FRANCHE-COMTÉ
Axe 8 : Actions transversales

Renforcement de la cybervigilance : acquérir les bons réflexes

Contexte

Les établissements de santé sont des cibles particulièrement vulnérables aux cyberattaques, comme l'illustre l'augmentation des attaques par rançongiciel qui les affectent actuellement, avec en particulier pour conséquences la perturbation du fonctionnement des services médicaux, dans un contexte de crise sanitaire grave. En cohérence avec la feuille de route stratégique du numérique en santé de « Ma santé 2022 », un plan de renforcement de la cyber sécurité des hôpitaux a été validé en juin 2019, appuyé par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). En lien avec l'ANSSI et l'Agence du numérique en santé (ANS), le ministère de la santé déploie un plan de formation pour outiller les directions des établissements de santé (et GHT) dans la préparation et l'accompagnement de leurs équipes (personnel médical et non médical) au risque cyber. Dans ce contexte, un ensemble d'actions est lancé sur le terrain dont une campagne de communication nationale « tous cyber-vigilants »et un accompagnement dans le cadre du Ségur numérique. En appui à cette campagne, l'objectif est de prioriser des actions de formation continue dédiées à ce nouvel enjeu.

Objectifs

Voir programme ci-dessous

Renseignements complémentaires

- Durée : 1 jour
- Lieu de la formation : Besançon
- Programmation : 1 groupe par semestre
- Financement : pas de coût pédagogique à prévoir pour l'établissement.
- Modalités d'inscriptions : le service formation de l'établissement adresse ses demandes d'inscriptions à l'ANFH.

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.

Modalités pédagogiques:

- Tours de tables
- Travail de groupe
- Exposés interactifs
- Jeu de cartes
- Analyse réflexive
- Démonstration de hacking
- Entrainements par atelier
- Cas concret

Public
Tout agent de la Fonction Publique Hospitalière

Exercice
2025

Nature
AFN

Organisé par
CHRYSALIDE

Durée
7 heures