

CENTRE

Axe 2 : Prévention et gestion des risques

# Module n°2 : Renforcement de la cybervigilance - Actions de sensibilisation et de gestion des incidents liés au risque cyber

## Contexte

---

L'écosystème du secteur de la santé évolue considérablement, le développement de nouveaux outils numériques et de nouveaux acteurs, accompagnés de leur lot d'avantages et de risques numériques. Ces risques numériques ne sont plus à prendre à la légère, en effet une panne informatique peut aujourd'hui mettre à l'arrêt des services complets et impacter la continuité des soins. Face à ces risques nouveaux, les agents de la fonction publique hospitalière sont les premiers impactés. En réponse à ces risques croissants, il convient pour chaque agent de renforcer sa capacité à faire face aux risques et aux attaques en renforçant ses compétences en cybervigilance. Le but de cette journée de formation est de permettre aux agents de connaître les risques et les types d'attaques et de savoir y faire face tout en s'insérant de manière efficiente dans la politique de sécurité informatique de leur établissement.

## Objectifs

---

N°1 : Appréhender la cybercriminalité, ses objectifs, et les risques inhérents aux établissements de santé

N°2 : Prendre conscience du rôle contributeur de chacun dans la cybersécurité des établissements de santé

N°3 : Être en mesure de détecter les menaces les plus courantes et de réagir

N°4 : Accompagner l'adoption du numérique au sein des établissements de santé en adoptant une posture de vigie et de diffusion des bonnes pratiques.

## Renseignements complémentaires

---

Financement : Crédits nationaux Anfh

## Programme

---

### JOUR 1

#### Module 1 : Appréhender la cybercriminalité

- Travail de groupe "Dessins internet"
- Exposé interactif sur les cybercriminels

[https://www.anfh.fr/les-offres-de-formation/AZaA\\_kRValQILBFyZ8Yr](https://www.anfh.fr/les-offres-de-formation/AZaA_kRValQILBFyZ8Yr)

- Jeu de cartes "Simulation d'une cyberattaque"

### **Module 2 : Prendre conscience du rôle de contributeur de chacun**

- Analyse réflexive des pratiques professionnelles
- Exposé interactif sur la cybersécurité

### **Module 3 : Être en mesure de détecter les menaces**

- Démonstration de hacking via email malveillant
- Exercice de représentation sur les critères suspects
- Entraînement par atelier pour trouver les emails malveillants
- Exposé interactif sur les pièces jointes.

#### Les arnaques et fraudes

- Exposé interactif de présentation des diverses fraudes par email et SMS.

#### Mots de passe et authentification forte

- Démonstration de hacking liées au mot de passe
- Reformulation et synthèse par les apprenants
- Démonstration commentée sur l'utilisation des gestionnaires de mots de passe.

#### **Public**

**Tout agent de la FPH**

#### **Exercice**

**2026**

#### **Code de formation**

**AFN 2022**

#### **Nature**

**AFN**

#### **Organisé par**

**Déméter Santé- Fin de marché 12/06/2026**

#### **Durée**

**7 heures**

#### **Typologie**

**Formation continue ou Développement des connaissances et des compétences**