεί τόσο για εξ αποστάσεως όσο και για δια ζώσης εκπαίδευση. Το πλήρες πρόγραμμα κατάρτισης αποτελείται από 30 ώρες που αντιστοιχούν σε 1 ECTS. Προτείνεται να ληφθεί υπόψη ο ίδιος αριθμός ωρών ανά ενότητα για αυτοδιδασκαλία και αξιολόγηση.

Το πρόγραμμα σπουδών είναι δομημένο σε τέσσερα διακριτά μέρη (ενότητες):

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.

Το πλήρες Πρόγραμμα Σπουδών μπορείτε να το βρείτε στην ιστοσελίδα του CyberPhish: https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EN_Cyberphish-Full-Curriculum-Final.pdf

4. ΔΙΟΡΓΆΝΩΣΗ ΠΙΛΟΤΙΚΉΣ ΕΚΠΑΊΔΕΥΣΗΣ CYBERPHISH

Η πιλοτική εκπαίδευση έχει σχεδιαστεί για να εκπαιδεύσει τους συμμετέχοντες να αναγνωρίζουν τις επιθέσεις phishing, να κατανοούν την κοινωνική μηχανική και να μαθαίνουν νέες και να βελτιώνουν τις υπάρχουσες δεξιότητες. Η αίτηση διευκρινίζει ότι τα προϊόντα που αναπτύσσονται κατά τη διάρκεια του έργου πρέπει να δοκιμαστούν πιλοτικά για την αξιολόγηση των αποτελεσμάτων και, εάν είναι απαραίτητο, για την προσαρμογή τους υπό το φως των σχολίων και των ανατροφοδοτήσεων των συμμετεχόντων και των εκπαιδευτικών/καθοδηγητών.

Συμμετέχοντες. Η πιλοτική κατάρτιση πραγματοποιήθηκε σε όλες τις χώρες εταίρους του έργου - Κύπρο, Εσθονία, Λετονία, Λιθουανία και Μάλτα. Συμμετείχαν μεταξύ άλλων:

- Φοιτητές τριτοβάθμιας εκπαίδευσης,
- Προσωπικό από ιδρύματα και οργανισμούς τριτοβάθμιας εκπαίδευσης,
- Εκπαιδευτικοί και προσωπικό από κέντρα εκπαίδευσης ενηλίκων.

Κάθε οργάνωση-εταίρος εκπαίδευσε τουλάχιστον 24 συμμετέχοντες στη χώρα της, επεκτείνοντας έτσι τον αντίκτυπο του έργου πέρα από τη δική της οργάνωση.

Διάρκεια. Με συμφωνία μεταξύ των εταίρων, η πιλοτική εκπαίδευση διήρκεσε αρκετούς μήνες (Μάιος-Σεπτέμβριος), λαμβάνοντας υπόψη τις θερινές διακοπές κάθε εταίρου. Ορισμένοι εταίροι μπόρεσαν να πραγματοποιήσουν την πιλοτική κατάρτιση στο τέλος του ακαδημαϊκού έτους, δηλαδή τον Μάιο, στο τέλος του εαρινού εξαμήνου. Άλλοι εταίροι μπορούσαν να ξεκινήσουν στην αρχή του ακαδημαϊκού έτους, τον Σεπτέμβριο, και να συγκεντρώσουν τους συμμετέχοντες για την πιλοτική κατάρτιση μέχρι το τέλος Σεπτεμβρίου.

Ο τρόπος. Η πιλοτική εκπαίδευση μπορεί να οργανωθεί ως μάθημα μικτής μάθησης ή, δεδομένων των περιορισμών της πανδημίας Covid-19, μπορεί να οργανωθεί εξ αποστάσεως.

Το Πανεπιστήμιο του Βίλνιους και το Πανεπιστήμιο του Ταρτού πραγματοποίησαν πιλοτικά την εκπαίδευση στους δικούς τους οργανισμούς, ενσωματώνοντας το μάθημα Cyberphish στα αντικείμενα σπουδών τους. Οι άλλοι εταίροι, Altacom, Dorea και MECB, διεξήγαγαν την πιλοτική κατάρτιση σε συνεργασία με άλλα ιδρύματα τριτοβάθμιας εκπαίδευσης ή προσκαλώντας εξωτερικούς συμμετέχοντες.

Πλατφόρμα μάθησης. Η πλατφόρμα εκμάθησης CyberPhish αναπτύχθηκε και δοκιμάστηκε σε πέντε γλώσσες - αγγλικά, εσθονικά, ελληνικά, λετονικά, λιθουανικά και λιθουανικά. Οι συμμετέχοντες έπρεπε να εξοικειωθούν με το μαθησιακό υλικό που αναπτύχθηκε, να κάνουν τεστ αυτοαξιολόγησης μετά από κάθε θέμα του μαθήματος, να επιλύσουν προσομοιώσεις και να κάνουν ένα τελικό τεστ γνώσεων.

Η οργάνωση της εκπαίδευσης των πιλότων

Πριν από την πιλοτική εκπαίδευση, οι πέντε εταίροι συμφώνησαν να οργανώσουν την εκπαίδευση στις χώρες τους για να διασφαλίσουν ότι:

- τουλάχιστον 24 συμμετέχοντες από κάθε χώρα εταίρο ολοκληρώνουν την πιλοτική κατάρτιση (τουλάχιστον 120 συμμετέχοντες συνολικά σε όλες τις χώρες),

- οι συμμετέχοντες συμπληρώνουν ένα ερωτηματολόγιο πριν από την πιλοτική εκπαίδευση, δηλαδή για να αξιολογήσουν τις υπάρχουσες γνώσεις τους πριν από την εκπαίδευση (τουλάχιστον 120 συμπληρωμένα ερωτηματολόγια συνολικά),

- η τελική δοκιμασία γνώσεων θεωρείται ότι έχει περάσει όταν ο συμμετέχων συγκεντρώσει τουλάχιστον 75%,

- οι συμμετέχοντες θα συμπληρώσουν ένα ερωτηματολόγιο στο τέλος της πιλοτικής κατάρτισης, δηλαδή για να αξιολογήσουν τις υπάρχουσες γνώσεις τους μετά την κατάρτιση (τουλάχιστον 120 συμπληρωμένα ερωτηματολόγια συνολικά),

- τουλάχιστον ένας εκπαιδευτής από κάθε χώρα εταίρο θα συμπληρώσει επίσης το ερωτηματολόγιο σχετικά με την κατάρτιση (τουλάχιστον 5 ερωτηματολόγια). Αυτό το ερωτηματολόγιο θα βοηθήσει στην αξιολόγηση της πιλοτικής κατάρτισης του έργου. Οι απαντήσεις (ανατροφοδότηση) που θα δοθούν από τους εκπαιδευτές θα παράσχουν πληροφορίες σχετικά με την ποιότητα του μαθήματος που αναπτύχθηκε, δηλαδή τη συνάφεια των θεμάτων με το κοινό-στόχο, την πληρότητα των θεμάτων του μαθήματος, τη δομή και το περιεχόμενο του εκπαιδευτικού υλικού και τη διάρκεια της κατάρτισης. Το πιο σημαντικό ερώτημα θα είναι σε ποιο βαθμό το μάθημα πέτυχε τον στόχο του να εισάγει το κοινό στην ασφάλεια στον κυβερνοχώρο και την απάτη.

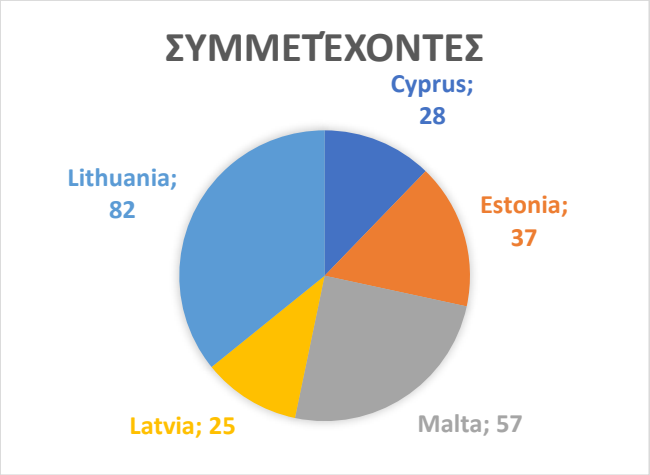
- Στο τέλος της πιλοτικής κατάρτισης, κάθε εταίρος θα υποβάλει περίληψη της πιλοτικής κατάρτισης στον Συντονιστή. Ο Συντονιστής θα χρησιμοποιήσει τις πληροφορίες αυτές για την προετοιμασία της έκθεσης IO6. Οι εταίροι θα προβούν σε επικαιροποίηση των πνευματικών αποτελεσμάτων (IO2, IO3, IO4 και IO5) μετά τη σύνθεση των αποτελεσμάτων της πιλοτικής κατάρτισης.

5. ΑΠΟΤΕΛΈΣΜΑΤΑ ΤΗΣ ΠΙΛΟΤΙΚΉΣ ΚΑΤΆΡΤΙΣΗΣ

Η πιλοτική κατάρτιση πραγματοποιήθηκε σε πέντε χώρες εταίρους - Κύπρο, Εσθονία, Λετονία, Λιθουανία και Μάλτα. Συνολικά 229 συμμετέχοντες έλαβαν μέρος στην κατάρτιση. Εκατόν εβδομήντα πέντε (175) συμμετέχοντες ολοκλήρωσαν την κατάρτιση με βαθμολογία 75% ή υψηλότερη.

Ερωτηματολόγιο προ-πιλοτικής εφαρμογής

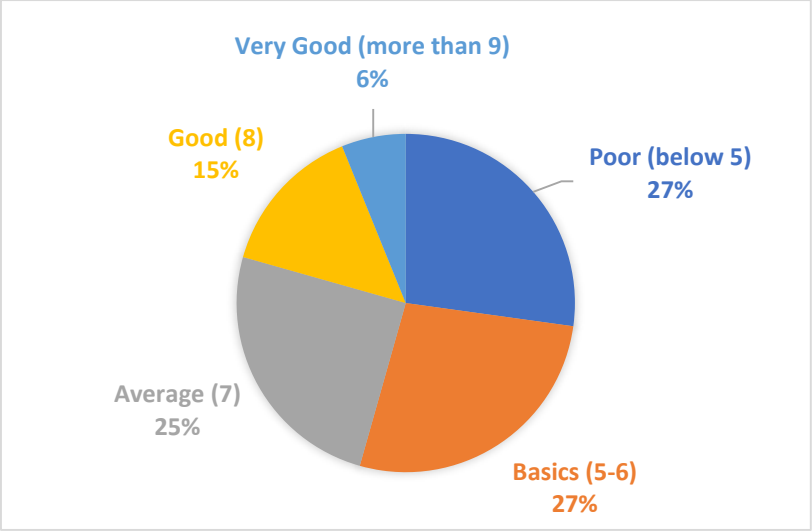
Πριν από την έναρξη της πιλοτικής κατάρτισης, όλοι οι συμμετέχοντες συμπλήρωσαν ένα ερωτηματολόγιο πριν από την κατάρτιση για να αξιολογήσουν τις αρχικές τους γνώσεις σχετικά με την απάτη και την ασφάλεια στον κυβερνοχώρο. Συνολικά 229 συμμετέχοντες συμπλήρωσαν αυτά τα προ-ερωτηματολόγια. Η κατανομή των συμμετεχόντων ανά χώρα παρουσιάζεται στο παρακάτω σχήμα.



Σχήμα 1. Συμμετέχοντες στην πιλοτική κατάρτιση ανά χώρα

Ένα αρχικό επίπεδο γνώσεων των συμμετεχόντων πριν από την κατάρτιση

Τα ερωτηματολόγια αναλύθηκαν για να εκτιμηθούν οι γνώσεις των συμμετεχόντων πριν από την κατάρτιση στην πιλοτική κατάρτιση. Το σχήμα 2 δείχνει την κατανομή των συμμετεχόντων σύμφωνα με τις βαθμολογίες που έλαβαν. Οι γνώσεις του 27% των συμμετεχόντων ήταν ανεπαρκείς σχετικά με το phishing (η βαθμολογία είναι μικρότερη από 5 μονάδες). Το ίδιο μέρος (27%) των συμμετεχόντων είχε μόνο βασικές γνώσεις (δηλαδή η βαθμολογία 5-6 μονάδες). Το 25% των συμμετεχόντων είχε βαθμολογία "μέτρια" (7 βαθμοί). Το 15% των συμμετεχόντων είχε γνώσεις που αξιολογήθηκαν ως "καλές" (δηλ. 8 βαθμοί), όταν μόνο το 6% των συμμετεχόντων είχε βαθμολογία "πολύ καλές" (9 βαθμοί ή περισσότερο). Οι γνώσεις των συμμετεχόντων αξιολογήθηκαν σε δεκάβαθμη κλίμακα.



Σχήμα 2. Γνώσεις των συμμετεχόντων στην πιλοτική εκπαίδευση πριν από την εκπαίδευση

Το σχήμα 3 δείχνει την κατανομή των γνώσεων των συμμετεχόντων (όπως βαθμολογήθηκαν) πριν από την πιλοτική εκπαίδευση σε δεκάβαθμη κλίμακα. Στο σχήμα 3 παρουσιάζεται η κατανομή των γνώσεων των συμμετεχόντων (σε δεκάβαθμη κλίμακα) πριν από την πιλοτική εκπαίδευση. Φαίνεται ότι λίγο πάνω από το ένα πέμπτο των ερωτηθέντων σημείωσε υψηλή βαθμολογία (δηλαδή βαθμολογία 8, 9 και 10).

Σχήμα 3. Κατανομή της βαθμολογίας γνώσεων από τους συμμετέχοντες στην πιλοτική εκπαίδευση

Η δυσκολία των ερωτήσεων: 5 πιο απλές ερωτήσεις

Η ανάλυση των ερωτηματολογίων των συμμετεχόντων έδειξε ποιες ερωτήσεις ήταν δύσκολες και ποιες αρκετά εύκολες. Με βάση τις απαντήσεις που έδωσαν οι συμμετέχοντες, εντοπίσαμε τις πέντε πιο εύκολες ερωτήσεις. Περίπου το 70-75% όλων των συμμετεχόντων απάντησε σωστά σε αυτές τις ερωτήσεις. Οι ερωτήσεις αυτές παρουσιάζονται στον παρακάτω πίνακα.

Κορυφή 1. 15. Είναι αλήθεια ότι η επίθεση phishing πραγματοποιείται μόνο μέσω ηλεκτρονικού ταχυδρομείου;

Όχι
Ναι

Top 2. 13. Ποιες ενέργειες μπορούν να αποτρέψουν τις επιθέσεις κοινωνικής μηχανικής;

Όλα τα αναφερόμενα
Γνωρίζετε ποιες προσωπικές σας πληροφορίες είναι διαθέσιμες στο διαδίκτυο
Χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων
Ενεργοποίηση φίλτρου spam
Διατηρήστε το λογισμικό ενημερωμένο

Top 3. 5. Ποιο καλύπτει καλύτερα το πεδίο εφαρμογής του όρου "κυβερνοεπίθεση";

Οποιαδήποτε κακόβουλη δραστηριότητα στον κυβερνοχώρο, ακόμη και αν είναι ανεπιτυχής
Επιβλαβείς ενέργειες μέσω διαδικτύου
Αποστολή ιών και trojans μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου ή SMS
Επιτυχημένες επιθέσεις phishing

Top 4. 12. Η κοινωνική μηχανική είναι

Χειραγώγηση ανθρώπων, συνήθως μέσω ψυχολογικής πειθούς, για να αποκτήσουν πρόσβαση σε συστήματα πληροφοριών ή δεδομένα.
επίθεση που χρησιμοποιεί ένα κακόβουλο πρόγραμμα που είναι κρυμμένο μέσα σε ένα φαινομενικά νόμιμο πρόγραμμα

κακόβουλο λογισμικό που απειλεί να δημοσιεύσει τα προσωπικά δεδομένα του θύματος ή να αποκλείσει διαρκώς την πρόσβαση σε αυτά, εκτός αν καταβληθεί αμοιβή
όταν ένας επιτιθέμενος υποκλέπτει μια συναλλαγή μεταξύ δύο μερών, μπαίνοντας στη μέση.
ένας τύπος προγράμματος που εγκαθίσταται για τη συλλογή πληροφοριών σχετικά με τους χρήστες, τα συστήματά τους ή τις συνήθειες περιήγησης, αποστέλλοντας τα δεδομένα σε έναν απομακρυσμένο χρήστη

Top 5. 14. Ποιες είναι οι τακτικές που χρησιμοποιούνται στα ηλεκτρονικά μηνύματα phishing;

Αίτημα αποστολής εμπιστευτικών πληροφοριών μέσω ηλεκτρονικού ταχυδρομείου
Παρακαλώ κάντε κλικ στο σύνδεσμο στο email
Παροχή πληροφοριών σχετικά με τον αριθμό και τα αποτελέσματα των επιθέσεων ηλεκτρονικού "ψαρέματος" που πραγματοποιήθηκαν με επιτυχία κατά τη διάρκεια του περασμένου έτους
Ζητώντας δωρεά για τον καθαρισμό του ωκεανού
Αίτημα τηλεφωνικής επικοινωνίας με τον αποστολέα

Πίνακας 1. Οι πιο εύκολες ερωτήσεις για τους συμμετέχοντες (Top 5)

Η πρώτη ερώτηση αφορά τα εργαλεία απάτης. Η δεύτερη αφορά τα μέτρα πρόληψης. Η τρίτη αφορά τον ορισμό των επιθέσεων στον κυβερνοχώρο. Η τέταρτη αφορά την κοινωνική μηχανική, και η πέμπτη αφορά τις τακτικές απάτης που χρησιμοποιούνται στα μηνύματα ηλεκτρονικού ταχυδρομείου.

Έτσι, μπορούμε να δούμε τι γνώριζαν αρκετά οι συμμετέχοντες πριν από την εκπαίδευση.

Εκπαίδευση πιλότων: η πολυπλοκότητα των ερωτήσεων: οι 5 πιο δύσκολες ερωτήσεις

Η ανάλυση των απαντήσεων που έδωσαν οι συμμετέχοντες προσδιόρισε τις πιο δύσκολες ερωτήσεις. Οι ερωτήσεις αυτές δεν απαντήθηκαν ή απαντήθηκαν ανεπαρκώς από το 60-80% των συμμετεχόντων. Οι ερωτήσεις αυτές παρουσιάζονται στον παρακάτω πίνακα.

Κορυφή 1. 7. Ποιος είναι ο σκοπός ενός πλαισίου πιστοποίησης της ασφάλειας στον κυβερνοχώρο;

Πιστοποίηση προϊόντων, διαδικασιών και υπηρεσιών ΤΠΕ
Παροχή πιστοποίησης για τις αποκτηθείσες ικανότητες ασφάλειας στον κυβερνοχώρο, αναγνωρίσιμες σε ολόκληρη την ΕΕ.
Παροχή πιστοποίησης ΤΠΕ αναγνωρίσιμης εκτός ΕΕ
Καμία από τις παρεχόμενες απαντήσεις

Top 2. 8. Ποια οδηγία ήταν η πρώτη νομοθεσία για την κυβερνοασφάλεια σε επίπεδο ΕΕ που εισήγαγε απαιτήσεις ασφάλειας ως νομικές υποχρεώσεις για τους παρόχους ψηφιακών υπηρεσιών (ΠΨΥ) και τους φορείς εκμετάλλευσης βασικών υπηρεσιών (ΠΥΥ);

Η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες
Η πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο
Η οδηγία NIS
Ευρωπαϊκή οδηγία για τον κώδικα ηλεκτρονικών επικοινωνιών

Top 3. 3. Ποιες δηλώσεις σχετικά με τους τηλεφωνικούς απατεώνες είναι σωστές;

Οι Phone Phreaks έμαθαν να ελέγχουν τις τηλεφωνικές γραμμές ακούγοντας τους ήχους καθώς οι κλήσεις συνδέονταν από τους χειριστές
Phone Phreaks διαβάζουν τεχνικά περιοδικά τηλεφωνικών εταιρειών
Οι Phone Phreaks δεν εισέβαλαν σε γραφεία για να αναπτύξουν το δικό τους υλικό
Οι Phone Phreaks δεν ψάχνουν στους κάδους απορριμμάτων των τηλεφωνικών εταιρειών για να βρουν "μυστικά" έγγραφα

Top 4. 4. Ποια είναι η διαφορά μεταξύ της ασφάλειας στον κυβερνοχώρο και της ασφάλειας των υπολογιστών;

Η ασφάλεια στον κυβερνοχώρο καλύπτει διάφορους τομείς της πληροφορικής είναι το ίδιο η κυβερνοασφάλεια είναι μέρος της ασφάλειας των υπολογιστών η κυβερνοασφάλεια ασχολείται μόνο με τις απειλές του Διαδικτύου η κυβερνοασφάλεια αφορά ιούς κ.λπ.
Top 5. 11. Ποιες δηλώσεις σχετικά με την επίθεση Phishing είναι σωστές;
Το "ψάρεμα" είναι μια απάτη κοινωνικής μηχανικής που μπορεί να οδηγήσει σε απώλεια δεδομένων, βλάβη της φήμης, κλοπή ταυτότητας, απώλεια χρημάτων και πολλές άλλες ζημιές σε ανθρώπους και οργανισμούς. **Μια απάτη phishing ξεκινά συνήθως με ένα μήνυμα ηλεκτρονικού ταχυδρομείου που προσπαθεί να κερδίσει την εμπιστοσύνη του δυνητικού θύματος και να το πείσει να προβεί στις επιθυμητές ενέργειες του επιτιθέμενου.** Το phishing είναι ένα χαρακτηριστικό ενός περιουσιακού στοιχείου του συστήματος που μπορεί να αποτελέσει αδυναμία ή ελάττωμα όσον αφορά την ασφάλεια του συστήματος. Το Phishing περιγράφει ένα τυπικό μέσο με το οποίο ένας φορέας απειλής πραγματοποιεί μια απειλή

Πίνακας 2. Οι πιο δύσκολες ερωτήσεις για τους συμμετέχοντες (Top 5)

Η πρώτη ερώτηση αφορούσε τον σκοπό ενός συστήματος πιστοποίησης της κυβερνοασφάλειας- η δεύτερη ερώτηση αφορούσε τα οφέλη της κρυπτογράφησης- η τρίτη ερώτηση αφορούσε τα χαρακτηριστικά μιας παραβιασμένης συσκευής- η τέταρτη ερώτηση αφορούσε την οδηγία NIS- η πέμπτη ερώτηση αφορούσε τις διαφορές μεταξύ της ασφάλειας στον κυβερνοχώρο και της ασφάλειας των υπολογιστών.

