Organisme de formation
Ch. des Fleurettes 28
Lausanne, Suisse
Tél. 021 626 08 00
www.cyberiade.ch

Formation continue

Cybersécurité (CyberCitizen)

Gestes de sécurité au quotidien numérique



Résumé

Préparation au test Tosa Cybersécurité (CyberCitizen). On part des acteurs et des mots de passe, puis on protège le poste et les données, on adopte les bons réflexes en déplacement, et on reconnaît les attaques. Le score, de 1 à 1 000, situe le niveau d'Initial à Expert.

Objectifs

Repérer les acteurs et les types d'attaque.
Protéger comptes, poste et fichiers.
Adopter les bons réflexes en déplacement et à la maison.
Reconnaître une fraude et réagir.

Public cible

Étudiants et adultes qui veulent les gestes de sécurité du quotidien numérique, au bureau, en déplacement et à la maison.

C'est une certification complémentaire à une formation de type CFC ou à une formation continue, pour étayer votre CV et mettre vos connaissances à jour.

Contenu

1. Situer CyberCitizen

- Définir une attaque informatique et l'intérêt d'un mot de passe
- Reconnaître une connexion HTTPS, un cookie et un captcha
- Savoir que le test porte sur CyberCitizen, dure 60 minutes, compte 35 questions, et certifie à partir de 351

2. L'écosystème de la cybersécurité

- Identifier les rôles internes : RSSI, DPO et SOC, et nommer les champs d'action d'un SOC
- Identifier les acteurs publics : ANSSI, CERT-FR et CERT-EU
- Nommer la norme ISO 27001, et savoir à quoi servent un test d'intrusion et un exercice de type Capture The Flag
- Citer des profils d'attaquants, leurs motivations et leurs cibles
- Distinguer les impacts d'un hameçonnage, d'un rançongiciel et d'un déni de service, et en évaluer la criticité
- Créer un mot de passe robuste, en varier, et utiliser un gestionnaire, avec KeePass comme exemple du test
- Ajouter ou modifier un mot de passe dans le gestionnaire, et utiliser une authentification à plusieurs facteurs
- Savoir qui alerter, se déconnecter, et collecter des éléments utiles en cas d'intrusion

3. Données, comptes et équipements

- Verrouiller son poste en cas d'absence, et appliquer les procédures prévues en cas d'attaque
- Mettre à jour logiciels et systèmes, et retrouver la version d'un logiciel ou du système
- Choisir une source de confiance, et reconnaître le risque d'un logiciel cracké ou inconnu

Organisme de formation
Ch. des Fleurettes 28
Lausanne, Suisse
Tél. 021 626 08 00
www.cyberiade.ch

- Lire un certificat SSL et son autorité de certification
- Savoir quand utiliser un VPN, et distinguer l'intérêt d'un proxy
- Manipuler une clé ou un disque inconnu, chiffrer un support amovible, distinguer un transfert public d'un transfert sensible, et envoyer un fichier volumineux public
- Vérifier l'extension d'un fichier, analyser une pièce jointe, avec VirusTotal comme exemple du test, et extraire ses métadonnées
- Stocker sur le cloud, utiliser une gestion électronique des documents, séparer les documents personnels et professionnels, sauvegarder, et assurer la continuité d'activité
- Traiter un document papier sensible, et désactiver un processus Windows

4. Comportement numérique

- Mesurer les risques d'un déplacement : vol, écran visible, propos et documents laissés derrière soi
- Connaître les risques d'un Wi-Fi public, classer les protocoles, et utiliser un réseau sans fil sécurisé, y compris en Bluetooth
- Utiliser le mode avion et un filtre de confidentialité
- Protéger l'accès d'un smartphone, et distinguer les avantages et les limites d'une gestion des appareils mobiles
- Sécuriser cartes d'accès et badges, et préparer un poste dans un hôtel ou une salle de réunion
- Séparer les usages personnels et professionnels, régler la confidentialité des réseaux sociaux, et prévenir une fuite vers un réseau personnel ou professionnel
- Connaître les champs d'action du RGPD, et les droits de rectification et de suppression

5. Cybermenaces

- Reconnaître un hameçonnage par courriel, par SMS ou par appel, et les éléments qui le trahissent
- Reconnaître une manipulation ou une personne inconnue dans les locaux
- Appliquer les précautions devant un fichier inconnu ou une pièce jointe
- Reconnaître un rançongiciel, un déni de service, une menace persistante et un logiciel malveillant
- Réagir en cas de suspicion : ne pas cliquer, alerter, et couper la connexion

Tarifs

Cours individuel selon calendrier	**CHF 400.–/jour**
Cours en entreprise	**Sur demande**
Coaching privé	**CHF 100.–/heure**

La durée à prévoir se discute en fonction de votre niveau initial et du niveau attendu (score).

Certification	**CHF 65.–**
Certification + 1 évaluation	**CHF 80.–**
Certification + 2 évaluations	**CHF 92.–**

Lieu

Chemin des Fleurettes 36, 1007 Lausanne
En ligne

Modalités

Cours en ligne
Cours en présentiel