Cybersécurité – Sensibilisation

Programme *(Mis à jour le 25/07/2025)*

Comprendre et détecter les cybermenaces

Introduction à la cybersécurité et enjeux

- 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

Bonnes pratiques et sécurisation des accès

- 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

Détection et réaction face aux cyberattaques

- 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

Protection des données et mise en place d'une charte

Identifier et protéger les données sensibles

- 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

Mesures de protection et bonnes pratiques

- 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

Élaboration d'une charte informatique et sensibilisation

- 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

Référence

THIS3627

Durée

1 jour / 7 heures

Prix HT / stagiaire

640€

Objectifs pédagogiques

- 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)

Niveau requis

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

Public concerné

- Toute personne souhaitant être sensibilisé à la sécurité informatique

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez pas à nous contacter pour en discuter) équipée d'un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices
Mise à disposition en ligne de documents supports à la suite de la formation

Dispositif de suivi de l'éxécution de