|  |
| --- |
|  |
| Plan de Sensibilisation à la Cybersécurité |
| CHU de Ynov |

|  |
| --- |
| VIOLLET Yoan, ETESSE Tristan |

# 1. Objectif du programme

Renforcer la culture de cybersécurité au sein du personnel hospitalier afin de réduire les risques liés aux comportements humains. L’objectif est de faire en sorte que chaque utilisateur adopte les bons réflexes face aux menaces numériques courantes.

# 2. Public visé

L’ensemble du personnel du CHU est concerné, avec des actions adaptées à chaque profil :  
- Personnel médical (médecins, infirmiers, soignants)  
- Personnel administratif  
- Techniciens et prestataires externes  
- Direction et encadrement

# 3. Thèmes abordés

- Reconnaître les e-mails de phishing  
- Sécurité des mots de passe  
- Risques liés aux clés USB et périphériques  
- Utilisation sécurisée des postes de travail  
- Comportement à adopter en cas de suspicion d’incident  
- Confidentialité des données médicales et personnelles

# 4. Moyens utilisés

- Sessions de formation en présentiel ou visio (30 min à 1h)  
- Affiches et fiches réflexes distribuées dans les services  
- Simulations de phishing internes (campagnes contrôlées)  
- Envoi régulier de conseils de cybersécurité par e-mail  
- Intégration d’un module de sensibilisation dans les parcours de formation RH

# 5. Fréquence et durée

- Formation initiale à la prise de poste  
- Rappel annuel obligatoire  
- Sensibilisation spécifique en cas d’incident ou de changement majeur

# 6. Évaluation et suivi

- Tests de reconnaissance de mails frauduleux (après formation)  
- Statistiques de participation aux formations  
- Rapports de simulation de phishing  
- Questionnaire de validation des acquis en fin de session

# 7. Supports prévus

- Présentation PowerPoint (livrée lors des sessions)  
- Fiches réflexes par thème (1 page)  
- Affiches synthétiques pour affichage dans les services  
- FAQ cybersécurité disponible sur l’intranet

# 8. Calendrier de déploiement

- Mois 1 : lancement et communication interne  
- Mois 2 : formation du personnel médical  
- Mois 3 : formation du personnel administratif et direction  
- Mois 4 : simulation de phishing et analyse des retours  
- Mois 5 : bilan intermédiaire et ajustements  
- Mois 6 : validation finale et intégration dans le parcours RH