AUVERGNE
Axe 3 : ADAPTATION AUX ACTUALITES REGLEMENTAIRES

Renforcement de la cybervigilance : acquérir les bons réflexes

Contexte

Cette formation a pour but de renforcer les connaissances et la vigilance des agents de la fonction publique hospitalière face aux enjeux de cybersécurité. A travers cette formation, les apprenants seront sensibilisés à la cybervigilance au quotidien dans leur travail, pour être en mesure de détecter les menaces, alerter, et appliquer les premières mesures réflexes en cas de cyberattaque. La formation alterne des contenus théoriques, des temps d'échanges, des démonstrations et des jeux de mise en situation. Ces derniers permettent d'illustrer, très concrètement, la manière dont un agent pourrait ouvrir accidentellement la porte à une cyberattaque.

Objectifs

- Appréhender la cybercriminalité, ses objectifs, et les risques inhérents aux établissements de santé
- Prendre conscience du rôle contributeur de chacun dans la cybersécurité des établissements de santé
- Être en mesure de détecter les menaces les plus courantes et de réagir
- 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

Merci de nous faire parvenir vos demandes d'inscription avant le 01/02 afin que nous puissions organiser un groupe en fonction des besoins

Programme

Appréhender la cybercriminalité :

- Travail de groupe "Dessinons internet"
- Exposé interactif sur les cybercriminels
- Jeu de cartes "Simulation d'une cyberattaque"

Prendre conscience du rôle de contributeur de chacun :

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

Être en mesure de détecter les menaces :

- Les emails malveillants
- Les arnaques et fraudes
- Mots de passe et authentification forte

Public
Tout agent de la Fonction Publique Hospitalière (FPH)

Exercice
2025

Code de formation
16AFR

Nature
AFR

Organisé par
CRISALYDE

Durée
7 heures