POITOU-CHARENTES
Axe 6 : Compétences transversales

Renforcement de la cybervigilance - Actions de sensibilisation et de gestion des incidents liés au risque cyber

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

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

Programme

Module 1 : Appréhender la cybercriminalité :

- Travail de groupe "Dessinons internet"
- Exposé interactif sur les cybercriminels
- 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 :

Les emails malveillants

- 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 public, mais certains personnels pourront être plus sensibilisés dans le cadre de leur activité : Chefs d'établissement et équipes de direction, le personnel soignant et les personnels administratifs et techniques

Exercice
2024

Nature
AFN

Organisé par
CHRISALYDE - DEMETER

Durée
7 heures