Όπως γίνεται αντιληπτό, οι ερωτήσεις αφορούσαν είτε τεχνικά θέματα είτε συγκεκριμένα ζητήματα, όπως το πλαίσιο για την ασφάλεια στον κυβερνοχώρο ή η οδηγία.

Διαδικτυακό περιβάλλον μάθησης

Η πιλοτική εκπαίδευση διεξάγεται σε ένα σύστημα που αναπτύχθηκε και συντηρείται από τον συντονιστή του έργου Πανεπιστήμιο του Βίλνιους. Το σύστημα είναι προσβάσιμο μέσω του συνδέσμου https://cyberphish.vuknf.lt/. Η πλατφόρμα μάθησης μπορεί να χρησιμοποιηθεί τόσο από εγγεγραμμένους όσο και από μη εγγεγραμμένους συμμετέχοντες. Οι μη εγγεγραμμένοι συμμετέχοντες μπορούν να βλέπουν γενικές πληροφορίες σχετικά με το πρόγραμμα κατάρτισης, να βλέπουν πίνακες αξιολόγησης και να βλέπουν ή να κατεβάζουν εκπαιδευτικό υλικό σε όλες τις γλώσσες των εταίρων: Αγγλικά, εσθονικά, ελληνικά, λετονικά και λιθουανικά.

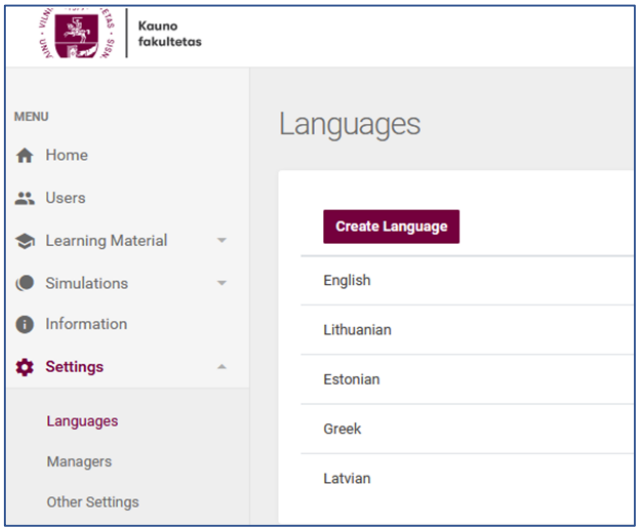
Σχήμα 4. Διαδικτυακό περιβάλλον μάθησης

Σχήμα 5. Μαθησιακό υλικό στο διαδικτυακό περιβάλλον μάθησης

Οι τρεις ρόλοι ενός διαδικτυακού μαθησιακού περιβάλλοντος

Υπάρχουν τρεις ρόλοι χρηστών σε ένα διαδικτυακό περιβάλλον μάθησης: διαχειριστής, τοπικός διαχειριστής και συμμετέχων στο μάθημα.

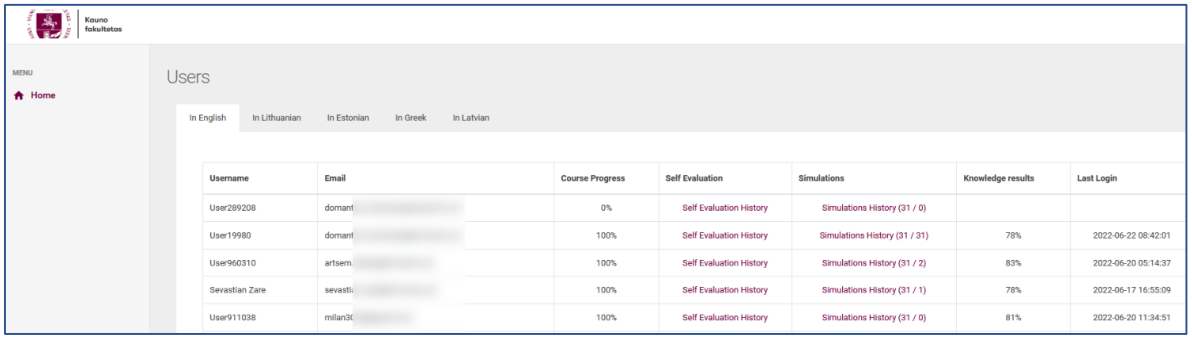
Ο διαχειριστής μπορεί να προβάλλει στατιστικά στοιχεία όλων των χρηστών, όπως η τελευταία σύνδεση, η διεύθυνση IP, η κατάσταση και η διεύθυνση ηλεκτρονικού ταχυδρομείου.



Εικόνα 6. Παράθυρο διαχειριστή συστήματος

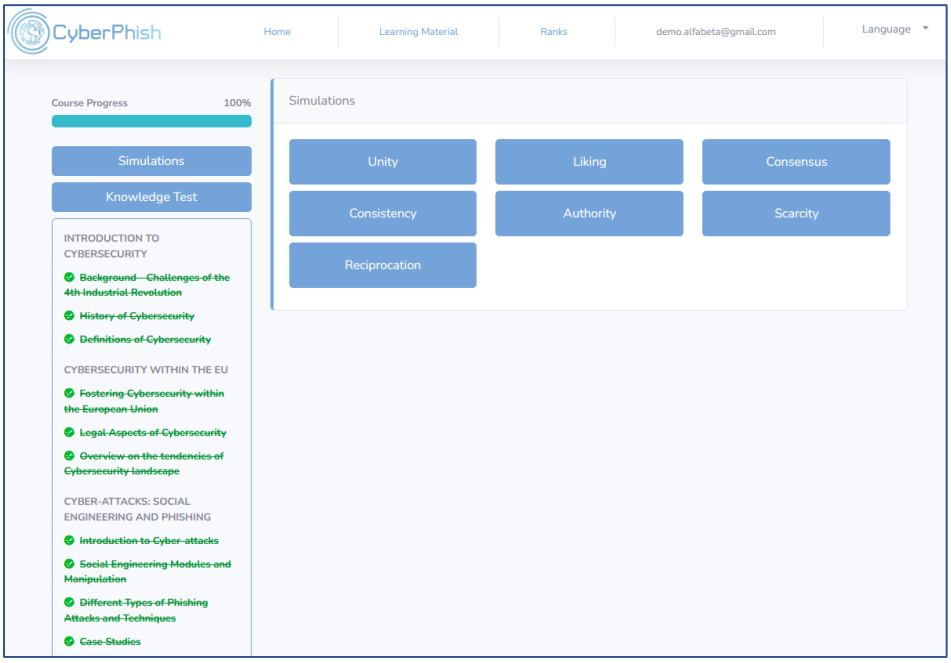
Ο διαχειριστής μπορεί να ανεβάζει εκπαιδευτικό υλικό, να εισάγει και να επεξεργάζεται προσομοιώσεις, να δημιουργεί τοπικούς χρήστες διαχειριστές και να καθορίζει άλλες ενέργειες που σχετίζονται με την ηλεκτρονική πλατφόρμα και δεν είναι διαθέσιμες στους άλλους χρήστες.

Ο τοπικός διαχειριστής μπορεί να βλέπει στατιστικά στοιχεία σχετικά με την πρόοδο των χρηστών, καθώς και πληροφορίες σχετικά με τις εξετάσεις αυτοαξιολόγησης που έχουν πραγματοποιηθεί, τις προσομοιώσεις που έχουν επιλυθεί, την τελευταία σύνδεση και τα αποτελέσματα των εξετάσεων αξιολόγησης γνώσεων. Ο χρήστης μπορεί επίσης να δει τις λυμένες ερωτήσεις και τα σενάρια αυτοαξιολόγησης, να δει πώς ο συμμετέχων έλυσε ένα συγκεκριμένο σενάριο και πόσους πόντους συγκέντρωσε για κάθε απάντηση.



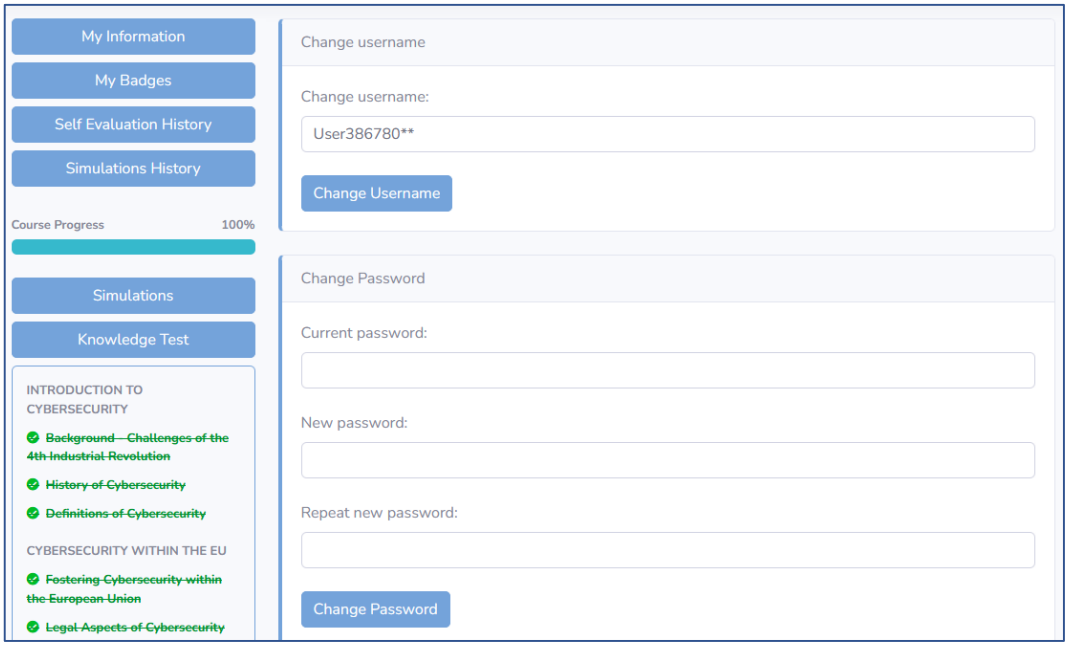
Εικόνα 7. Παράθυρο τοπικού διαχειριστή

Ο εγγεγραμμένος συμμετέχων μπορεί να χρησιμοποιήσει το μαθησιακό περιβάλλον για μαθησιακούς σκοπούς. Στην Εικόνα 8 παρουσιάζεται ένα παράδειγμα παραθύρου ενός συμμετέχοντα στο μάθημα.



Εικόνα 8. Παράθυρο μαθησιακού περιβάλλοντος για τους συμμετέχοντες στο μάθημα

Αφού εγγραφεί στο μάθημα, ο συμμετέχων μπορεί να αλλάξει τις πληροφορίες για τον εαυτό του, δηλαδή το όνομα χρήστη και τον κωδικό πρόσβασης (βλ. Εικόνα 9).



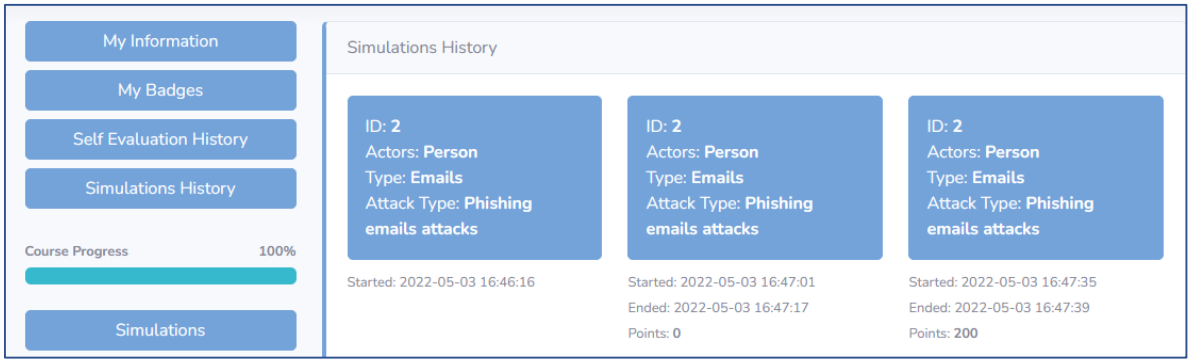
Εικόνα 9. Παράθυρο για τη ρύθμιση των προσωπικών στοιχείων του συμμετέχοντα στο μάθημα

Ως εγγεγραμμένος συμμετέχων στα μαθήματα, μπορείτε να παρακολουθείτε το ιστορικό των αυτοελέγχων και των δοκιμασιών γνώσεων και να βλέπετε πόσα σήματα έχετε κερδίσει (βλ. Εικόνα 10).

Εικόνα 10. Παράθυρο ιστορικού τεστ αυτοαξιολόγησης του συμμετέχοντα στο μάθημα

Ως εγγεγραμμένος συμμετέχων στα μαθήματα, μπορείτε να παρακολουθείτε το ιστορικό των προσομοιώσεων που έχετε ολοκληρώσει/επιλύσει:

- πότε και πώς απαντήσατε στις ερωτήσεις,
- Ποια σενάρια λύσατε,
- Πόσους πόντους πήρατε για καθένα από αυτά.



Εικόνα 11. Παράθυρο ιστορικού προσομοίωσης μαθητών

Κονκάρδες

Πριν από την πιλοτική εκπαίδευση, οι εταίροι συμφώνησαν σε έξι σήματα. Ωστόσο, κατά τη διάρκεια του έργου δημιουργήθηκαν οκτώ κονκάρδες:

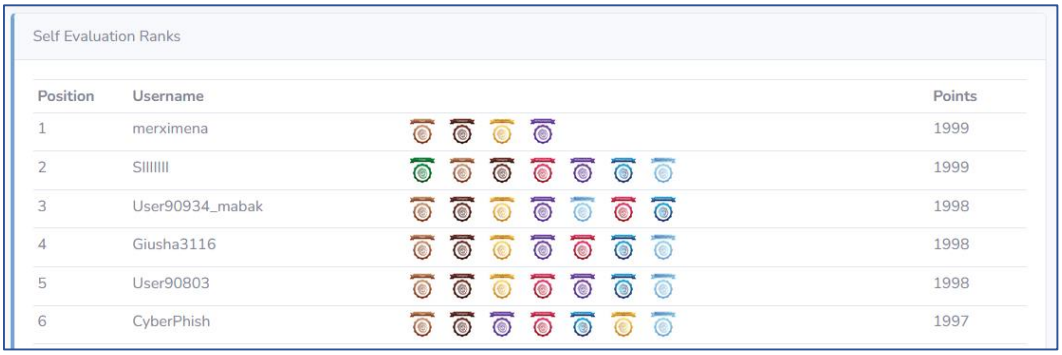
- περνώντας το τεστ,
- ολοκλήρωση του μαθήματος,
- ολοκλήρωση όλων των προσομοιώσεων,
- την πρώτη δοκιμασία αυτοαξιολόγησης,
- συμπληρώνοντας την κατηγορία και το θέμα,
- επιτυγχάνοντας όλες τις παρουσιάσεις,
- σύνδεση στο σύστημα κάθε μέρα για δέκα ημέρες.

Εικόνα 12 παραδείγματα κονκάρδων.

Εικόνα 12. Παραδείγματα κονκάρδων

Βαθμολόγηση

Οι εγγεγραμμένοι συμμετέχοντες στα μαθήματα μπορούν να συλλέγουν πόντους για αυτοελέγχους σύμφωνα με τους κανόνες που έχουν συμφωνηθεί από τους εταίρους. Αυτές οι βαθμολογίες εμφανίζονται στον πίνακα Κατάταξη αυτοαξιολόγησης. Το όνομα του συμμετέχοντα στο μάθημα και οι συλλεχθέντες εμφανίζονται μαζί.



Εικόνα 13. Κατάταξη των εγγεγραμμένων συμμετεχόντων στα μαθήματα

Εκπαιδευτικό υλικό σε διαδικτυακό περιβάλλον μάθησης

Η κοινοπραξία των εταίρων ανέπτυξε το διαδικτυακό εκπαιδευτικό υλικό σύμφωνα με το πρόγραμμα σπουδών του CyberPhish[2] και σύμφωνα με τις ανάγκες της 4ης Βιομηχανικής Επανάστασης. Το εκπαιδευτικό υλικό που αναπτύχθηκε αξιολογήθηκε από ανεξάρτητους εμπειρογνώμονες (ένας ανά χώρα εταίρο).

Ο πίνακας 4 που ακολουθεί παρουσιάζει συνοπτικά το εκπαιδευτικό υλικό που αναπτύχθηκε.

