Sensibilisation des utilisateurs à la cybersécurité

0,5 jour, soit 3,5 heures

Programme de formation

Public visé
Tout public

Pré-requis
Familiarité avec les ordinateurs : Les participants doivent être à l'aise avec l'utilisation d'un ordinateur personnel, y compris l'ouverture et la fermeture de programmes, la navigation sur Internet, et la gestion de fichiers.

Compétences de navigation en ligne : Une connaissance de base de la navigation sur Internet est souhaitable. Les participants doivent savoir comment utiliser un navigateur web pour accéder à des sites web.

Notions de base de la messagerie électronique : Comprendre comment envoyer, recevoir et ouvrir des e-mails est un atout, car les e-mails sont souvent utilisés comme vecteurs d'attaques.

Aucune connaissance préalable en cybersécurité n'est requise : Cette formation est conçue pour les novices en cybersécurité. Les participants ne sont pas tenus d'avoir des connaissances préalables dans ce domaine.

Objectifs pédagogiques
Comprendre les Principes de Base de la Cybersécurité
Créer et Gérer des Mots de Passe Forts
Reconnaître les Techniques de phishing
Sécuriser les Appareils et les Réseaux
Sensibiliser aux Malwares
Comprendre la Cybersécurité au Travail

Description / Contenu
Introduction à la Cybersécurité
Présentation des concepts de base en cybersécurité.
Les types de menaces en ligne.
Les conséquences possibles des attaques.

Mots de Passe Forts et Gestion des Identifiants
Création de mots de passe robustes.
Utilisation de gestionnaires de mots de passe.
Les erreurs courantes à éviter.

Phishing et Ingénierie Sociale
Comprendre le phishing.
Reconnaître les techniques d'ingénierie sociale.
Comment éviter de tomber dans le piège.

Sécurité des Appareils et des Réseaux
Mises à jour et patchs.

JCD and CO – 193 RUE DU GENERAL METMAN, 57070 METZ France – 03 87 37 97 70 – formation@jcd-groupe.fr – SIRET : 80187958600031
Déclaration d'activité enregistrée sous le numéro 41570348657 auprès du préfet de région Lorraine

Utilisation de réseaux Wi-Fi publics en toute sécurité.
Sécurisation de vos appareils.

Sensibilisation aux Malwares
Qu'est-ce qu'un malware ?
Les méthodes pour éviter les infections.
Utilisation d'antivirus et d'anti-malware.

Cybersécurité au Travail
Les responsabilités des employés en matière de cybersécurité.
Politiques de sécurité de l'entreprise.
La cybersécurité et le télétravail.
Signalement des incidents de sécurité.

Conclusion et Questions
Résumé des points clés.
Questions des participants et discussions

Modalités pédagogiques
Pédagogie active, avec alternance de phases théoriques et d'exercices pratiques. Ces derniers permettent une utilisation immédiate et quotidienne des outils proposés.

Moyens et supports pédagogiques
Fourniture de documents et supports de cours qui restent la propriété des stagiaires
Salles équipées : vidéoprojecteur, paperboard, ordinateur individuel, support de cours papier ou électronique, outils de prise de notes

Modalités d’évaluation et de suivi
Compte rendu de fin de formation et analyse interne
Questionnaire « évaluation de la formation » rempli par le stagiaire

Validation de stage
Attestation de stage

Profil du formateur
Formateur Expert en Cybersécurité

Lieu
JCD and CO - 193 RUE DU GENERAL METMAN, 57070 METZ France

Informations sur l'accessibilité
La formation est accessible aux personnes à mobilité réduite et toute demande d’adaptation peut être étudiée en amont de la formation en fonction du besoin des personnes. Nous contacter pour plus d’informations.