SYNDESIN
ACCOMPAGNEMENT NUMERIQUE

Mes fiches mémos

INTRODUCTION

Vous est-il déjà arrivé de décliner les mises à jour suggérées par vos applications ? De repousser les correctifs proposés par vos logiciels ? Pensez-vous à vérifier régulièrement si une nouvelle mise à jour n'est pas disponible pour votre ordinateur ou votre téléphone ?

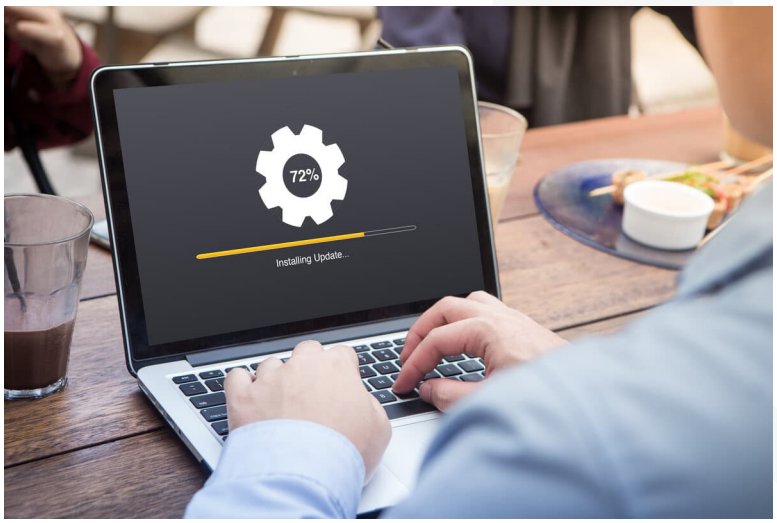
Les mises à jour sont souvent perçues comme une contrainte, pourtant elles sont essentielles pour garantir votre sécurité informatique. Découvrez à quoi elles servent et comment procéder pour rester protégé au quotidien.

Proposées par les éditeurs et les fabricants afin de corriger des failles de sécurité, les mises à jour informatiques sont pourtant souvent négligées par les utilisateurs : des demandes qui ne tombent pas toujours au bon moment – au travail, pendant un film… – ou qui paraissent trop contraignantes car elles nécessitent par exemple de redémarrer votre appareil. Il est ainsi tentant de les repousser au lendemain, voire davantage, puis de les oublier définitivement. C'est une erreur, car les mises à jour sont essentielles pour garantir la sécurité de vos appareils et de vos logiciels. En les repoussant, vous vous exposez inévitablement à des risques pour votre sécurité informatique.

Pour qu'effectuer vos mises à jour d'appareils numériques, d'applications ou de logiciels deviennent un réflexe de votre vie quotidienne, il est important de comprendre **pourquoi elles sont essentielles** et **comment bien les réaliser**, aussi bien dans votre usage personnel que professionnel :

- Dans le cadre privé, c'est à vous de régulièrement mettre à jour vos appareils, logiciels et applications.
- En entreprise, le service informatique se charge généralement des mises à jour des outils professionnels. Toutefois, lorsque ce n'est pas le cas, c'est aux collaborateurs de s'en charger, sous la responsabilité du chef d'entreprise.

https://www.dailymotion.com/video/x7n127n



LES MISES A JOUR SONT IMPORTANTES POUR CORRIGER D'EVENTUELLES FAILLES DE SECURITE

Qu'est-ce qu'une mise à jour ? Il en existe deux types :

- La mise à jour **importante** ou **critique**
- La mise à jour de **version**

La **mise à jour importante ou critique** est la publication d'une version corrigée d'un logiciel ou du système d'exploitation d'un appareil. Elle vous protège des failles de sécurité identifiées dans la version précédente.

La **mise à jour de version** est la publication d'une version plus avancée d'un logiciel ou du système d'exploitation d'un équipement. Elle vous permet de corriger des failles de sécurité mais aussi d'installer de nouvelles fonctionnalités, de corriger des bugs, de simplifier l'expérience utilisateur, etc. Parfois, ces mises à jour de version sont payantes.

