

Comment savoir si votre téléphone contient des logiciels malveillants

Votre téléphone a-t-il agi ?

Voici comment vérifier si les logiciels malveillants sont à blâmer et ce qu'il faut faire si c'est le cas.

Jason Cohen :



Votre smartphone est comme un mini-ordinateur qui tient dans votre poche, donc, tout comme votre ordinateur portable, il est également [vulnérable aux logiciels malveillants](#), qui peuvent prendre la forme de [logiciels espions](#), publicitaires ou [rançongiciels](#).

Malheureusement, il peut parfois être difficile de déterminer si votre appareil a été infecté. C'est voulu, car ceux qui sont derrière le malware ne veulent pas que vous trouviez leur logiciel et que vous le supprimiez, c'est donc à vous de rechercher des signes d'activité troublante.

iOS vs Android: quel système d'exploitation est le plus vulnérable?



(Crédit : Apple/Samsung)

Android est un écosystème ouvert par conception, ce qui a ses avantages, mais rend également le système d'exploitation plus vulnérable aux applications malveillantes que l'iOS d'Apple.

Google a fait des progrès dans ce domaine; un [rapport de 2021](#) a noté que les mauvais acteurs ont dû faire preuve de plus de créativité pour obtenir leurs applications chargées de logiciels malveillants sur les appareils Android.

Malheureusement, ce même rapport a révélé que les applications compte-gouttes du cheval de Troie ont encore enregistré plus de 300 000 téléchargements sur Google Play en seulement quatre mois cette année-là afin de récupérer les coordonnées bancaires des gens.

Si vous avez un iPhone, vous pensez peut-être que rien de tout cela ne s'applique à vous. Après tout, l'idée que les Mac n'attrapent pas de virus s'étend certainement à tous les autres appareils Apple, non?

Erreur.

Il est [vrai](#) que les iPhones sont moins susceptibles d'être infectés par des logiciels malveillants que les téléphones Android grâce au processus d'approbation rigoureux d'Apple, mais cela ne signifie pas qu'ils sont immunisés contre l'infection.

Rien qu'en 2023, des [logiciels espions ont été découverts](#) sur des iPhones appartenant à des employés de Kaspersky, et une entreprise israélienne a été découverte pour [infecter des téléphones](#) via le calendrier iCloud d'Apple.

Quel que soit le [système d'exploitation mobile](#) que vous utilisez, il est important de rester vigilant.

Vous ne savez jamais quand une application apparemment inoffensive contient une charge utile infâme.

Signes que votre téléphone peut être infecté



(Crédit : Apple)

Alors, comment pouvez-vous réellement savoir si votre téléphone a été infecté par des logiciels malveillants? Ce n'est pas toujours évident, mais voici quelques points à surveiller :

1. Publicités pop-up qui ne disparaîtront pas

Si vous voyez soudainement beaucoup de publicités dans une application spécifique, ou même lorsqu'aucune application n'est ouverte, vous pouvez être infecté par un logiciel publicitaire. Ces pop-ups ennuyeux peuvent générer de l'argent à partir de clics publicitaires, essayer de vous infecter avec des logiciels malveillants pires ou créer un lien vers des offres frauduleuses.

Bitdefender a récemment découvert [que 60 000 applications Android](#) sur le Google Play Store étaient chargées de logiciels publicitaires, c'est donc un problème assez courant. Quoi que vous fassiez, ne cliquez pas!

2. Frais inexplicables sur votre facture

Jetez un coup d'œil à votre facture de téléphone ou à vos relevés de carte de crédit et assurez-vous de pouvoir comptabiliser chaque charge.

Sinon, il est possible que vous soyez victime d'une escroquerie qui ajoute des services indésirables à votre téléphone et des frais à votre facture de téléphone, également connue sous le nom de [bachotage](#).

Les fournisseurs de services sans fil ont été accusés de [détourner le](#) regard dans certains cas afin d'empocher un pourcentage du tarif mensuel, de sorte qu'il vous incombe d'être diligent et d'attraper les faux frais.

3. Votre batterie se décharge plus rapidement que prévu

Bien que les batteries [se dégradent naturellement avec le temps](#), vous ne devriez pas voir un changement soudain dans la durée de vie de la batterie avec une usure normale.

Les logiciels malveillants peuvent détourner les composants de votre téléphone afin d'effectuer des tâches en arrière-plan, ou même lire [secrètement des vidéos](#), ce qui entraîne une recharge de la batterie plus rapide que prévu.

4. Votre téléphone surchauffe

Dans des circonstances normales, votre téléphone ne devrait jamais être chaud au toucher, mais certains logiciels malveillants peuvent surcharger le processeur interne ou le mécanisme de charge.

Par exemple, le malware Loapi est capable de surchauffer – et [même de faire fondre](#) – votre téléphone.

