**«Ηλεκτρονική ασφάλεια και προστασία για επιχειρήσεις ηλεκτρονικού εμπορίου»**

|  |
| --- |
| **Στόχος προγράμματος** Οι συμμετέχοντες του προγράμματος θα ενημερωθούν για την προστασία και ασφάλεια ενός ηλεκτρονικού καταστήματος καθώς και για τις διαδικασίες που θα πρέπει να ακολουθηθούν κατά τη λειτουργία του καταστήματος  για αν επιτευχθεί αυτό. Επίσης θα πληροφορηθούν  σε ποιες ενέργειες πρέπει να προβούν όταν το κατάστημα τους γίνει στόχος ηλεκτρονικής επίθεσης |
| **Αναγκαιότητα προγράμματος** Οι εταιρείες ηλεκτρονικού εμπορίου είναι ευάλωτες σε απειλές για την ασφάλεια στο Internet , επειδή αυτές οι επιχειρήσεις χρησιμοποιούν τα στοιχεία του τραπεζικού λογαριασμού και των πιστωτικών καρτών των πελατών, τις διευθύνσεις ηλεκτρονικού ταχυδρομείου, τις διευθύνσεις αλληλογραφίας και τα ονόματα χρήστη και τους κωδικούς πρόσβασης. Επίσης  ευαίσθητα δεδομένα θα μπορούσαν επίσης να κρατηθούν για λύτρα. Ο χρήστης του ηλεκτρονικού καταστήματος απαιτεί τα δεδομένα να μη διατεθούν σε μη εξουσιοδοτημένα άτομα ή να αποκαλυφθούν  Ο ιδιοκτήτης του ηλεκτρονικού καταστήματος πρέπει να λαμβάνει τα δεδομένα όπως αυτά του στάλθηκαν . Ο ιδιόκτητης πρέπει να είναι βέβαιος για την ταυτότητα του πελάτη. Όλα αυτές οι συνθήκες για να ικανοποιηθούν απαιτούν τη δημιουργία και το λειτουργία  πολύπλοκων πληροφοριακών συστημάτων και επιχειρησιακών διαδικασιών και λειτουργιών , τις οποίες τα μέλη του ΕΒΕΘ οφείλουν να γνωρίζουν καθώς και τις δράσεις στις οποίες πρέπει να προβούν αν γίνουν στόχος κυβερνοεπίθεσης.  |
| **Σε ποιους απευθύνεται** Στα μέλη του ΕΒΕΘ που επιθυμούν να ενημερωθούν και να εφαρμόσουν σύγχρονες πολιτικές ηλεκτρονικής ασφάλειας στο ηλεκτρονικού τους κατάστημα  |
| **Μαθησιακά αποτελέσματα**  Να μπορούν να δημιουργήσουν τις πολιτικές ασφάλειας και προστασίας. Να επιλέγουν τη βέλτιστη τεχνολογική λύση για την ηλεκτρονική ασφάλεια του καταστήματος. Να γνωρίζουν τις διαδικασίες και πολιτικές ασφάλειας .των συστημάτων ηλεκτρονικών πληρωμών Να μπορούν να διαχειριστούν με τις κατάλληλες ενέργειες περιστατικό κυβερνοεπίθεσης στο δικό τους ηλεκτρονικό κατάστημα.   |

**3.    Δομή και περιεχόμενο του Προγράμματος**

 1.    Εκμάθηση των τεχνικών **Transport Layer Security (TLS), Secure Sockets Layer (SSL), and HTTPS authentication.**

2.    Αποφυγή των λογισμικών **Malware and ransomware**.  Όπου παραμένετε κλειδωμένοι έξω από όλα τα σημαντικά δεδομένα και τα πληροφοριακά συστήματά του ηλεκτρονικού καταστήματος

3.    Αποφυγή του **Εskimming**. Αναφέρεται σε  μεθόδους κλοπής στοιχείων πιστωτικών καρτών και προσωπικών δεδομένων από σελίδες επεξεργασίας καρτών και πληρωμής σε ιστότοπους ηλεκτρονικού εμπορίου

4.    Αποφυγή του **Cross-site scripting (XSS**). περιλαμβάνει την εισαγωγή ενός κακόβουλου κώδικα σε μια ιστοσελίδα.

5.    Πώς να εμποδίσετε το  **Phishing.** Όπου αναφέρονται σε μεθόδους  κλοπής δεδομένών

6.    Εκμάθηση των τρόπων δράσεων έναντι των **social engineering attempts.**

7.    Εφαρμογή πρόσθετων στοιχείων  ελέγχου ταυτότητας.

8.    Δημιουργία σχεδίου για συνεχή ενημέρωση των πολίτικων ασφάλειας

9.    Εκμάθηση των απαραίτητων ενεργειών που πρέπει να γίνουν μετά από ηλεκτρονική επίθεση σε ηλεκτρονικό κατάστημα

Επιστημονικός υπεύθυνος είναι ο κ. Σταμάτης Τζελέπης.