Sensibilisation à la Cybersécurité - Personnel Hospitalier

Introduction

Cybersécurité au CHU : Tous concernés !

Cette présentation vise à sensibiliser le personnel hospitalier aux cybermenaces et aux bons gestes à adopter pour protéger les données de santé des patients.

Pourquoi l'hôpital est une cible ?

- Les données médicales ont une valeur marchande élevée (dossiers patients, identifiants, prescriptions...)
- Les services hospitaliers sont critiques : toute indisponibilité peut mettre des vies en danger
- Le secteur de la santé est souvent moins préparé aux risques informatiques que d'autres secteurs

Les principales menaces

- Phishing (hameçonnage)
- Clés USB ou appareils inconnus
- Vol ou perte d'appareils
- Mots de passe faibles ou partagés
- Utilisation de réseaux Wi-Fi publics ou non sécurisés

Exemples d'attaques réelles

- CHU de Rouen (2019) : attaque par ransomware -> blocage de l'informatique médicale
- Hôpital de Dax (2021) : arrêt complet du SI, dossiers papier ressortis
- HSE Dublin (2021) : piratage massif, blocage des soins, données volées

Conséquences :
- Retards ou annulations de soins
- Réputation de l'établissement atteinte
- Confidentialité des patients compromise

Bonnes pratiques à adopter

Sensibilisation à la Cybersécurité - Personnel Hospitalier

[ok] Verrouiller son écran dès qu'on s'éloigne

[ok] Ne jamais cliquer sur un lien douteux dans un mail

[ok] Ne pas connecter de clé USB inconnue

[ok] Utiliser des mots de passe robustes et différents pour chaque service

[ok] Ne jamais partager son mot de passe, même à un collègue

[ok] Signaler toute anomalie ou comportement suspect

Exercice pratique : Démasquez le phishing !

Exemple d'un faux email reçu :

"Votre compte CHU expire aujourd'hui ! Cliquez ici pour le réactiver."

[loupe] Indices à repérer :

- Adresse email suspecte
- Ton alarmiste ou urgence
- Fautes d'orthographe
- Demande d'informations confidentielles

Que faire en cas d'incident ?

1. Rester calme
2. Ne pas utiliser davantage l'ordinateur concerné
3. Débrancher le réseau (si conseillé)
4. Contacter immédiatement l'équipe informatique ou le référent cybersécurité
5. Ne pas tenter de résoudre seul(e) la situation

Conclusion

[idee] La cybersécurité est l'affaire de tous.

[cadenas] En protégeant les systèmes du CHU, nous protégeons la santé et la vie de nos patients.

[objectif] Chaque geste compte !