Si votre téléphone [surchauffe](#), nous vous recommandons de le débrancher de toute source d'alimentation et de l'éteindre. Laissé sans surveillance, un téléphone chaud peut provoquer des incendies et même [exploser](#).

5. Votre téléphone est plus lent que la normale

Tout comme un ordinateur, votre smartphone contient un processeur qui est utilisé pour effectuer certaines tâches de calcul.

Si votre appareil a été piraté, le logiciel malveillant peut surcharger les composants de votre téléphone et entraîner des tâches simples plus longues qu'elles ne le devraient.

Au fil des ans, nous avons vu des [vidéos de farces](#), des [caractères](#) indiens, des [vulnérabilités logicielles](#), des fonds d'écran et [des chaînes de texte](#) planter les téléphones, mais si le vôtre souffre d'un ralentissement soudain, voire d'un plantage, les logiciels malveillants pourraient en être la raison.

6. Appels interrompus et mauvaises connexions

Si votre téléphone a été infecté par un logiciel malveillant, une connexion sortante à un serveur étranger peut interférer avec la capacité de votre téléphone à maintenir une connexion Wi-Fi ou cellulaire stable, ce qui entraîne une mauvaise qualité de connexion et des appels interrompus fréquents.

Si d'autres appareils sur la même connexion Wi-Fi fonctionnent correctement et que les membres de votre foyer ne subissent pas d'appels interrompus, les logiciels malveillants peuvent être le coupable de votre téléphone.

(Une mauvaise qualité d'appel et des sons invasifs peuvent également être un signe que [votre téléphone a été mis sur écoute](#), ce qui est un problème distinct.)

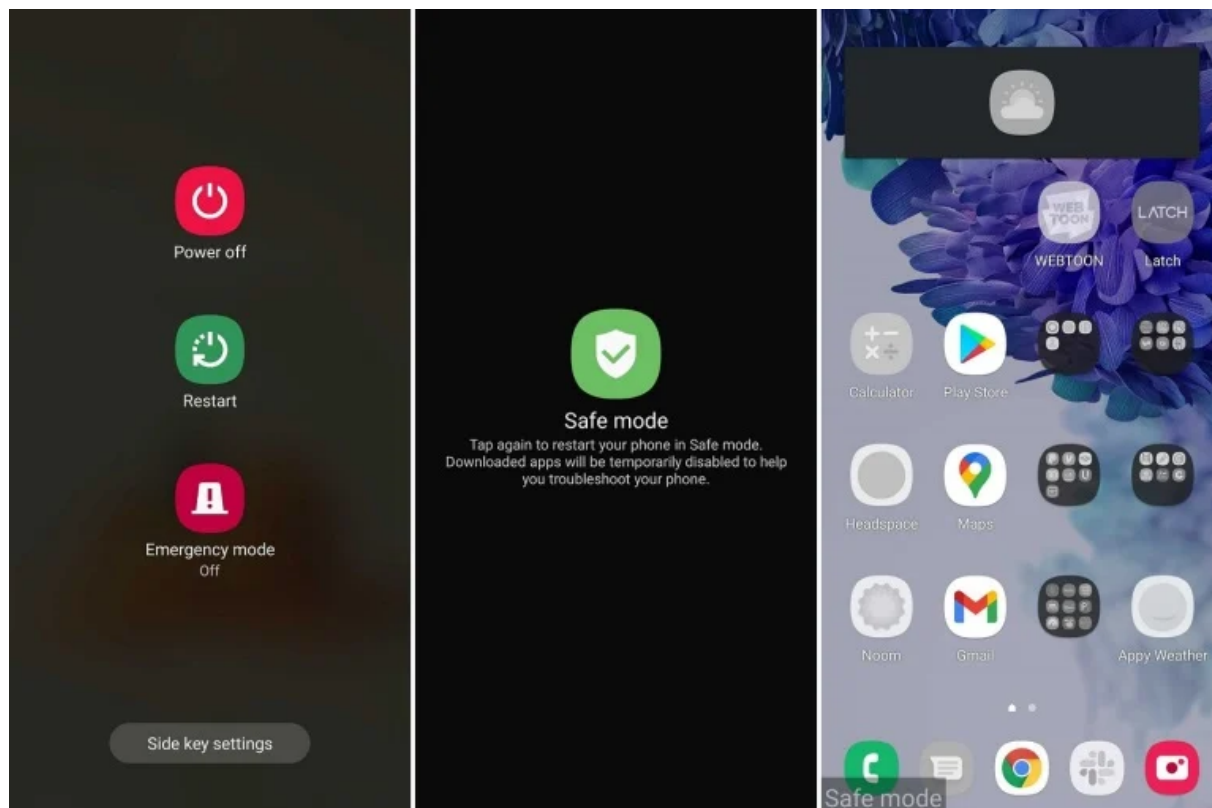
7. Une application inattendue apparaît

Parfois, une application que vous téléchargez peut être chargée avec des logiciels malveillants qui installent des programmes supplémentaires.

