Cybersécurité : les réflexes à adopter

CONTEXTE

Exposés à des risques majeurs d'atteinte aux données de santé, les professionnels de santé libéraux doivent désormais adopter des mesures de sécurité pour protéger les informations de leurs patients contre les accès non autorisés, les ransomwares et toutes autres formes de cyberattaques.

L'UNPS vous partage le Mémento de sécurité informatique pour les professionnels de santé en exercice libéral élaboré par l'Agence du Numérique en Santé (ANS).
Ce mémento très rapide à lire propose des pratiques simples et efficaces pour se protéger contre la majorité des attaques, ou en atténuer les impacts, sans nécessiter de connaissances techniques approfondies. Chacun peut s'en emparer et appliquer les mesures préconisées sans difficulté.

QUELQUES DÉFINITIONS

- Ransomwares ou rançongiciels : logiciels malveillants qui chiffrent vos fichiers et exigent une rançon pour les débloquer.
- Phishing ou hameçonnage : attaques par e-mail ou messages trompeurs visant à voler vos informations personnelles.
- Vol d'identité : utilisation frauduleuse de vos données personnelles.
- Malware : logiciels malveillants qui infectent vos appareils.
- Spyware : logiciels espions qui collectent vos informations sans votre consentement.

POUR ALLER PLUS LOIN

- Mémento de sécurité informatique pour les professionnels de santé en exercice libéral élaboré par l'Agence du Numérique en Santé (ANS)
- Plateforme e sante-formation : modules de formation de 5 à 10 minutes. Pour y accéder, créer un compte sur https://esante-formation.coorpacademy.com
- Site internet Cybermalveillance.gouv.fr : conseils et attitudes à adopter en cas de cyberattaque.

Cybersécurité : les réflexes à adopter

1- Maîtriser l'accès physique au lieu d'exercice et la sécurité physique des équipements informatiques

2- Protéger le poste de travail et l'accès aux applications

Respecter les règles de sécurité pour les cartes CPx et e-CPS, utiliser des mots de passe robustes, protéger l'accès au poste de travail en cas d'absence, veiller à la mise à niveau du système et des outils logiciels, séparer les usages professionnels des usages personnels

3- Maîtriser les accès aux informations

Utiliser une messagerie sécurisée de santé et renforcer la protection des comptes informatiques les plus sensibles

4- Connaître les principes de sécurité et les diffuser

Se renseigner sur les cyber menaces et les usages de l'informatique

5- Anticiper la survenue d'incidents de sécurité

Sauvegarder les données, détruire celles qui doivent être supprimées, savoir réagir en cas d'incident de sécurité informatique

6- Respecter les règles d'échange et de partage des données de santé à caractère personnel

7- Respecter les principes de la protection des données de santé à caractère personnel

Connaitre et appliquer les principes du règlement général sur la protection des données (RGPD), élaborer un registre des activités de traitement de données à caractère personnel

8- Répondre aux obligations de conservation et de restitution des données

Appliquer les durées règlementaires ou recommandées de conservation des données
S'assurer de la capacité de restitution des données à caractère personnel

9- Intégrer la sécurité dans les contrats avec les tiers

Définir l'objet des fournitures de service informatique et les limites d'engagement
Réunir les conditions pour travailler en toute sécurité au sein d'environnements maîtrisés par un tiers
Respecter les règles relatives à l'hébergement de données de santé à caractère personnel