Les mises à jour sont essentielles car l'ensemble de vos outils informatiques sont exposés à des risques :

- Les appareils informatiques comme les ordinateurs, les smartphones, les tablettes ou les objets connectés
- Les logiciels
- Les applications web et mobiles

Les principaux risques de cyberattaques sont le vol de données personnelles, la fraude bancaire, le piratage de compte en ligne et l'usurpation d'identité.

À mesure que le système d'exploitation d'un appareil ou qu'un logiciel vieillit, les cybercriminels sont de plus en plus susceptibles d'y identifier **une faille de sécurité**.

Une faille de sécurité est une brèche par laquelle il devient possible d'accéder à votre appareil ou à votre logiciel et d'en prendre le contrôle afin de s'y introduire pour soutirer des données personnelles.

C'est pourquoi les éditeurs et les fabricants proposent des mises à jour dès qu'une nouvelle faille est détectée. Ainsi, vous êtes régulièrement notifié de nouvelles versions à installer pour :

- Le système d'exploitation de vos appareils : mises à jour de Windows, d'iOS, d'Android, de Linux…
- Le logiciel interne de vos objets connectés : mise à jour du logiciel interne de votre assistant vocal, de votre montre connectée, de votre imprimante, etc.
- Chacun de vos logiciels, applications web et applications mobiles

Il est conseillé d'installer les mises à jour immédiatement, même si la tâche peut parfois apparaître comme chronophage ou fastidieuse. Remettre ces mesures de sécurité à plus tard, c'est prendre le risque de laisser le temps aux cybercriminels de profiter des failles de sécurité de vos versions actuelles. En effet, dans les jours qui suivent la publication d'une mise à jour de sécurité il est généralement constaté une augmentation significative des attaques visant à exploiter les failles de sécurité corrigées.

Par ailleurs, il n'est en général pas suffisant d'installer les mises à jour d'une partie seulement de votre équipement informatique. En effet, de nombreux appareils et logiciels sont connectés entre eux : il suffit parfois d'une faille de sécurité dans l'un d'eux pour qu'un pirate ait accès à l'ensemble de vos équipements.

https://www.dailymotion.com/video/x7txg0d

LES 5 BONNES PRATIQUES POUR INSTALLER LES MISES A JOUR EN TOUTE SECURITE

Pour que l'installation de vos mises à jour devienne moins contraignante et que vous soyez assuré d'être bien protégé, nous vous conseillons d'adopter les bonnes pratiques suivantes :

Télécharger les mises à jour depuis les sites officiels

L'objectif d'une mise à jour est d'améliorer la sécurité de votre appareil ou logiciel.

Attention cependant : **il existe de fausses mises à jour** et celles-ci ne sont pas sans danger. Ce sont des pièges pour vous faire télécharger un programme infecté par un virus *(malware)* ou même un rançongiciel *(ransomware).*

La seule façon de vous assurer **de l'authenticité d'une mise à jour** est de la télécharger depuis **le site officiel du fabricant ou de l'éditeur**.

De même, prenez garde **aux fausses notifications de mises à jour**. Lorsque vous naviguez sur Internet, des alertes apparaissent parfois sous forme de notifications ou de fenêtres *pop-up*. Elles vous invitent à installer une mise à jour, en insistant souvent sur le caractère urgent de l'action.

Ne cliquez pas sur ces alertes. Rendez-vous directement sur le site officiel pour vérifier la véracité de l'information.

Activer les mises à jour automatiques

Lorsque cela est possible, activez les mises à jour automatiques.

De cette façon, le téléchargement et l'installation d'une nouvelle version se font automatiquement, dès la publication de la mise à jour et dès que votre appareil se trouve dans les conditions requises : connexion au WI-FI, batterie suffisante…

Par exemple, lorsque vous activez la mise à jour automatique de vos applications mobiles, celles-ci se lancent dès que votre smartphone ou votre tablette est connectée au Wi-Fi. Cette astuce vous permet d'effectuer vos mises à jour sans avoir à intervenir ni même y penser.