Jetez un coup d'œil à votre liste d'applications et assurez-vous de reconnaître et de vouloir tout sur le téléphone.

Si vous trouvez quelque chose d'inattendu, n'ouvrez pas l'application.

Comment supprimer les logiciels malveillants de votre téléphone



(Crédit : Google)

Vous avez examiné votre téléphone et trouvé quelque chose de suspect, ou vous présentez un ou plusieurs symptômes de logiciels malveillants.

Quoi encore?

Voici quelques mesures que vous pouvez prendre :

Recommandé par nos rédacteurs

1. Entrez en mode sans échec sur Android

Si vous utilisez un [téléphone Android](#), essayez le mode sans échec.

Le processus peut varier en fonction du fabricant de votre téléphone, mais la plupart des nouveaux appareils nécessitent que vous mainteniez le bouton d'alimentation enfoncé, puis appuyez longuement sur Éteindre jusqu'à ce que vous ayez la possibilité de passer en mode sans échec.

Semblable au [mode sans échec dans Windows](#), cela désactive les applications tierces sur votre téléphone afin que vous puissiez inspecter en toute sécurité tout ce qui sort de l'ordinaire.

Vous pouvez ensuite supprimer toutes les applications que vous pensez être infectées, puis revenir au mode normal pour voir si le problème a été résolu.

Pour ce faire sur un iPhone, votre téléphone doit être jailbreaké, ce ne sera donc pas une solution viable pour la plupart des utilisateurs. Cependant, Apple dispose d'une fonctionnalité appelée [Mode de verrouillage](#), qui limite les fonctionnalités de l'appareil si vous êtes ciblé par des logiciels malveillants ou des pirates.

2. Recherche de virus

Si vous ne trouvez rien par vous-même, il est temps de faire appel à un bon antivirus, surtout si vous utilisez un appareil Android.

Mais [ne téléchargez pas d'application](#) gratuite avec « antivirus » dans sa description. Beaucoup ne fonctionnent pas ou sont secrètement des logiciels malveillants eux-mêmes. Optez pour un nom de confiance dans le domaine de la sécurité, tel que Bitdefender, Kaspersky, Norton et McAfee, qui ont tous leurs propres [applications antivirus](#).

Nous vous recommandons d'investir dans l'un d'entre eux, de rechercher les virus et de permettre au programme d'identifier et de supprimer tout logiciel malveillant détecté.

3. Réinitialisez votre appareil

Si aucune autre solution ne peut être trouvée pour libérer votre appareil des logiciels malveillants, votre seul choix peut être de lancer une [réinitialisation d'usine](#) et de recommencer à zéro.

Cela effacera votre téléphone et, espérons-le, supprimera tout logiciel malveillant dans le processus.

Si vous avez une sauvegarde de votre téléphone d'avant qu'il ne soit mis sur le fritz (et vous devriez), vous pouvez essayer de restaurer à partir de ce point.

Sur un iPhone, accédez à **Paramètres > Général > Réinitialiser** et effacez l'appareil.

Si vous avez une sauvegarde iCloud viable, vous pouvez suivre [nos instructions](#).

Les propriétaires d'Android peuvent avoir besoin de trouver des instructions spécifiques au fabricant de leur téléphone.

Pour un appareil Samsung, ouvrez **Paramètres > Gestion générale > Réinitialiser > Réinitialisation des données d'usine** pour faire le travail.

Vous pouvez restaurer à partir d'une sauvegarde sur Google Drive si vous suivez [ces instructions](#).

Comment éviter les logiciels malveillants



(Photo : Jaiz Anuar / Shutterstock)

Les logiciels malveillants ne sont pas une blague.

Évitez d'être victime d'une attaque en faisant attention à ce que vous téléchargez et en prêtant attention aux autorisations que vous accordez à vos applications.

Par exemple, avant de télécharger quoi que ce soit, lisez attentivement les critiques de l'application pour vous assurer que les gens obtiennent ce qui est annoncé, mais soyez à l'affût des notes suspectes et des critiques répétitives sur les applications sans nom.

Il pourrait s'agir d'une situation payante.

Si une application que vous installez vous présente une offre à laquelle vous ne vous attendiez peut-être pas ou vous demande des informations personnelles, réfléchissez-y à deux fois avant de la remettre.

En règle générale, vous ne devez accorder l'accès qu'aux fonctionnalités dont vous pensez que l'application aura besoin.

S'il s'agit d'une application de messagerie, par exemple, et que vous demandez de passer des appels téléphoniques ou d'accéder à votre appareil photo, cela pourrait être un mauvais signe.

Les utilisateurs d'Android et d'iPhone peuvent accéder à un gestionnaire d'autorisations sous leurs paramètres de confidentialité respectifs.

Recherche et mise en page:

Michel Cloutier

CIVBDL

20230815

"C'est ensemble qu'on avance"