Fiche pratique

CYBERSÉCURITÉ

POURQUOI SE PROTÉGER ?

Un risque devenu concret pour les cabinets dentaires

Les cabinets dentaires sont aujourd'hui des cibles privilégiées des cybercriminels.

- Les données de santé peuvent se revendre jusqu'à 250 € par dossier
- En 2025, 43 % des cyberattaques en santé ont visé des structures de moins de 50 salariés

Les cabinets libéraux sont directement concernés.

Des attaques simples…mais redoutablement efficaces

Dans la majorité des cas, les attaques prennent des formes relativement simples.

- **Le rançongiciel (ransomware)** est l'une des plus fréquentes. Il bloque l'accès aux fichiers du cabinet et exige le paiement d'une rançon pour les restituer. Dans ce cas, l'activité peut être paralysée du jour au lendemain.
- **Le phishing (hameçonnage)** repose sur l'envoi d'emails frauduleux imitant des organismes de confiance (banque, fournisseur, administration). Un simple clic ou la transmission d'informations sensibles peut suffire à compromettre l'ensemble du système informatique du cabinet.

Ces attaques ne reposent pas uniquement sur des failles techniques, mais très souvent sur des erreurs humaines ou un manque de vigilance.

Des conséquences lourdes pour le cabinet

Au-delà de l'incident technique, une cyberattaque entraîne des conséquences très concrètes :

- interruption de l'activité, parfois pendant plusieurs jours
- perte de chiffre d'affaires
- désorganisation du cabinet
- stress important pour le praticien et l'équipe
- risque juridique lié à la protection des données de santé

Dans certains cas, des rançons peuvent être exigées, sans garantie de récupération des données. Des sanctions peuvent également être appliquées en cas de protection insuffisante des données patients.

CYBERSÉCURITÉ

FAIRE UN DIAGNOSTIC

Votre cabinet est-il vulnérable ?

Face à ces risques, la première étape consiste à évaluer simplement le niveau de sécurité de son cabinet.

Un cabinet est considéré comme vulnérable lorsque certaines bases ne sont pas respectées : mots de passe partagés, absence de sauvegarde fiable, logiciels non mis à jour, équipe peu sensibilisée ou encore absence de protocole en cas d'incident.

Ce diagnostic ne nécessite pas d'expertise technique avancée, mais une prise de conscience des points sensibles de l'organisation quotidienne.

Identifier votre vulnérabilité

- [ ] Chaque membre de l'équipe a un mot de passe unique et fort
- [ ] L'authentification à deux facteurs est activée
- [ ] Les sauvegardes sont automatiques ET testées régulièrement
- [ ] Le Wi-Fi patient est séparé du réseau professionnel
- [ ] Les logiciels sont à jour (Plage de mise à jour prévue dans l'agenda)
- [ ] L'équipe est formée au phishing
- [ ] Les postes se verrouillent automatiquement
- [ ] Aucune donnée patient ne circule par email personnel ou clé USB
- [ ] L'hébergeur des données est certifié HDS
- [ ] Les postes de travail sont inaccessibles à la patientèle et à tout visiteur.
- [ ] Un protocole de crise existe

Un score inférieur ou égal à 6 indique un niveau de risque élevé.

Toutefois, l'absence d'une mesure critique (sauvegardes testées, sécurisation des accès, hébergement HDS ou protection des données) classe le cabinet en risque élevé, quel que soit le score obtenu.

CYBERSÉCURITÉ

ANTICIPER

Prendre des mesures simples mais efficaces

La cybersécurité ne repose pas uniquement sur des solutions techniques complexes : elle passe avant tout par une organisation rigoureuse et des réflexes partagés par toute l'équipe.

- ☐ ***Former et sensibiliser l'équipe dentaire***. Savoir reconnaître un email suspect, vérifier un expéditeur ou éviter de cliquer sur un lien douteux permet déjà de prévenir une grande partie des attaques.
- ☐ ***Sécuriser les accès***. Chaque utilisateur doit disposer d'un mot de passe personnel, robuste, et les accès doivent être adaptés aux responsabilités de chacun. Le verrouillage automatique des postes est un réflexe simple mais efficace.
- ☐ ***Sauvegarder les données***. Elle doit être automatique, régulière et testée. La règle dite "3-2-1" (3 copies : 2 supports différents et 1 hors ligne) reste une référence. Les données de santé doivent impérativement être hébergées chez un prestataire certifié.
- ☐ ***Sécuriser le réseau*** : un réseau distinct pour les patients, un accès sécurisé pour les professionnels et aucune connexion d'appareils personnels sur le réseau professionnel.
- ☐ ***Maintenir les systèmes à jour*** : logiciels métiers, antivirus, systèmes d'exploitation. Ces mises à jour corrigent des failles régulièrement exploitées par les cybercriminels.
- ☐ ***S'appuyer sur un prestataire informatique spécialisé en santé*** : pour garantir un niveau de sécurité adapté.
- ☐ ***Prendre une assurance*** qui pourra prendre en charge votre perte d'exploitation
- ☐ ***Etablir un protocole informatique*** expliqué et connu de toute l'équipe

CYBERSÉCURITÉ

COMMENT RÉAGIR ?

S'appuyer sur un Protocole établit en amont

Malgré toutes les précautions, le risque zéro n'existe pas. Il est donc indispensable d'anticiper la réaction en cas d'incident.

Protocole à activer en cas d'incident :

Contacter immédiatement votre prestataire informatique

Isoler sans délai les postes ou systèmes infectés

Déposer plainte dans un délai de 72 heures auprès du commissariat le plus proche

Avertir votre assurance

Signaler l'incident :
cert-sante@esante.gouv.fr
Service d'appui à la gestion des cybermenaces
09 72 43 91 25 - 24h/24, 7j/7

Ne pas payer de rançon

(aucune garantie de récupération des données)

URPS CHIRURGIENS-DENTISTES OCCITANIE

285, rue Alfred Nobel
34000 Montpellier

04 67 69 75 28

contact@urps-chirurgiensdentistes-oc.f