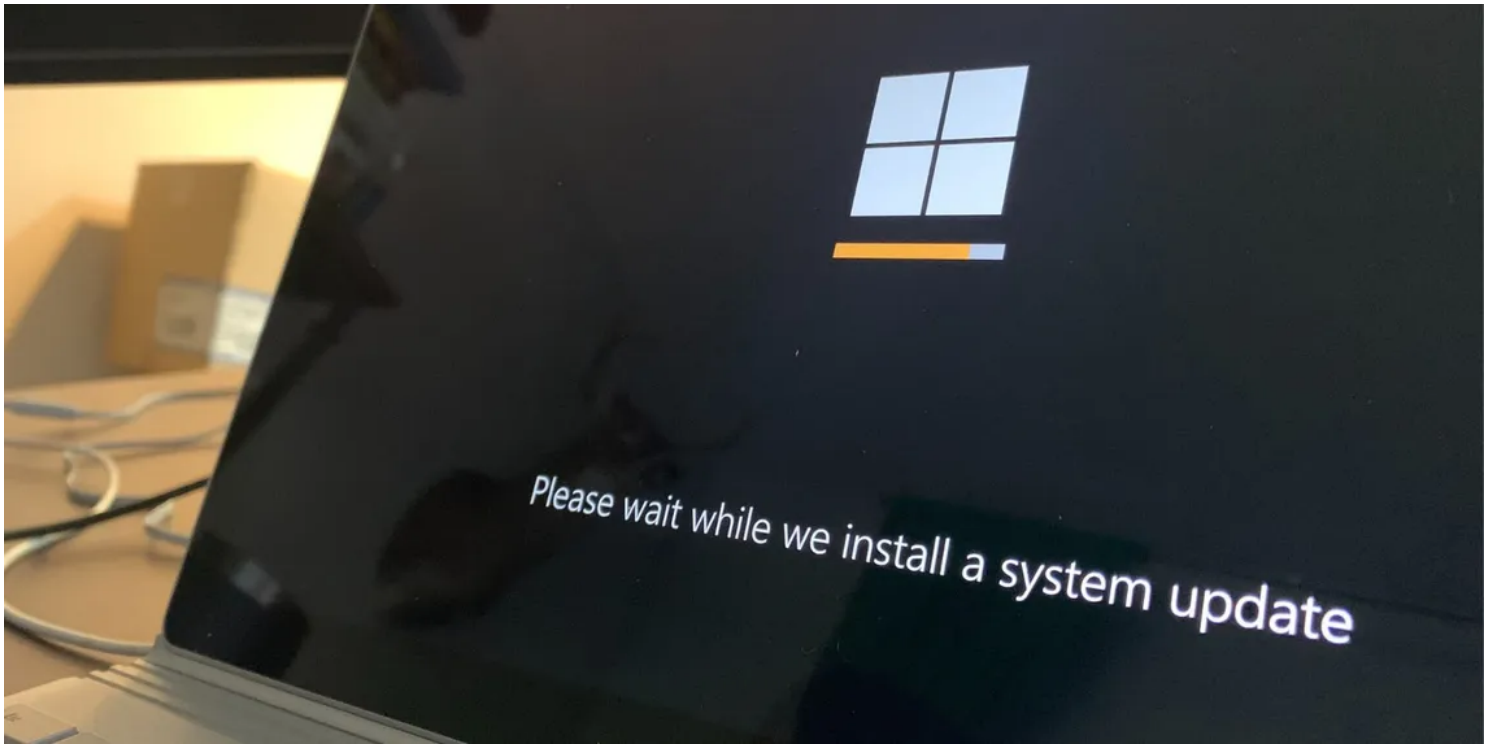
www.makeuseof.com /why-software-updates-help-keep-you-safe/

Voici pourquoi les mises à jour logicielles vous aident à rester en sécurité

Garder votre système d'exploitation et vos applications à jour peut être ennuyeux, mais cela est essentiel pour votre sécurité.

