

Protéger son PC

des virus et logiciels malveillants

Les virus d'aujourd'hui ne ressemblent plus à ceux d'avant. Ils volent vos mots de passe, chiffrent vos fichiers contre rançon, espionnent votre webcam — sans que vous voyiez quoi que ce soit. Voici comment vous en protéger efficacement.

01 Avoir un antivirus à jour

Un antivirus qui n'est pas mis à jour ne reconnaît pas les nouvelles menaces — il est aussi utile qu'un cadenas rouillé. Les virus évoluent chaque jour ; votre protection doit faire de même.

Sur Windows 10 et 11 :

Windows Defender (intégré à Windows) est suffisant pour la grande majorité des utilisateurs. Vérifiez qu'il est actif : **Démarrer > Sécurité Windows > Protection contre les virus**. Le bouton doit être vert. S'il ne l'est pas, cliquez sur **Activer**.

Sur Mac :

macOS intègre des protections natives (Gatekeeper, XProtect) qui se mettent à jour automatiquement. Elles sont efficaces si votre Mac est à jour. Pour une protection renforcée, **Malwarebytes** (version gratuite) est une bonne option complémentaire.

Bon à savoir : Évitez d'installer plusieurs antivirus en même temps — ils se bloquent mutuellement et ralentissent votre PC sans vous protéger mieux.

02 Ne jamais télécharger depuis un site inconnu

La majorité des infections viennent de logiciels téléchargés sur des sites douteux : faux lecteurs vidéo, générateurs de clés, versions 'gratuites' de logiciels payants. Le fichier fonctionne, mais il installe un virus en même temps.

Les sources sûres :

Téléchargez toujours depuis le **site officiel** de l'éditeur (Adobe, VLC, 7-Zip...) ou depuis le **Microsoft Store / Mac App Store**. Si un site vous propose un logiciel payant gratuitement, c'est un piège.

Les signaux d'alarme :

Un site qui affiche plusieurs boutons **Télécharger** (seul un est le bon). Une extension de fichier inattendue (.exe déguisé en PDF ou en image). Votre navigateur qui affiche un avertissement de sécurité sur le site.

Attention : Ne désactivez jamais votre antivirus pour installer un logiciel, même si le site vous le demande. C'est systématiquement un signe d'infection.

03 Faire les mises à jour Windows et Mac

Les mises à jour ne servent pas qu'à ajouter des fonctions : elles bouchent des failles de sécurité connues et exploitées activement par des pirates. Un PC non mis à jour est une cible facile.

Sur Windows :

Démarrer > Paramètres > Windows Update > Rechercher des mises à jour. Installez tout ce qui est disponible et redémarrez quand le système le demande. Activez les mises à jour automatiques pour ne plus y penser.

Sur Mac :

Pomme > Réglages système > Général > Mise à jour de logiciels. Cochez "**Maintenir mon Mac à jour automatiquement**".

Bon à savoir : Ne reportez pas les mises à jour indéfiniment. Une semaine de retard peut suffire pour qu'un pirate exploite une faille déjà connue et corrigée.

Votre PC se comporte bizarrement ou vous avez un doute ?

On diagnostique et nettoie votre ordinateur à distance ou à domicile.

Appelez-nous : 09.81.65.35.09