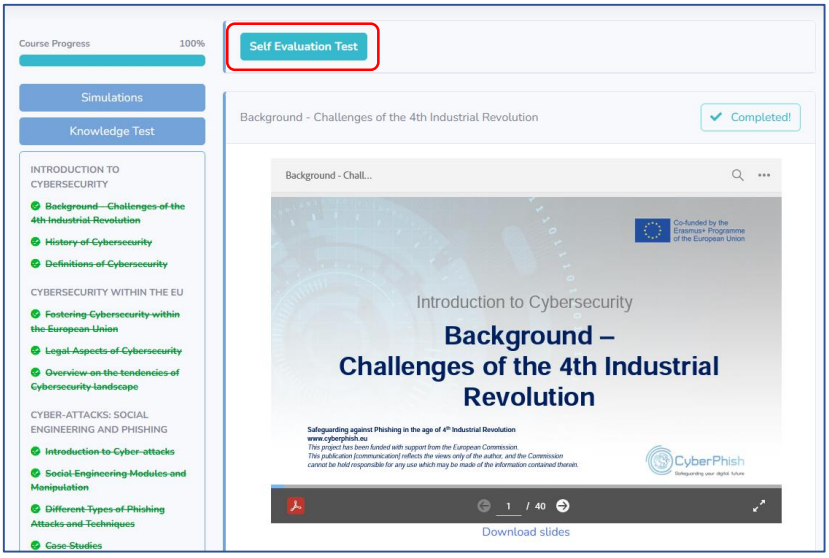
Ενότητες και επιμέρους θέματα				**Αριθμός διαφανειών**
1	**Εισαγωγή στην κυβερνοασφάλεια**	1.1	Ιστορικό - Προκλήσεις της 4ης βιομηχανικής επανάστασης	40
		1.2	Ιστορία της ασφάλειας στον κυβερνοχώρο	31
		1.3	Ορισμοί της ασφάλειας στον κυβερνοχώρο	15
2	**Κυβερνοασφάλεια στην Ευρωπαϊκή Ένωση (ΕΕ)**	2.1	Προώθηση της ασφάλειας στον κυβερνοχώρο στην Ευρωπαϊκή Ένωση	31
		2.2	Νομικές πτυχές της ασφάλειας στον κυβερνοχώρο	14
		2.3	Επισκόπηση των τάσεων του τοπίου της κυβερνοασφάλειας	41
3	**Επιθέσεις στον κυβερνοχώρο: Ψάρεμα: Κοινωνική Μηχανική και Phishing**	3.1	Εισαγωγή στις επιθέσεις στον κυβερνοχώρο	20
		3.2	Ενότητες κοινωνικής μηχανικής και χειραγώγησης	73
		3.3	Διαφορετικοί τύποι επιθέσεων Phishing και τεχνικές	37
		3.4	Μελέτες περιπτώσεων	37
4	**Επισκόπηση της κατανόησης και του χειρισμού των επιθέσεων στον κυβερνοχώρο**	4.1	Βασικές γνώσεις για την ηλεκτρονική ασφάλεια	22
		4.2	Προληπτικές ενέργειες	59
		4.3	Αναγνώριση επιθέσεων phishing	108
		4.4	Χειρισμός κυβερνοεπιθέσεων	87
		4.5	Ελαχιστοποίηση των ζημιών μέσω της αντιμετώπισης περιστατικών	34
			Σύνολο:	**649**

Πίνακας 3. Σύνοψη του μαθησιακού υλικού

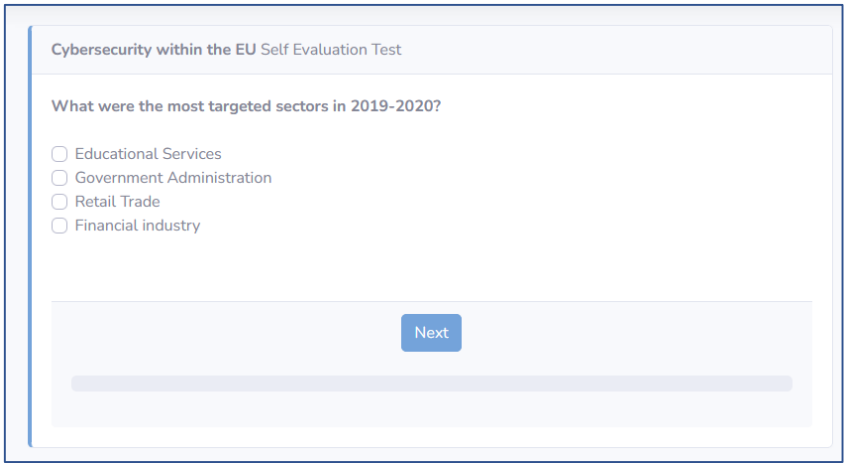
[2] **Εκτεταμένο πρόγραμμα σπουδών CyberPhish:** https://cyberphish.eu/wp-content/uploads/2021/07/IO2-A2_EN_Cyberphish-Full-Curriculum-Final.pdf

Καθήκοντα σε ένα διαδικτυακό περιβάλλον μάθησης

Το περιεχόμενο του μαθήματος μπορεί να προβληθεί στην οθόνη ή/και να μεταφορτωθεί σε μορφή .pdf. Μόλις ένας εγγεγραμμένος συμμετέχων εξετάσει όλο το εκπαιδευτικό υλικό για ένα συγκεκριμένο θέμα, μπορεί να ελέγξει τις γνώσεις του κάνοντας ένα αυτοτελές τεστ. Για το σκοπό αυτό θα χορηγηθούν βαθμοί.



Εικόνα 14. Κουμπί τεστ αυτοαξιολόγησης στο περιβάλλον του συμμετέχοντα στο μάθημα



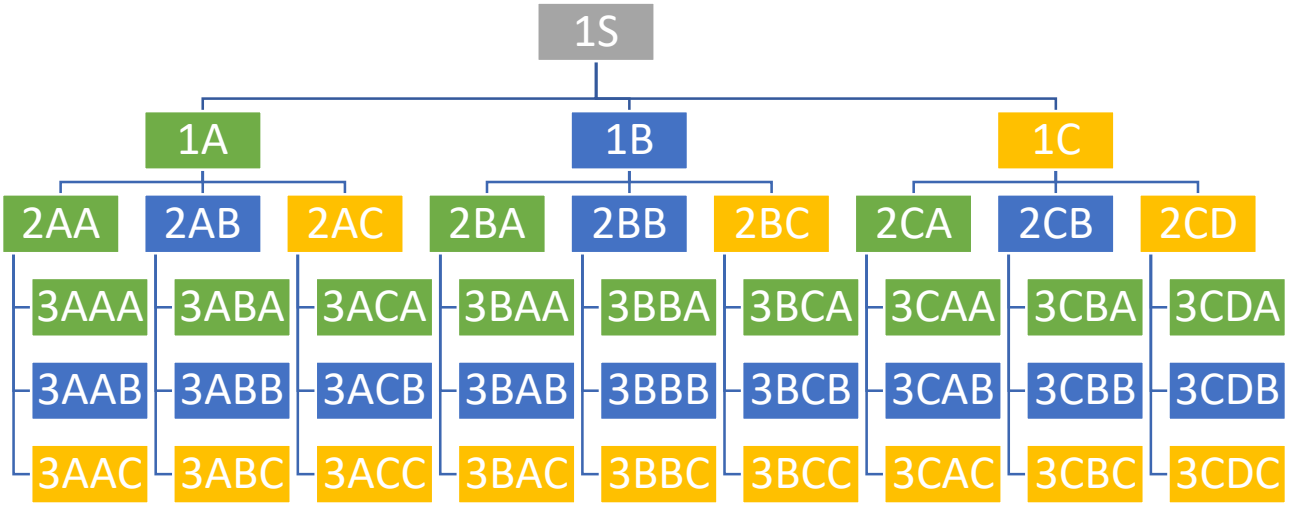
Εικόνα 15. Ένα τμήμα του τεστ αυτοαξιολόγησης

Προσομοιώσεις

Η προσομοίωση προσομοιώνει τις πραγματικές επιθέσεις απάτης παρουσιάζοντας τη διαδικασία στο χρήστη με παιγνιώδη τρόπο. Στόχος της προσομοίωσης είναι να βοηθήσει τους ανθρώπους να βελτιώσουν την κριτική τους σκέψη σχετικά με την ασφάλεια στον κυβερνοχώρο και την απάτη, αναγνωρίζοντας το phishing, το spam, τον εκφοβισμό στον κυβερνοχώρο και άλλα περιστατικά. Οι εταίροι του έργου ανέπτυξαν 55 προσομοιώσεις.

Μια προσομοίωση αποτελείται από μια περιγραφή της κατάστασης, του στόχου, των παραγόντων, του τύπου της επίθεσης και πολλών (3-4) επιλογών αντίδρασης για την επιλογή της συμπεριφοράς του χρήστη.

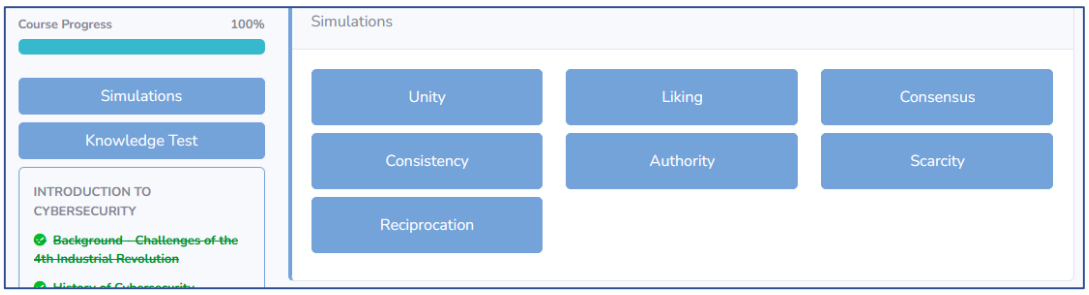
Όλες οι προσομοιώσεις βασίζονται σε μια προσέγγιση με δέντρα αποφάσεων. Στο σχήμα 15 παρουσιάζεται το μοντέλο προσομοίωσης. Κάθε προσομοίωση έχει τρία επίπεδα. Ο συνολικός αριθμός των επιλογών (πιθανές επιλογές) είναι τουλάχιστον 50, με μέγιστο αριθμό 84 επιλογές.



Εικόνα 16. Το μοντέλο προσομοίωσης βασίζεται σε μια προσέγγιση με δέντρα αποφάσεων

Στην προσομοίωση, κάθε απάντηση που επιλέγει ο χρήστης οδηγεί στο επόμενο επίπεδο πιθανών επιλογών απάντησης. Η προσομοίωση έχει τρεις τύπους λύσεων: σωστές, μερικώς σωστές και λανθασμένες. Για κάθε απάντηση, το σύστημα απονέμει συγκεκριμένο αριθμό πόντων στον συμμετέχοντα στο μάθημα. Το σύστημα παρέχει ανατροφοδότηση στην οθόνη εάν επιλεγεί μια μερικώς σωστή ή λανθασμένη απάντηση. Δίνονται επίσης προτάσεις σχετικά με το ποιο μέρος της ύλης θα πρέπει να επαναλάβει ο μαθητής και ποιο θέμα θα πρέπει να μελετήσει περαιτέρω.

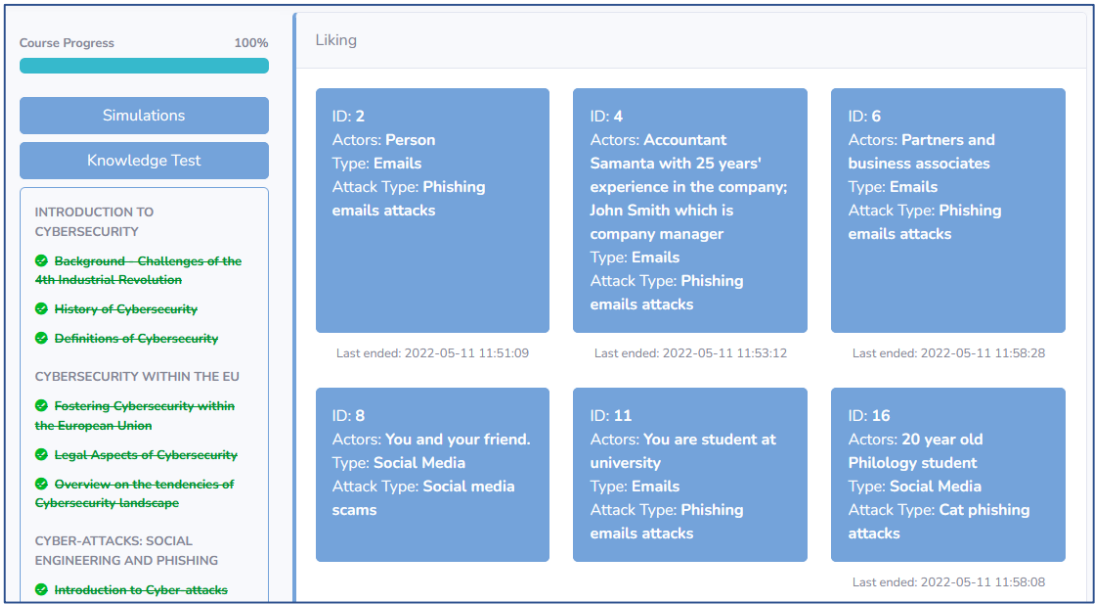
Ο συμμετέχων μπορεί να επιλέξει προσομοιώσεις ανά θέμα/κατηγορία.



Εικόνα 17. Κατηγορίες/θέματα προσομοίωσης

Οι προσομοιώσεις μπορούν να χρησιμοποιηθούν με δύο τρόπους: για μάθηση και για έλεγχο των γνώσεων. Με τον ένα τρόπο, η ανατροφοδότηση δίνεται στον εκπαιδευόμενο μετά από κάθε κατάσταση και με τον άλλο τρόπο, η ανατροφοδότηση δίνεται μόνο μετά την ολοκλήρωση ολόκληρου του σεναρίου προσομοίωσης. Για την επίλυση των προσομοιώσεων απονέμονται βαθμοί και για την επίλυση όλων των σεναρίων απονέμεται σήμα.

.



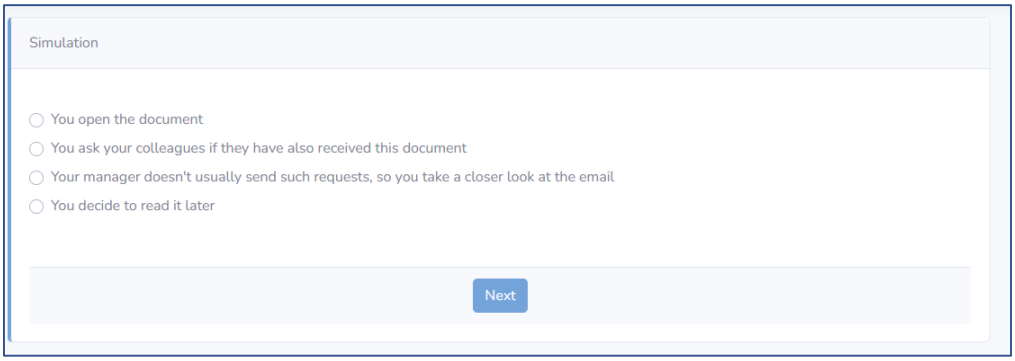
Εικόνα 18. Επιλογή προσομοιώσεων στο θέμα Liking

Αφού επιλέξει μια προσομοίωση, ο συμμετέχων στο μάθημα λαμβάνει μια περιγραφή της κατάστασης, τον σκοπό της προσομοίωσης, τους χαρακτήρες, τον τύπο της επίθεσης phishing και άλλα χαρακτηριστικά. Συχνά (αλλά όχι πάντα), προβάλλεται μια εικόνα για να ενισχυθεί η εντύπωση (για να γίνει ο συμμετέχων πιο ενσυναίσθητος).

Στη συνέχεια, υπάρχει η δυνατότητα επιλογής του σκοπού της προσομοίωσης: για σκοπούς μάθησης ή για τον έλεγχο των γνώσεων.

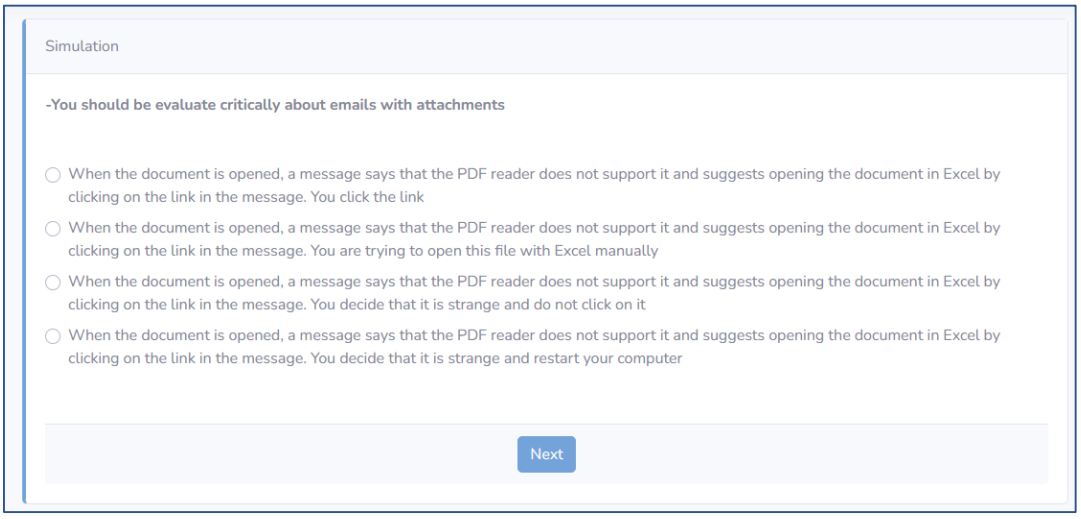
Εικόνα 19. Παράδειγμα λύσης προσομοίωσης

Μόλις ξεκινήσει η προσομοίωση, ο συμμετέχων έχει επιλογές. Πρέπει να επιλέξει πώς θα συμπεριφερόταν σε μια τέτοια κατάσταση. Το παρακάτω σχήμα δείχνει ένα παράδειγμα λύσης προσομοίωσης.



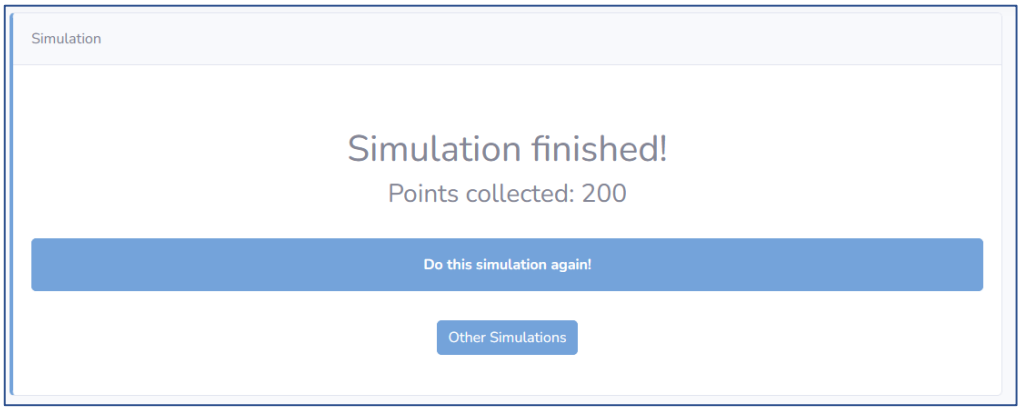
Εικόνα 20. Μια λύση προσομοίωσης

Κατά τη διάρκεια της προσομοίωσης, ο χρήστης λαμβάνει ανατροφοδότηση στην οθόνη όταν επιλέγει μια λανθασμένη ή μερικώς σωστή απάντηση. Το Σχήμα 21 απεικονίζει την ανατροφοδότηση επί της οθόνης προς τον χρήστη κατά τη διάρκεια της λύσης προσομοίωσης.



Εικόνα 21. Ανατροφοδότηση του χρήστη στην οθόνη κατά τη διάρκεια της λύσης προσομοίωσης

Όταν η προσομοίωση ολοκληρωθεί, ο χρήστης λαμβάνει ένα μήνυμα που δείχνει τον αριθμό των βαθμών που συγκέντρωσε και τον καλεί να λύσει άλλες προσομοιώσεις. Εάν η προσομοίωση επιλύθηκε λανθασμένα, δίνεται σύσταση να επιλυθεί ξανά η προσομοίωση (βλ. Εικόνα 22).



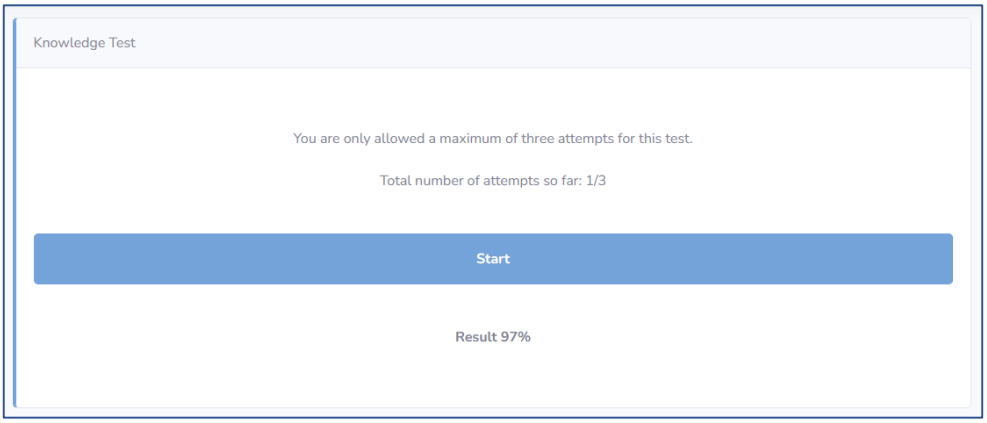
Εικόνα 22. Παράθυρο ολοκληρωμένης προσομοίωσης

Τεστ αξιολόγησης γνώσεων

Αφού μελετήσει το εκπαιδευτικό υλικό (αυτοδοκιμές και προσομοιώσεις), ο συμμετέχων εμφανίζεται με ένα κουμπί στο περιβάλλον μάθησης για να συμμετάσχει σε ένα τεστ γνώσεων. Κατά τη διάρκεια της πιλοτικής εκπαίδευσης, το τεστ γνώσεων μπορεί να πραγματοποιηθεί τρεις φορές.

Εικόνα 23. Παράδειγμα ερώτησης τεστ αξιολόγησης γνώσεων

Στο τέλος του τεστ γνώσεων, ο συμμετέχων στο μάθημα βλέπει ένα ποσοστό της αξιολόγησης των γνώσεών του.



