UNIVERSITÉ LIBRE DE BRUXELLES

Configuration de base sécurisée pour Windows

Version:	1.1
Date de la version:	11/02/2022
Créé par :	Alex GENATZY
Approuvé par :	CBA – C2i
Niveau de confidentialité :	Usage public

1 Comment maintenir votre ordinateur sous le système d'exploitation Windows sécurisé

Saviez-vous que même si votre ordinateur dispose des dernières mises à jour, l'anti-virus le plus récent et comporte un pare-feu (firewall), il peut malgré tout être infecté. Lorsque les ordinateurs sont utilisés de façon personnelle, plutôt que professionnelle, les risques d'infections ou d'autres incidents de sécurité augmentent (les films, jeux, musiques et autres applications personnelles entrainent tous des risques). Si vous gérez votre propre ordinateur ou installez vos propres applications, vous êtes aussi responsables de leur sécurité.

2 Utilisez une solution de sécurité pour les terminaux (antivirus) qui est automatiquement mise à jour

De nouveaux virus apparaissent quotidiennement. Les ordinateurs sous le système d'exploitation Windows doivent être équipés d'une solution de sécurité (antivirus) automatiquement mise à jour afin de limiter les dommages des virus connus. Si un virus est découvert, la solution de sécurité (antivirus) vous le signalera, et l'empêchera de fonctionner (en le mettant en quarantaine).
Si vous installez la solution préconisée par l'ULB (« **Microsoft Defender for Endpoint** »), vous pourrez continuer de travailler normalement, le service support sera automatiquement informé et vous contactera si d'autres actions sont nécessaires.
Parfois, l'antivirus ne peut pas empêcher complètement les dommages, si vous rencontrez des problèmes, contactez **support@ulb.be** (tél: 3737), fournissez les détails du message d'erreur et du problème, et demandez une vérification complète de virus.

Toute personne gérant son propre ordinateur utilisant le système d'exploitation Windows est aussi responsable d'obtenir, d'installer et de mettre à jour son antivirus. Cela s'applique à tous les ordinateurs se connectant sur le réseau de l'ULB, y compris ceux des visiteurs. Le personnel de l'Université utilisant le système d'exploitation Windows doivent utiliser la solution fournie par l'institution « **Microsoft Defender for Endpoint** ». [1]

Sur un ordinateur personnel, les utilisateurs doivent installer une solution antivirus de leur choix.

Une solution de sécurité (antivirus) mise à jour régulièrement est particulièrement importante pour les ordinateurs utilisant le système d'exploitation Windows qui sont utilisés dans divers endroits et connectés à d'autres fournisseurs d'accès à Internet, vu qu'ils évitent les protections de sécurité de l'Université.
Non seulement cela augmente leur risque d'infection, mais soumet le réseau ULB à des dangers, puisqu'une fois infectés, ils peuvent propager l'infection depuis l'intérieur du pare-feu de l'ULB.

3 Permettez l'installation automatique des mises à jour

De nombreux problèmes de sécurité sont causés par des logiciels qui n'ont pas les dernières mises à jour installées. La plupart des logiciels peuvent installer les mises à jour automatiquement. Assurez-vous que les logiciels installés ont cette fonctionnalité activée.

- Assurez-vous que la « **Mise à jour Windows** » (« **Windows Update** ») est activée et est exécutée régulièrement.

[1] https://support.ulb.be/web/support/-/comment-installer-et-executer-windows-defender-atp-sur-windows-

Si vous utilisez les systèmes institutionnels (**PA**rc **Bu**reautique, **mobile.it**) la configuration est gérée centralement pour vous.

3.1 L'utilisation de logiciels non supportés (ou en fin de vie – « End of Life »).

Un logiciel qui n'est plus pris en charge est un logiciel en fin de vie. Pourtant, l'utilisation de ces logiciels en fin de vie et donc qui ne sont plus à jour présente des risques majeurs. Ils peuvent notamment contenir des failles qui vont menacer la sécurité d'un ordinateur ou les données personnelles de son utilisateur.
Pour vérifier, si vous utilisez des logiciels en fin de vie : **https://endoflife.date/**

- Site officiel Microsoft:
  https://docs.microsoft.com/fr-be/lifecycle/products/?terms=Windows
  https://docs.microsoft.com/en-gb/lifecycle/products/?terms=Windows

3.2 Configuring Automated Operating System Patch Management Tools via Windows Settings
Configuration des mises à jour automatisé via les paramètres Windows

