ΠΟΛΥΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΚΑΤΑΡΤΙΣΗΣ

ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΕΡΓΑΖΟΜΕΝΩΝ ΓΙΑ ΤΑ ΠΡΟΒΛΗΜΑΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Στοιχεία Διεξαγωγής

Ημερομηνίες & Ώρες Διεξαγωγής:
17/10/2024
22/10/2024

Διάρκεια Προγράμματος:
Σύνολο 7 ώρες

Online Seminar

Κόστος Συμμετοχής

Αρχικό Κόστος:
€200

Κόστος με επιδότηση:
€60

Κόστος για Μη Δικαιούχους ΑνΑΔ:
€150

ΑΙΤΗΣΗ ΕΝΔΙΑΦΕΡΟΝΤΟΣ

Η συμμετοχή γίνεται μέσω της πλατφόρμας ΕΡΜΗΣ

Σκοπός του προγράμματος

Οι κυβερνοεπιθέσεις αποτελούν αναμφίβολα μια από τις ταχύτερα αναπτυσσόμενες μορφές εγκλημάτων σε παγκόσμιο επίπεδο. Στη σημερινή ψηφιακή εποχή, η ανάγκη για αντίληψη από τους εργαζόμενους των κινδύνων στον κυβερνοχώρο, έχει γίνει ολοένα και πιο σημαντική. Στην πράξη της ΕΕ για την κυβερνοασφάλεια, αυτή ορίζεται ως «οι δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων. Ο πολλαπλασιασμός των ψηφιακών συσκευών, των δικτύων και των υπηρεσιών που βασίζονται σε σύννεφο (cloud services) και η τεράστια ανάπτυξη διαδικτυακών υπηρεσιών, έχει οδηγήσει σε αύξηση των επιθέσεων στον κυβερνοχώρο. Ενδεικτικά, εμφανίζεται σημαντική αύξηση των παραβιάσεων δεδομένων, επιθέσεων Κοινωνικής Μηχανικής (Social Engineering), απάτες με χρήση διαδικτύου και μολύνσεων από κακόβουλο λογισμικό (Ransomware). Αυτές οι επιθέσεις μπορεί να οδηγήσουν σε σημαντικές οικονομικές απώλειες, ζημιά στη φήμη του οργανισμού και νομική ευθύνη. Ασφαλώς, η ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο αναφέρεται στη γνώση και την κατανόηση των κινδύνων που σχετίζονται με τη χρήση ψηφιακών συσκευών και δικτύων, καθώς και στα μέτρα που μπορούν να λάβουν άτομα και οργανισμοί για να μετριάσουν αυτούς τους κινδύνους.

Η ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο είναι ένα κρίσιμο συστατικό της σύγχρονης ψηφιακής ασφάλειας. Βοηθά άτομα και οργανισμούς να προστατεύονται από απειλές στον κυβερνοχώρο, να συμμορφώνονται με τις κανονιστικές απαιτήσεις και να αποφεύγουν τις νομικές κυρώσεις. Δίνοντας προτεραιότητα στη συνειδητοποίηση της κυβερνοασφάλειας, τα άτομα και οι οργανισμοί μπορούν να προστατεύσουν τα ψηφιακά τους περιουσιακά στοιχεία και να διατηρήσουν την εμπιστοσύνη με τους πελάτες και τα ενδιαφερόμενα μέρη τους.

Η θεματολογία του σεμιναρίου είναι ιδανική για:

- Οι συμμετέχοντες στο παρόν πρόγραμμα μπορεί να είναι:
- Εργαζόμενοι σε φορείς και επιχειρήσεις που χρησιμοποιούν τεχνολογίες πληροφορικής και επικοινωνιών στην εργασία τους

ΤΟ ΠΡΟΓΡΑΜΜΑ ΕΧΕΙ ΕΓΚΡΙΘΕΙ ΑΠΟ ΤΗΝ ΑΝΑΔ ΚΥΠΡΟΥ.
Οι επιχειρήσεις που συμμετέχουν με εργοδοτούμενους τους οι οποίοι ικανοποιούν τα κριτήρια της Αρχής θα τύχουν της σχετικής επιχορήγησης.

Contact Us

Mind The Gap Ltd

Tel: 25251435

Fax: 25251436

info@mindthegap.com.cy

www.mindthegap.com.cy

Με την ολοκλήρωση της Εκπαίδευσης οι Συμμετέχοντες θα λάβουν Πιστοποιητικό Παρακολούθησης.

- Νομικοί, Λογιστές και Σύμβουλοι Επιχειρήσεων
- Άνεργοι όπως προβλέπεται στον Οδηγό του Προγράμματος.

Στόχοι του προγράμματος

Με την ολοκλήρωση του προγράμματος οι συμμετέχοντες θα είναι σε θέση να:

- Κατονομάζουν τις απειλές στον κυβερνοχώρο
- Διατυπώνουν έννοιες σχετικές με τις κυβερνοεπιθέσεις
- Διαχωρίζουν και διατυπώνουν τις βασικές αρχές ασφάλειας πληροφοριών
- Απαριθμούν τους κινδύνους στο διαδίκτυο για το φορέα τους
- Περιγράφουν τις απειλές στο διαδίκτυο
- Οργανώνουν την άμυνα σε κυβερνοεπιθέσεις
- Αντικρούουν την έλλειψη κανόνων ασφάλειας σε κωδικούς
- Αντιπαραβάλλουν τεχνικές ασφάλειας με τις εφαρμοζόμενες στο φορέα τους
- Συνεργάζονται στην αντιμετώπιση περιστατικών επιθέσεων

Προφίλ Εισηγητή

Ο εισηγητής Δημητρίου Κυριάκος, είναι εγκεκριμένος Εκπαιδευτής Επαγγελματικής Κατάρτισης, με μακρόχρονη εμπειρία στην εκπαίδευση Ενηλίκων σε διάφορες Ευρωπαϊκές Χώρες. Διαθέτει εξειδικευμένες γνώσεις στην Προστασία Προσωπικών Δεδομένων και στην Ασφάλεια των Πληροφοριών και έχει βοηθήσει συμβουλευτικά πάρα πολλές επιχειρήσεις στην συμμόρφωση τους με τον Κανονισμό GDPR.

Θεματολόγιο

- Εισαγωγική Ενότητα
- Ενότητα 1: Εισαγωγή και Τελική Ενότητα
- Ενότητα 2: Ιστορική Αναδρομή της Απάτης στον Κυβερνοχώρο
- Ενότητα 3: Οι βασικές και Συμπληρωματικές Αρχές της Ασφάλειας Πληροφοριών και η σχέση τους με τις κυβερνοεπιθέσεις
- Ενότητα 4: Οι Κίνδυνοι στο διαδίκτυο για τους φορείς
- Ενότητα 5: Βασικές απειλές στον κυβερνοχώρο
- Ενότητα 6: Βέλτιστες πρακτικές για την ασφάλεια στον κυβερνοχώρο
- Ενότητα 7: Κίνητρο και στόχοι μιας κυβερνοεπίθεσης