



Comment survivre à une attaque de rançongiciel

Vos fichiers ne s'ouvrent plus, leurs noms ont changé, et un message réclame un paiement pour les débloquent. Un rançongiciel **continue de chiffrer tant que l'appareil reste connecté** : la première minute compte plus que tout le reste.



Dans les premières minutes

URGENCE

- 1 Coupez la connexion.**
Wi-Fi désactivé, câble réseau débranché. C'est le geste qui limite la propagation aux autres appareils et aux dossiers partagés.
- 2 Débranchez les supports externes.**
Disques durs, clés USB, et déconnectez les dossiers synchronisés dans le cloud : un rançongiciel chiffre aussi les sauvegardes qu'il peut atteindre.
- 3 Ne payez pas la rançon.**
Rien ne garantit la restitution des fichiers, et le paiement finance l'attaque suivante — souvent contre vous à nouveau.
- 4 Photographiez l'écran de rançon.**
Avec votre téléphone, ainsi qu'un nom de fichier chiffré. Ces éléments permettent d'identifier la souche et, parfois, de trouver un outil de déchiffrement gratuit.
- 5 Alerte les personnes concernées.**
Responsable informatique, établissement, collègues partageant le même réseau. S'il s'agit d'un poste professionnel, ne tentez rien seul.
- 6 Signalez l'incident aux autorités compétentes.**
Une attaque par rançongiciel est une infraction pénale, même quand aucune rançon n'a été versée.



- **Identifiez la souche** à partir du message et de l'extension ajoutée aux fichiers. Des déchiffreurs gratuits existent pour plusieurs familles connues — cherchez avant de renoncer à vos données.
- **Conservez une copie des fichiers chiffrés**, même sans solution immédiate : des clés de déchiffrement sont publiées régulièrement, parfois des mois après.
- **Réinstallez complètement le système** avant toute restauration. Un simple nettoyage antivirus ne garantit pas la disparition du logiciel.
- **Restaurer ensuite depuis une sauvegarde antérieure à l'infection**, en vérifiant qu'elle n'est pas elle-même chiffrée.
- **Changez tous les mots de passe enregistrés sur l'appareil**, depuis une autre machine : les rançongiciels récents volent les données avant de les chiffrer.



À ne pas faire

- ✗ Payer, même une « petite » somme, même sous la pression d'un compte à rebours affiché à l'écran.
- ✗ Rebrancher un disque de sauvegarde sur la machine encore infectée.
- ✗ Télécharger un outil de déchiffrement trouvé dans une publicité ou une vidéo : c'est fréquemment le même logiciel malveillant, une seconde fois.
- ✗ Réutiliser la machine « en attendant », pour consulter ses mails ou ses comptes.



Pour éviter que cela recommence

- **Trois copies, deux supports, une hors ligne.** Une sauvegarde débranchée est la seule qu'un rançongiciel ne peut pas atteindre — c'est ce qui transforme l'attaque en contrariété.
- **Testez la restauration** au moins une fois : une sauvegarde jamais vérifiée n'est pas une sauvegarde.
- **Mises à jour automatiques** du système et des logiciels : la plupart des infections exploitent des failles déjà corrigées.
- **Méfiance envers les pièces jointes** et les macros de documents reçus par e-mail, même d'un expéditeur connu.