SENSIBILISATION A LA CYBERSECURITE

Informatique

13/10/2026

Public et prérequis

Cette formation s'adresse à toute personne utilisant un système informatique

Lire et écrire, avoir des notions et connaissances de l'outil bureautique et de la navigation sur internet

Les objectifs

- Être capable d'appréhender les différents concepts de la sécurité informatique.
- Identifier les risques et les appréhender pour y faire face.
- Adopter une bonne hygiène informatique

Les méthodes pédagogiques et d'encadrement

- Cours théoriques,
- Cas pratiques
- Mise en situation

Contenu de la formation

L'écosystème numérique de l'entreprise (10 mins)

- Internet
- Le réseau de l'entreprise
- L'information, actif primordial des entreprises

Panorama des menaces (45 mins)

- Phishing (Hameçonnage)
- Logiciels malveillants
- Ingénierie sociale (Usurpation d'identité, manipulation, faux support technique…)
- Dénis de service
- Fuites d'informations
- Vulnérabilités logicielles & matérielle

Les bonnes pratiques de l'hygiène informatique (45 mins)

- La gestion des mots de passe + Authentification multifactorielle
- Les anti-virus
- Les mises à jour
- Les wifi
- Les sauvegardes
- La messagerie, les liens hypertextes et les pièces jointes
- Sécurité des appareils mobiles
- Différencier les usages professionnels et personnels

Les bons réflexes en cas d'attaque (15 mins)

RÉFÉRENCE
INFMAI300183

CENTRES DE FORMATION
CHALON-SUR-SAÔNE, DIJON

DURÉE DE LA FORMATION
3.5 heures

ACCUEIL PSH
Formation ouverte aux personnes en situation de handicap. Moyens de compensation à étudier avec le référent handicap du centre concerné.

Les + Formation 21-71

• 682 jeunes formés par an
• 291 contrats d'alternance à pourvoir
• 769 entreprises partenaires
• Accompagnement individualisé
• Diplômes reconnus par l'Etat

• Savoir être, management, sécurité
• Pédagogie innovante (par projets, en îlots, projet Voltaire, Olympiades des métiers)
• Equipement en machines modernes qui préparent aux métiers de demain

3 CENTRES en Bourgogne

- Alerter et se faire aider (professionnel extérieure comptent)
- Bien communiquer (En interne et en externe)
- L'organisation et le sang froid

Partie démonstration et discussion (30 mins)

- Démonstration d'exécution d'un malware
- Démonstration d'une attaque réseau Wifi
- Discussions, échanges, questions

Suite de parcours et passerelles possibles

Après cette formation, les apprenants peuvent :

- Approfondir avec des formations techniques : Cybersécurité avancée, Pentesting, Sécurité réseau, RGPD, Analyse de vulnérabilités
- Accéder à des certifications professionnelles (CEH, Sec+ CompTIA, etc.)
- Intégrer des parcours diplômants ou certifiants en sécurité informatique
- Participer à des MOOC ou formations labellisées par l'ANSSI

Métiers - Débouchés

Cette formation d'initiation ne vise pas un métier spécifique à court terme, mais elle constitue une base essentielle pour évoluer dans les secteurs suivants :

- Technicien systèmes et réseaux
- Analyste cybersécurité (après formations complémentaires)
- Administrateur systèmes
- Développeur logiciel (avec une orientation sécurité)
- Consultant en sécurité informatique
- Responsable informatique ou RSSI junior (dans une logique de montée en compétences)

Elle est également pertinente pour tout professionnel exposé à des risques numériques (télétravail, manipulation de données sensibles, usage des outils cloud, etc.).

Validation et certification

Attestation de fin de formation

Version documentaire

V0-2024