Formation

Hygiène de sécurité informatique

Durée : 7h00

Cette formation aborde les grands principes de l'hygiène informatique pour apprendre à faire face aux principales attaques Cyber et réduire efficacement le risque lié à l'utilisation d'un PC.

Celle-ci place l'apprenant dans la peau d'un hacker pour mieux percevoir les conséquences d'une attaque cyber et acquérir les bons réflexes pour s'en protéger.

Une formation pratique qui alterne théorie et mises en situation, grâce à des démonstrations d'attaques réelles.

Public visé : Profils non techniques et utilisateurs d'outils digitaux

Prérequis : Aucun

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, le stagiaire est en capacité de :

- Evaluer les enjeux et impacts d'une attaque cyber
- Identifier les mails frauduleux et les signaler
- Connecter des appareils, naviguer ou télécharger des applications sur des sites officiels et sécurisés
- Expliquer l'utilité d'une politique de mots de passe et comment faciliter son application
- Déceler les tentatives d'attaque par abus de confiance
- Evaluer les conséquences d'une connexion depuis un réseau hors de l'entreprise

PROGRAMME

1. Les enjeux de la cybersécurité

- Paysage de l'écosystème national et européen de la cybersécurité
- Les ressources clés de la cybersécurité
- Identifier les enjeux et les risques cybersécurité
- Comment s'impliquer dans la cybersécurité (BIA, la législation, …)

Travaux pratiques :

Approche offensive : Observer les attaques en live sur un serveur compromis

Approche défensive : Les basiques de sécurité, Business Impact Analysis

2. Identifier les mails frauduleux et les signaler

- Phishing/hameçonnage/e-mails malveillants
- Vol de données sensibles
- Usurpation d'identité

Travaux pratiques :

Approche offensive : Monter une attaque de phishing

Approche défensive : Identifier les e-mails frauduleux

Informations pratiques

Durée : 7h00

Ressources
Supports de cours
70% d'exercices pratiques

Tarifs 2023
En inter : 260€ HT/stagiaire
En intra : contactez-nous pour un devis

Modalités
Sur inscription
Contact et information par mail
Session de 8 stagiaires minimum

Lieu
Sur site Client, LUPISE ou distanciel

Accessibilité aux personnes en situation de handicap
Contactez-nous pour étudier la faisabilité de votre demande.

Taux de satisfaction

★ ★ ★ ★ ★

Compétences des formateurs

Nos formateurs sont des spécialistes certifiés de la cybersécurité avec une expérience terrain dans la sécurité des systèmes d'information. Ils ont été validés par notre équipe pédagogique sur le plan des connaissances métiers et sur celui de la pédagogie, et sont évalués régulièrement. Une veille permanente ainsi qu'une pratique régulière dans leur domaine garantit leur niveau d'expertise.

Modalités d'évaluation des stagiaires

Les objectifs sont régulièrement évalués tout au long de la formation moyen de quizz, de mises en situation et de travaux pratiques et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur
Le participant complète un test de positionnement en amont et en aval de la formation pour valider les compétences acquises.

Moyens techniques et pédagogiques

Aides audiovisuelles, environnement de formation en ligne, support de cours et exercices, études de cas ou présentation de cas réels, sessions de questions-réponses.

contact@lupise.fr

3. Connecter des appareils et supports amovibles sécurisés

- Branchement d'une clé USB malveillante
- Ransomware, virus, malware
- BYOD, antivirus

Travaux pratiques :

Approche offensive : Attaque par clé USB

4. Naviguer et télécharger des applications sur des sites officiels sécurisés

- Vulnérabilités liées à la consultation de pages web
- Téléchargement d'applications vérolées

Travaux pratiques :

Approche offensive : Attaque par injection de code malveillant sur un site web

5. Expliquer l'utilité d'une politique de mots de passe et comment faciliter son application

- Politique de mots de passe
- Cracking de mots de passe
- Gestionnaire de mots de passe et coffre-fort numérique
- Pourquoi une authentification, activer le MFA

Travaux pratiques :

Approche offensive : Attaque par dictionnaire sur les mots de passe

Approche défensive : Identifier la compromission de son mail

6. Déceler les tentatives d'attaque par abus de confiance

- Les aspects sociaux : Ingénierie sociale, OSINT
- Techniques de recherche d'information sur internet

Travaux pratiques :

Approche offensive : Attaque par recueil d'information ouverte/public

Approche défensive : Identifier les tentatives d'attaque par abus de confiance

7. Evaluer les conséquences d'une connexion depuis un réseau hors de l'entreprise (ex: gare ou aéroport)

- Connexion Wifi sécurisée
- Interception de données
- Utilisation de VPN

Travaux pratiques :

Approche offensive : Attaque par « l'homme du milieu »

Approche défensive : Identifier les tentatives d'attaque

Informations complémentaires

- **Matériel nécessaire**

Les stagiaires devront être munis d'un PC pendant la formation.

- **Evaluation et validation de la formation**

À la fin de chaque formation, les participants complètent un questionnaire d'évaluation qui est analysé par nos équipes pédagogiques.

Une feuille d'émargement par demi-journée de présence est signée par le stagiaire. A l'issue de la formation, un certificat de réalisation de formation est remis au stagiaire si celui-ci a bien assisté à la totalité de la session.

contact@lupise.fr