1. Cliquez sur le bouton Démarrer de Windows. Le menu Démarrer de Windows s'affiche avec la barre de recherche.
2. Saisissez « mise à jour de Windows » dans la barre de recherche. Le menu Démarrer est rempli d'options de mise à jour Windows.
3. Sélectionnez Paramètres de mise à jour Windows. Le panneau Windows Update s'affiche. Cet écran affiche l'état des mises à jour de l'ordinateur. S'il y a des mises à jour, elles seront répertoriées.
4. Sélectionnez Rechercher des mises à jour pour voir si des mises à jour sont disponibles. La sélection des options avancées fournira des paramètres de mise à jour du système supplémentaires.
5. Sélectionnez Options avancées. Assurez-vous que suspendre les mises à jour est désactivé.

1. Click the Windows Start button. The Windows Start menu displays with the search bar.
2. Enter «windows update» in the search bar. The Start Menu populates with Windows update options.
3. Select Windows Update Settings. The Windows Update panel displays. This screen shows the status of updates for the computer. If there are updates, they will be listed.
4. Select Check for updates to see if updates are available. Selecting Advanced options will provide additional system update settings.
5. Select Advanced options. Ensure that Pause Updates is set to Off.

3.3 Automatic Application Updates via the Microsoft Store
Mises à jour automatiques des applications via Microsoft Store

1. Cliquez sur Démarrer. Le menu Démarrer de Windows s'affiche avec la barre de recherche.
2. Saisissez « Microsoft Store » dans le champ de recherche.
3. Sélectionnez l'application « Microsoft Store » dans les résultats de la recherche. L'écran d'accueil du Microsoft Store s'affiche.
4. Sélectionnez les trois points (. . .) en haut à droite sous le « x ». La liste déroulante Paramètres s'affiche.
5. Sélectionnez Paramètres. L'écran Paramètres s'affiche.
6. Assurez-vous que Mettre à jour automatiquement les applications est activé.

1. Click Start. The Windows Start menu displays with the search bar.
2. Enter « Microsoft Store » in the search field.
3. Select the Microsoft Store app in the search results. The Microsoft Store Home Screen displays.
4. Select the three dots (. . .) in the top right under the «x». The Settings drop-down list displays.
5. Select Settings. The Settings screen displays.
6. Ensure that Update apps automatically is set to On.

Activer les mises à jour automatiques des applications :
FR :
https://support.microsoft.com/fr-fr/windows/activer-les-mises-%C3%A0-jour-automatiques-des-applications-70634d32-4657-dc76-632b-66048978e51b

UK :
https://support.microsoft.com/en-gb/windows/turn-on-automatic-app-updates-70634d32-4657-dc76-632b-66048978e51b

Impact:
Sans mise à jour automatique, les mises à jour peuvent ne pas être effectuées en temps voulu et le système sera exposé à des risques supplémentaires. Un logiciel non corrigé présente des vulnérabilités qui peuvent être exploitées

4 Desktop & Screen Saver – Bureau et économiseur d'écran

Trop souvent, les ordinateurs sont laissés sans surveillance sans être verrouillés. Les ordinateurs déverrouillés permettent à quiconque d'accéder aux informations et aux applications sur un système. Cet objectif s'applique à plus qu'un simple système informatique, car les smartphones et les tablettes peuvent également être laissés déverrouillés

Too often computers are left unattended without being locked. Unlocked computers allow anyone to access the information and applications open on a system. This control applies to more than just a computer system since smartphones and tablets can also be left unlocked.

4.1 Set an inactivity interval of 20 minutes or less for the screen saver – Définir un intervalle d'inactivité de 20 minutes ou moins pour l'économiseur d'écran

Lorsque vous quittez votre poste de travail, vous pouvez le verrouiller avec le raccourci clavier Windows + L. En mettant en place un fond d'écran, vous pouvez le verrouiller automatiquement en cas d'inactivité. Votre mot de passe sera demandé pour déverrouiller le système.

4.1.1 Verrouiller les sessions de poste de travail après l'inactivité

Cliquez avec le bouton droit de la souris sur un espace vide du bureau puis cliquez sur Personnaliser.

1. Dans la colonne de gauche, cliquez sur « Écran de verrouillage ».
2. Cliquez sur « Paramètres » de l'écran de veille.
3. Sélectionnez un écran de veille dans la liste.
4. Choisissez ensuite le délai d'inactivité avant l'activation de l'écran de veille, 20 minutes par exemple. Cochez la case « A la reprise, demander l'ouverture du session » afin de verrouiller l'ordinateur avec l'écran de veille.
5. Validez par OK. Désormais, après 20 minutes d'inactivité, l'écran de veille est mis en route et votre ordinateur verrouillé. Votre mot de passe sera demandé pour revenir sur votre session..

