Les risques d'une cyberattaque dans le secteur de la santé

Clics sur des mails frauduleux, usage personnel des outils professionnels, mot de passe partagé et facile à déchiffrer, ces mauvaises pratiques peuvent mener à de lourdes conséquences : coupure réseau, inaccessibilité des planning, divulgations de données de santé sur le web.

Adoptez les bons réflexes en matière d'hygiène informatique

- → **Utilisez des mots de passe uniques**, difficiles à décoder (majuscule + minuscule + caractères spéciaux) ou des phrases longues mais simples à retenir (exemple: OuSaMaMètMonBanLinèt!)
- → **Utilisez la double-authentification** dès que possible
- → **Installez un coffre-fort de mots de passes** (Keypass, Bitwarden, Dashlane...) pour ne plus avoir à les retenir et renforcer la sécurité de vos accès
- → **Reconnaissez les mails suspects** (offre alléchante, demande urgente, fautes d'orthographe...) pour ne pas les ouvrir
- → **Verrouillez votre session d'ordinateur** qui contient des données sensibles lorsque vous ne l'utilisez plus
- → **Séparez votre messagerie professionnelle et personnelle**
- → **Stockez les données de vos patients** uniquement sur des outils professionnels adaptés
- → **Mettez régulièrement à jour vos logiciels**
- → **Contactez votre gestionnaire informatique** ou votre éditeur de logiciel pour vous accompagner

NOU VEY
CYBERSÉCURITÉ SANTÉ RÉUNION

Informez-vous sur www.nouvey.re