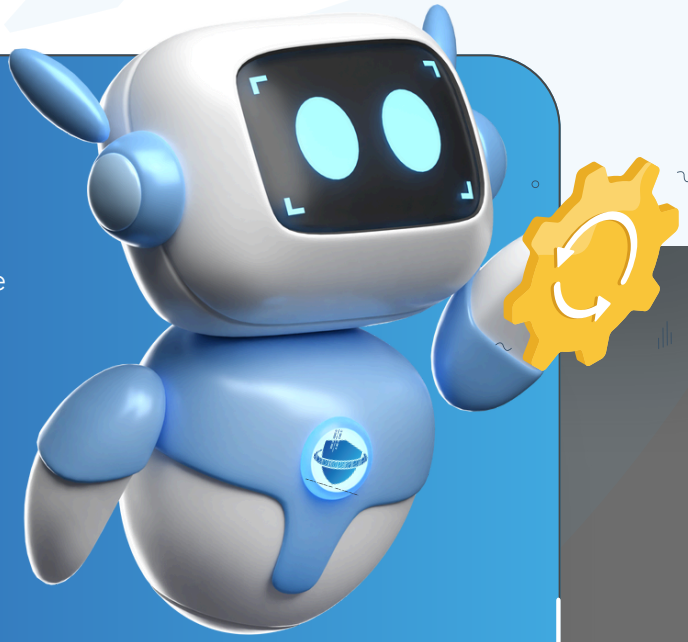
LES MISES À JOUR

CENTRE CYBER DU PACIFIQUE

EN BREF

POURQUOI C'EST IMPORTANT ?

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'un équipement mobile ou encore d'une montre connectée. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (patch en anglais) visant à corriger ces failles. Si l'opération de mise à jour est souvent ressentie comme une contrainte, il s'agit pourtant d'un acte essentiel pour se protéger.



Voici 10 bonnes pratiques à adopter pour vos mises à jour

1. METTEZ À JOUR VOS APPAREILS ET LOGICIELS
2. TÉLÉCHARGEZ LES MISES À JOUR DE SOURCES OFFICIELLES
3. IDENTIFIEZ TOUS VOS APPAREILS ET LOGICIELS
4. ACTIVEZ LES MISES À JOUR AUTOMATIQUES
5. DÉFINISSEZ LES RÈGLES DES MISES À JOUR
6. PLANIFIEZ LES MISES À JOUR EN PÉRIODE D'INACTIVITÉ
7. MÉFIEZ-VOUS DES FAUSSES MISES À JOUR
8. SUIVEZ LES PUBLICATIONS DES ÉDITEURS
9. TESTEZ ET SAUVEGARDEZ AVANT LES MISES À JOUR
10. PROTÉGEZ LES APPAREILS NON MIS À JOUR

▶ Voir détail page "ADOPTEZ LES BONNES PRATIQUES"

LES MISES À JOUR

CENTRE CYBER DU PACIFIQUE

ADOPTEZ LES BONNES PRATIQUES

Voici 10 bonnes pratiques à adopter pour vos mises à jour.

1. METTRE À JOUR SANS TARDER L'ENSEMBLE DE VOS APPAREILS ET LOGICIELS

Ordinateurs, téléphones, systèmes d'exploitation, logiciels, objets connectés… il suffit qu'un seul appareil ou logiciel ne soit pas à jour pour créer une faille de sécurité. Réalisez les mises à jour dès qu'elles sont disponibles pour empêcher les cybercriminels d'exploiter ces failles.

2. TÉLÉCHARGEZ LES MISES À JOUR UNIQUEMENT DEPUIS LES SITES OFFICIELS

Utilisez uniquement les sites officiels des éditeurs et fabricants pour éviter les mises à jour infectées par des virus. Faites attention aux conditions d'utilisation ou aux cases pré-cochées qui pourraient installer des logiciels non désirés.

3. IDENTIFIEZ L'ENSEMBLE DES APPAREILS ET LOGICIELS UTILISÉS

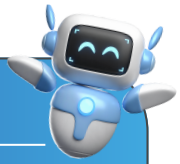
Identifiez tous les appareils, matériels et logiciels à mettre à jour. Pour les nouveaux appareils, réinitialisez-les et installez les mises à jour depuis les sites des fabricants.

