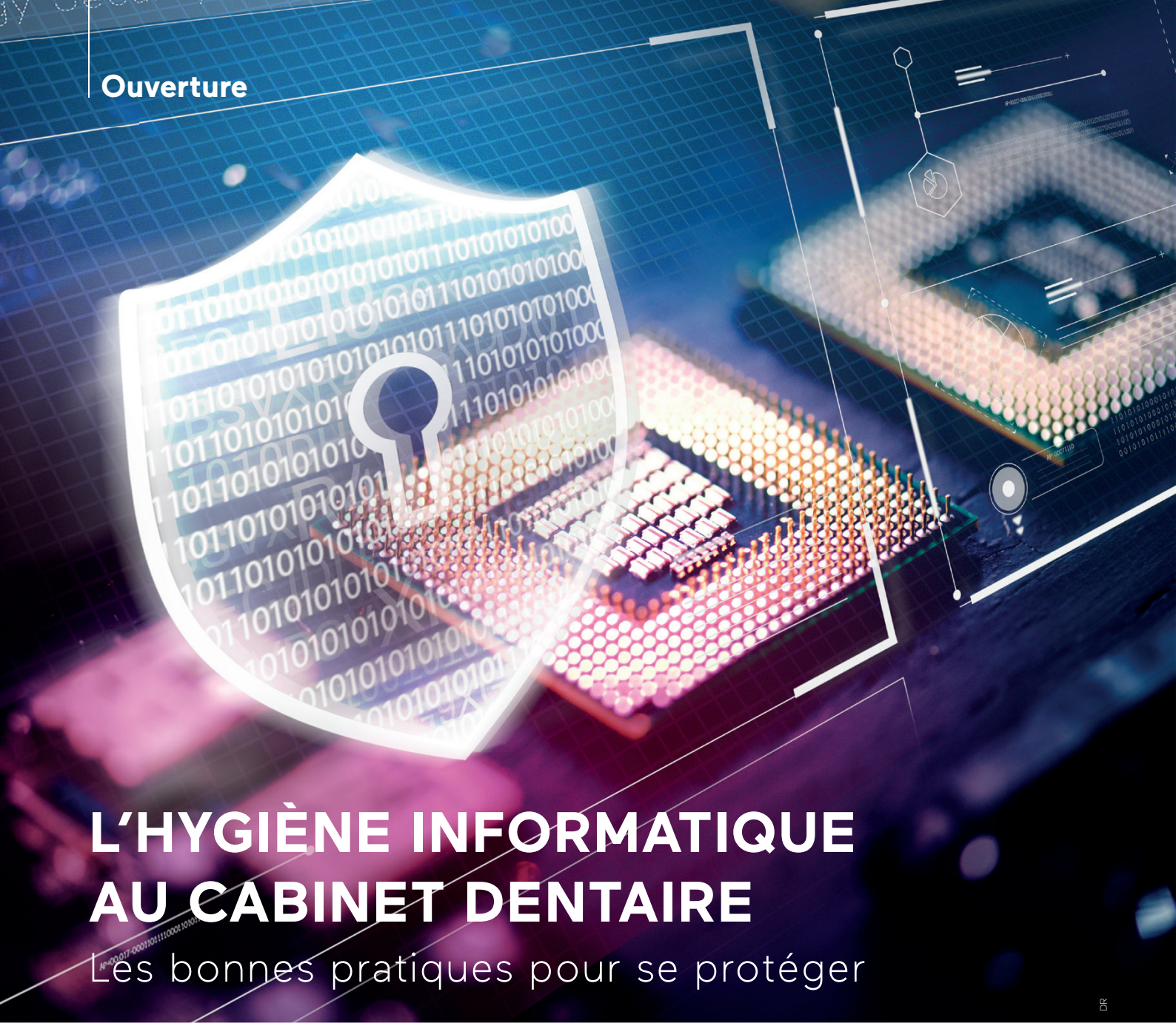


L'HYGIÈNE INFORMATIQUE AU CABINET DENTAIRE

Les bonnes pratiques pour se protéger

DR

JACQUES WEMAERE
PRATIQUE LIBÉRALE
(BORDEAUX)

Dans un monde de plus en plus connecté, les cabinets dentaires sont devenus des cibles potentielles pour les cyberattaques. Car celles-ci ne concernent pas uniquement les grandes entreprises. Les structures plus petites sont souvent moins protégées et donc plus vulnérables. De plus, du fait de leur accès à des données médicales, les professionnels de santé sont une cible pour les hackers. Cabinets, laboratoires de biologie, hôpitaux, les exemples de cyberattaques dans le domaine de la santé ne manquent pas... La question n'est pas de savoir « si » mais « quand » une cyberattaque aura lieu... Que faire pour l'éviter ? Il est notamment important de reconnaître les signes d'un système compromis en identifiant les différentes attaques possibles et d'acquérir les bonnes pratiques en prévention.

