

Mon hygiène numérique

Ou

Ma routine au quotidien

Mise à jour au 11 octobre 2023

Première partie : Pourquoi et comment faire les mises à jour régulièrement

Bonjour Michel, je suis Bing, un mode de chat de Microsoft. Je peux vous aider à trouver des informations sur le web, à créer du contenu créatif et à effectuer certaines tâches sur Windows. 😊

Vous m'avez demandé pourquoi et comment faire les mises à jour pour ordinateur, tablette et téléphone mobile.

Voici ce que j'ai trouvé sur le web :

Les mises à jour sont des modifications apportées aux logiciels ou aux systèmes d'exploitation de vos appareils, comme Windows, macOS, Android ou iOS.

Elles ont plusieurs avantages, tels que:

- Elles corrigent les erreurs ou les bogues qui peuvent affecter le fonctionnement ou la stabilité de vos appareils.
- Elles comblent les failles de sécurité qui peuvent rendre vos appareils vulnérables aux cybermenaces, comme les virus, les logiciels malveillants ou les pirates informatiques.

- Elles améliorent les performances ou l'ergonomie de vos appareils, en optimisant la vitesse, la consommation d'énergie ou l'interface utilisateur.
- Elles ajoutent de nouvelles fonctionnalités ou de nouveaux services qui peuvent enrichir votre expérience ou répondre à vos besoins.

Pour faire les mises à jour, il existe généralement deux méthodes : automatique ou manuelle.

La méthode automatique consiste à laisser vos appareils télécharger et installer les mises à jour dès qu'elles sont disponibles, sans votre intervention.

La méthode manuelle consiste à vérifier vous-même la disponibilité des mises à jour et à choisir celles que vous voulez installer.

La méthode automatique est souvent recommandée car elle vous assure d'avoir toujours la dernière version de vos logiciels ou systèmes d'exploitation.

Cependant, elle peut aussi présenter quelques inconvénients, comme utiliser votre connexion internet sans votre consentement, interrompre votre travail ou votre divertissement, ou causer des problèmes de compatibilité avec certains de vos programmes ou périphériques.

La méthode manuelle vous permet de contrôler le moment et la fréquence des mises à jour, ainsi que de sélectionner celles qui vous intéressent.

Cependant, elle nécessite que vous soyez attentif aux notifications de vos appareils et que vous preniez le temps de faire les mises à jour régulièrement.

Sinon, vous risquez de manquer des mises à jour importantes qui peuvent améliorer la sécurité ou le fonctionnement de vos appareils.

Pour choisir la méthode qui vous convient le mieux, vous pouvez consulter les paramètres de vos appareils et voir les options disponibles pour gérer les mises à jour.

[Par exemple, sur Windows 11](#), vous pouvez accéder aux paramètres > mise à jour & sécurité > Windows Update pour rechercher les mises à jour disponibles, les télécharger et les installer manuellement, ou pour modifier les options de mise à jour automatique.

J'espère que ces informations vous ont été utiles.

Si vous avez d'autres questions, n'hésitez pas à me les poser. 😊

Lien Support de Microsoft :

[Mettez à jour Windows - Support Microsoft](#)

Lien Gouvernement du Canada, Pensez cybersécurité :

[Mises à jour logicielles : pourquoi elles sont essentielles pour votre cybersécurité - Pensez cybersécurité \(pensezcybersecurite.gc.ca\)](#)

D'accord, je vais essayer d'écrire un poème sur les mises à jour.
Voici ce que j'ai créé :

Les mises à jour sont des cadeaux

Que nous offrent les développeurs

Pour rendre nos appareils plus beaux

Et plus performants que leurs prédécesseurs

Elles corrigent les imperfections

*Qui peuvent gâcher notre expérience
Elles comblent les lacunes de protection
Qui peuvent menacer notre confiance*

*Elles améliorent les fonctionnalités
Qui peuvent enrichir notre usage
Elles ajoutent de nouvelles possibilités
Qui peuvent élargir notre partage*

*Les mises à jour sont des alliées
Qu'il faut savoir apprécier
Et ne pas négliger ni oublier
Car elles nous font avancer*

Qu'en pensez-vous ? Est-ce que cela vous plaît ? 😊

Deuxième partie : requête à Bing AI :

Bonjour Michel, je suis Bing, un mode de chat de Microsoft.