Εικόνα 24. Παράδειγμα του παραθύρου αξιολόγησης για το τεστ αξιολόγησης γνώσεων

Σημείωση: Το τεστ γνώσεων έχει σχεδιαστεί για την αξιολόγηση των γνώσεων. Το τεστ αυτό δεν προορίζεται για σκοπούς μάθησης. Τα τεστ γνώσεων δεν κοινοποιούνται στους συμμετέχοντες, τους μέντορες ή/και τους καθηγητές. Οι ερωτήσεις είναι διαθέσιμες σε μορφή κειμένου σε όλους τους εταίρους/αναπτυξιακούς φορείς του έργου και το σύστημα δεν παρέχει πρόσβαση στα λεπτομερή αποτελέσματα του τεστ. Άλλοι μέντορες/εκπαιδευτικοί δεν θα μπορούν επίσης να δουν τα πλήρη αποτελέσματα του τεστ.

Δοκιμασίες γνώσεων

Οι εταίροι συμφώνησαν να αναπτύξουν τις ερωτήσεις για τις αυτοδοκιμασίες και τις ερωτήσεις για τις δοκιμασίες γνώσεων με βάση τις πληροφορίες που παρέχονται στην αίτηση. Οι ερωτήσεις θα είναι των ακόλουθων τύπων.

Οι δοκιμασίες αυτοαξιολόγησης θα περιλαμβάνουν τρεις τύπους ερωτήσεων:

- ερωτήσεις πολλαπλής επιλογής με μία σωστή απάντηση (αριθμός πιθανών απαντήσεων: 3-6),

- ερωτήσεις πολλαπλής επιλογής (4-6 πιθανές απαντήσεις),

- ερωτήσεις ναι/όχι.

Οι εταίροι έχουν συμφωνήσει/αποφασίσει σχετικά με το πλήθος των ερωτήσεων/την ποσότητα των ερωτήσεων ανά θέμα του μαθησιακού υλικού. Για παράδειγμα, 8-14 ερωτήσεις από τα θέματα "Εισαγωγή στην ασφάλεια στον κυβερνοχώρο" και "Επισκόπηση της ασφάλειας στον κυβερνοχώρο στην ΕΕ". Δημιουργία 12-20 ερωτήσεων το καθένα

από τα θέματα "Επιθέσεις στον κυβερνοχώρο - κοινωνική μηχανική και phishing" και "Κατανόηση και διαχείριση επιθέσεων στον κυβερνοχώρο".

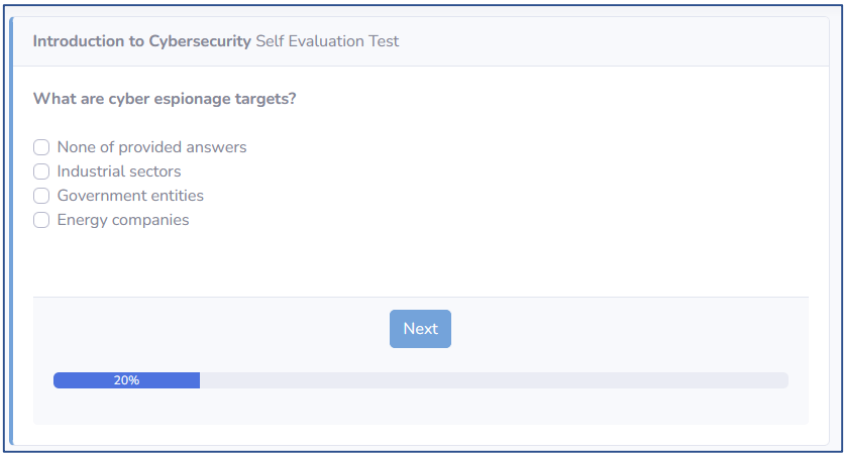
Προδιαγραφές για τις ερωτήσεις αυτοαξιολόγησης:

Ενότητες	Ανάπτυξη ερωτήσεων αυτοαξιολόγησης
Εισαγωγή στην ασφάλεια στον κυβερνοχώρο	13
Επισκόπηση της ασφάλειας στον κυβερνοχώρο στην ΕΕ	12
Επιθέσεις στον κυβερνοχώρο - κοινωνική μηχανική και phishing	16
Κατανόηση και διαχείριση κυβερνοεπιθέσεων	19
Σύνολο:	**60**

Πίνακας 4. Προδιαγραφές των ερωτήσεων του τεστ αυτοαξιολόγησης

Ένα κουμπί "Τεστ αυτοαξιολόγησης" εμφανίζεται στο μαθησιακό περιβάλλον όταν όλα τα επιμέρους θέματα μιας συγκεκριμένης ενότητας έχουν εξεταστεί. Το τεστ αποτελείται από πέντε ερωτήσεις. Οι ερωτήσεις επιλέγονται τυχαία από την τράπεζα ερωτήσεων της τρέχουσας κατηγορίας.

Στο κάτω μέρος της οθόνης εμφανίζεται μια μπάρα προόδου κατά τη διάρκεια του τεστ αυτοαξιολόγησης, η οποία δείχνει το ποσοστό των ερωτήσεων που απαντήθηκαν και τον αριθμό των ερωτήσεων που απομένουν.

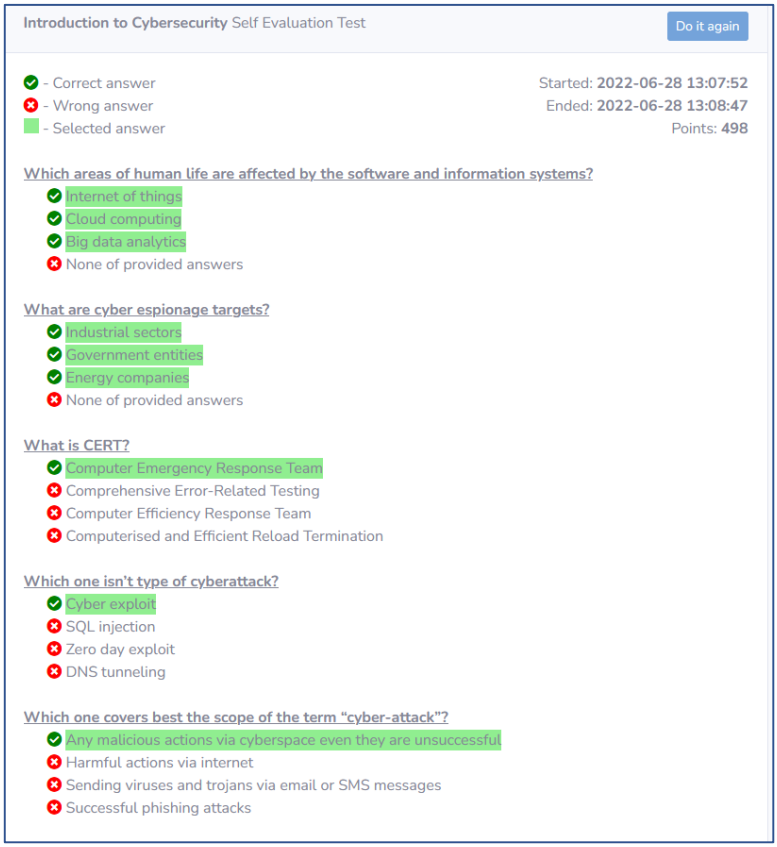


Εικόνα 25. Παράδειγμα ερώτησης του τεστ αυτοαξιολόγησης στην κατηγορία "Εισαγωγή στην κυβερνοασφάλεια"

Στο τέλος του τεστ αυτοαξιολόγησης, οι σωστές και οι λανθασμένες απαντήσεις εμφανίζονται στον συμμετέχοντα. Οι απαντήσεις που σημειώνονται από τον εκπαιδευόμενο επισημαίνονται με πράσινο χρώμα. Ο συμμετέχων βλέπει την ημερομηνία και την ώρα έναρξης, την ημερομηνία και την ώρα λήξης, καθώς και τον αριθμό των βαθμών που συγκέντρωσε στην επάνω δεξιά πλευρά της οθόνης.

Δεν υπάρχει όριο στον αριθμό των δοκιμασιών αυτοαξιολόγησης. Οι συμμετέχοντες στο μάθημα μπορούν να το κάνουν όσο συχνά επιθυμούν. Την επόμενη φορά που θα κάνουν το τεστ, θα τους παρουσιαστούν άλλες ερωτήσεις που θα επιλεγούν τυχαία.

Στους συμμετέχοντες απονέμεται επίσης ένα σήμα σύμφωνα με έναν κανόνα που συμφωνείται από τους εταίρους.



Introduction to Cybersecurity Self Evaluation Test

Do it again

- Correct answer
- Wrong answer
- Selected answer

Started: 2022-06-28 13:07:52
Ended: 2022-06-28 13:08:47
Points: 498

Which areas of human life are affected by the software and information systems?
- Internet of things
- Cloud computing
- Big data analytics
- None of provided answers

What are cyber espionage targets?
- Industrial sectors
- Government entities
- Energy companies
- None of provided answers

What is CERT?
- Computer Emergency Response Team
- Comprehensive Error-Related Testing
- Computer Efficiency Response Team
- Computerised and Efficient Reload Termination

Which one isn't type of cyberattack?
- Cyber exploit
- SQL injection
- Zero day exploit
- DNS tunneling

Which one covers best the scope of the term "cyber-attack"?
- Any malicious actions via cyberspace even they are unsuccessful
- Harmful actions via internet
- Sending viruses and trojans via email or SMS messages
- Successful phishing attacks

Εικόνα 26. Παράδειγμα αποτελεσμάτων αυτοελέγχου

Τεστ γνώσεων. Οι εταίροι συμφώνησαν επίσης σχετικά με τον αριθμό των ερωτήσεων που θα τεθούν στις εξετάσεις γνώσεων.

- Όλες οι ερωτήσεις θα έχουν τέσσερις απαντήσεις, εκ των οποίων μόνο μία θα είναι σωστή.

- Δημιουργήστε 144 ερωτήσεις τεστ γνώσεων.

Το τεστ γνώσεων θα αποτελείται από ένα σύνολο 36 ερωτήσεων. Η εξέταση θα διαρκέσει έως και 45 λεπτά. Το ποσοστό επιτυχίας θα είναι 75 %.

Οι εταίροι έχουν συμφωνήσει σχετικά με τον αριθμό των ερωτήσεων για κάθε θέμα του εκπαιδευτικού υλικού. Για παράδειγμα, 20-25 ερωτήσεις από τα θέματα "Εισαγωγή στην ασφάλεια στον κυβερνοχώρο" και "Επισκόπηση της ασφάλειας στον κυβερνοχώρο στην ΕΕ". Ανάπτυξη 45-65 ερωτήσεων η καθεμία από τα θέματα "Επιθέσεις στον κυβερνοχώρο - κοινωνική μηχανική και phishing" και "Κατανόηση και διαχείριση των επιθέσεων στον κυβερνοχώρο".

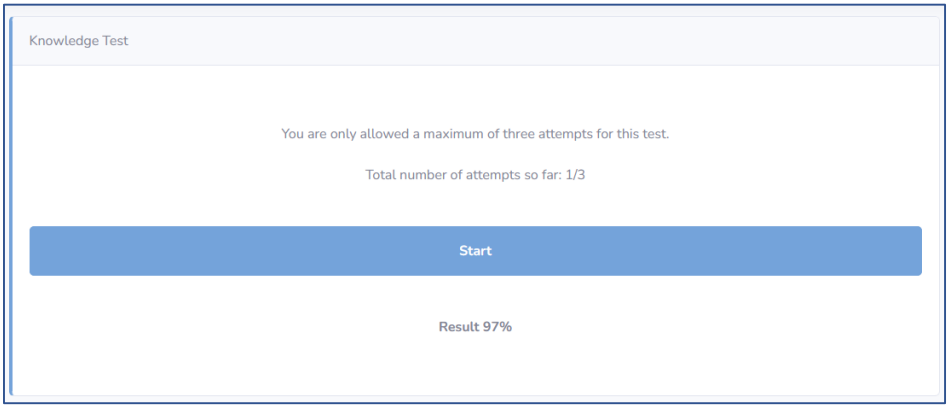
Προδιαγραφές ερωτήσεων για τις δοκιμασίες αξιολόγησης γνώσεων**:**

Ενότητες	Ανάπτυξη ερωτήσεων τεστ γνώσεων
Εισαγωγή στην ασφάλεια στον κυβερνοχώρο	24
Επισκόπηση της ασφάλειας στον κυβερνοχώρο στην ΕΕ	20
Επιθέσεις στον κυβερνοχώρο - κοινωνική μηχανική και phishing	62
Κατανόηση και διαχείριση κυβερνοεπιθέσεων	46
Σύνολο:	**152**

Πίνακας 5. Προδιαγραφές των ερωτήσεων για τις δοκιμασίες αξιολόγησης γνώσεων

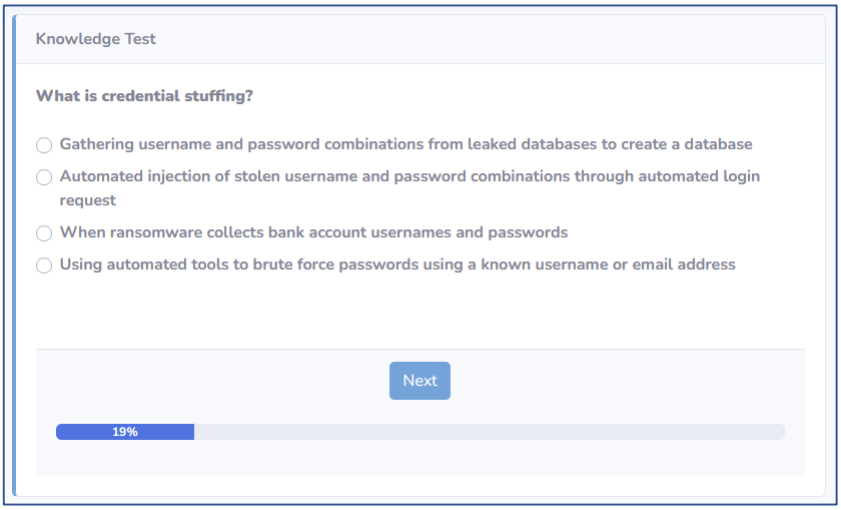
Ο αριθμός των δοκιμασιών γνώσεων ήταν περιορισμένος κατά τη διάρκεια της πιλοτικής εκπαίδευσης. Ο μέγιστος αριθμός φορών που μπορεί να γίνει αυτή η δοκιμασία είναι 3.

Στο περιβάλλον εκμάθησης, το κουμπί τεστ γνώσεων εμφανίζεται όταν ολοκληρωθεί ολόκληρο το μάθημα. Κάνοντας κλικ στο κουμπί τεστ εμφανίζεται ο αριθμός των προσπαθειών που θα κάνει ο συμμετέχων για να ολοκληρώσει το τεστ. Εάν το τεστ έχει πραγματοποιηθεί και στο παρελθόν, το αποτέλεσμα του προηγούμενου τεστ εμφανίζεται ως ποσοστό.



Εικόνα 27. Παράθυρο έναρξης του τεστ γνώσεων

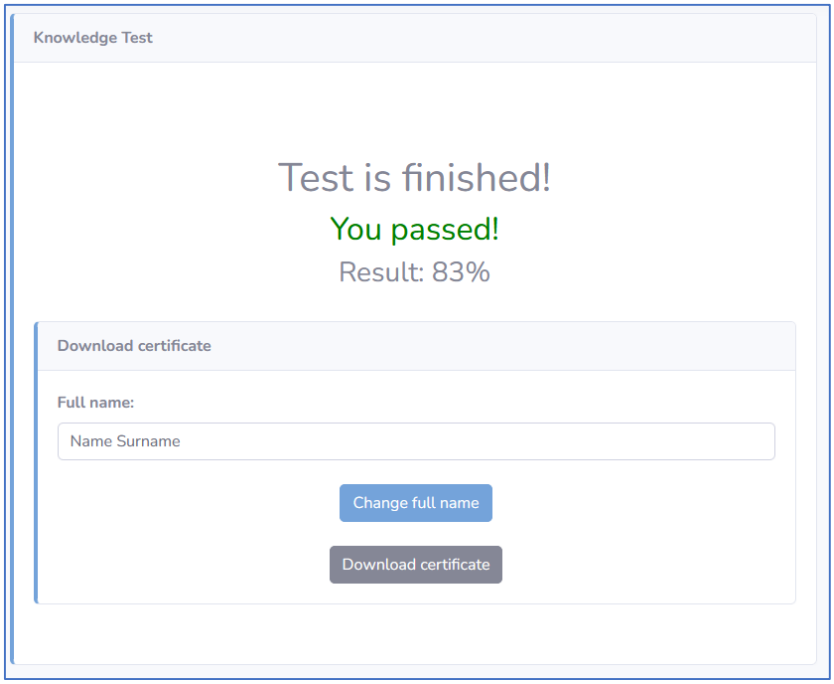
Το τεστ γνώσεων αποτελείται από μια τυχαία επιλογή 36 ερωτήσεων. Ορίζεται ένας κανόνας για τον αριθμό των ερωτήσεων που θα επιλεγούν τυχαία από κάθε κατηγορία. Κατά τη διάρκεια του τεστ, μια μπάρα προόδου δείχνει το ποσοστό των ερωτήσεων που απαντήθηκαν και τον αριθμό των ερωτήσεων που απομένουν. Στο τέλος του τεστ, εμφανίζεται η βαθμολογία του τεστ, αλλά ο συμμετέχων δεν μπορεί να δει πώς απάντησε στις ερωτήσεις, καθώς πρόκειται για τεστ αξιολόγησης γνώσεων.



Εικόνα 28. Παράδειγμα ερώτησης του τεστ γνώσεων

Εάν οι συμμετέχοντες αποτύχουν στη δοκιμασία, μπορούν να προσπαθήσουν να επαναλάβουν το εκπαιδευτικό υλικό, να λάβουν μέρος στις δοκιμασίες αυτοαξιολόγησης και να προσπαθήσουν ξανά να περάσουν τη δοκιμασία γνώσεων.

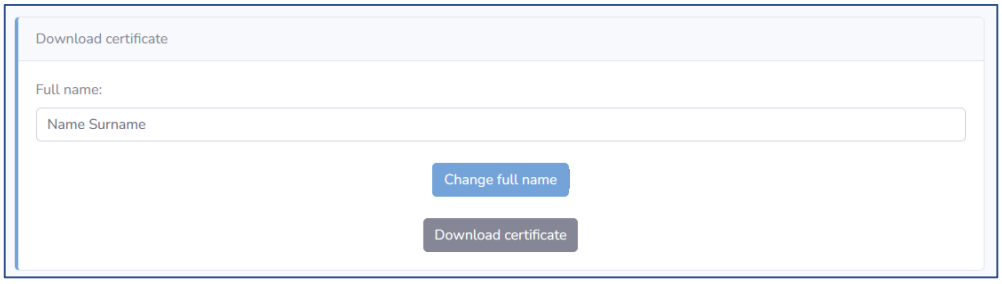
Σε περίπτωση επιτυχίας, ο συμμετέχων έχει τη δυνατότητα να καταχωρίσει το όνομά του και να κατεβάσει το πιστοποιητικό σε μορφή .pdf.



Εικόνα 29. Παράθυρο επιτυχούς δοκιμασίας γνώσεων

Πιστοποιητικό

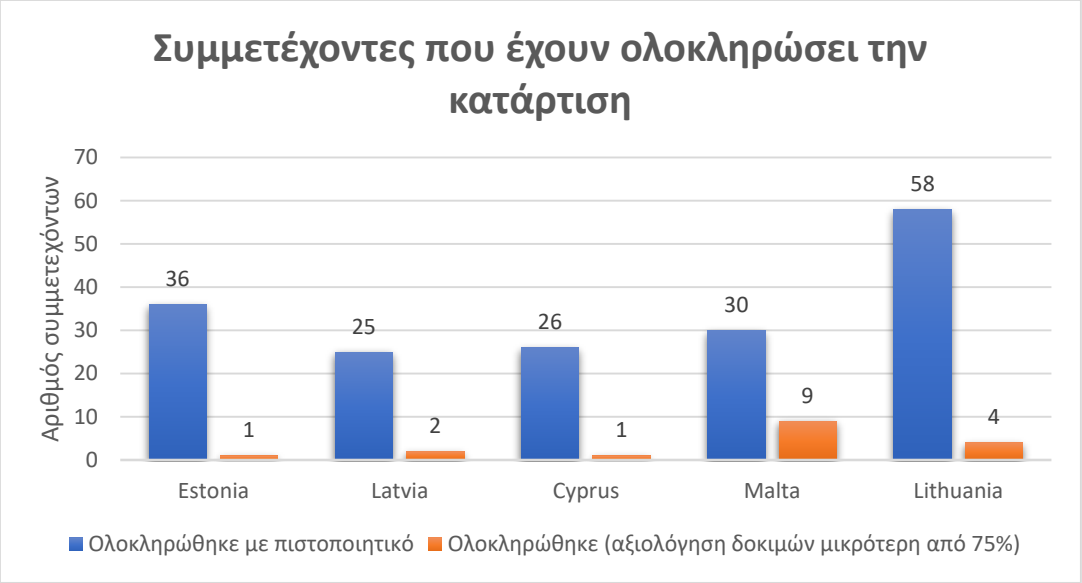
Αφού περάσει το τεστ, ο συμμετέχων λαμβάνει έναν σύνδεσμο για να συμπληρώσει ένα ερωτηματολόγιο μετά το τεστ, μετά το οποίο μπορεί να συμπληρώσει το όνομά του και να κατεβάσει το πιστοποιητικό σε μορφή PDF. Αυτή η μέθοδος έκδοσης του πιστοποιητικού διευκολύνει τη διαδικασία έκδοσης του πιστοποιητικού.



