10 POINTS

comment prévenir facilement les cyberattaques

Des dossiers médicaux numériques, aux ordonnances électroniques jusqu'aux agendas en ligne... Les soins de santé se font de plus en plus de façon numérique. Parallèlement, la cybercriminalité augmente à un rythme préoccupant, et les données médicales sont souvent une cible appréciée.

Découvrez 10 points (douloureux) comment prévenir facilement les cyberattaques et comment armer votre cabinet médical ou votre pharmacie contre les cybercriminels.

ENVOI DE DONNÉES À CARACTÈRE PERSONNEL PAR E-MAIL

N'envoyez des e-mails que si votre e-mail (ou pièce jointe) ne contient aucune information confidentielle. Sinon, utilisez un portail en ligne sécurisé.

CHOISISSEZ DES MOTS DE PASSE FORTS

Créez des mots de passe complexes et uniques comportant au moins 15 caractères et modifiez-les régulièrement, surtout si vous pensez que votre appareil a été compromis.

RESTREINDRE L'ACCÈS AUX DONNÉES MÉDICALES

Gardez une trace de qui a consulté quels fichiers, où et quand grâce à la journalisation. Et parlez aux salariés s'ils ont consulté illégalement des données sensibles.

FAITES DES SAUVEGARDES RÉGULIÈRES DE VOS DONNÉES

Ne vous précipitez pas pour choisir votre fournisseur de cloud. Comparez différents acteurs et choisissez de préférence quelqu'un qui peut fournir les certificats ISO nécessaires.

INSTALLER UN ANTIVIRUS

Lorsque vous achetez un logiciel antivirus, il est recommandé d'effectuer des mises à jour régulières pour garantir que votre appareil ou logiciel continue de fonctionner correctement et en toute sécurité.

SOYEZ ALERTE AU PHISHING ET AUX RANSOMWARE

Ne cliquez jamais sur des liens non fiables dans les e-mails ou les SMS.

SENSIBILISEZ VOTRE PERSONNEL AUX RISQUES

Assurez-vous que votre personnel ayant accès aux données médicales est également correctement formé et conscient des exigences en matière de confidentialité. Proposer une formation régulière à ce sujet.

GARDEZ VOTRE SYSTÈME D'EXPLOITATION À JOUR

La mise à jour fréquente de votre système d'exploitation existant est essentielle, mais pas toujours suffisante. Installer une nouvelle version est bien plus drastique et souvent mieux adapté pour bloquer les cyberattaques.

SÉCURISEZ VOTRE RÉSEAU WIFI

Ne vous contentez pas de donner à tout le monde accès à votre réseau WiFi professionnel. Fournir un réseau séparé pour les patients. De cette façon, vous réduisez le risque que des pirates informatiques pénètrent dans votre logiciel.

FOURNIR UN CONNEXION UNIQUE PAR UTILISATEUR

Quelqu'un quitte-t-il l'organisation ou change-t-il de poste ? Ajustez ensuite les droits d'accès le plus rapidement possible.

Grâce au Corilus Security Check, notre expert examine votre matériel et vos logiciels, et répertorie les différents risques et suggestions.

DEMANDEZ VOTRE SECUIRTY CHECK

Vous souhaitez déjà sécuriser et sauvegarder votre cabinet à partir de €4

CLIQUEZ ICI

CORILUS
Connecting Care