Katie Rees :



Lorsque vous recevez une notification de mise à jour logicielle, il est naturel de la reporter. Après tout, les mises à jour peuvent prendre beaucoup de temps et vous laisser souvent sans accès à votre appareil pendant le processus.
Mais si vous tenez à votre sécurité, vous devriez envisager de mettre à jour le logiciel de votre appareil.
Alors, que font réellement les mises à jour logicielles?
Pourquoi sont-ils importants pour votre sécurité ?

Que font les mises à jour logicielles ?

De nouvelles applications, protocoles et fonctionnalités sont développés chaque jour, de sorte que votre logiciel ne peut pas rester le même pour toujours.
Si vous ne mettez jamais à jour le logiciel de votre appareil, il est probable que vous rencontrerez des problèmes sur toute la ligne.

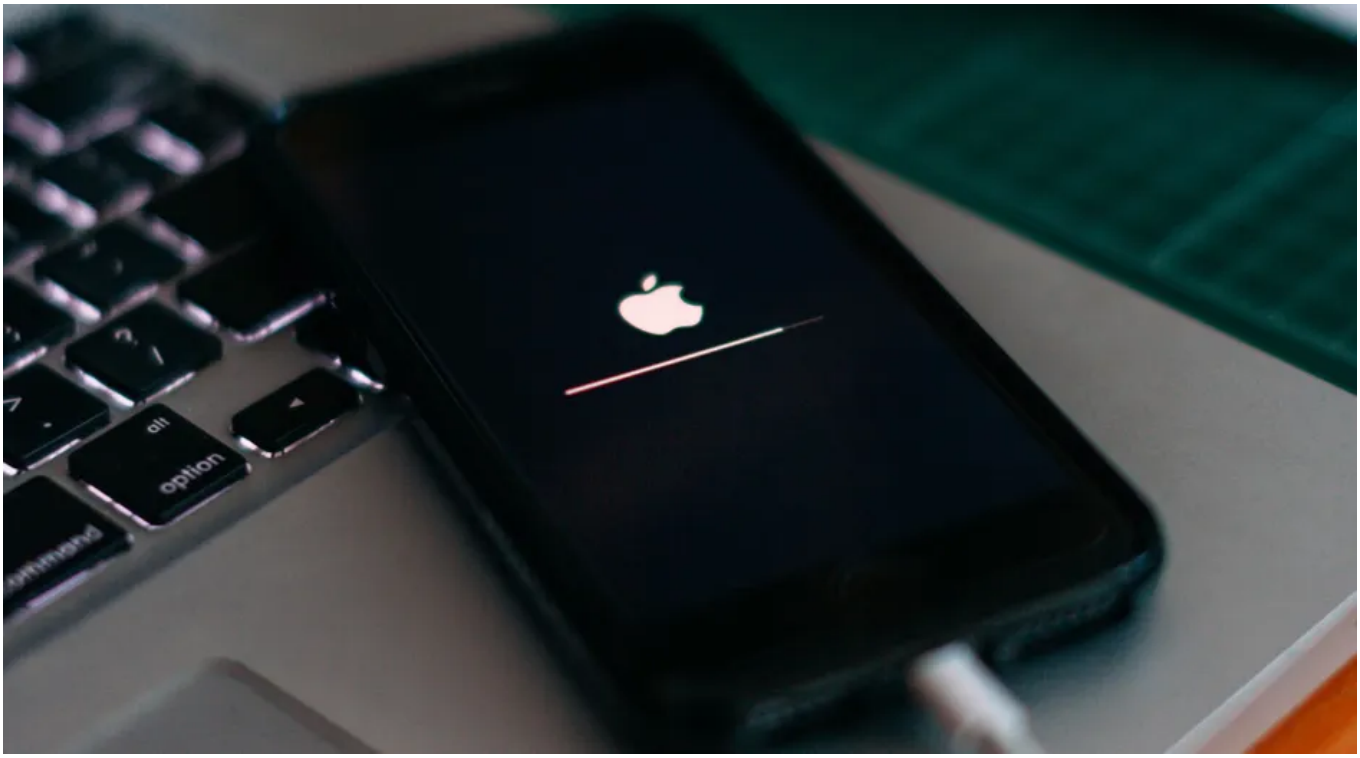
Une mise à jour logicielle peut être très transformatrice ou mineure, selon ce que les développeurs ont publié.
Une mise à jour peut contenir un simple correctif ou deux, mais peut également modifier sensiblement l'interface et les capacités de votre appareil.