Εικόνα 30. Παράθυρο δημιουργίας πιστοποιητικού

Οι συμμετέχοντες ολοκλήρωσαν την εκπαίδευση

Το παρακάτω σχήμα δείχνει τα αποτελέσματα του εκπαιδευτικού προγράμματος. Εκατόν εβδομήντα πέντε συμμετέχοντες ολοκλήρωσαν (175) το μάθημα κατάρτισης και έλαβαν πιστοποιητικό: 36 στην Εσθονία, 25 στη Λετονία, 26 στην Κύπρο, 30 στη Μάλτα και 58 στη Λιθουανία. Άλλοι 17 συμμετέχοντες ολοκλήρωσαν το μάθημα χωρίς πιστοποιητικό, δηλαδή η βαθμολογία τους στο τεστ γνώσεων ήταν κάτω από 75%.



Εικόνα 31. Στατιστικά στοιχεία για τους χρήστες που ολοκλήρωσαν την κατάρτιση

Τα ερωτηματολόγια μετά την κατάρτιση συμπληρώθηκαν και υποβλήθηκαν από 139 συμμετέχοντες: 31 στην Εσθονία, 24 στη Λετονία, 16 στην Κύπρο, 27 στη Μάλτα και 40 στη Λιθουανία.

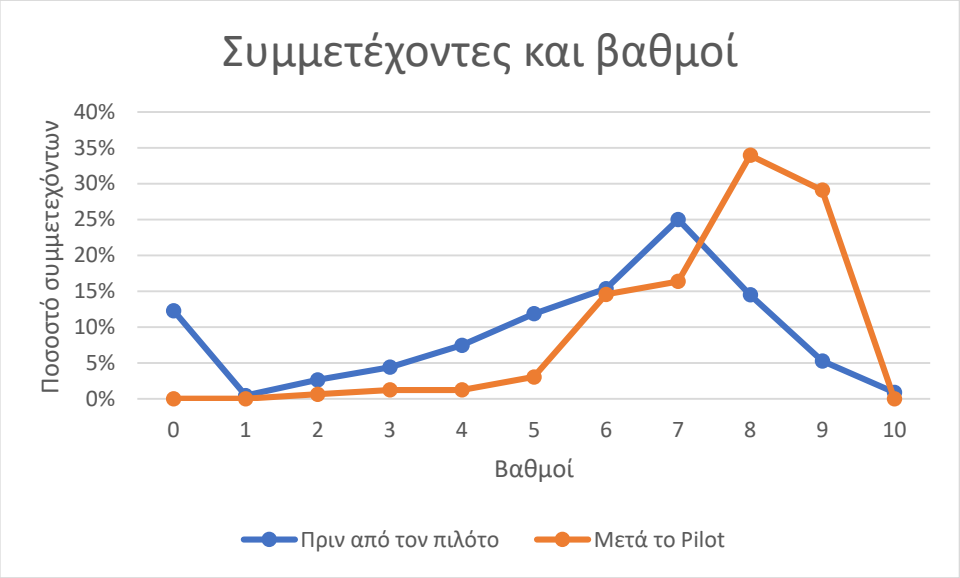
Τα ερωτηματολόγια μετά την επιμόρφωση συμπληρώθηκαν από 8 εκπαιδευτικούς: 2 στη Μάλτα, 3 στη Λιθουανία και από 1 στην Εσθονία, τη Λετονία και την Κύπρο. Οι εκπαιδευτικοί συμφώνησαν ότι το μάθημα πέτυχε τον στόχο του να εισαγάγει την ασφάλεια στον κυβερνοχώρο και το phishing στους μαθητές (το ίδιο ποσοστό των ερωτηθέντων δήλωσε ότι συμφωνεί και ότι συμφωνεί απόλυτα με τη δήλωση). Οι ερωτηθέντες συμφωνούν (62,5%) και συμφωνούν απόλυτα (37,5%) ότι ο βαθμός λεπτομέρειας που δόθηκε για τα θέματα που καλύφθηκαν από το πρόγραμμα ήταν κατάλληλος. Η πλειονότητα των εκπαιδευτικών (62,5%) συμφωνεί απόλυτα με τις δηλώσεις "Ο χρόνος που δόθηκε στους συμμετέχοντες για την ολοκλήρωση του πιλοτικού προγράμματος ήταν επαρκής" και "Οι τομείς των θεμάτων που καλύφθηκαν από το πρόγραμμα ήταν κατάλληλοι για το κοινό-στόχο".

Οι εκπαιδευτικοί σχολίασαν ότι το μάθημα είναι καλά σχεδιασμένο και αναπτύσσει την ευαισθητοποίηση και την κριτική σκέψη των συμμετεχόντων. Η εισαγωγή του δεν θα πρέπει να περιορίζεται σε μαθήματα που σχετίζονται με τις ΤΠΕ, αλλά θα πρέπει να εισαχθεί σε διάφορα μαθήματα, είτε εν μέρει είτε εξ ολοκλήρου. Τα πιο θετικά σχόλια προέρχονται από τις λύσεις σεναρίων.

Σύγκριση των γνώσεων των συμμετεχόντων πριν και μετά την πιλοτική εκπαίδευση

Η σύγκριση της αξιολόγησης των γνώσεων πριν και μετά την κατάρτιση έδειξε ότι οι συμμετέχοντες βελτίωσαν σημαντικά τις γνώσεις τους σχετικά με την ασφάλεια στον κυβερνοχώρο και το phishing. Το παρακάτω γράφημα δείχνει πώς φαίνονταν οι γνώσεις των συμμετεχόντων σχετικά με την ασφάλεια στον κυβερνοχώρο και την απάτη πριν και μετά την πιλοτική εκπαίδευση. Ο οριζόντιος άξονας δείχνει τα εύρη των βαθμολογιών (βαθμών) και ο κάθετος άξονας δείχνει το ποσοστό των μαθητών με την αντίστοιχη βαθμολογία.

Έτσι, το σχήμα δείχνει ότι μετά την εκπαίδευση στο CyberPhish, οι επιδόσεις των συμμετεχόντων βελτιώθηκαν σημαντικά, δηλαδή περισσότεροι μαθητές έλαβαν βαθμούς 8 ή υψηλότερους. Παράλληλα, μειώθηκε ο αριθμός των συμμετεχόντων που απέτυχαν στο τεστ γνώσεων, δηλαδή με βαθμολογία μεταξύ 0 και 6.



Εικόνα 32. Γνώσεις των συμμετεχόντων για την ασφάλεια στον κυβερνοχώρο και το phishing πριν και μετά την πιλοτική εκπαίδευση

6. ΕΚΠΑΙΔΕΥΣΗ ΠΙΛΟΤΩΝ ΣΕ ΧΩΡΕΣ ΣΥΝΕΡΓΑΤΩΝ

Στο κεφάλαιο αυτό παρουσιάζεται η εμπειρία των χωρών-εταίρων - Εσθονία, Κύπρος, Λετονία, Λιθουανία και Μάλτα - από την εφαρμογή προγραμμάτων κατάρτισης. Κάθε χώρα παρέχει πληροφορίες σχετικά με τομείς όπως η ενημέρωση των συμμετεχόντων και η διαδικασία επιλογής, το προφίλ των συμμετεχόντων, τα κίνητρα των σπουδαστών να συμμετάσχουν στην πιλοτική εκπαίδευση, η οργάνωση της εκπαιδευτικής διαδικασίας και η γνώμη των συμμετεχόντων για το περιεχόμενο.

Λιθουανία

Ενημέρωση των συμμετεχόντων και διαδικασία επιλογής

Για να αξιολογήσουν την ποιότητα του μαθήματος CyberPhish, οι εταίροι του έργου πραγματοποίησαν πιλοτική εκπαίδευση στις χώρες τους. Στη Λιθουανία, η πιλοτική εκπαίδευση πραγματοποιήθηκε με την πρόσκληση μελών της κοινότητας των καθηγητών του VU Kaunas, κυρίως φοιτητών. Οι προσκλήσεις αναρτήθηκαν στη σελίδα της Σχολής στο Facebook, στον ιστότοπο και οι καθηγητές παρουσίασαν το έργο κατά τη διάρκεια των διαλέξεών τους. Ο εταίρος του έργου, το Ινστιτούτο Πληροφορικής, προετοίμασε κατευθυντήριες γραμμές, ανέπτυξε ερωτηματολόγια πριν και μετά την εκπαίδευση, παρακολούθησε την πρόοδο της πιλοτικής εκπαίδευσης για όλους τους εταίρους και παρείχε στατιστικές πληροφορίες στους εταίρους μετά τη συστηματοποίηση των δεδομένων της εκπαίδευσης.

Προφίλ των συμμετεχόντων

Οι συμμετέχοντες στην πιλοτική εκπαίδευση ήταν ηλικίας 20-23 ετών και οι άνδρες ήταν ελαφρώς περισσότεροι από τις γυναίκες, με το 60% των συμμετεχόντων να είναι άνδρες.

Φοιτητές "κίνητρο για να ενταχθούν στην εκπαίδευση πιλότου κατάρτισης

Οι μαθητές παρακινήθηκαν από το γεγονός ότι με την πρόσφατη αύξηση των κυβερνοεπιθέσεων και της κλοπής προσωπικών δεδομένων, όλοι πρέπει να έχουν καλή γνώση της κυβερνοασφάλειας. Όλοι πρέπει να κατανοούν την κυβερνοϋγιεινή, πώς λειτουργούν οι επιθέσεις phishing και τι είναι η κοινωνική μηχανική. Όλα αυτά αυξάνουν τη δική μας ανθεκτικότητα απέναντι στους εγκληματίες του κυβερνοχώρου. Αυτός είναι ο λόγος για τον οποίο οι φοιτητές ήταν πρόθυμοι να συμμετάσχουν στο μάθημα εξ αποστάσεως εκπαίδευσης Cyberphish. Οι φοιτητές που ολοκληρώνουν το μάθημα και λαμβάνουν πιστοποιητικό λαμβάνουν έναν επιπλέον βαθμό για τον βαθμό του μαθήματός τους. Το μάθημα ήταν μια υποχρεωτική εργαστηριακή άσκηση για τη μελέτη των Πληροφοριακών Συστημάτων και της Ασφάλειας στον Κυβερνοχώρο. Οι φοιτητές ενθαρρύνονταν όχι μόνο να εξοικειωθούν με το υλικό του μαθήματος και

να δοκιμάσουν προσομοιώσεις, αλλά και να παρατηρήσουν πιθανές ανακρίβειες του συστήματος και λάθη που αφήνουν πίσω τους. Επίσης, επιβραβεύτηκαν για αυτή τους τη δραστηριότητα.

Οργάνωση της διαδικασίας κατάρτισης

Στην πιλοτική εκπαίδευση στη Λιθουανία συμμετείχαν φοιτητές από τους τομείς Οικονομίας και Διοίκησης, Λιθουανικής Φιλολογίας και Προώθησης, Εφαρμοσμένων Συστημάτων Χρηματοοικονομικής και Λογιστικής και Πληροφοριακών Συστημάτων και Κυβερνοασφάλειας. Αποφασίστηκε να προσκληθούν φοιτητές από ένα ευρύ φάσμα προγραμμάτων σπουδών για να ληφθεί όσο το δυνατόν περισσότερη ανατροφοδότηση, αξιολογώντας όχι μόνο το εκπαιδευτικό υλικό, τη φιλικότητα του μαθησιακού περιβάλλοντος προς το χρήστη, αλλά και την ποιότητα του μαθήματος. Η αίτηση του έργου προέβλεπε την πρόσκληση τουλάχιστον 24 συμμετεχόντων σε κάθε χώρα εταίρο. Αξίζει να σημειωθεί ότι ο αριθμός των συμμετεχόντων στην πιλοτική εκπαίδευση στη Λιθουανία ήταν σημαντικά υψηλότερος, με περισσότερους από 90 συμμετέχοντες να έχουν ενταχθεί μέχρι στιγμής στο μάθημα CyberPhish, 58 από τους οποίους έχουν ολοκληρώσει το μάθημα και τους έχει χορηγηθεί πιστοποιητικό ολοκλήρωσης του μαθήματος.

Γνώμη των συμμετεχόντων σχετικά με το περιεχόμενο

Ο κύριος στόχος της πιλοτικής κατάρτισης CyberPhish ήταν να ελεγχθούν και να αξιολογηθούν οι γνώσεις τους σχετικά με την ηλεκτρονική απάτη. Είναι ενθαρρυντικό ότι οι περισσότεροι συμμετέχοντες στην πιλοτική εκπαίδευση στη Λιθουανία έμειναν ικανοποιημένοι από το μάθημα CyberPhish. Το 43% των συμμετεχόντων δήλωσε ότι οι προσομοιώσεις που ενσωματώθηκαν στο μάθημα CyberPhish βελτίωσαν την ικανότητά τους να εντοπίζουν επιθέσεις απάτης στο διαδίκτυο, ενώ ένα επιπλέον 52% δήλωσε ότι βελτίωσαν την ικανότητά τους να εντοπίζουν επιθέσεις απάτης στο διαδίκτυο ακόμη και πολύ.

Μεταξύ 40% και 60% των συμμετεχόντων που ολοκλήρωσαν το μάθημα δήλωσαν ότι έμαθαν πολλά νέα πράγματα. Οι συμμετέχοντες ήταν πολύ αισιόδοξοι για τα ακόλουθα θέματα. Δήλωσαν ότι είχαν μάθει πολλά νέα πράγματα: "Αντιμετώπιση επιθέσεων στον κυβερνοχώρο", "Νομικές πτυχές της ασφάλειας στον κυβερνοχώρο", "Διαφορετικοί τύποι επιθέσεων και τεχνικών phishing" και "Μονάδες κοινωνικής μηχανικής και χειραγώγησης".

Η ανατροφοδότηση που παρείχαν οι συμμετέχοντες στην πιλοτική εκπαίδευση CyberPhish επιβεβαίωσε τη φιλοδοξία των εταίρων να συμβάλουν στην ανάπτυξη δεξιοτήτων κυβερνοασφάλειας και στη διαμόρφωση μιας ασφαλέστερης κοινωνίας μέσω του μαθήματος CyberPhish.

Εσθονία

Ενημέρωση των συμμετεχόντων και διαδικασία επιλογής

Οι συμμετέχοντες παρακολούθησαν το μάθημα "Principles of Secure Software Design" στο Πανεπιστήμιο του Tartu. Ο πιλότος αποτέλεσε μέρος του μαθήματος. Οι συμμετέχοντες ήταν κυρίως φοιτητές του προγράμματος σπουδών Κυβερνοασφάλειας που δόθηκε από κοινού στο Πανεπιστήμιο του Ταρτού (UT) και στο Τεχνολογικό Πανεπιστήμιο του Ταλίν (TalTech). Επιπλέον, στο πιλοτικό πρόγραμμα συμμετείχαν μερικοί φοιτητές του προγράμματος Erasmus+, οι οποίοι παρακολουθούσαν επίσης το προαναφερθέν μάθημα.

Επιλογή: ο πιλότος συμπεριλήφθηκε ως μέρος αυτού του μαθήματος για τους ακόλουθους λόγους:

1. Δεδομένου ότι το Phishing αναφέρθηκε πρόσφατα ως ο νούμερο 1 κίνδυνος ασφάλειας στην Εσθονία, οι μελλοντικοί ειδικοί της κυβερνοασφάλειας πρέπει να γνωρίζουν αυτόν τον κίνδυνο, να είναι έτοιμοι να αντιδράσουν και να μπορούν να διδάξουν στους άλλους τις επιπτώσεις του,

2. Το υπόβαθρο των συμμετεχόντων είναι πολύ κατάλληλο για την πιλοτική εφαρμογή αυτού του τύπου μαθημάτων. Είναι νέοι ειδικοί τόσο στην κυβερνοασφάλεια όσο και στην επιστήμη των υπολογιστών και μπορούν να σχολιάσουν τις ελλείψεις τόσο του περιεχομένου του μαθήματος όσο και της πλατφόρμας λογισμικού που αναπτύχθηκε.

3. Το περιεχόμενο του μαθήματος συμπλήρωσε το υλικό "Αρχές ασφαλούς σχεδίασης λογισμικού". Το "ψάρεμα" είναι ένας ακόμη τύπος επίθεσης. Έτσι, παρόμοιες αρχές (όπως και σε άλλους κινδύνους ασφάλειας) απεικονίστηκαν μέσω των δοθέντων πιλοτικών διαλέξεων, σεναρίων και αναγνώρισης κινδύνων.

Προφίλ των συμμετεχόντων

Ο μέσος όρος ηλικίας των συμμετεχόντων στην εκπαίδευση πιλότων ήταν 31 έτη, με τον μεγαλύτερο 47 ετών και τον μικρότερο 22 ετών. Οι άνδρες συμμετέχοντες ήταν έξι φορές περισσότεροι από τις γυναίκες (31 άνδρες και πέντε γυναίκες). Όλοι οι συμμετέχοντες ήταν μεταπτυχιακοί φοιτητές του 1ου έτους του προγράμματος Cybersecurity, 2ο

εξάμηνο. Υπήρχε ίσος αριθμός Εσθονών και συμμετεχόντων, υποδεικνύοντας άλλες χώρες (18 συμμετέχοντες ο καθένας).

Κίνητρα των σπουδαστών να ενταχθούν στην εκπαίδευση πιλότων

Η πιλοτική εφαρμογή ήταν μέρος του μαθήματος "Αρχές ασφαλούς σχεδίασης λογισμικού. Οι φοιτητές μπορούσαν να κερδίσουν έως και 10 βαθμούς στην αξιολόγηση του μαθήματος (ανάλογα με το τελικό τεστ γνώσεων).

Οργάνωση της διαδικασίας κατάρτισης

Η εκπαίδευση πραγματοποιήθηκε διαδικτυακά. Η διάλεξη αρχικοποίησης δόθηκε στις 5 Μαΐου. Τα υπόλοιπα δόθηκαν ως εργασία αυτοδιδασκαλίας. Οι σπουδαστές μπορούσαν να στείλουν τις ερωτήσεις και τα σχόλιά τους μέσω ηλεκτρονικού ταχυδρομείου ή να ρωτήσουν σχετικά με την εκπαίδευση κατά τη διάρκεια άλλων διαλέξεων του μαθήματος.

Γνώμες των συμμετεχόντων σχετικά με το περιεχόμενο

Μια έρευνα των μαθητών μετά την πιλοτική εκπαίδευση έδειξε ότι όλοι οι μαθητές βελτίωσαν τις γνώσεις τους σχετικά με το Phishing. Ιδιαίτερα η βελτίωση των γνώσεων παρατηρήθηκε στις νομικές πτυχές της κυβερνοασφάλειας, στο χειρισμό κυβερνοεπιθέσεων, στις τάσεις του τοπίου της κυβερνοασφάλειας, στα είδη και τις τεχνικές των επιθέσεων Phishing, στην κοινωνική μηχανική και στην αναγνώριση επιθέσεων Phishing. Όλοι οι συμμετέχοντες έμειναν ικανοποιημένοι από τις γνώσεις τους σε θέματα κυβερνοασφάλειας μετά την ολοκλήρωση του μαθήματος CyberPhish. Σχεδόν όλοι οι σπουδαστές συμφώνησαν ότι οι προσομοιώσεις βοήθησαν στη βελτίωση των δεξιοτήτων τους στην αναγνώριση του phishing. Όλοι οι συμμετέχοντες συμφώνησαν έντονα ότι η διαδικτυακή προσέγγιση ήταν κατάλληλη για το αντικείμενο του μαθήματος, ότι ο χρόνος που δόθηκε για την ολοκλήρωση του μαθήματος ήταν επαρκής και ότι θα συνιστούσαν το μάθημα αυτό σε άλλα άτομα. Η πλειονότητα των μαθητών συμφώνησε ότι είχαν κατανοήσει σαφώς τους στόχους του μαθήματος, ότι το περιεχόμενο του μαθήματος κάλυπτε τους στόχους του μαθήματος και ότι η υποστήριξη κατά τη διάρκεια του μαθήματος ήταν κατάλληλη.