Les cyberattaques possibles

1. Le hameçonnage (ou phishing)

(voir exemple ci-contre)

C'est une technique de fraude où un attaquant se fait passer pour une entité de confiance (banque, administration, fournisseur...) afin d'obtenir des informations sensibles, notamment bancaires. Ces attaques passent souvent par des mails frauduleux contenant des liens ou pièces jointes malveillants.

Les bonnes pratiques :

- Vérifier l'adresse mail de l'expéditeur en cliquant sur le nom qui s'affiche.
- Ne jamais cliquer sur un lien suspect.
- Se méfier des demandes urgentes ou alarmistes.
- Ne jamais fournir d'informations sensibles par mail.
- Utiliser un filtre anti-spam efficace.
- Se former aux bonnes pratiques de détection des mails frauduleux.

2. Les ransomwares

(voir exemple page suivante)

Ce sont des logiciels malveillants qui chiffrent les données du cabinet et exigent une rançon pour les restituer. Une infection peut provenir d'un mail, d'un site internet compromis ou d'une clé USB infectée.

Les bonnes pratiques :

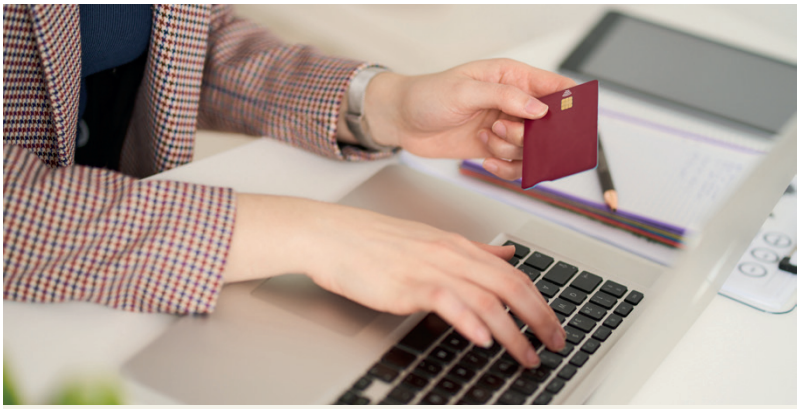
- Sauvegarder régulièrement les données sur un support externe sécurisé et tester les sauvegardes.
- Mettre à jour tous les logiciels et systèmes d'exploitation.
- Ne jamais ouvrir une pièce jointe non attendue.
- Installer un antivirus et un pare-feu efficaces.

3. Fraude au président (ou fraude aux faux virements)

Les cybercriminels exploitent la confiance des employés pour obtenir des accès ou des informations confidentielles.

Exemples de techniques utilisées :

- Faux appels téléphoniques se faisant passer pour un technicien informatique.
- Messages frauduleux demandant une action urgente (exemple : changer un mot de passe immédiatement).
- Usurpation d'identité d'un responsable pour demander un virement bancaire.



DR

La livraison manquante (phishing bancaire)

Contexte : l'équipe dentaire attend toujours du matériel pour faire fonctionner le cabinet. L'assistante reçoit un mail.

Objet du mail : Livraison échouée – Action requise.

Contenu du message : « Bonjour, votre colis contenant le matériel dentaire n'a pas pu être livré ce jour. Veuillez reprogrammer la livraison sous 24 heures en réglant les frais de dossier (1,49 €) via le lien suivant : Replanifier la livraison ». L'assistante clique sur le lien et saisit les **coordonnées de la carte bancaire professionnelle.** Résultat : quelques heures plus tard, des débits suspects apparaissent sur le compte du cabinet (abonnements en ligne, achats à l'étranger...).

À retenir :

- Les transporteurs ne demandent jamais de paiement par lien pour une reprogrammation.
- Toujours vérifier l'adresse de l'expéditeur et appeler directement le fournisseur ou le livreur s'il y a un doute.

La protection du cabinet et des données des patients repose ainsi sur **une bonne hygiène informatique**, qui s'applique sur plusieurs niveaux.

Sécurisation des accès

- Utiliser des mots de passe robustes : au moins 12 caractères avec lettres, chiffres et symboles.
- Activer l'authentification à deux facteurs pour les accès sensibles.
- Ne jamais réutiliser un mot de passe pour plusieurs services et les changer régulièrement.
- Utiliser un gestionnaire de mots de passe certifié pour stocker et générer des identifiants sécurisés (par exemple, le logiciel KeePass, certifié par l'Anssi).