Toutes les mises à jour logicielles ne sont pas identiques, mais elles apportent souvent un ou plusieurs des éléments suivants :

- Correctifs de bogues et de vulnérabilités.
- Nouvelles fonctionnalités.
- Amélioration de la vitesse et de l'efficacité.
- Compatibilité des applications.

Le premier de cette liste est ce sur quoi nous allons nous concentrer ici, car ce sont les correctifs de bogues et de vulnérabilité qui peuvent améliorer la sécurité globale de votre appareil.

Comment les mises à jour logicielles vous protègent



De nombreux logiciels sont longs et complexes, y compris les jeux, les médias sociaux et les applications de divertissement.

Selon Softonic, le nombre de lignes de code dans les programmes populaires est le suivant:

- **iOS :** 12 millions de lignes.
- **Android :** 12 millions de lignes.
- **Windows 10 : 80** millions de lignes.
- **Facebook :** 62 millions de lignes.
- **Instagram :** un million de lignes.
- **Adobe Photoshop :** 10 millions de lignes.
- **Minecraft :** 500 000 lignes.

De toute évidence, il y a beaucoup de travail à faire pour développer un logiciel.
Et, dans ces milliers ou millions de lignes de code, il est normal qu'il y ait quelques erreurs.

Si ces erreurs causent d'énormes problèmes, comme des plantages immédiats, des problèmes d'interface ou un autre défaut notable, elles sont souvent corrigées avant la sortie du programme.
Mais certaines failles de code sont plus discrètes et mineures, ce qui les rend plus difficiles à remarquer pour les développeurs.

C'est ce qui fait que les programmes publiés ont des bogues et des vulnérabilités.
Un bogue peut être totalement inoffensif dans la nature, alors qu'une vulnérabilité est quelque chose qui peut être exploité.

Par exemple, un bogue dans l'application Instagram peut vous empêcher d'aimer les publications, ce qui est frustrant, mais pas dangereux.
D'autre part, une vulnérabilité dans l'application Instagram peut vous empêcher de bloquer un utilisateur, de rendre votre profil privé ou d'utiliser l'authentification à deux facteurs.
C'est ici que les choses deviennent risquées.

Les cybercriminels recherchent souvent les vulnérabilités logicielles lorsqu'ils tentent d'attaquer un programme.
Certaines vulnérabilités ne sont pas très utiles, tandis que d'autres peuvent donner à un attaquant l'accès à des pans entiers d'informations privées.

Certaines vulnérabilités logicielles ont causé d'énormes problèmes dans le passé, comme la faille Log4Shell.
Log4Shell est une vulnérabilité de code basée sur Java qui permet l'exécution de code à distance dans Apache Log4j 2, un utilitaire de journalisation.

L'exécution de code à distance permet à un attaquant de déployer des logiciels malveillants sur un appareil à distance, ce qui rend les piratages beaucoup plus faciles.

Certains grands programmes, y compris Minecraft, utilisent cet utilitaire, les serveurs et les clients devenant vulnérables aux attaques.
Les utilisateurs de Minecraft ont été invités à mettre à jour leur logiciel pour corriger cette vulnérabilité, un correctif dont nous discuterons bientôt.

Les vulnérabilités seront remarquées par les créateurs d'un programme, l'équipe de maintenance ou par les utilisateurs moyens.
Les logiciels open source peuvent être approuvés par n'importe qui, ce qui facilite la détection des problèmes.
Les programmes à code source fermé, d'autre part, peuvent s'appuyer sur des failles visibles qui causent des problèmes notables pour les utilisateurs de repérer un problème, car leur code ne peut pas être approuvé publiquement.