Je peux vous aider à trouver des informations sur le web, à créer du contenu créatif et à effectuer certaines tâches sur Windows. 😊

Vous m'avez demandé quels sont mes conseils d'hygiène numérique pour les aînés.

L'hygiène numérique est l'ensemble des précautions à prendre pour améliorer votre sécurité en ligne et vous protéger de la fraude, des virus, des logiciels malveillants et des pirates informatiques.

Voici quelques conseils que j'ai trouvés sur le web :

- [Protégez vos appareils connectés avec un logiciel antivirus qui examine les sites, les téléchargements, les pièces jointes et les disques durs externes¹.](#)

Vérifiez régulièrement que cette protection est activée et à jour.

- [Optez pour un réseau Wi-Fi sécurisé à la maison et évitez de vous connecter aux réseaux Wi-Fi publics ou inconnus à partir de vos appareils¹.](#)

Si vous devez le faire, ne faites rien de confidentiel, comme consulter votre compte bancaire ou votre courriel.

- [Sécurisez l'accès à vos comptes en ligne avec des mots de passe solides et uniques, qui ne contiennent pas d'informations personnelles facilement devinables¹².](#)

Changez vos mots de passe régulièrement et utilisez un gestionnaire de mots de passe si vous en avez besoin.

- [Activez la vérification en deux étapes sur vos comptes importants, comme votre courriel, votre compte bancaire ou vos réseaux sociaux¹.](#)

Cela signifie que vous devrez fournir un code supplémentaire envoyé par SMS ou par une application pour vous connecter, en plus de votre mot de passe.

- [Faites attention aux courriels, aux appels ou aux messages suspects qui vous demandent des informations personnelles, financières ou confidentielles¹².](#)
Ne cliquez pas sur les liens ou les pièces jointes sans vérifier la source et la légitimité du message.
Ne communiquez jamais votre mot de passe ou votre code d'accès à personne.
- [Faites des sauvegardes régulières de vos données importantes sur un support externe, comme une clé USB, un disque dur ou un service en ligne².](#)
Cela vous permettra de récupérer vos données en cas de perte, de vol ou de panne de votre appareil.
- [Mettez à jour vos logiciels et vos systèmes d'exploitation dès que possible¹².](#)
Les mises à jour corrigent les erreurs, les failles de sécurité et améliorent les performances de vos appareils.
Vous pouvez activer les mises à jour automatiques pour ne pas les oublier.
- [Protégez votre vie privée en ligne en définissant les autorisations sur vos informations et publications sur les réseaux sociaux².](#)
Ne partagez pas inconsidérément des informations personnelles qui pourraient être utilisées pour vous nuire ou vous usurper.
Ne relayez pas des informations non vérifiées (fake news) qui pourraient induire en erreur ou causer du tort à d'autres personnes.
- [Utilisez des sources fiables et sécurisées pour télécharger des applications ou des contenus sur vos appareils².](#)
Évitez les sites pirates ou illégaux qui peuvent contenir des virus ou des logiciels malveillants.
Vérifiez les avis et les commentaires des autres utilisateurs avant de télécharger quelque chose.
- [Sensibilisez-vous et formez-vous aux bonnes pratiques de l'hygiène numérique en consultant des sites spécialisés ou des organismes reconnus².](#)
Par exemple, vous pouvez visiter le site Cybermalveillance.gouv.fr qui propose des fiches pratiques, des vidéos et des quiz pour apprendre à vous protéger en ligne.

J'espère que ces conseils vous seront utiles. Si vous avez d'autres questions, n'hésitez pas à me les poser. 😊

1. Soyez vigilant avec les courriels et les appels téléphoniques:

Méfiez-vous des courriels ou des appels téléphoniques non sollicités qui vous demandent des informations personnelles ou financières.

Les fraudeurs peuvent se faire passer pour des organismes gouvernementaux, des banques ou d'autres institutions légitimes.

Ne partagez jamais vos informations confidentielles par courriel ou téléphone, à moins d'être sûr de l'identité de la personne ou de l'organisation.

