ALPES
Axe 3 : ADAPTATION AUX ACTUALITES REGLEMENTAIRES

Module n°1 : Cybervigilance : actions de sensibilisation et de gestion des incidents

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 et de permettre aux agents de connaitre 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

Comprendre à quoi sert la Sécurité des Système d’Information (SSI) dans un établissement de santé (protection des données, réputation de l’établissement, continuité des soins).

Comprendre son rôle dans la sécurité informatique de son établissement.

Connaitre et détecter les différents types de menaces (motivations des cybers criminels, victimes potentielles, etc.).

Développer un esprit critique et devenir vigilant.

Connaitre les actions concrètes mobilisables à son niveau (points de vigilances et bonnes pratiques).

Programme

Proposition de structure : JOUR 1 :

> Comprendre à quoi sert la SSI dans un établissement de santé (protection des données, réputation de l’établissement, continuité des soins)
>
> - Etat de la menace cyber aujourd’hui.
> - Quel rôle pour la SSI.
> - L’impact des agents sur la sécurité d’un établissement. Comprendre son rôle dans la sécurité IT de son établissement
> - L’agent un acteur clé de la SSI.

- Le rôle de l’agent au quotidien.
- Le rôle de l’agent en période de crise.
- Le rôle de l’agent dans l’évolution du SI

Connaitre et détecter les différents types de menaces:

- L’environnement technique et les menaces.
- Les types de cyberattaques et leurs impacts.

Développer un esprit critique et devenir vigilant.

- Lutter à son niveau contre la cybercriminalité.

Acquérir des réflexes de protection.

- Les points de vigilance dans sa pratique.
- Méthode d’analyse des droits d’accès.
- Méthode d’analyse d’un email.
- Comment détecter de l’ingénierie sociale.

Connaitre les actions concrètes mobilisables à son niveau (Points de vigilances et bonnes pratiques).

- Choisir avec soin ses mots de passe.
- Mettre à jour régulièrement ses logiciels.
- Bien connaître ses utilisateurs et ses prestataires.
- Effectuer des sauvegardes régulières.
- Sécuriser l’accès Wi-Fi de son établissement.
- Être aussi prudent avec son ordiphone (smartphone).
- Protéger ses données lors de ses déplacements.
- Être prudent lors de l’utilisation de sa messagerie.
- Télécharger ses programmes sur les sites officiels.
- Être vigilant lors d’un paiement sur Internet.
- Séparer les usages personnels des usages pros.
- Prendre soin de ses informations.

Public
Tout agent de la FPH

Exercice
2025

Nature
AFR

Organisé par
Déméter Santé

Durée
7 heures

Typologie
Formation continue ou Développement des connaissances et des compétences