Malheureusement, cette fonctionnalité n'est pas disponible avec l'ensemble des systèmes d'exploitation, des logiciels ou des applications. Or, l'installation manuelle d'une mise à jour demande du temps et mobilise souvent l'appareil, vous obligeant à interrompre votre activité informatique l'espace d'un instant.

Lorsque la notification d'une nouvelle mise à jour arrive au mauvais moment, nous vous recommandons de prendre un instant pour **planifier la mise à jour sur une période d'inactivité de l'appareil** : la nuit, durant une pause-déjeuner, pendant une réunion…

Vérifier la fréquence des mises à jour d'un nouvel appareil ou d'un nouveau logiciel

Avant de faire l'acquisition d'un nouvel appareil ou d'un nouveau logiciel, vérifiez que l'éditeur ou le fabricant propose des mises à jour de façon régulière.

N'achetez pas un logiciel ou un équipement qui n'est plus mis à jour. Cela signifie que le fournisseur ne s'assure plus de la sécurité informatique du produit. Les failles de sécurité ne sont plus corrigées et le programme deviendra rapidement obsolète.

Vous venez d'acheter un appareil ou un logiciel ?

Avant de l'utiliser, veillez à **installer l'ensemble des mises à jour disponibles**.

Systématiser la mise à jour des logiciels et des appareils

Pour garantir votre sécurité informatique sur le long terme, vous devez veiller à effectuer vos mises à jour de façon régulière.

Pour cela, rien ne vaut la mise en place d'un système organisé. Avec de l'organisation et de la planification, vous créerez une routine efficace et pérenne :

1. **Identifiez tous les logiciels et appareils utilisés**. À cette fin, nous vous recommandons d'utiliser une application d'inventaire – application proposée par votre fournisseur d'accès à internet (FAI) pour lister l'ensemble des appareils connectés au réseau.
2. **Activez la mise à jour automatique et les notifications** de mise à jour pour tous les outils qui disposent de cette option.
3. **Faites une sauvegarde de vos données** avant une mise à jour importante et testez les mises à jour. Parfois, elles peuvent provoquer des erreurs ou des incompatibilités entre les logiciels. Si cela se produit, faites marche arrière grâce à votre sauvegarde et attendez que la mise à jour soit corrigée par l'éditeur.
4. **Surveillez la régularité des publications de mises à jour** de la part des éditeurs. Si un programme n'est plus mis à jour, il sera rapidement obsolète. Il est alors temps de chercher un logiciel alternatif plus sécurisé ou de protéger ce logiciel autrement (voir l'étape suivante). Planifiez régulièrement cette session de vérification.
5. **Déterminez comment protéger les logiciels et les appareils qui ne peuvent pas ou plus être mis à jour**. Les programmes trop anciens ou qui ne sont plus sous garantie représentent des risques de sécurité. La meilleure décision est alors de changer de dispositif. Cependant, si ces programmes fonctionnent sans être connectés, ils restent utilisables en suivant quelques consignes de sécurité : déconnectez le programme obsolète d'internet, séparez-le du reste du réseau et désactivez les services vulnérables.

En entreprise, il est recommandé de formaliser ce système **en rédigeant des règles de réalisation de mises à jour**. Reprenez les étapes précédentes et spécifiez qui intervient et quand.

CONCLUSION

Les mises à jour des appareils numériques, des logiciels et des applications sont essentielles pour garantir votre sécurité informatique car elles corrigent leurs failles de sécurité.

Il est donc nécessaire de les faire dès que possible **: activez pour cela les notifications de mise à jour et planifiez les installations qui ne peuvent être automatisées** ou que vous n'êtes pas en mesure d'effectuer immédiatement.

Enfin, gardez en tête que **les mises à jour ne répondent pas uniquement à des enjeux de sécurité** : nouvelles fonctionnalités, compatibilité entre dispositifs, expérience utilisateur améliorée… Vous avez donc tout à gagner à installer vos mises à jour régulièrement !