4. ACTIVEZ L'OPTION DE TÉLÉCHARGEMENT ET D'INSTALLATION AUTOMATIQUE

Si possible, configurez vos logiciels pour qu'ils se mettent à jour automatiquement. Cela garantit que vous disposez toujours de la dernière version à jour. Vérifiez manuellement si nécessaire.

5. DÉFINISSEZ LES RÈGLES DE RÉALISATION DES MISES À JOUR *PRO*

Pour sécuriser votre environnement numérique, définissez des règles concernant la manière de faire l'inventaire des appareils et logiciels, où et comment trouver les mises à jour, et qui en est responsable.



DIFFÉRENTS TYPES DE MÀJ

Les mises à jour importantes ou critiques corrigent des failles de sécurité qui peuvent être utilisées pour pirater votre équipement. Les mises à jour de version apportent en général de nouvelles fonctionnalités et corrigent également des failles de sécurité. Ce type de mise à jour peut être payant.

BON À SAVOIR

En entreprise, s'il existe un service informatique, il est généralement chargé de la mise à jour des appareils et des logiciels. Dans le cas contraire, ce sont les collaborateurs qui effectuent cette opération, sous l'autorité du chef d'entreprise.

LES MISES À JOUR

CENTRE CYBER DU PACIFIQUE

ADOPTEZ LES BONNES PRATIQUES

6. PLANIFIEZ LES MISES À JOUR LORS DE PÉRIODES D'INACTIVITÉ

Pour éviter les interruptions lors de vos activités, profitez des périodes d'inactivité (déjeuner, nuit, réunions) pour effectuer les mises à jour, qui peuvent prendre de quelques secondes à plusieurs heures.

7. MÉFIEZ-VOUS DES FAUSSES MISES À JOUR SUR INTERNET

Sur Internet, des fenêtres apparaissant comme des alertes de mise à jour peuvent être des publicités malveillantes. Soyez vigilant et n'installez pas de mise à jour suspecte qui pourrait contenir un virus.

8. INFORMEZ-VOUS SUR LA PUBLICATION RÉGULIÈRE DES MÀJ DE L'ÉDITEUR PRO

Si un appareil ou logiciel n'est plus mis à jour, il devient plus vulnérable. Avant d'acquérir du nouveau matériel, vérifiez que l'éditeur propose des mises à jour régulières et la date de fin de leur disponibilité.

9. TESTEZ LES MÀJ LORSQUE CELA EST POSSIBLE ET FAITES DES SAUVEGARDES PRO

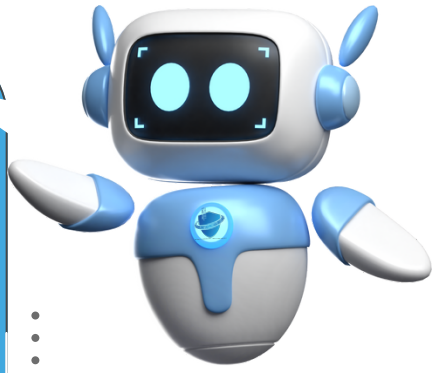
Certaines mises à jour peuvent rendre un appareil incompatible avec d'autres. Testez-les quand c'est possible et sauvegardez vos données et logiciels avant de procéder, afin de revenir en arrière si nécessaire.

10. PROTÉGEZ AUTREMENT LES APPAREILS QUI NE PEUVENT PAS ÊTRE MÀJ PRO

Certains appareils ne peuvent plus être mis à jour (ancienneté, perte de garantie). Dans ce cas, protégez-les autrement, par exemple en les déconnectant d'Internet ou en désactivant les services vulnérables.

QUELQUES EXEMPLES DE FAILLES DE SÉCURITÉ

- Aux États-Unis, des cybercriminels ont réussi à dérober des données confidentielles d'un casino grâce au thermomètre connecté présent dans un aquarium de l'établissement.
- En France, la trottinette électrique connaît un succès grandissant. Une faille de sécurité sur certains modèles a été découverte. Elle permettait d'exécuter certaines commandes sans avoir besoin du mot de passe comme les déverrouiller, contrôler l'accélération ou le freinage. Une mise à jour a été publiée pour corriger cette faille.



PRO = *Destiné principalement aux professionnels*