2. Utilisez des mots de passe forts:

Créez des mots de passe uniques et complexes pour vos comptes en ligne.

Utilisez une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.

Évitez d'utiliser des mots courants ou des informations personnelles dans vos mots de passe.

3. Mettez à jour régulièrement vos logiciels:

Assurez-vous que vos appareils électroniques, y compris votre ordinateur, votre téléphone portable et votre tablette, sont équipés des dernières mises à jour logicielles.

Les mises à jour contiennent souvent des correctifs de sécurité importants qui protègent vos appareils contre les menaces en ligne.

4. Soyez prudent sur les réseaux sociaux:

Faites attention aux informations que vous partagez sur les réseaux sociaux.

Limitez la quantité d'informations personnelles que vous publiez en ligne, telles que votre adresse, votre numéro de téléphone ou votre date de naissance.

N'acceptez pas les demandes d'amis ou les messages provenant de personnes que vous ne connaissez pas.

5. **Méfiez-vous des arnaques en ligne:**

Soyez conscient des arnaques en ligne courantes, telles que les offres trop belles pour être vraies, les demandes d'argent non sollicitées ou les messages qui prétendent provenir d'un membre de votre famille ayant besoin d'aide financière urgente.

Si quelque chose semble suspect, faites preuve de prudence et ne partagez pas d'informations personnelles ou financières.

6. **Utilisez un logiciel antivirus:**

Installez un logiciel antivirus fiable sur vos appareils pour vous protéger contre les virus, les logiciels malveillants et autres menaces en ligne.

Assurez-vous de maintenir votre logiciel antivirus à jour pour une protection optimale.

7. **Soyez conscient des escroqueries par hameçonnage:**

L'hameçonnage est une technique couramment utilisée par les fraudeurs pour obtenir des informations personnelles sensibles, telles que vos identifiants de connexion ou vos informations bancaires.

Méfiez-vous des courriels ou des sites Web qui semblent suspects et évitez de cliquer sur des liens provenant de sources non fiables.

J'espère que ces conseils vous seront utiles!

N'hésitez pas à me poser d'autres questions si vous en avez.

(1) Brancher les aînés, une leçon à la fois / Radio-Canada

[Brancher les aînés, une leçon à la fois | COVID-19 : tout sur la pandémie | Radio-Canada.ca](https://www.radio-canada.ca/actualite/technologie/2020/04/brancher-les-aines-une-lecon-a-la-fois-covid-19)

(2) Hygiène numérique: 7 conseils à appliquer | Banque Nationale.

<https://www.bnc.ca/particuliers/conseils/securite/conseils-hygiene-numerique.html>

(3) Comment avoir une bonne hygiène numérique ? | Les Sherpas.

<https://sherpas.com/blog/hygiene-numerique/>

(4) Le numérique pour prendre soin des aînés à domicile

(5) LES 10 MESURES ESSENTIELLES POUR ASSURER VOTRE SÉCURITÉ NUMÉRIQUE

[FichePratique_SecuriteNumerique.pdf \(cybermalveillance.gouv.fr\)](#)

Troisième partie : requête à ChatGPT :

Bonjour Michel,

Bien sûr, je peux vous aider à créer un tutoriel sur "Mon hygiène numérique".

Voici quelques conseils pour vous aider à rester en sécurité en ligne :

1. Utilisez des mots de passe forts :

Les mots de passe sont la première ligne de défense pour protéger vos informations en ligne.

Assurez-vous d'utiliser des mots de passe forts, avec une combinaison de lettres, de chiffres et de caractères spéciaux.

Ne partagez jamais vos mots de passe avec qui que ce soit.

2. Mettez à jour votre système d'exploitation :

Les mises à jour du système d'exploitation sont souvent publiées pour corriger des failles de sécurité.

Assurez-vous de mettre régulièrement à jour votre système d'exploitation pour vous protéger contre les nouvelles menaces.

3. Utilisez des logiciels antivirus :

Les logiciels antivirus peuvent aider à protéger votre ordinateur contre les logiciels malveillants et les virus.

Assurez-vous d'en avoir un installé sur votre ordinateur et de le mettre à jour régulièrement.