Μάλτα

Ενημέρωση των συμμετεχόντων και διαδικασία επιλογής

Το Cyber phishing επηρεάζει διάφορους τομείς και όχι μόνο την Πληροφορική. Στο πλαίσιο αυτό, στο στόχαστρο βρέθηκαν φοιτητές από διαφορετικά προγράμματα σπουδών. Η MECB προσκάλεσε τους συμμετέχοντες φοιτητές από τα Ανώτατα Εκπαιδευτικά Ιδρύματα (AEI) μέσω των κοινωνικών εταίρων της. Στην πιλοτική εκπαίδευση συμμετείχαν σπουδαστές από το Malta College of Arts, Science and Technology (MCAST), το οποίο είναι ο κύριος πάροχος επαγγελματικής εκπαίδευσης και κατάρτισης (VET) στο νησί, και το University of Malta (UoM) - Junior College. Εκτός από τους σπουδαστές, η MECB Ltd επικεντρώθηκε επίσης σε άλλους ενδιαφερόμενους φορείς, συμπεριλαμβανομένων, μεταξύ άλλων, εμπειρογνωμόνων, υπευθύνων χάραξης πολιτικής και εκπαιδευτικών. Αυτοί κλήθηκαν να συμμετάσχουν μέσω του δικτυακού τόπου της MECB. Το εκπαιδευτικό υλικό, τα σενάρια, η αυτοαξιολόγηση και τα τεστ αξιολόγησης των γνώσεων που αναπτύχθηκαν κατά τη διάρκεια του έργου CyberPhish χρησιμοποιήθηκαν επίσης για να προσδιοριστεί το επίπεδο γνώσεων των ενδιαφερομένων πριν και μετά το μάθημα.

Επιλέχθηκαν επίσης εκπαιδευτές και συντονιστές από το AEI και την MECB Ltd για να δώσουν λεπτομέρειες σχετικά με το έργο CyberPhish και να παρακολουθήσουν την πιλοτική εκπαίδευση. Πριν από την πιλοτική εκπαίδευση, οι εκπαιδευτές ενημερώθηκαν σχετικά με το συνολικό έργο CyberPhish, συμπεριλαμβανομένων, μεταξύ άλλων, της έρευνας μελέτης (IO1), του προγράμματος σπουδών CyberPhish (IO2) και του υλικού μαθημάτων (IO3) και των σεναρίων που αναπτύχθηκαν (IO4). Με τον τρόπο αυτό επιδιώχθηκε να δημιουργηθεί ευαισθητοποίηση για το έργο και να μπορέσουν οι εκπαιδευτές να βοηθήσουν τους ενδιαφερόμενους σε τυχόν δυσκολίες. Επιπλέον, τους παρουσιάστηκε ο τρόπος χρήσης της ηλεκτρονικής πλατφόρμας, της αυτοαξιολόγησης και των τεστ αξιολόγησης των γνώσεων. Πριν από την πιλοτική εφαρμογή πραγματοποιήθηκε επίσης συζήτηση και ενημέρωση για τις μεθόδους μάθησης που θα μπορούσαν να χρησιμοποιηθούν για την αποτελεσματική εργασία με τα ενδιαφερόμενα μέρη. Κατά τη διάρκεια αυτής της συνεδρίασης, δόθηκαν στους εκπαιδευτές μεθοδολογικές κατευθυντήριες γραμμές που αναπτύχθηκαν ρητά για τους εκπαιδευτές μαζί με και άλλες κατευθυντήριες γραμμές για τους σπουδαστές, οι οποίες διανεμήθηκαν στους σπουδαστές κατά την έναρξη της πιλοτικής κατάρτισης.

Προφίλ των συμμετεχόντων

Σαράντα τρεις συμμετέχοντες έλαβαν μέρος στην πιλοτική εκπαίδευση. Περισσότεροι από τα δύο τρίτα των συμμετεχόντων ήταν άνδρες (71,4%) και σχεδόν το ένα τρίτο ήταν γυναίκες (28,6%). Οι περισσότεροι συμμετέχοντες ήταν υπάλληλοι (60,7%), το 21,4% ήταν φοιτητές και το ένα δέκατο (10,7%) ήταν επιχειρηματίες. Οι υπόλοιποι συμμετέχοντες δήλωσαν ότι ήταν αυτοαπασχολούμενοι και άλλοι.

Οργάνωση της διαδικασίας κατάρτισης

Συνολικά πραγματοποιήθηκαν τρεις πιλοτικές εκπαιδεύσεις στη Μάλτα ως εξής:

1) Πρόσωπο με πρόσωπο (φοιτητές από το Ινστιτούτο Διοίκησης Επιχειρήσεων και Εμπορίου (IBMC) στο MCAST)
2) Online (φοιτητές που παρακολουθούν μαθήματα Πληροφορικής στο Junior College UoM)
3) Ανοικτό μάθημα (με πρόσκληση όλων των ενδιαφερομένων, συμπεριλαμβανομένων των εκπαιδευομένων, των εμπειρογνωμόνων, των φορέων χάραξης πολιτικής και των εκπαιδευτικών)

Συνολικά 75 εκπαιδευόμενοι εγγράφηκαν στο σύστημα, εκ των οποίων το 57% (43) ολοκλήρωσε πλήρως το τελικό μάθημα. Από αυτούς, το 67% επιχείρησε τις προσομοιώσεις, ενώ το 91% πήγε στην τελική αξιολόγηση. Τριάντα εκπαιδευόμενοι που επιχείρησαν την αξιολόγηση κατάφεραν να λάβουν 75% και άνω της συνολικής βαθμολογίας.

Γνώμες των συμμετεχόντων σχετικά με το περιεχόμενο

Μια έρευνα των συμμετεχόντων μετά την πιλοτική εκπαίδευση έδειξε ότι βελτίωσαν τις γνώσεις τους σχετικά με το phishing σε όλα τα θέματα κυβερνοασφάλειας του μαθήματος CyberPhish. Οι συμμετέχοντες σημείωσαν επίσης ότι είχαν αποκτήσει πολλές νέες γνώσεις σχετικά με το phishing. Όλοι οι συμμετέχοντες ήταν ικανοποιημένοι με τις γνώσεις τους σε θέματα κυβερνοασφάλειας μετά την ολοκλήρωση του μαθήματος CyberPhish. Σχεδόν όλοι οι μαθητές συμφώνησαν ότι οι προσομοιώσεις βοήθησαν στη βελτίωση των δεξιοτήτων τους αναγνωρίζοντας το phishing. Η πλειονότητα των ερωτηθέντων συμφώνησε ή συμφώνησε απόλυτα με τις δηλώσεις:

- ο χρόνος που δίνεται για την ολοκλήρωση του μαθήματος να είναι επαρκής,
- η κατάρτιση και η υποστήριξη καθ' όλη τη διάρκεια των μαθημάτων να είναι κατάλληλες,
- είχαν σαφή κατανόηση των στόχων του μαθήματος,
- το περιεχόμενο του μαθήματος κάλυπτε τους στόχους του μαθήματος,
- η διαδικτυακή προσέγγιση της μάθησης ήταν κατάλληλη για το μάθημα,
- θα συνιστούσαν αυτό το μάθημα σε άλλους ανθρώπους.

Κύπρος

Ενημέρωση των συμμετεχόντων και διαδικασία επιλογής

Κατά τη διάρκεια της πιλοτικής κατάρτισης στην Κύπρο, στόχος ήταν φοιτητές από διαφορετικά προγράμματα σπουδών - συγκεκριμένα, σπουδές πληροφορικής, ευρωπαϊκές σπουδές, σπουδές μάρκετινγκ και ούτω καθεξής. Η DOREA προσκάλεσε επίσης οργανισμούς (άλλα ιδρύματα εκπαίδευσης ενηλίκων καθώς και ΜΜΕ και τους υπαλλήλους τους από το δίκτυό μας) να συμμετάσχουν στο πιλοτικό πρόγραμμα.

Η DOREA απηύθυνε ανοιχτή πρόσκληση και κάλεσε όλους τους ενδιαφερόμενους να συμμετάσχουν στο πιλοτικό πρόγραμμα, λαμβάνοντας υπόψη ότι όλοι οι άνθρωποι πρέπει να έχουν αυτές τις δεξιότητες, όχι μόνο οι φοιτητές των προγραμμάτων πληροφορικής. Οι προσκλήσεις έγιναν μέσω ηλεκτρονικού ταχυδρομείου, τηλεφωνικών κλήσεων και προσωπικών συναντήσεων.

Προφίλ των συμμετεχόντων

Είκοσι έξι συμμετέχοντες έλαβαν μέρος στην πιλοτική εκπαίδευση. Η πλειονότητα των συμμετεχόντων ήταν φοιτητές στην ηλικία των 20 ετών (92,3%) και το υπόλοιπο 7,7% ήταν υπάλληλοι. Περισσότερα από τα δύο τρίτα των συμμετεχόντων ήταν γυναίκες (76,9%) και σχεδόν το ένα τρίτο ήταν άνδρες (23,1%).

Οργάνωση της διαδικασίας κατάρτισης

Η κατάρτιση στην Κύπρο οργανώθηκε κυρίως διαδικτυακά με διαδικτυακή ανατροφοδότηση/βοήθεια από τον εκπαιδευτή. Σε ορισμένες περιπτώσεις πραγματοποιήθηκαν και δια ζώσης διαβουλεύσεις.

Για τη διαδικτυακή κατάρτιση, κάθε συμμετέχων που εκδήλωσε ενδιαφέρον να συμμετάσχει έλαβε ηλεκτρονικό μήνυμα με τις οδηγίες και τα βήματα που έπρεπε να ακολουθήσει για να εγγραφεί στο μάθημα. Όλοι οι σπουδαστές κλήθηκαν να συμπληρώσουν το τεστ αυτοαξιολόγησης πριν από την εγγραφή τους στο μάθημα και αφού παρακολουθήσουν το μάθημα.

Κατά τη διάρκεια του μαθήματος, ο εκπαιδευτής συμβουλευόταν τους συμμετέχοντες μέσω ηλεκτρονικών μηνυμάτων, τηλεφωνημάτων και διαδικτυακών και προσωπικών συναντήσεων (όταν ήταν δυνατόν), καθοδηγώντας τους, απαντώντας στις ερωτήσεις τους ή παρέχοντας πρόσθετες πηγές πληροφοριών.

Οι περισσότεροι από τους συμμετέχοντες παρακολούθησαν το σεμινάριο καθώς ενδιαφέρονταν γενικά για το θέμα και άλλοι εξήγησαν ότι πιστεύουν ότι το πιστοποιητικό που έλαβαν θα τους φανεί χρήσιμο στο μέλλον. Είκοσι πέντε από τους 26 συμμετέχοντες ολοκλήρωσαν πλήρως το μάθημα και έλαβαν πιστοποιητικά.

Γνώμη των συμμετεχόντων σχετικά με το περιεχόμενο

Όλοι οι συμμετέχοντες δήλωσαν ότι απέκτησαν πολλές νέες γνώσεις ή βελτίωσαν τις γνώσεις τους σε όλους τους τομείς. Η πλειονότητα των συμμετεχόντων ανέφερε ότι απέκτησε πολλές νέες γνώσεις στα θέματα "Κοινωνική μηχανική" και "Τύποι επιθέσεων και τεχνικών phishing". Η πλειονότητα των συμμετεχόντων βελτίωσε τις γνώσεις της στους τομείς "Νομικές πτυχές της ασφάλειας στον κυβερνοχώρο", "Προληπτικές ενέργειες για περιστατικά στον κυβερνοχώρο" και "Χειρισμός περιστατικών στον κυβερνοχώρο". Μόνο ένας συμμετέχων δήλωσε ότι δεν έμαθε τίποτα καινούργιο όσον αφορά την "Αναγνώριση επιθέσεων phishing".

Η πλειονότητα των συμμετεχόντων δήλωσε ότι είναι ικανοποιημένοι με τις γνώσεις τους σχετικά με τα θέματα κυβερνοασφάλειας που διδάχθηκαν στο μάθημα μετά την ολοκλήρωσή του. Κάποιο μικρό ποσοστό των συμμετεχόντων (από 3,8% έως 11,5%) ήταν ουδέτερο κατά την αξιολόγηση των γνώσεών τους. Αυτό μπορεί να υποδηλώνει ότι, ενώ πίστευαν ότι απέκτησαν πολλές γνώσεις, υπάρχει ακόμη χώρος για βελτίωση. Η πλειονότητα των συμμετεχόντων ανέφερε ότι οι προσομοιώσεις είτε "τους βοήθησαν πολύ" είτε "τους βοήθησαν" να κατανοήσουν τα διδαχθέντα θέματα του κυβερνοχώρου. Η πλειονότητα των συμμετεχόντων είχε μεγάλη εμπειρία με το μάθημα όσον αφορά την κατανόηση των στόχων του μαθήματος, την εύρεση της διαδικτυακής προσέγγισης και του περιεχομένου κατάλληλου, την ύπαρξη αρκετού χρόνου για την ολοκλήρωση του μαθήματος κ.λπ. Ένας1 συμμετέχων ανέφερε ότι δεν βρήκε την ηλεκτρονική προσέγγιση της μάθησης κατάλληλη για το μάθημα, ένας συμμετέχων βρήκε την πλατφόρμα δύσκολη στη χρήση και ένα άτομο δεν θα συνιστούσε το μάθημα αυτό σε άλλα άτομα.

Ο εκπαιδευτής του CyberPhish δηλώνει ότι το μάθημα είναι πολύ κατατοπιστικό και καλύπτει όλα τα σημαντικά θέματα που είναι απαραίτητα για να κατανοήσουν οι μαθητές τα θέματα κυβερνοασφάλειας, ιδίως το phishing, καθώς και να μάθουν πώς να προστατεύονται. Τόνισε ότι το μάθημα είναι σίγουρα χρήσιμο όχι μόνο για τους φοιτητές πληροφορικής για την ανανέωση των δεξιοτήτων και των γνώσεών τους, αλλά και για τους φοιτητές άλλων τομέων, τους εργαζόμενους και τη γενική κοινωνία.

Λετονία

Ενημέρωση των συμμετεχόντων και διαδικασία επιλογής

Η πιλοτική κατάρτιση υλοποιήθηκε με τους κοινωνικούς εταίρους, το Τεχνικό Πανεπιστήμιο της Ρίγα (RTU) και το Κολέγιο Πολιτισμού της Λετονίας. Η Altacom διοργάνωσε ξεχωριστές συναντήσεις με τις φοιτητικές κυβερνήσεις του RTU και του LKK προκειμένου να παρουσιάσει το έργο CyberPhish και την προβλεπόμενη πιλοτική εκπαίδευση. Οι φοιτητές μετά τη συνάντηση κατευθύνθηκαν στον υπεύθυνο για τη μη τυπική εκπαίδευση στα ΑΕΙ τους. Οι κοινωνικοί εταίροι και οι επαφές από το κολλέγιο πολιτισμού της Λετονίας, έστειλαν προσκλήσεις σε φοιτητές (κυρίως από σχολές μη πληροφορικής).

Προφίλ των συμμετεχόντων

Είκοσι επτά συμμετέχοντες έλαβαν μέρος στην πιλοτική εκπαίδευση. Ο μέσος όρος ηλικίας των συμμετεχόντων στην πιλοτική εκπαίδευση ήταν 23 έτη, με τον μεγαλύτερο - 26 ετών και τον νεότερο - 19 ετών. Οι άνδρες συμμετέχοντες ήταν μιάμιση φορά περισσότεροι από τις γυναίκες (60% άνδρες και 40% γυναίκες). Σε γενικές γραμμές, οι συμμετέχοντες ήταν φοιτητές από τεχνικούς και πολιτιστικούς τομείς. Οι περισσότεροι από τους συμμετέχοντες ήταν Λετονοί που ζουν σήμερα στη Ρίγα, αλλά υπήρχαν και φοιτητές ανταλλαγής που προέρχονταν από διαφορετικές χώρες και σπούδαζαν στη Λετονία.

Κίνητρα των σπουδαστών να ενταχθούν στην εκπαίδευση πιλότων

Το πιλοτικό πρόγραμμα εισήχθη ως νέο πρόσθετο μέσο μη τυπικής εκπαίδευσης που μπορεί να βοηθήσει τους μαθητές να αποκτήσουν πολύτιμες θεωρητικές και πρακτικές δεξιότητες στην ασφάλεια στον κυβερνοχώρο. Σήμερα, οι δεξιότητες αυτές είναι πολύ χρήσιμες όχι μόνο για προσωπική χρήση αλλά και σε όλους σχεδόν τους χώρους εργασίας όπου χρησιμοποιούνται υπολογιστές. Ως εκ τούτου, ορισμένοι από τους προσκεκλημένους μαθητές αποφάσισαν ότι η συμμετοχή στο πιλοτικό πρόγραμμα μπορεί να είναι πραγματικά επωφελής γι' αυτούς και συμφώνησαν να συμμετάσχουν.

Οργάνωση της διαδικασίας κατάρτισης

Οι κύριες πληροφορίες σχετικά με το πιλοτικό πρόγραμμα δόθηκαν κατά τη διάρκεια της συνάντησης με τις φοιτητικές κυβερνήσεις του RTU και του LKK και στην πρόσκληση. Επιπλέον, οι συμμετέχοντες μπορούσαν να επικοινωνήσουν απευθείας με τις ερωτήσεις και τα σχόλιά τους μέσω ηλεκτρονικού ταχυδρομείου ή άλλων επαφών (π.χ. μήνυμα σε ένα κοινωνικό δίκτυο).

Υπήρχαν 45 εγγεγραμμένοι συμμετέχοντες στην πλατφόρμα μάθησης. 25 συμμετέχοντες πέρασαν το τεστ γνώσεων με βαθμολογία άνω του 75%. 2 συμμετέχοντες πέρασαν το τεστ γνώσεων (στα λετονικά) με βαθμολογία κάτω του 75%.

Γνώμη των συμμετεχόντων σχετικά με το περιεχόμενο

Μια έρευνα των συμμετεχόντων μετά την πιλοτική εκπαίδευση έδειξε ότι απέκτησαν πολλές γνώσεις σχετικά με το phishing σε όλα σχεδόν τα θέματα κυβερνοασφάλειας του μαθήματος CyberPhish. Οι συμμετέχοντες βελτίωσαν τις γνώσεις τους σχετικά με το phishing στις ενότητες "Νομικές πτυχές της κυβερνοασφάλειας", "Οι τάσεις της κυβερνοασφάλειας", "Προληπτικές ενέργειες της κυβερνοασφάλειας" και "Αντιμετώπιση κυβερνοεπιθέσεων". Η πλειονότητα των συμμετεχόντων ήταν ικανοποιημένοι με τις γνώσεις τους σε θέματα κυβερνοασφάλειας μετά την ολοκλήρωση του μαθήματος CyberPhish, ιδίως με τις ενότητες "Επιθέσεις στον κυβερνοχώρο - Κοινωνική μηχανική και Phishing" και "Κατανόηση και χειρισμός επιθέσεων στον κυβερνοχώρο". Σχεδόν όλοι οι σπουδαστές συμφώνησαν ότι οι προσομοιώσεις βοήθησαν στη βελτίωση των δεξιοτήτων τους αναγνωρίζοντας το phishing. Η πλειονότητα των ερωτηθέντων συμφώνησε ή συμφώνησε απόλυτα με τις δηλώσεις:

- θα συνιστούσαν αυτό το μάθημα σε άλλους ανθρώπους
- η κατάρτιση και η υποστήριξη καθ' όλη τη διάρκεια των μαθημάτων να είναι κατάλληλες,
- η ηλεκτρονική πλατφόρμα μάθησης ήταν εύχρηστη,
- ο χρόνος που δίνεται για την ολοκλήρωση του μαθήματος να είναι επαρκής,
- το περιεχόμενο του μαθήματος κάλυπτε τους στόχους του μαθήματος,
- είχαν σαφή κατανόηση των στόχων του μαθήματος,
- η διαδικτυακή προσέγγιση της μάθησης ήταν κατάλληλη για το μάθημα.

ΣΥΜΠΕΡΆΣΜΑΤΑ

Με βάση μια ανάλυση αναγκών, η κοινοπραξία εταίρων ανέπτυξε ένα πρόγραμμα κατάρτισης σχετικά με την ασφάλεια στον κυβερνοχώρο, τις κυβερνοεπιθέσεις, την κοινωνική μηχανική, με ιδιαίτερη έμφαση στον εντοπισμό και την πρόληψη του phishing. Το πρόγραμμα σπουδών σχεδιάστηκε για μικτή μάθηση, αλλά η δομή του το καθιστά ευέλικτο και μπορεί να χρησιμοποιηθεί τόσο για εξ αποστάσεως όσο και για δια ζώσης εκπαίδευση. Το πλήρες εκπαιδευτικό πρόγραμμα αποτελείται από 30 ώρες που αντιστοιχούν σε 1 ECTS.

