Sensibilisation à la cybersécurité

Non-certifiante | Formation continue

Réf. : 26217859F — Mise à jour : 11 août 2026

Organisme responsable : **ATOUT FORMATION**

Présentation de la formation

Objectifs

Comprendre les enjeux de la cybersécurité et du RGPD afin de mieux protéger les données personnelles et adopter les bons réflexes dans les pratiques professionnelles quotidiennes.

Compétences visées :
À l'issue de la formation, vous serez capable de :

- Comprendre les enjeux liés au cyberespace et à la protection des données.
- Acquérir les fondamentaux de la cybersécurité : principes, menaces, attaques et motivations des cybercriminels.
- Maîtriser les principaux termes et notions liés à la cybersécurité.
- Identifier les risques et menaces cyber, tant individuels que professionnels.
- Comprendre le rôle des mesures de sécurité et appliquer les principes d'hygiène numérique.
- Identifier les données personnelles et sensibles ainsi que leurs principaux traitements.
- Comprendre les obligations et principes fondamentaux du RGPD.
- Adopter les bonnes pratiques pour protéger les données et les équipements.
- Identifier une situation à risque, une vulnérabilité ou une faille de sécurité.
- Réagir de manière appropriée en cas de tentative d'attaque ou d'incident.
- Appliquer les principes du RGPD dans ses activités professionnelles.
- Développer une posture de vigilance et adopter des comportements responsables face aux risques numériques.

Programme

Conférence « Voyage dans le cyberespace » – 3h30

- Enjeux et chiffres clés de la cybersécurité.
- Concepts fondamentaux de sécurité et principaux risques cyber.
- Menaces visant les organisations : usurpation d'identité, phishing, compromission de messagerie, etc.
- 10 bonnes pratiques : mots de passe, VPN, mises à jour, vigilance, etc.
- Réflexes à adopter en cas d'incident.

Modules thématiques adaptés aux métiers
Module RGPD – 2h

- Principes fondamentaux du RGPD : licéité, minimisation et sécurité.
- Protection des données personnelles et sensibles dans le contexte MSA.
- Risques liés aux fuites de données et aux erreurs humaines.
- Obligations légales et responsabilités.
- **Cas pratique :** analyse d'un incident de fuite de données et élaboration d'un plan d'actions correctives et préventives.

Module Fraude & arnaques – 2h

- Phishing, vishing, fraude au président et ingénierie sociale.

- Identification des signaux faibles et comportements suspects.
- **Cas pratique :** analyse de courriels frauduleux et simulation de validation d'une demande financière.

Module TT et Nomadisme – 2h

- Risques liés au télétravail et à la mobilité.
- Sécurisation des réseaux Wi-Fi, VPN et authentification.
- Protection des équipements et des données.
- **Cas pratique :** audit d'un environnement de travail à domicile et identification des failles de sécurité.

Module IA & cybersécurité – 2h

- Opportunités et risques liés à l'intelligence artificielle.
- Menaces émergentes : deepfakes, automatisation des attaques, etc.
- Risques de fuite de données et enjeux RGPD.
- **Cas pratique :** analyse de prompts à risque et détection de contenus générés ou manipulés par l'IA.

Atelier ludique « Challenge cybersécurité » – 1h30

- Challenge sur la robustesse des mots de passe.
- Identification et classement des situations à risque.
- Analyse d'un poste de travail non sécurisé.
- **Battle en équipe :** identification des failles, recherche de solutions et justification des choix.

Certifications préparées et métiers visés

Niveau d'entrée	Niveau de sortie
Sans niveau spécifique	Sans niveau spécifique

Métiers associés

K1903 — Défense et conseil juridique
M1801 — Administration de systèmes d'information
M1802 — Expertise et support en systèmes d'information
M1803 — Direction des systèmes d'information
M1806 — Conseil et maîtrise d'ouvrage en systèmes d'information

Dates et lieux de formation

N° session	Modalité	Lieu	Du	Au
2364244S	À distance	—	26/03/2027	26/03/2027
2364246S	À distance	—	28/09/2027	28/09/2027

Source : GREF Bretagne #26217859F