



Une cyberattaque peut bloquer un ordinateur, chiffrer des fichiers, détourner une boîte mail ou exposer des données. L'objectif n'est pas de tout résoudre seul : il faut limiter la propagation, préserver les preuves et alerter rapidement.

Urgence : les 4 gestes qui comptent

À retenir : débranchez l'appareil du réseau, n'éteignez pas la machine, prévenez le support informatique ou le responsable, notez l'heure et prenez une photo de l'écran.

Dans les 15 premières minutes

1 Isoler sans éteindre

Coupez le Wi-Fi, débranchez le câble réseau ou désactivez la connexion. Ne redémarrez pas l'ordinateur : des traces utiles pourraient disparaître.

2 Alerter immédiatement

Prévenez la personne référente : direction, support informatique, prestataire, DPO ou référent RGPD. Ne gardez pas l'incident pour vous.

3 Documenter simplement

Notez l'heure, le poste concerné, l'utilisateur, les messages affichés. Prenez une photo de l'écran avec un téléphone si nécessaire.

4 Limiter les actions

Ne payez pas de rançon, ne supprimez pas les fichiers, ne lancez pas d'outil trouvé sur Internet et ne communiquez pas seul aux patients ou partenaires.

5 Sécuriser les accès

Si un compte est suspect, changez le mot de passe depuis un appareil sain et activez la double authentification si possible.

6 Préserver l'activité

Si le cabinet ou service est bloqué, basculez sur une procédure papier temporaire pour les rendez-vous, soins, appels urgents et transmissions indispensables.

Si des données personnelles ou de santé sont concernées

Réflexe RGPD

Informez le responsable et le DPO/référent RGPD. Il faut évaluer si l'incident constitue une violation de données : perte, destruction, modification, divulgation ou accès non autorisé. Si la violation présente un risque pour les personnes, une notification à la CNIL doit être réalisée dans les meilleurs délais et, si possible, sous 72 heures. Si le risque est élevé, les personnes concernées peuvent aussi devoir être informées.

Contacts à compléter avant diffusion

Support informatique / prestataire : _____ Téléphone : _____

DPO / référent RGPD : _____ E-mail : _____



La sécurité comme fondation.

Fiche gratuite fournie par Cerberis Conseil - rubrique Guides & outils

© 2026 Cerberis Conseil · Licence CC BY-NC-ND 4.0

Libre diffusion gratuite avec mention de Cerberis Conseil. Modification et reprise sur un support payant interdites.

cerberis-conseil.fr



Dans les heures qui suivent

À faire

1. Centraliser les décisions

Désignez une personne qui pilote la situation : technique, continuité d'activité, juridique/RGPD et communication.

2. Faire intervenir les bons acteurs

Contactez le support informatique, le prestataire cyber, l'assurance, le DPO et, selon la gravité, les autorités compétentes.

3. Conserver les preuves

Gardez les journaux, captures, e-mails suspects, SMS, pièces jointes et informations utiles. Elles aideront l'analyse et le dépôt de plainte.

4. Vérifier les sauvegardes

Ne restaurez pas trop vite. Il faut d'abord comprendre l'origine de l'incident pour éviter de réinfecter le système.

À faire aussi

5. Prévenir la propagation

Désactivez les comptes compromis, changez les mots de passe critiques depuis un appareil sain et contrôlez les accès à distance.

6. Gérer les données personnelles

Inscrivez l'incident dans le registre interne des violations. Analysez les risques pour les patients, salariés, partenaires ou usagers.

7. Communiquer avec prudence

Préparez un message simple, factuel et validé. Évitez les promesses techniques ou les conclusions avant l'analyse.

8. Reprendre progressivement

La reprise doit être contrôlée : postes vérifiés, comptes sécurisés, mises à jour appliquées et mots de passe renouvelés.

Les erreurs à éviter

Ce qui peut aggraver la situation

Ne pas redémarrer ou formater trop vite. Ne pas payer une rançon sans accompagnement spécialisé. Ne pas utiliser une clé USB inconnue pour transférer des fichiers. Ne pas annoncer publiquement une cause ou un niveau de gravité non vérifié. Ne pas oublier le volet RGPD si des données personnelles ou de santé sont touchées.

Préparer le cabinet ou la structure avant un incident

Sauvegardes	Prévoir des sauvegardes régulières, testées et déconnectées du réseau.
Mots de passe	Utiliser des mots de passe robustes, uniques, stockés dans un gestionnaire sécurisé.
Double authentification	Activer la MFA sur messagerie, cloud, logiciels sensibles et accès à distance.
Mises à jour	Maintenir ordinateurs, logiciels, box, antivirus et outils métiers à jour.
Procédure papier	Prévoir une continuité minimale : agenda, contacts, ordonnances, transmissions urgentes.
Exercice simple	Tester une fois par an : qui appeler, quoi couper, où sont les sauvegardes, qui communique.

Pour aller plus loin

Sources utiles : Cybermalveillance.gouv.fr - Que faire en cas de cyberattaque ; ANSSI - gestion de crise cyber ; CNIL - notification des violations de données personnelles. Cette fiche est un outil de sensibilisation et ne remplace pas une assistance technique, juridique ou RGPD individualisée.