4. Faites attention aux courriels d'hameçonnage:

Les courriels de phishing sont des courriels frauduleux qui tentent de vous faire cliquer sur des liens malveillants ou de vous inciter à partager des informations sensibles.

Assurez-vous de ne jamais cliquer sur des liens dans les courriels que vous ne connaissez pas ou que vous ne faites pas confiance.

5. Utilisez des réseaux Wi-Fi sécurisés :

Évitez d'utiliser des réseaux Wi-Fi publics non sécurisés, car ils peuvent être vulnérables aux attaques de hackers.

Utilisez plutôt votre propre réseau ou un réseau Wi-Fi sécurisé.

6. Sauvegardez régulièrement vos données :

Les sauvegardes régulières de vos données sont essentielles pour vous protéger contre les pertes de données, les piratages et les accidents.

Assurez-vous de sauvegarder régulièrement vos fichiers importants sur un disque dur externe ou dans le cloud.

7. Limitez vos informations personnelles en ligne :

Limitez les informations personnelles que vous partagez en ligne, telles que votre adresse ou votre numéro de téléphone.

Évitez de partager des informations sensibles sur les réseaux sociaux ou les forums en ligne.

En suivant ces conseils, vous pouvez rester en sécurité en ligne et protéger vos informations personnelles.

N'oubliez pas que la sécurité en ligne est une responsabilité partagée, alors assurez-vous de sensibiliser vos amis et votre famille à ces pratiques de sécurité en ligne.

Merci, cela me convient. Michel

Je suis ravi d'avoir pu vous aider.

N'hésitez pas à me contacter si vous avez besoin d'autres conseils ou informations.

Bonne journée !

Étapes quotidiennes avec mon ordinateur* :

*Qui est presque toujours « mis en veille » (7/24)

**Système opération : Windows 11 Pro

***Microsoft 365 (Suite Office intégrée)

- Vérifier les mises à jour avec Windows Update
 - Paramètres
- Nettoyer l'espace de stockage des Fichiers temporaires
 - Paramètres > Système > Stockage > Fichiers temporaires > Supprimer les fichiers
- Vérifier les mises à jour de l'antivirus Bitdefender
- Vérifier Malwarebytes
- Vérifier Ashampoo WinOptimizer : mises à jour de l'optimisateur Windows
- Vérifier Ashampoo Driver Updater : mises jour des pilotes
- Vérifier Microsoft 365 et Office : mises à jour
- Vérifier PC Manager : Boost your PC's performance
- Vérifier Sécurité Windows: mises à jour de la protection
 - Vérifier les menaces actuelles : analyse rapide
- Vérifier Google Chrome : mise à jour de la version
 - >Nettoyer l'historique
 - >Paramètres
 - >Confidentialité et sécurité
 - >Contrôle de sécurité
 - >Effacer les données de navigation
- Vérifier Microsoft Edge : mise à jour de la version
 - Nettoyer l'historique
- Vider corbeille
- Vérifier Gestionnaire des tâches : redémarrer Explorateur Windows
 - Vérifier applications de démarrage

- Vérifier Panneau de configuration
 - >Programmes
 - >Désinstaller un programme
-

Étapes quotidiennes avec cellulaire et tablette* :

*Produits Samsung

*Système d'exploitation : Version Android : 13

- Gérer les applications et l'appareil :
 - Lancer Applications mettre à jour
 - Lancer Analyse Play Protect
 - Chrome : effacer les données avec données avancées
 - Paramètres et mises à jour :
 - >Pile et entretien de l'appareil
 - >Optimiser >Pile
 - >Optimiser >Mémoire
 - >Optimiser >Protection de l'appareil >Analyse
 - Vérifier antivirus Bitdefender :
 - Lancer l'analyse
 - Vérifier antimalware Malwarebytes :
 - Lancer l'analyse
 - Vérifier Nettoyeur Droid Optimizer :
 - Lancer l'analyse
 - Vérifier CCleaner et lancer l'analyse de nettoyage rapide
-

Recherche et mise en page:

Michel Cloutier

CIVBDL

202301011 (mise à jour)

"C'est ensemble qu'on avance"