Cybermenaces
au cabinet dentaire

FICHE REPÈRE

La question n'est pas de savoir si, **mais quand une cyberattaque impactera le cabinet !**

Les exemples de cyberattaques dans le domaine de la santé ne manquent pas. Du fait de leurs accès à des données sensibles, les cabinets dentaires sont une cible pour les hackers…

L'intensification des usages numériques représente, pour les cybercriminels, une opportunité de développer leurs attaques.

Comment se protéger au mieux face à ces risques ?

Quelques bonnes « cyber » pratiques

Mots de passe

- Protéger ses accès avec **un mot de passe long et complexe**
- Choisir **un mot de passe différent** pour chaque service
- Il doit être particulièrement **robuste pour la messagerie**

Un mot de passe sécurisé doit compter au moins **12 caractères mêlant majuscules, minuscules, chiffres et caractères spéciaux.**

Sauvegardes

- Effectuer des **sauvegardes régulières**
- Identifier les appareils et supports qui contiennent des données
- Vérifier la **planification** des sauvegardes
- **Tester** les sauvegardes

Règle des « 3-2-1 »
3 copies des données
sur **2** supports différents
dont **1** copie hors ligne

Mises à jour

- Appliquer les mises à jour sur **l'ensemble des appareils et logiciels** du cabinet
- Les télécharger uniquement à partir **des sites officiels**

Usages professionnels et personnels

- **Ne pas mélanger** la messagerie professionnelle et personnelle
- **Ne pas utiliser** de service de stockage en ligne personnel à des fins professionnelles
- **Éviter d'utiliser ses appareils numériques professionnels pour un usage personnel** (et inversement)

Réseaux sociaux

- **Protéger l'accès** à ses comptes
- Vérifier les paramètres de **confidentialité**
- Avant de publier un message, **penser à l'utilisation** qui pourrait en être faite

Au quotidien au cabinet dentaire

- Ne pas transmettre **le code WiFi** aux patients
- Respecter **les règles de confidentialité** notamment dans l'espace du secrétariat et de la salle d'attente
- **Ne pas laisser les appareils numériques accessibles** et visibles aux patients, activer le verrouillage automatique
- **Informer et former** le personnel du cabinet

Cybermenaces au cabinet dentaire

Pour sensibiliser votre équipe

Découvrez les outils URPS !

Le jeu des 8 erreurs

L'escape game numérique

Connaissez-vous le croissantage ?

Toute personne laissant son ordinateur sans surveillance avec sa session ouverte (écran non verrouillé) se verra « croissantée ». Elle devra ramener des pâtisseries pour toute l'équipe !
Il existe plusieurs sites qui proposent ce type d'animation, ludique et bienveillante, pour sensibiliser les professionnels de votre cabinet.

Que faire **en cas de cyberattaque ?**

« Je pensais que mon cabinet était une structure trop petite pour intéresser les hackers. Jusqu'au jour où une cyberattaque a tout bloqué.

Ce sont plusieurs petites négligences qui se sont additionnées.

Aujourd'hui, mots de passe robustes, sauvegardes régulières et bonnes pratiques font partie de notre quotidien. La cybersécurité, c'est aussi la sécurité des patients et la continuité des soins. »

- ✓ Isoler les systèmes attaqués en **coupant toutes les connexions à Internet** et au réseau local, **ne pas les éteindre**
- ✓ Collecter les preuves
- ✓ **Déposer plainte**
- ✓ Identifier l'origine de l'attaque et son étendue, **en se faisant accompagner par des professionnels**
- ✓ Notifier l'incident à la CNIL dans les 72h **en cas de violation de données à caractère personnel**
- ✓ **Informer les personnes concernées** par les violations de ces données personnelles

Notifier la CNIL

Pour **se faire accompagner** par des professionnels spécialisés

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en cybersécurité

Pour **déposer plainte**

En cas de cyberattaque

cybermenaces-bordeaux@interieur.gouv.fr
ou **appeler le 17**