Association nationale pour la formation permanente du personnel hospitalier

Formation sur la cybervigilance : Les 7 modules

Module	Objectifs	Durée	Publics
Module n°1 : Webinaire : Se sensibiliser à la cybersécurité	• 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	**2 heures**	Tout public
Module n°2 : Mise en situation cyberattaque pour les bureaux des entrées	• Comprendre à quoi sert la SSI dans un établissement de santé et plus particulièrement dans son service • Lister les outils SI utilisés dans son service et les risques associés à chaque outil qui dysfonctionnerait • Concevoir l'activité du service sans ces outils • Etablir quels documents papier, supports, outils, peuvent pallier l'absence de système SI opérationnel • Reconnaître une situation de cyberattaque • Définir une procédure d'activité en mode dégradé spécifique à son service/pôle	**1 jour**	Tout personnel du Bureau des admissions
Module n°3 : Mise en situation cyberattaque dans un service de génie biomédical	• Comprendre à quoi sert la SSI dans un établissement de santé (protection des données, réputation de l'établissement, continuité des soins) • Comprendre les interactions entre le service biomédical et le service sécurité informatique • Connaître le risque de piratage des appareils médicaux • Communiquer efficacement avec le SSI • Savoir être vigilant lors de la maintenance des appareils médicaux (en présentiel ou à distance) • Définir un protocole de mise au rebus des disques durs contenant des données de santé	**1 jour**	Tout personnel du service biomédical

	• Etablir des protocoles d'action en cas de cyberattaque		
Module n°4 : Mise en situation d'une cyberattaque pour les services techniques	• Comprendre à quoi sert la SSI dans un établissement de santé (protection des données, réputation de l'établissement, continuité des soins). • Comprendre les interactions entre les différents appareils connectés et le service sécurité informatique • Connaître le risque de piratage des appareils • Être confronté à des scénarii d'attaque mettant en cause ces appareils connectés • Apprendre à réagir efficacement en cas de cyberattaque	**1 jour**	Tout personnel du service technique
Module n°5 : Mise en situation d'une cyberattaque pour les services de Direction	• Définir la chaîne de décision et le rôle de chacun en cas d'attaque • Travailler sur un protocole d'action.	**1 jour**	Tout personnel de l'équipe de direction de l'établissement
Module n°6 : Comment piloter un plan de continuité des activités	• Acquérir la méthodologie d'élaboration du Plan de Continuité des Activités spécifiques à son domaine • Assurer le lien entre les services de soins et le service informatique	**2 jours**	Personnel d'un même domaine d'activités et personne(s) de la direction des services informatiques en charge de l'applicatif du domaine
Module n°7 : Formation-action : simuler une attaque/défense pour les agents des services informatiques	• Entraîner les administrateurs et techniciens des SI à faire face à différents scénarii de cyberattaque, en fonction d'environnements types.	**2 jours**	Professionnels des SI, équipe SSI et administrateurs