Reconnaître les menaces

> **Référentiel BTS — BC3 / C3.6** « Se prémunir et réagir face aux incidents numériques ».

> **L'essentiel :** presque toutes les attaques réussies commencent par **une action humaine** — un clic, une pièce jointe ouverte, un virement accepté. Savoir reconnaître le scénario est donc la protection la plus efficace.

Objectif

À la fin de cette page, vous savez :

- identifier les principales familles d'attaques qui visent une structure de santé ;
- repérer les signaux d'alerte d'un message frauduleux ;
- nommer ce qui, dans un cabinet d'orthoprothèse, constitue une cible.

Ce qui intéresse un attaquant dans un cabinet

- Les **données de santé** — nominatives, sensibles, impossibles à changer (contrairement à un numéro de carte bancaire). Elles se revendent et servent au chantage.
- Les **coordonnées bancaires** du cabinet et des fournisseurs.
- L'**arrêt de l'activité** lui-même : un cabinet paralysé est prêt à payer vite.
- Le cabinet comme **rebond** vers un partenaire plus gros (établissement de santé, fournisseur).

1. L'hameçonnage (phishing)

Un message imite un interlocuteur de confiance — la banque, l'Assurance Maladie, l'éditeur du logiciel, un fournisseur, la direction — pour obtenir un identifiant, un mot de passe, un paiement, ou faire ouvrir une pièce jointe.

Les signaux d'alerte :

Signal	Exemple
Urgence et menace	« Votre compte sera suspendu sous 24 h », « dernier rappel avant poursuite »
Demande d'identifiants	Un lien vers une page de connexion qui ressemble à celle que vous connaissez
Adresse d'expéditeur approximative	`ameli-remboursement.net` au lieu du domaine officiel ; nom affiché correct mais adresse réelle différente
Pièce jointe inattendue	Une « facture » d'un fournisseur avec qui vous n'avez rien en cours
Contexte qui ne colle pas	Un organisme qui vous écrit sur un canal qu'il n'utilise jamais
Français maladroit	Moins fiable qu'avant — beaucoup de messages sont désormais parfaitement rédigés

Le réflexe : ne jamais utiliser le lien du message. **Revenir au canal connu** — taper soi-même l'adresse du site, appeler le numéro habituel du fournisseur (pas celui indiqué dans le message).

Variantes : **smishing** (par SMS), **vishing** (par téléphone, souvent un « technicien informatique » très serviable), **hameçonnage ciblé** (le message mentionne votre nom, votre poste, un dossier réel — il faut supposer que l'attaquant s'est renseigné).

2. Le rançongiciel (ransomware)

Le scénario le plus redouté. Un programme chiffre l'ensemble des fichiers — dossiers patients, modèles 3D, comptabilité, sauvegardes accessibles depuis le réseau — puis réclame une rançon. De plus en plus souvent, les données sont **aussi volées** avant d'être chiffrées, avec menace de publication : c'est la **double extorsion**.

Comment il entre : pièce jointe ou lien d'hameçonnage, accès distant mal protégé, faille non corrigée sur un équipement exposé, mot de passe faible sur un compte d'administration.

Ce qui limite les dégâts : des **sauvegardes déconnectées** du réseau (voir *Sauvegardes et continuité d'activité*), des comptes à droits limités, un parc à jour, une segmentation réseau.

Faut-il payer ? Les autorités le déconseillent : payer ne garantit ni la restitution, ni l'absence de publication, finance l'activité criminelle et désigne le cabinet comme une cible qui paie. La décision

appartient au dirigeant, mais elle se prend **après** le dépôt de plainte et le signalement, pas dans la panique.

3. La fraude au virement

Pas de logiciel malveillant ici — de la manipulation. Deux formes :

- **Fraude au changement de RIB** : un « fournisseur » écrit que ses coordonnées bancaires ont changé. Le virement suivant part sur le compte de l'escroc.
- **Fraude au président** : un message qui semble venir du dirigeant demande un virement urgent et confidentiel.

La parade est organisationnelle, pas technique : tout changement de coordonnées bancaires est vérifié par **rappel téléphonique au numéro déjà connu** — jamais celui du message. Et aucun virement exceptionnel sans **double validation**.

4. Les supports amovibles et le matériel

- Une **clé USB trouvée** ou reçue en cadeau ne se branche pas sur un poste du cabinet.
- Une clé utilisée chez un fournisseur puis rebranchée au cabinet transporte ce qu'elle a croisé.
- Un **ordinateur ou un téléphone volé** non chiffré livre directement les dossiers.

5. Les risques internes et involontaires

Toutes les pertes de données ne sont pas des attaques :

- l'**erreur de destinataire** — un compte rendu envoyé au mauvais patient ;
- la **curiosité** — consulter le dossier d'une connaissance ; c'est tracé, et c'est une faute grave ;
- la **perte** d'un document papier, d'un téléphone, d'un carnet de rendez-vous ;
- la **conversation à voix haute** à l'accueil, entendue de la salle d'attente. Le secret professionnel ne s'arrête pas à l'écran.

Ces événements peuvent constituer des **violations de données** au sens du RGPD (voir *Formation métier — Données de santé & réglementation*).

À retenir

- La porte d'entrée la plus fréquente est **un humain qui clique**, pas une faille exotique.
- Face à une demande urgente : **ralentir** et **revenir au canal connu**.
- Un **changement de RIB** se vérifie toujours par téléphone au numéro déjà connu.
- Le rançongiciel se combat **avant** : sauvegardes déconnectées, mises à jour, droits limités.
- L'incident interne involontaire est aussi fréquent que l'attaque — et relève des mêmes obligations.

Revision #4
Created 2026-09-15 17:24:23 UTC by Antoine
Updated 2026-09-16 07:03:14 UTC by Antoine