



Comment survivre à un virus informatique

Un appareil infecté le montre presque toujours. **Le danger n'est pas seulement la panne** : la plupart des logiciels malveillants actuels servent à capter ce que vous tapez et à ouvrir un accès à distance. Tant que l'appareil n'est pas nettoyé, n'y saisissez plus aucun mot de passe.



Les signes qui doivent alerter

DIAGNOSTIC

- L'appareil est soudainement beaucoup plus lent.
- Des fichiers ont disparu ou ont été déplacés.
- Des messages d'erreur inhabituels apparaissent.
- L'appareil redémarre tout seul, sans raison.
- Le navigateur rame ou s'ouvre sur des pages inconnues.
- Le disque tourne en permanence, même à l'arrêt.
- Des applications que vous n'avez pas installées sont présentes.
- Le système plante à répétition.
- L'antivirus est désactivé ou refuse de se lancer.



La marche à suivre

URGENCE

- 1 Déconnectez l'appareil d'Internet.**
Cela coupe la communication du logiciel malveillant avec l'extérieur et l'empêche d'atteindre les autres appareils du réseau.
- 2 Ne saisissez plus aucun mot de passe.**
Sur cette machine, ne consultez ni vos comptes bancaires ni votre messagerie.
- 3 Démarrez en mode sans échec.**
De nombreux logiciels malveillants ne s'y chargent pas, ce qui rend leur suppression possible.
- 4 Mettez l'antivirus à jour.**
Si nécessaire depuis un autre appareil et une clé USB, puis lancez une **analyse complète**, pas une analyse rapide.
- 5 Mettez en quarantaine ou supprimez ce qui est détecté.**
Redémarrez, puis **relancez une seconde analyse** : la première passe en laisse souvent.
- 6 Changez vos mots de passe depuis un appareil sain.**
En commençant par la messagerie, une fois seulement la machine nettoyée.



- **Réinstallez complètement le système.** C'est la seule garantie réelle quand l'infection résiste ou revient après suppression.
- **Restaurez vos fichiers depuis une sauvegarde antérieure aux premiers symptômes**, et analysez-la avant de la rebrancher.
- **Vérifiez les extensions de navigateur et les programmes qui démarrent automatiquement** : c'est là que se cachent les résidus les plus courants.
- **Faites analyser les clés USB** utilisées sur l'appareil pendant la période d'infection.



À ne pas faire

- ✗ Suivre les fenêtres surgissantes qui annoncent une infection et proposent de « nettoyer » : c'est très souvent le logiciel malveillant lui-même.
- ✗ Installer un second antivirus en parallèle du premier — ils se neutralisent mutuellement.
- ✗ Continuer à utiliser l'appareil « normalement » en attendant d'avoir le temps de s'en occuper.
- ✗ Appeler le numéro d'assistance affiché par le message d'alerte.



Pour éviter que cela recommence

PRÉVENTION

- **Un antivirus actif et à jour**, avec l'analyse en temps réel maintenue allumée.
- **Les mises à jour automatiques** du système, du navigateur et des applications.
- **Des téléchargements depuis les sources officielles uniquement** : les versions « gratuites » de logiciels payants sont le premier vecteur d'infection.
- **Une sauvegarde régulière**, pour que la réinstallation ne signifie jamais la perte de vos fichiers.