PACA
Axe 2 : STRATÉGIE ET ORGANISATION

Module n°1 : Webinaire : Se sensibiliser à la cybersécurité

Contexte

Depuis 2020, les attaques informatiques se multiplient au sein des établissements publics de santé. La menace est préoccupante et réelle, ce qui a conduit l'Etat a faire de la cybersécurité un axe prioritaire du plan France Relance. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) pilote ainsi un plan d'accompagnement pour tout établissement volontaire, afin d'accroitre leur niveau de cybersécurité.

Au-delà des moyens qui peuvent être alloués sur le sujet, la sécurité informatique concerne chaque personne au sein des organisations. Chaque individu peut donc être acteur dans la sécurité du système d'information de son établissement, mais peut également représenter un risque si les bonnes pratiques ne sont pas maîtrisées.

Que ce soit en favorisant les bonnes pratiques numériques (cybervigilance) ou en accompagnant les professionnels des SI et les utilisateurs de NTIC à faire face en cas d'attaque (cyberdéfense), l'ANFH veut proposer différents outils de sensibilisation, de formation et d'entrainement à la gestion de crise cyber.

Objectifs

- Appréhender la cybercriminalité, ses objectifs, et prendre la mesure des conséquences pour les établissements de santé
- Être en mesure de détecter les menaces les plus courantes et de réagir

Renseignements complémentaires

Durée de la formation : varie selon les modules

Pour plus d'informations :

Audrey DAVID (a.david@anfh.fr) 04.91.17.71.28

Programme

Les cybercriminels et la cybercriminalité

- Comprendre les motivations des cybercriminels
- Découvrir quelques attaques du milieu de la santé

Les cyberattaques

- Comprendre les conséquences pour les établissements de santé

Les emails malveillants

- Détecter une tentative d’hameçonnage (phishing)
- Titres et liens qui poussent à l’action
- Expéditeur
- Liens douteux (et comment reconnaître un lien qui cherche à piéger)
- Les pièces jointes
- Les fichiers les plus utilisés par les cybercriminels (Documents office avec Macro, archives, PDF…)
- Les conséquences en cas d’ouverture
- Les bon réflexes suite à un email malveillant
- Signaler l’email
- Se manifester en cas de clic, d’ouverture de PJ, etc.

Public

Tout public

Exercice
2024

Code de formation
2.11

Nature
AFR

Organisé par
Organisme au choix selon module

Durée
2 heures

Typologie
Formation continue ou Développement des connaissances et des compétences