EduGroupe
Accompagner pour réussir

Cybersécurité - Sensibilisation

Référence : **SECUSERS** Durée : **1 jour (7 heures)** Certification : **Aucune**

Connaissances préalables

- Utiliser des outils informatiques et communicants (téléphone, ordinateur, messagerie, Internet, …).

Profil des stagiaires

- Toute personne souhaitant être sensibilisé à la sécurité informatique

Objectifs

- Comprendre les différents types de menaces en cybercriminalité
- S'acculturer aux bonnes pratiques (mot de passe unique par système...etc.)
- Détecter les intrusions et réagir face aux malveillances
- Comprendre les risques et les enjeux de sécurité
- Déterminer les données importantes à protéger
- Comprendre les actions à mettre en oeuvre pour protéger les données importantes (mise à jour antivirus, gestion des accès, sauvegarde...)
- Mettre en oeuvre une charte informatique à partager en interne (les pratiques)

Certification préparée

- Aucune

Méthodes pédagogiques

- Mise à disposition d'une poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

Formateur

- Consultant-formateur expert Cybersécurité

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Matin : Comprendre et détecter les cybermenaces (3h30)

2. Introduction à la cybersécurité et enjeux (30 min)

- Définition et importance de la cybersécurité
- Exemples récents d'attaques (ransomware, phishing, vol de données)
- Réglementation et obligations légales (RGPD, NIS2)

3. Panorama des menaces et techniques des attaquants (1h)

- Présentation des cyberattaques les plus courantes : Phishing & Spear Phishing ; Ransomware ; Ingénierie sociale ; Exploitation des failles réseaux et systèmes
- Démonstration d'une attaque de phishing
- 💡 *Étude de cas : analyse d'une attaque réelle*

4. Bonnes pratiques et sécurisation des accès (1h)

- Gestion des mots de passe et authentification forte
- Sécurisation des terminaux (PC, smartphones)
- Naviguer et utiliser les emails en toute sécurité
- 💡 *Exercice pratique : Test d'évaluation des mots de passe*

5. Détection et réaction face aux cyberattaques (1h)

- Signaux d'alerte d'une attaque en cours
- Réagir face à un email suspect ou un ransomware
- Plan de réponse aux incidents : Contenir et analyser ; Récupérer et sécuriser
- 💡 *Mise en situation : simulation d'un incident*

6. Après-midi : Protection des données et mise en place d'une charte (3h30)

7. Identifier et protéger les données sensibles (1h)

- Quelles sont les données critiques à protéger ?
- Cartographie des données et évaluation des risques
- Sauvegarde et chiffrement des données
- Gestion des accès et principe du moindre privilège

8. Mesures de protection et bonnes pratiques (1h)

- Antivirus, firewall et mises à jour : pourquoi et comment ?
- Sécurisation des accès à distance et VPN
- Gestion des droits utilisateurs et des privilèges
- 💡 *Exercice : Simulation d'une violation de données*

9. Élaboration d'une charte informatique et sensibilisation (1h30)

- Pourquoi une charte informatique ?
- Contenu essentiel : règles, obligations et sanctions
- Sensibilisation et formation continue des employés
- 💡 *Atelier pratique : élaboration d'une charte simplifiée à appliquer immédiatement*

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.