

Pour plus de contenu, connectez-vous !

Bonnes pratiques en cybersécurité

En naviguant sur Internet

En premier lieu, les antivirus commerciaux (Avast, McAfee, Kaspersky, Avira etc ...) sont inutiles. Sous Windows, Windows Defender fait parfaitement l'affaire, les autres antivirus vont juste être à l'origine de pas mal de blocages pénibles et inutiles. Les constructeurs d'ordinateurs et les antivirus passent des contrats pour mettre d'office leur antivirus sur des PC. La première chose à faire en recevant un PC neuf sous Windows est donc de désinstaller tout antivirus supplémentaire.

1. Garder son navigateur à jour

Un navigateur internet à jour permet de se prémunir des failles de sécurité qui sont découvertes très régulièrement, des correctifs sont déployés à chaque mise à jour.

- Sur Mozilla Firefox : Paramètres > Général > Mises à jour de Firefox
- Sur Google Chrome ou Chromium : Paramètres > Confidentialité et sécurité > Contrôle de sécurité
- Sur Edge : Paramètres > A propos de Microsoft Edge

2. Garder son système d'exploitation et ses applications à jour

Un système d'exploitation (OS) et des applications à jour permettent d'appliquer des correctifs réguliers lors que des failles sont découvertes.

Sur Ubuntu (Et autres distributions Linux) :

Gestionnaire de mises à jour puis Installer les mises à jour

Dans Logiciels et mises à jour, vérifier que "Lorsqu'il y a des mises à jour de sécurité" est bien sur "Télécharger et installer automatiquement"

Sur Windows :

Ouvrir Windows Update en le cherchant dans la barre de recherche puis cliquer sur "Rechercher des mises à jour", les installer s'il y en a.

A l'ouverture d'une application, si une fenêtre s'ouvre indiquant qu'une nouvelle version est disponible

3. Utiliser des mots de passe sécurisés

Les mots de passe trop simples sont la porte d'entrée idéal à votre machine, vos informations personnelles et bancaires.

Plusieurs points à surveiller :

- Un mot de passe différent à chaque fois, pas de mot de passe réutilisé
- Un mot de passe compliqué : 8 caractères grand minimum, 12 c'est mieux. On mélange les chiffres, les lettres, les symboles et on évite de faire des phrases.
- Utiliser la double authentification : lorsque c'est possible, activer la double authentification (Via mail, SMS ou bien application d'authentification)

Parce qu'il est impossible de se souvenir de tous ses mots de passe, utiliser un gestionnaire de mots de passe est indispensable.

-Les navigateurs comme Mozilla Firefox permettent d'enregistrer ses mots de passe qui vont

être liés à son compte.

-Autre solution, les gestionnaires de mots de passe, comme [KeePassXC](#) que nous utilisons dans l'équipe interne.

4. Utiliser un bloqueur de pubs

En plus de rendre votre navigation sur internet bien plus agréable, un bloqueur de pubs permet aussi (pour la plupart) de bloquer les pisteurs présents sur énormément de sites web. Leur fonctionnement basé sur des listes alimentées par la communauté permettent aussi d'être averti lors de navigation sur des domaines réputés malveillants.

Nous recommandons l'extension [uBlock Origin](#).

En consultant mes mails ou mes messages

1. Vérifier l'expéditeur

Created 2025-03-05 09:21:25 UTC by Michaël Duc

Updated 2026-05-05 14:13:51 UTC by Michaël Duc