Une fois que l'équipe logicielle est informée d'une vulnérabilité, elle s'efforce généralement de la corriger rapidement.
Lorsqu'une vulnérabilité est corrigée, la faille de codage est corrigée et ne peut donc plus être exploitée.

Pourquoi les mises à jour sont importantes

Les correctifs vont de pair avec les mises à jour logicielles et peuvent faire la différence entre éviter et être victime d'un exploit.
Si vous avez été informé qu'une de vos applications présente une vulnérabilité et qu'un correctif est disponible dans une mise à jour, il est préférable de lancer cette mise à jour dès que possible.

Même s'il n'y a pas de vulnérabilité connue dans votre version actuelle du logiciel, les mises à jour logicielles peuvent éliminer les bogues, améliorer la compatibilité de votre appareil avec d'autres programmes et même vous donner accès à de nouvelles fonctionnalités.

Les inconvénients des mises à jour logicielles

Les mises à jour logicielles peuvent offrir de nombreux avantages, mais il est important de discuter des inconvénients possibles que vous pouvez rencontrer lorsque vous actualisez vos applications et votre système d'exploitation.

Tout d'abord, les mises à jour logicielles peuvent apporter d'autres bogues ou vulnérabilités.
C'est un peu un catch-22, non?
Les mises à jour peuvent corriger des failles préexistantes, mais courent le risque d'apporter de nouveaux problèmes dans le code mis à jour.

Prenez les mises à jour iOS, par exemple.
De nombreux utilisateurs d'iPhone ont évité la mise à jour iOS 15 en 2021, car de nombreux problèmes ont été signalés.
Des problèmes de vidange de la batterie, de Wi-Fi et Bluetooth et de TouchID ont tous été signalés par les utilisateurs qui ont installé la mise à jour iOS 15.

iOS 16 est également venu avec quelques déceptions, y compris le décalage de l'interface utilisateur, le redémarrage spontané et les problèmes avec Safari.

Le cas est souvent similaire avec les mises à jour du système d'exploitation Android. Android 13 a apporté d'excellentes fonctionnalités, mais les utilisateurs ont également signalé des performances moins bonnes, des plantages du système et des fonctionnalités de personnalisation limitées lors de l'installation de la mise à jour.
La précédente mise à jour Android 12 était livrée avec son propre ensemble de problèmes, notamment une décharge de batterie inactive, des difficultés à répondre aux appels et des gels de médias.

Ces problèmes ne rendent pas les nouvelles versions du système d'exploitation intrinsèquement mauvaises, mais il convient de noter que les mises à jour sont rarement parfaites.
Il y a des avantages et des inconvénients qui accompagnent presque toutes les mises à jour, mais il est toujours préférable de garder votre logiciel à jour pour éviter d'être victime d'exploits inattendus.

Devriez-vous mettre à jour votre appareil

Assurément, oui.

Vous ne devriez pas reporter les mises à jour logicielles pour éviter le risque d'autres défauts.

Toutefois, si une nouvelle mise à jour sort et que votre appareil demande à la télécharger, lancez une recherche rapide dans le navigateur pour voir comment les autres utilisateurs la trouvent après l'installation.
Si vous voyez qu'il y a beaucoup plus d'inconvénients que d'avantages, vous voudrez peut-être attendre que les développeurs publient une version modifiée.

Les mises à jour logicielles sont là pour une raison

Bien que vous puissiez être tenté d'ignorer les mises à jour logicielles pour gagner du temps, cela peut exposer votre système d'exploitation et vos applications à des exploits de sécurité.
Pour éviter d'être la cible de cyberattaques via des vulnérabilités, il vaut la peine de mettre à jour votre logiciel assez régulièrement.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230731
"C'est ensemble qu'on avance"