Cybermenaces au cabinet dentaire

Comment les prévenir ?
Que faire en cas d'attaque ?

Les exemples de cyberattaques dans la santé ne manquent pas. Du fait de l'accès à des données de santé, les chirurgiens-dentistes sont une cible pour les hackers.

Si vous êtes victime d'une cyberattaque, la police judiciaire propose un point d'entrée unique pour la Nouvelle-Aquitaine : ***cybermenaces-bordeaux@interieur.gouv.fr***

Adopter les bonnes pratiques :

- Protéger les accès avec des **mots de passe** robustes et différents sur tous les équipements.
- Sauvegarder les données régulièrement et conserver une copie des sauvegardes sur un support externe.
- Appliquer les **mises à jour** sur tous vos appareils. Les télécharger uniquement à partir des sites officiels.
- Utiliser un **antivirus** et faire régulièrement des analyses (scans) pour vérifier l'absence d'infection.
- Séparer les **usages personnels et professionnels**. Par exemple, il est conseillé d'éviter de mélanger la messagerie personnelle avec la professionnelle, ainsi que d'utiliser ses appareils professionnels pour un usage personnel (et inversement).
- Maîtriser ses **réseaux sociaux** : protéger l'accès à ses comptes et vérifier les paramètres de confidentialité. Avant de publier un message, penser à l'utilisation qui pourrait en être faite.
- **Relayer** les informations à ses équipes et les **former** aux risques de cybermenaces.

Pour se faire assister par des professionnels spécialisés : ***www.cybermalveillance.gouv.fr***

Conduite à tenir en cas d'attaque :

- Après avoir suspecté ou reconnu les signes d'un système compromis (impossibilité de se connecter, fichiers disparus, ralentissement du système…), **mettre en quarantaine** les équipements en déconnectant les appareils du réseau (ne pas les éteindre).
- **Évaluer** l'étendue de l'intrusion et collecter les preuves.
- Déposer plainte
- Après avoir réalisé une **analyse antivirale** complète, réinstaller le système.
- **Changer les mots de passe** d'accès et **mettre à jour** les logiciels et équipements avant la remise en système du service.
- **Notifier l'intrusion à la CNIL** (*www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles*) en cas de violation de données à caractère personnel et informer de la situation les personnes concernées par ces données personnelles.