Το πρόγραμμα σπουδών είναι δομημένο σε τέσσερα διακριτά μέρη (ενότητες): Κατανοώντας και αντιμετωπίζοντας κυβερνοεπιθέσεις.

Η κοινοπραξία των εταίρων ανέπτυξε το διαδικτυακό εκπαιδευτικό υλικό σύμφωνα με το πρόγραμμα σπουδών CyberPhish και σύμφωνα με τις ανάγκες της 4ης βιομηχανικής επανάστασης. Κατά τη διάρκεια του έργου οι εταίροι δημιούργησαν εκπαιδευτικό υλικό το οποίο αποτελείται από διαφάνειες, αξιολογήσεις και συνδέσμους προς εξωτερικές πηγές και βίντεο. Το εκπαιδευτικό υλικό που αναπτύχθηκε αξιολογήθηκε καλά από ανεξάρτητους εμπειρογνώμονες.

Τα προγράμματα σπουδών, το εκπαιδευτικό υλικό και το μαθησιακό περιβάλλον που αναπτύχθηκαν μπορούν να χρησιμοποιηθούν για διάφορες ομάδες-στόχους, για παράδειγμα, φοιτητές, εκπαιδευτικοί, πανεπιστημιακό προσωπικό (μέλη της κοινότητας), κέντρα ενηλίκων και ο επιχειρηματικός τομέας (εργοδότες και εργαζόμενοι).

Το υλικό ηλεκτρονικής μάθησης που αναπτύχθηκε, το μικτό περιβάλλον μάθησης και οι προσομοιώσεις ενσωματώθηκαν στα μαθήματα των συμμετεχόντων πανεπιστημίων κατά τη διάρκεια της πιλοτικής κατάρτισης.

Το εκπαιδευτικό υλικό που αναπτύχθηκε, οι προσομοιώσεις, τα τεστ αυτοαξιολόγησης και τα τεστ αξιολόγησης των γνώσεων συμβάλλουν στην ενίσχυση της κριτικής σκέψης των συμμετεχόντων και των δεξιοτήτων τους στον τομέα της ασφάλειας στον κυβερνοχώρο, ώστε να εφαρμοστούν στην επαγγελματική τους πρακτική. Το μάθημα CyberPhish μπορεί να χρησιμοποιηθεί με επιτυχία για τη διοργάνωση κατάρτισης για άλλες ομάδες-στόχους, όχι μόνο κατά τη διάρκεια της πιλοτικής κατάρτισης στις συμμετέχουσες χώρες, αλλά και μέσω προσαρμογής σε άλλες ευρωπαϊκές χώρες.

Η σύγκριση της αξιολόγησης των γνώσεων πριν και μετά την κατάρτιση έδειξε ότι οι συμμετέχοντες βελτίωσαν σημαντικά τις γνώσεις τους σχετικά με την ασφάλεια στον κυβερνοχώρο και το phishing. Τα δεδομένα δείχνουν ότι οι επιδόσεις των συμμετεχόντων βελτιώθηκαν σημαντικά, δηλαδή περισσότεροι μαθητές έλαβαν βαθμό 8 ή υψηλότερο.

Εκατόν εβδομήντα πέντε συμμετέχοντες ολοκλήρωσαν (175) το πρόγραμμα κατάρτισης και έλαβαν πιστοποιητικό: 36 στην Εσθονία, 25 στη Λετονία, 26 στην Κύπρο, 30 στη Μάλτα και 58 στη Λιθουανία. Άλλοι 17 συμμετέχοντες ολοκλήρωσαν το μάθημα χωρίς πιστοποιητικό, δηλαδή η βαθμολογία τους στο τεστ γνώσεων ήταν κάτω από 75%.

ΑΝΑΦΟΡΈΣ

1. ENISA (2019): Ανάπτυξη δεξιοτήτων κυβερνοασφάλειας στην ΕΕ. Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια. Δεκέμβριος, 2019. URL: ENISA (europa.eu) (πρόσβαση 09/08/2022).
2. Συμβούλιο της Ευρωπαϊκής Ένωσης (2021): Σχέδιο συμπερασμάτων του Συμβουλίου σχετικά με τη στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο για την ψηφιακή δεκαετία, URL https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=Cybersecurity%3a+Council+adopts+conclusions+on+the+EU%27s+cybersecurity+strategy (πρόσβαση 09/08/2022)
3. Καλές πρακτικές στην καινοτομία για την ασφάλεια στον κυβερνοχώρο στο πλαίσιο του NCSS, 19 Νοεμβρίου 2019
4. IO1 A2: Results "Analysis of Existing Cybersecurity training programs", 2021, URL:https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A2_EN_CYBERPHISH-REPORT_study-analysis.pdf
5. Proofpoint (2019): URL https://www.proofpoint.com/us/resources/threat-reports/human-factor.
6. Οργανισμός της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο (2020): ENISA 2019-2020
7. IO1 A1 "ΑΝΑΓΝΏΡΙΣΗ ΤΟΥ PHISHING ΚΑΙ ΤΩΝ ΚΕΝΏΝ ΔΕΞΙΟΤΉΤΩΝ", 2021, URL:https://cyberphish.eu/wp-content/uploads/2021/07/IO1-A1_EN_CYBERPHISH-REPORT_survey-results.pdf
8. Robert B. Cialdini (2006) Η ψυχολογία της πειθούς. Harper Business, 336 σελ. ISBN: 978-0061241895
9. Ομάδα NCC (2020) :Ψυχολογία του Phish: Αξιοποίηση των επτά αρχών της επιρροής, URL: https://www.mynewsdesk.com/nccgroup/blog_posts/psychology-of-the-phish-leveraging-the-seven-principles-of-influence-95433

ΠΑΡΆΡΤΗΜΑ 1

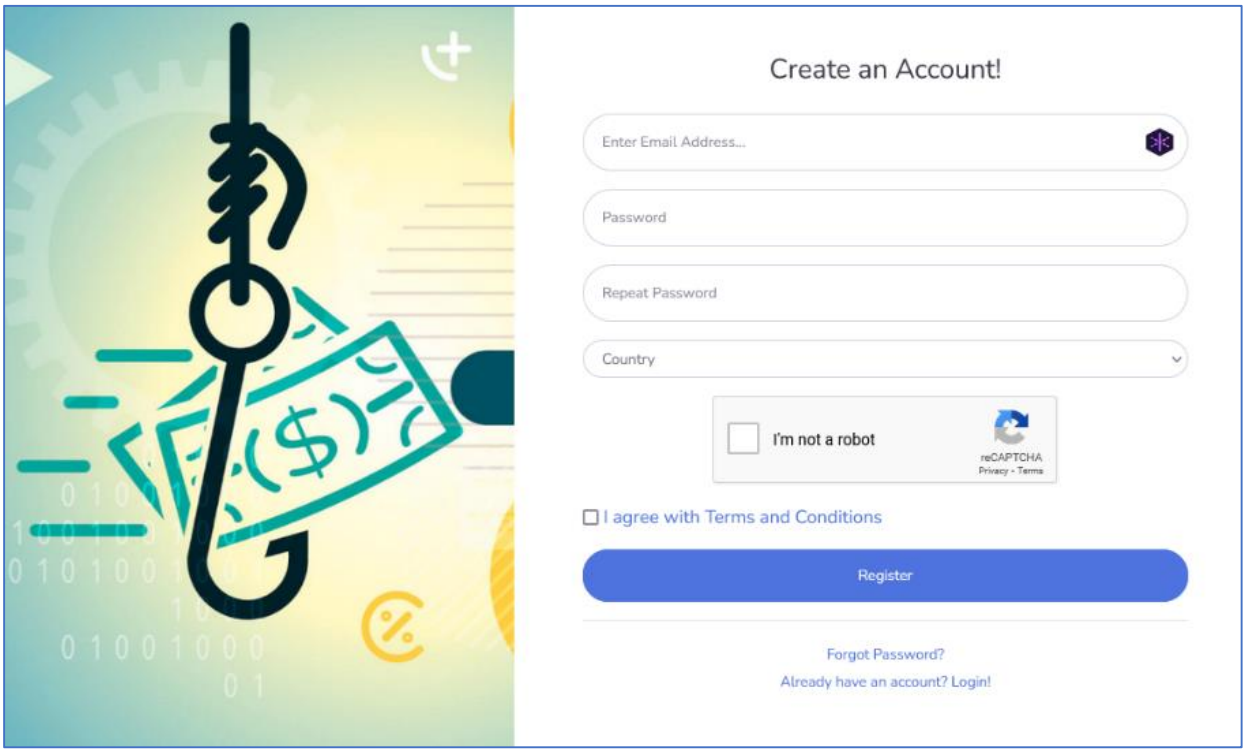
ΠΕΡΙΒΆΛΛΟΝ ΜΆΘΗΣΗΣ CYBERPHISH

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.

Εγγραφή στο περιβάλλον ηλεκτρονικής μάθησης

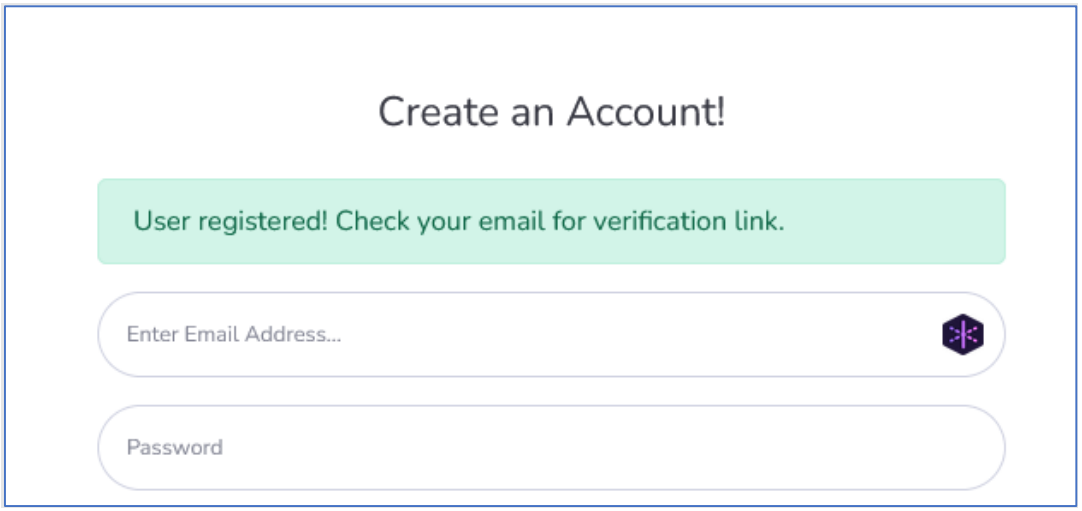
Για να γίνετε εγγεγραμμένος χρήστης, δημιουργήστε έναν λογαριασμό κάνοντας κλικ στο κουμπί "Εγγραφή".

Αφού κάνετε κλικ στο κουμπί **Sign up** στο πάνω μέρος της σελίδας t ype το email σας, τον κωδικό πρόσβασης, επαναλάβετε τον κωδικό πρόσβασης και επιλέξτε τη χώρα σας. Πρέπει επίσης να επιβεβαιώσετε ότι δεν είστε ρομπότ και ότι αποδέχεστε τους όρους και τις προϋποθέσεις και στη συνέχεια να κάνετε κλικ στο κουμπί **Εγγραφή**.

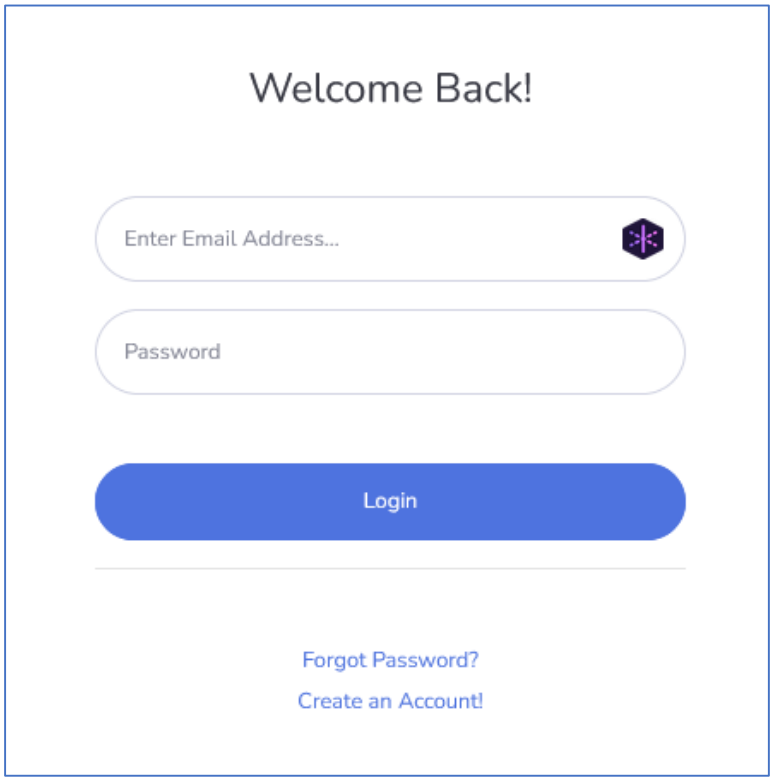


Ένας σύνδεσμος επιβεβαίωσης θα σας αποσταλεί μέσω email μόλις εγγραφείτε. Κάντε κλικ στον σύνδεσμο.

Σημείωση: Εάν ο μαθητής δεν έχει λάβει το email επιβεβαίωσης από το σύστημα, είναι απαραίτητο να ελέγξει την ανεπιθύμητη αλληλογραφία. Είναι πιθανό το email επιβεβαίωσης να καταλήξει στο φάκελο spam/unk.

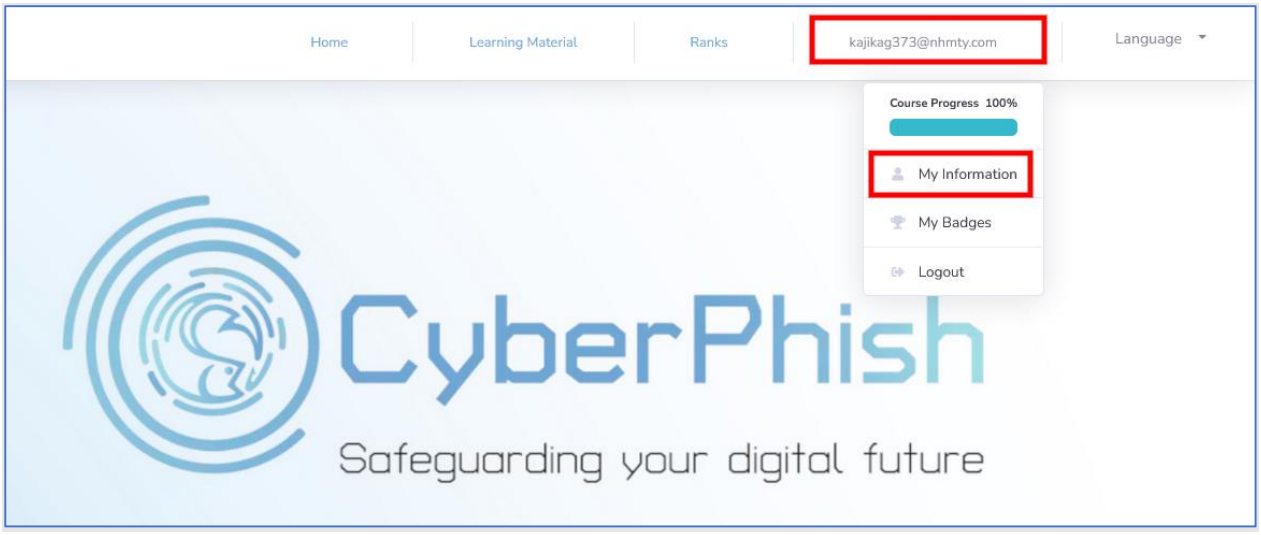


Κάντε κλικ στο σύνδεσμο επιβεβαίωσης για να συνδεθείτε στο σύστημα.



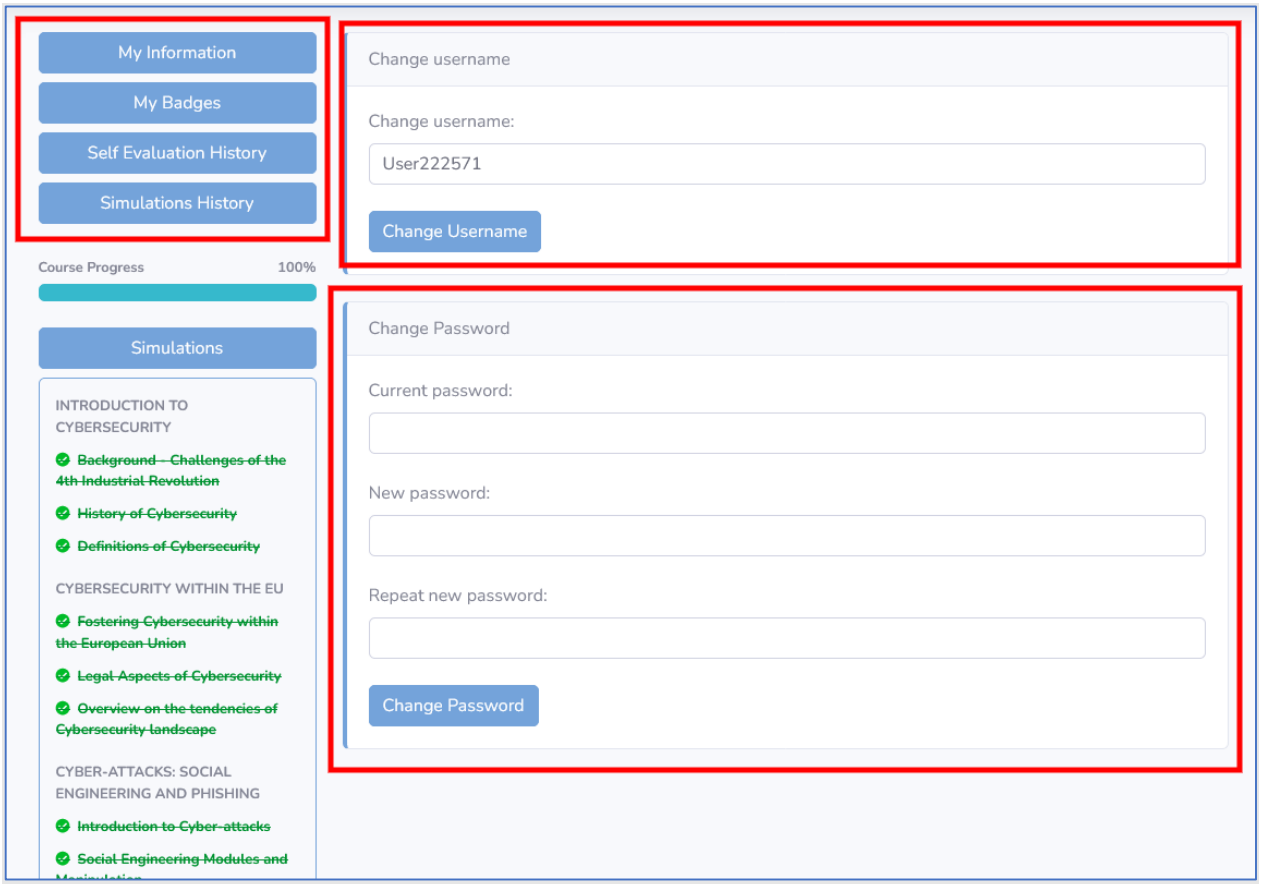
Λογαριασμός χρήστη

Μόλις συνδεθείτε, κάντε κλικ στη διεύθυνση ηλεκτρονικού ταχυδρομείου σας στο επάνω μέρος της σελίδας και επιλέξτε το στοιχείο **Οι πληροφορίες μου.**



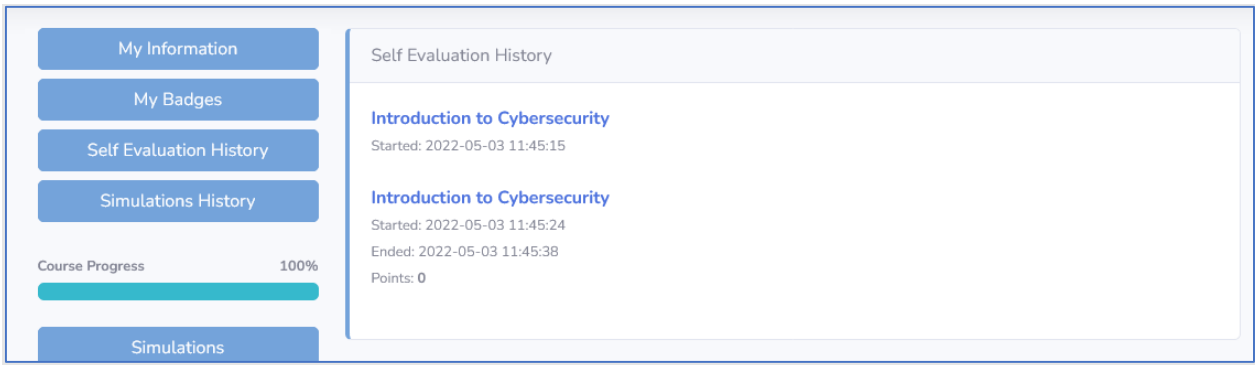
Στην αριστερή πλευρά της σελίδας **Οι πληροφορίες μου**, θα δείτε το κύριο μενού χρήστη, το οποίο οδηγεί στη σελίδα **Οι πληροφορίες μου** (η τρέχουσα σελίδα σας), στη **σελίδα Τα σήματά** μου, στις σελίδες **Ιστορικό αυτοαξιολόγησης** και **Ιστορικό προσομοιώσεων.**

Μπορείτε να αλλάξετε το όνομα χρήστη και τον κωδικό πρόσβασής σας στη σελίδα **Οι πληροφορίες μου.**



Στη σελίδα **Τα παράσημά μου**, θα δείτε όλα τα παράσημα που έχετε συλλέξει για τις διάφορες εργασίες που έχετε ολοκληρώσει.

