LA CYBERSÉCURITÉ AU QUOTIDIEN : IDENTIFIER LES BONNES PRATIQUES

Objectifs

Reconnaître les menaces informatiques courantes
Appliquer les bonnes pratiques
Préparer un plan minimum de continuité et de reprise d'activité

Programme

1-INTRODUCTION À LA CYBERSÉCURITÉ

Principes de base de la cybersecurité
Confidentialité, intégrité et disponibilité des informations - Concepts de menace, vulnérabilité et risque

2-LES MENACES COURANTES

Malware (logiciels malveillants)
Types de malware : virus, chevaux de Troie, ransomwares, spyware, etc. - Méthodes de propagation et signes d'infection

Phishing et ingénierie sociale
Reconnaître les tentatives de phishing par mail, téléphone ou réseaux sociaux - Techniques d'ingénierie sociale courantes et comment s'en protéger

Attaques par déni de service (DoS) et Déni de Service Distribué (DDoS)
Fonctionnement et impact des attaques DoS et DDoS

Intrusions et violations de données
Techniques d'intrusion courantes : exploitation des vulnérabilités, attaques par force brute, etc - Conséquences des violations de données et importance de la protection des informations sensibles

3-LES BONNES PRATIQUES EN MATIÈRE DE CYBERSÉCURITÉ

Principe de base des bonnes pratiques
Hygiène numérique - Configuration sécurisée des systèmes - Gestion des mots de passe et utilisation d'un gestionnaire

Authentification multi-facteurs (MFA)
Importance et mise en place de la MFA

Sécurité des Emails et des communications
Reconnaître les emails frauduleux et tentative de phishing - Bonnes pratiques pour sécuriser les communications électroniques

Navigation sécurisée sur internet
Utiliser des navigateurs sécurisés et à jour - Reconnaître les sites web de confiance et éviter les sites douteux

Utilisation Sécurisée des dispositifs mobiles
Mettre en place des mesures de sécurité sur les smartphones et tablettes - Installer des applications provenant de sources fiables uniquement - Sécurité des usages pro-perso

4-LA GESTION DES INCIDENTS DE SÉCURITÉ

Détection et réponse aux incidents
Reconnaître les signes d'un incident de sécurité - Procédures de signalement des incidents

Plans de continuité et de reprise d'activité
Importance de la planification de la continuité des opérations - Stratégies de sauvegarde et de récupération des données

Public

Tout utilisateur des outils informatiques

Méthodes pédagogiques

Test de positionnement
Alternance apports théoriques et mises en situations
Échanges et validations régulières
Quiz de vérification des acquis

Intervenant

Formateur expérimenté (minimum 5 ans)

Sanction de la formation

Attestation de formation

Modalités de formation

☑ intra-établissement

Étude de faisabilité sur demande

☑ inter APDHES - 1 jour, 07 heures

❶ 17 mars 2026
Date limite d'inscription 23 février 2026

❷ 09 juin 2026
Date limite d'inscription 18 mai 2026

470 € par participant

Contact

05-56-24-49-39
info@apdhes.fr

Référence

8.20.