RANSOMWARE CIBLANT UN CABINET DENTAIRE

Contexte : un cabinet dentaire reçoit un e-mail semblant provenir de l'Urssaf. C'est l'assistante dentaire qui consulte la boîte mail du cabinet ce matin-là.

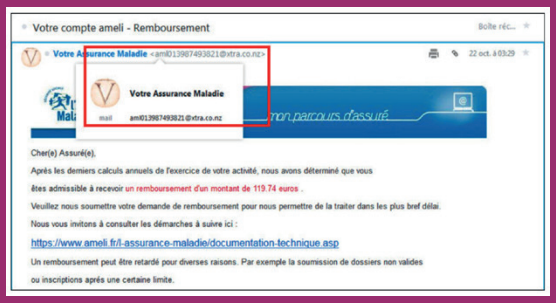
Objet du mail : Trop-perçu sur vos cotisations - Demande de remboursement.

Contenu du message : « Madame, Monsieur, après vérification de votre dossier, un trop-versé de 1482,16 € a été identifié sur vos cotisations du dernier trimestre. Pour obtenir votre remboursement, merci de cliquer sur le lien suivant et de compléter le formulaire sécurisé : Demander le remboursement. Cordialement, Service comptable de l'Urssaf. »

Scénario : l'assistante, croyant bien faire, clique sur le lien depuis l'ordinateur du cabinet. Rien ne se passe visiblement. Elle pense à un bug… et passe à autre chose. Mais, 24 heures plus tard, l'ordinateur est complètement bloqué. Une fenêtre s'ouvre à l'écran avec un message glaçant : « Vos fichiers ont été chiffrés. Les dossiers patients, les radiographies, les devis et les historiques de soins sont désormais inaccessibles. Pour récupérer vos données, vous devez verser 1,2 bitcoin (environ 60 000 €) à l'adresse suivante : [adresse crypto]. Vous disposez de 72 heures avant suppression définitive. »

Conséquences pour le cabinet :

- Perte d'accès au dossier médical des patients.
- Interruption de l'activité pendant plusieurs jours.
- Déclaration obligatoire à la Cnil (fuite de données de santé).
- Stress intense pour l'équipe et perte de confiance des patients.
- Coûts élevés (intervention d'un prestataire, restauration système, parfois impossibilité de récupérer les données).



Exemple de fausse alerte semblant provenir d'un compte Ameli.

Une fiche synthétique pour prévenir les cybermenaces au cabinet dentaire est disponible sur le site de l'URPS en flashant le QR-Code ci-dessus

Sécurisation des réseaux et équipements

- Protéger l'accès au réseau par un mot de passe sécurisé.
- Installer un antivirus et un pare-feu sur tous les appareils.
- Restreindre l'usage des clés USB et supports amovibles non sécurisés.
- Vérifier les accès physiques aux ordinateurs et aux serveurs.
- S'assurer que les mises à jour logicielles sont effectuées automatiquement.

Sécurisation des données

- Effectuer des sauvegardes régulières et vérifier leur bon fonctionnement.
- Stocker les sauvegardes sur un support externe déconnecté du réseau (par exemple, un disque dur externe, à conserver dans un lieu sécurisé).
- Limiter l'accès aux données sensibles uniquement aux personnes autorisées.
- Crypter les fichiers sensibles pour empêcher leur exploitation en cas de vol.
- Utiliser un système de journalisation pour suivre les accès et les modifications des fichiers importants.

Séparation des usages professionnels et personnels

- Ne pas utiliser son adresse mail professionnelle pour des usages personnels, et inversement.
- Éviter d'accéder aux réseaux sociaux et d'utiliser Internet à des fins personnelles depuis les ordinateurs du cabinet.
- Ne pas installer d'applications non autorisées sur les appareils professionnels.
- Interdire l'utilisation de supports de stockage personnels (clés USB, disques durs externes) sur les ordinateurs du cabinet.

Sensibilisation et formation

La meilleure protection reste la vigilance humaine. Il est essentiel que tous les salariés, mais également les praticiens d'un même cabinet se forment régulièrement aux risques cyber et aux gestes de précaution. L'hygiène informatique est un enjeu majeur pour les cabinets dentaires. En adoptant ces bonnes pratiques, assistant(e)s dentaires et praticiens peuvent limiter considérablement les risques de cyberattaques et protéger efficacement les données sensibles de leurs patients.

Face à la multiplication des cyberattaques, chaque membre du cabinet a un rôle à jouer. Même une simple négligence peut entraîner des conséquences importantes. Une bonne gestion de la cybersécurité ne se limite pas à installer un antivirus : elle repose avant tout sur des comportements responsables et une vigilance quotidienne.