Στη σελίδα **Ιστορικό αυτοαξιολόγησης**, θα μπορείτε να δείτε το ιστορικό όλων των δοκιμασιών αυτοαξιολόγησης που ξεκινήσατε ή ολοκληρώσατε. Εάν το τεστ Αυτοαξιολόγησης είναι ελλιπές, μπορείτε να το κάνετε κάνοντας κλικ στο όνομα του τεστ. Εάν το τεστ έχει ολοκληρωθεί, μπορείτε να κάνετε κλικ σε αυτό για να δείτε τα αποτελέσματα.

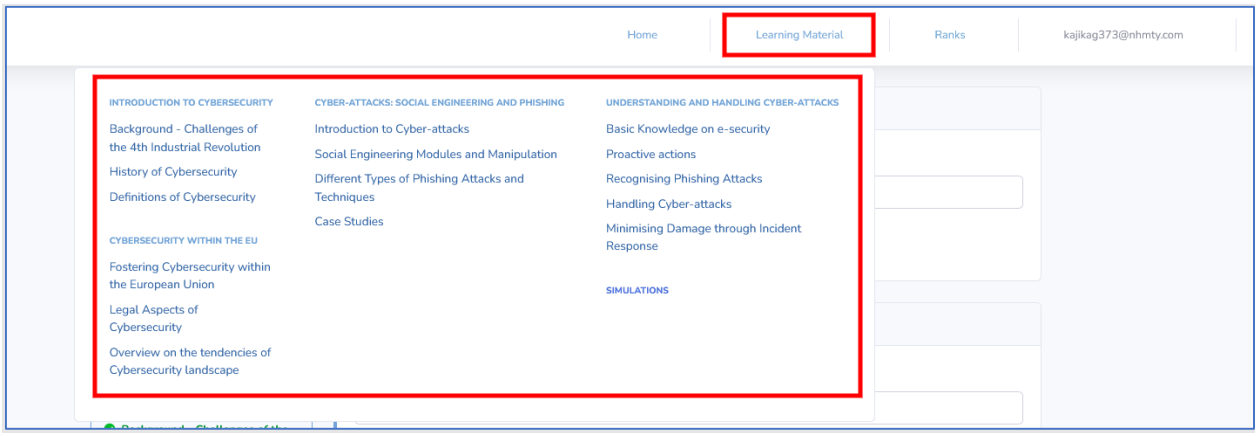


Στη σελίδα **Ιστορικό προσομοιώσεων**, μπορείτε να δείτε το ιστορικό των προσομοιώσεων που έχετε ξεκινήσει ή ολοκληρώσει. Εάν μια προσομοίωση δεν έχει ολοκληρωθεί, μπορείτε να το κάνετε κάνοντας κλικ στο όνομα της προσομοίωσης. Εάν η προσομοίωση έχει ολοκληρωθεί, μπορείτε να δείτε τα αποτελέσματα κάνοντας κλικ σε αυτήν.

Εκπαιδευτικό υλικό

Μπορείτε να αποκτήσετε πρόσβαση στο εκπαιδευτικό υλικό στο επάνω μέρος της σελίδας, επιλέγοντας το στοιχείο του μενού **Μαθησιακό υλικό** και επιλέγοντας το θέμα που σας ενδιαφέρει*.

**Όλο το υλικό που στηρίζεται είναι προσβάσιμο χωρίς εγγραφή, αλλά ορισμένες λειτουργίες μπορεί να είναι περιορισμένες. Ο εκπαιδευόμενος μπορεί να διαβάσει το εκπαιδευτικό υλικό χωρίς να συνδεθεί στο σύστημα, αλλά δεν θα είναι σε θέση να επιβεβαιώσει την κατάσταση προβολής του εκπαιδευτικού υλικού, ούτε θα έχει πρόσβαση στα τεστ και τις προσομοιώσεις.*

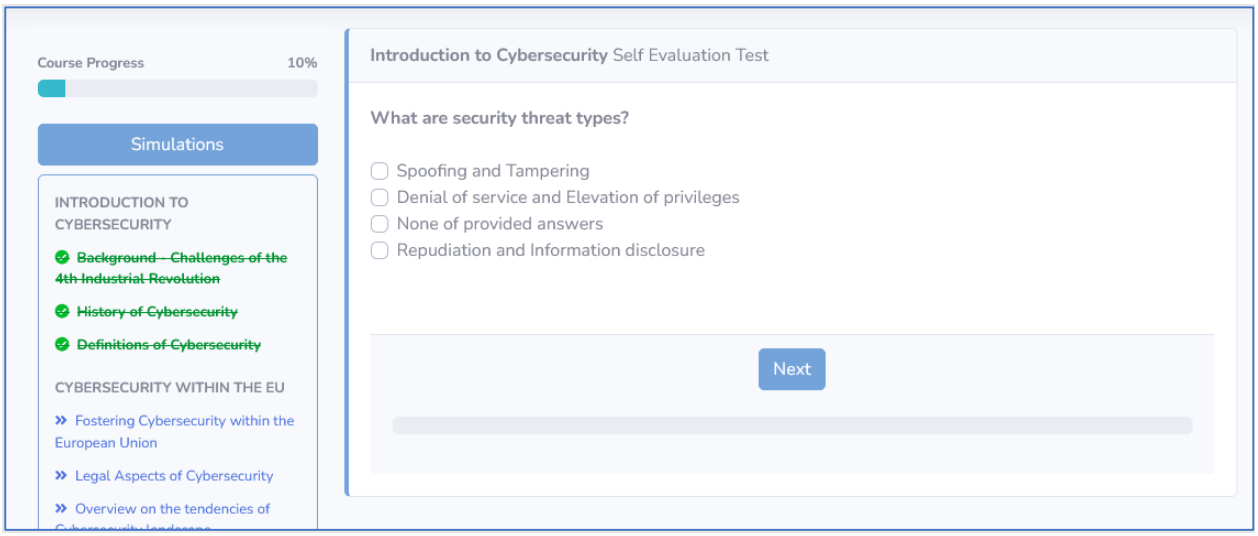


Αν επιλέξετε κάποιο θέμα, θα δείτε τις διαφάνειες για το συγκεκριμένο θέμα στο κύριο μέρος της σελίδας και συνδέσμους προς όλα τα θέματα στην αριστερή πλευρά της σελίδας. Εάν είστε συνδεδεμένοι, μπορείτε να επισημάνετε τα θέματα ως ολοκληρωμένα πατώντας το κουμπί **Mark as Completed! στη** δεξιά πλευρά του επάνω μέρους της σελίδας και να δείτε την πρόοδο του μαθήματός σας στην αριστερή πλευρά της σελίδας.

Τεστ αυτοαξιολόγησης

Για να αποκτήσετε πρόσβαση στις ερωτήσεις αυτοαξιολόγησης, πρέπει να επισημάνετε κάθε θέμα της κατηγορίας ως ολοκληρωμένο. Στη συνέχεια, θα δείτε το κουμπί **Δοκιμασία αυτοαξιολόγησης** στο πάνω μέρος της κεντρικής σελίδας. Πρέπει να συνδεθείτε για να αποκτήσετε πρόσβαση στο **τεστ αυτοαξιολόγησης**.

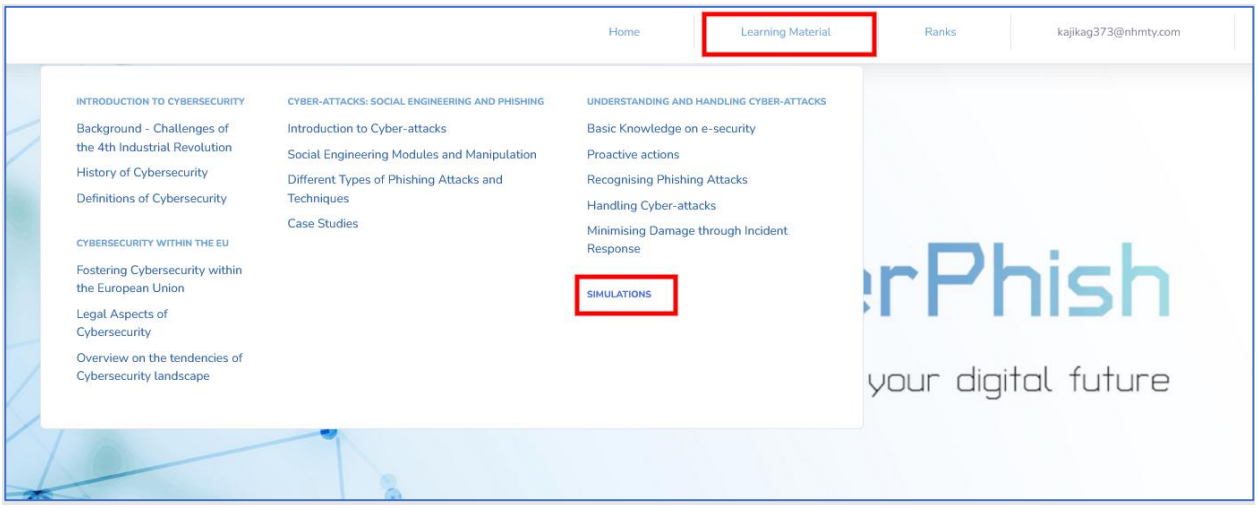
Εάν κάνετε κλικ στο κουμπί **Δοκιμασία αυτοαξιολόγησης**, θα λάβετε 5 ερωτήσεις για την εν λόγω κατηγορία για να αξιολογήσετε τις γνώσεις σας.



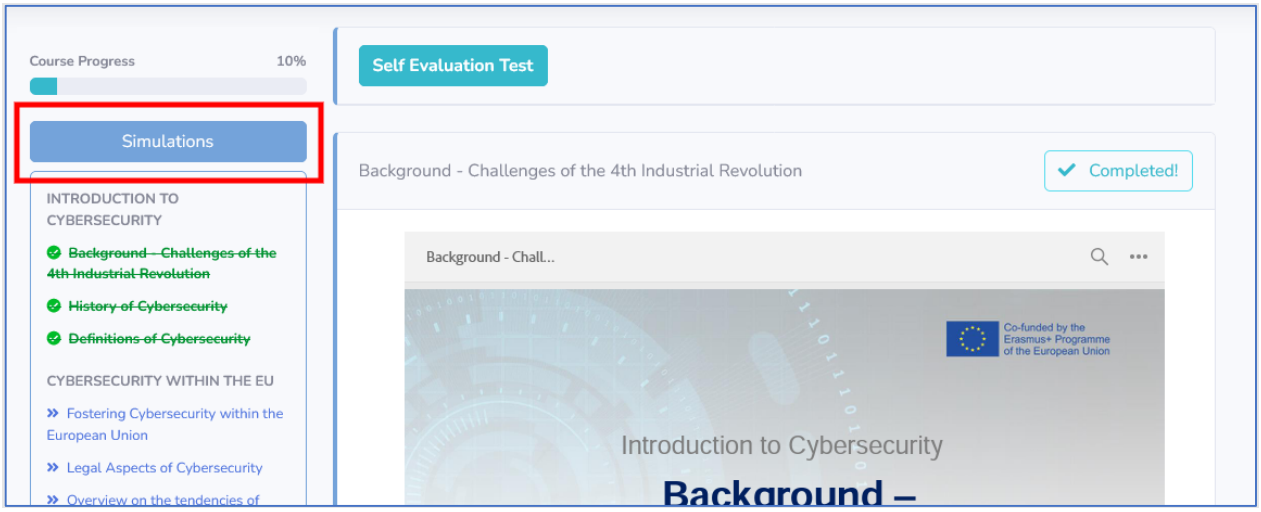
Προσομοιώσεις

Οι χρήστες μπορούν να έχουν πρόσβαση στις προσομοιώσεις μόνο με σύνδεση.

Μπορείτε να αποκτήσετε πρόσβαση στις προσομοιώσεις κάνοντας κλικ στο **Μαθησιακό υλικό** και επιλέγοντας **Προσομοιώσεις.**

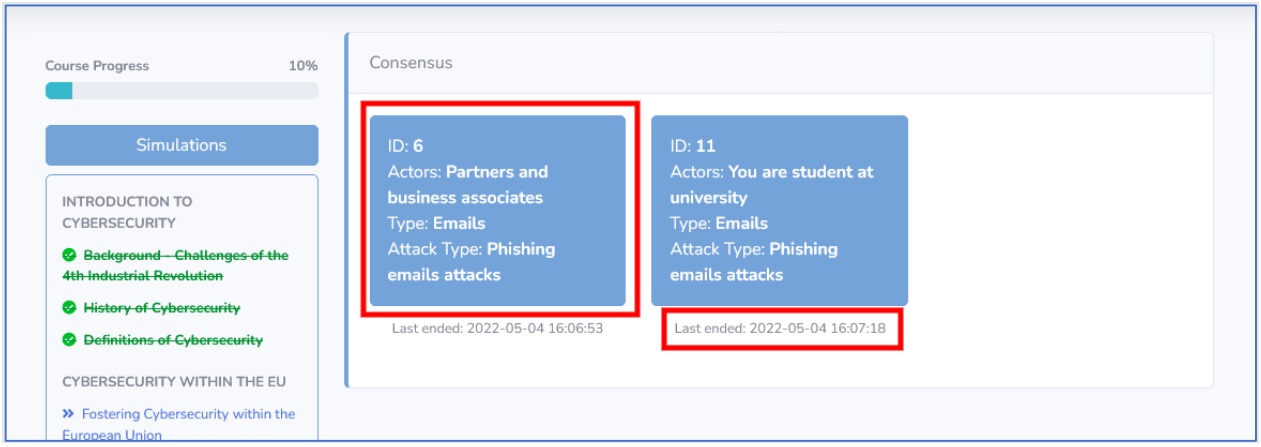


Μπορείτε επίσης να έχετε πρόσβαση σε προσομοιώσεις από οποιαδήποτε επιλεγμένη θεματική σελίδα του **Μαθησιακού Υλικού.**



Όταν κάνετε κλικ στην επιλογή **Προσομοιώσεις, πρέπει** να επιλέξετε μια κατηγορία προσομοιώσεων. Μια προσομοίωση μπορεί να περιλαμβάνεται σε πολλές κατηγορίες.

Η επιλογή της κατηγορίας Προσομοιώσεις θα σας επιτρέψει να επιλέξετε προσομοιώσεις στην εν λόγω κατηγορία. Εάν έχετε ολοκληρώσει ποτέ μια συγκεκριμένη προσομοίωση, θα δείτε μια χρονοσφραγίδα κάτω από την εν λόγω προσομοίωση.

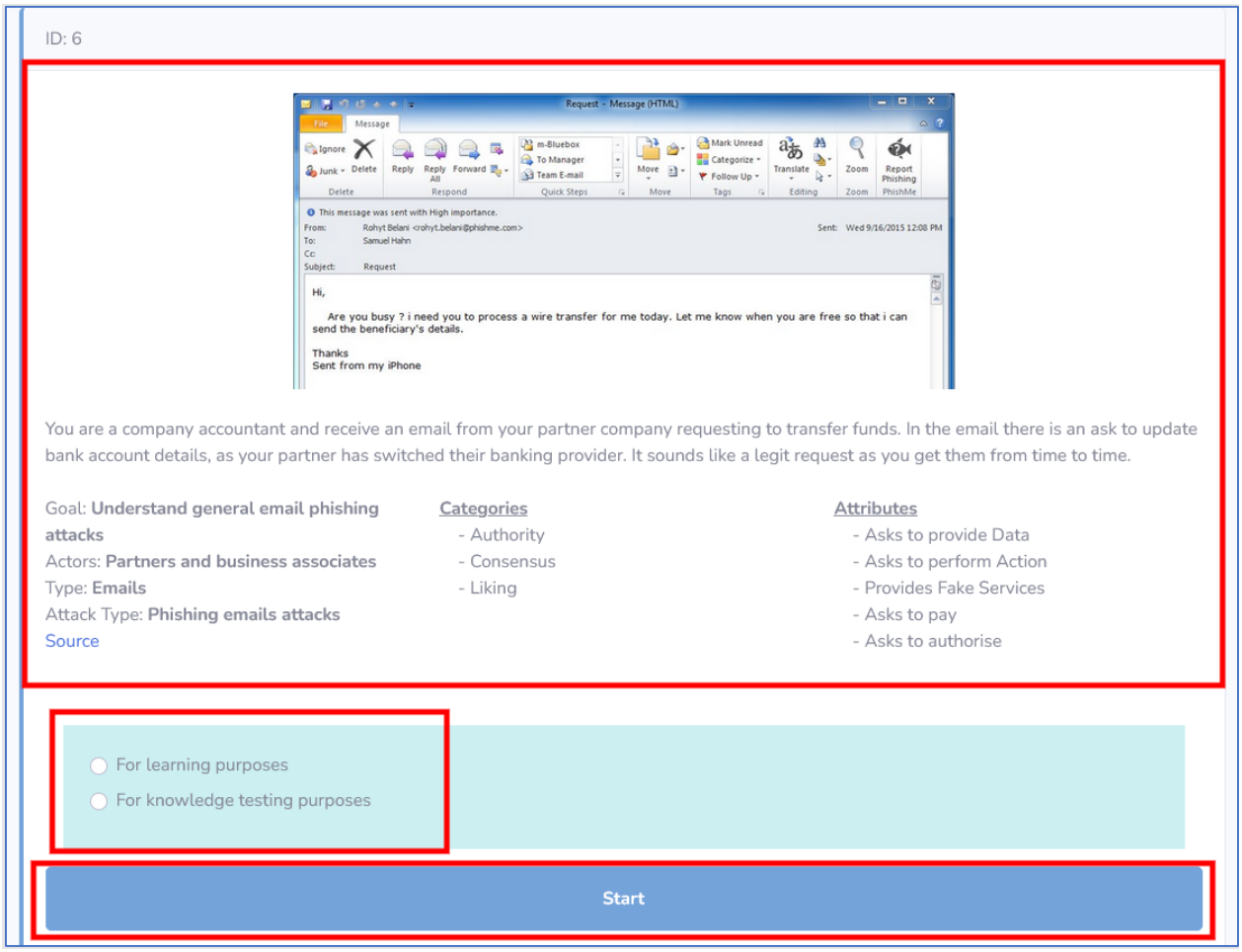


Όταν επιλέγετε οποιαδήποτε προσομοίωση, βλέπετε την περιγραφή της κατάστασης πριν αρχίσετε να την επιλύετε. Πριν ξεκινήσετε, πρέπει να επιλέξετε αν θέλετε να το κάνετε για **σκοπούς εκμάθησης** ή **για σκοπούς ελέγχου γνώσεων**.

Αν επιλέξετε **για σκοπούς μάθησης**, θα βλέπετε την ανατροφοδότηση μετά από κάθε ερώτηση που απαντάτε.

Αν επιλέξετε **για σκοπούς ελέγχου γνώσεων**, θα δείτε ανατροφοδότηση μόνο αφού ολοκληρώσετε την προσομοίωση.

Κάντε κλικ στο κουμπί **Έναρξη**.



Κατατάξεις χρηστών

Αυτή η επιλογή κατατάσσει τους χρήστες σύμφωνα με την καλύτερη επίδοσή τους στα **τεστ αυτοαξιολόγησης** και στις **προσομοιώσεις**. Μπορείτε να αποκτήσετε πρόσβαση στις κατατάξεις των χρηστών κάνοντας κλικ στην επιλογή **Κατατάξεις** στο επάνω μέρος της σελίδας και επιλέγοντας είτε **Αυτοαξιολόγηση** είτε **Προσομοιώσεις**.