4.1.2 Lock workstation sessions after inactivity.

1. For instance, you could right click the taskbar at the bottom of your screen and select « Show the Desktop ».
2. Right-click and select « Personalize ».
3. In the Settings window that opens, select « Lock Screen » (near the left side).
4. Click « Screen saver settings » near the bottom.
5. In the popup window that opens, in the box marked « Screen saver »:
6. Set the Wait entry in minutes, to say 20.
7. Make sure that you check the box for « On resume, display logon screen ».
8. Click OK to apply these settings and close the popup window.

4.1.3 Lock your workstation via « Bluetooth » when you step away from it (alternative) Verrouillez votre poste de travail via « Bluetooth » lorsque vous vous en éloignez (alternative)

FR :
https://support.microsoft.com/fr-fr/windows/verrouiller-automatiquement-windows-pc-lorsque-vous-vous-en-%C3%A9loignez-d0a5f536-74ac-0859-820a-4140dac9fcaf
UK :
https://support.microsoft.com/en-us/windows/lock-your-windows-pc-automatically-when-you-step-away-from-it-d0a5f536-74ac-0859-820a-4140dac9fcaf

Impact:
Si l'économiseur d'écran n'est pas défini, les utilisateurs peuvent laisser l'ordinateur disponible à une personne malintentionnée pour accéder aux informations.

5 Security & Privacy - Sécurité et confidentialité

5.1 Encryption - Chiffrement

5.1.1 Enable « BitLocker » - Activer « BitLocker »

- Activer le chiffrement de l'ordinateur :
  https://support.microsoft.com/fr-be/help/4028713/windows-10-turn-on-device-encryption

- Vue d'ensemble du chiffrement de l'appareil « BitLocker » dans Windows10
  https://docs.microsoft.com/fr-fr/windows/security/information-protection/bitlocker/bitlocker-device-encryption-overview-windows-10

Sur les systèmes où il est disponible, « **BitLocker** » présente l'avantage de la simplicité : chiffrer un disque revient essentiellement à cocher une case pour l'activer.
Voici la procédure proposée par Microsoft :

1. Cliquez sur le bouton Démarrer de Windows. Le menu Démarrer de Windows s'affiche avec la barre de recherche.
2. Saisissez « BitLocker » dans la barre de recherche. Résultats de recherche liés à l'affichage « BitLocker ». Sélectionnez « Gérer BitLocker » dans les résultats de la recherche. L'écran Chiffrement de lecteur BitLocker s'affiche.
3. Sélectionnez Activer BitLocker.

1. Click the Windows Start button. The Windows Start menu displays with the search bar.
2. Enter « BitLocker » in the search bar. Search results related to « BitLocker » display. Select « Manage Bitlocker » in the search results. The BitLocker Drive Encryption screen displays.
3. Select Turn on BitLocker.

5.1.1.1 Protéger vos informations de récupération (clef BitLocker)

BitLocker est conçu pour rendre le lecteur chiffré irrécupérable sans l'authentification requise. En mode de récupération, l'utilisateur doit entrer le mot de passe ou la clé de récupération pour déverrouiller le lecteur chiffré.

Important

- Stockez les informations de récupération dans un autre emplacement sécurisé

BitLocker is designed to make the encrypted drive unrecoverable without the required authentication. When in recovery mode, the user needs the recovery password or recovery key to unlock the encrypted drive.

Important

- Store the recovery information in another safe location.

5.1.2 Chiffrement alternatif pour notamment vos lecteurs réseaux (« cryptomator»)

La seule tâche de « **Cryptomator** » est le chiffrement. « **Cryptomator** » est un outil qui chiffre vos fichiers et vous permet de les synchroniser entre les périphériques via le cloud ou les lecteurs USB en toute sécurité. Ceci est très utile lorsque vous travaillez avec des informations privées et/ou

sensibles, car il vous permet de chiffrer vos informations (les rendre illisibles) pour qu'elles ne soient consultées que lorsque vous le souhaitez et de les synchroniser sur vos différents appareils.
Installation et documentation:

- **Dépôt :** https://cryptomator.org/downloads/
- **Références** : https://docs.cryptomator.org/en/latest/

5.1.3 Chiffrement alternatif du système d'exploitation (« VeraCrypt »)

Vous pouvez utiliser « **VeraCrypt** », un logiciel open-source et gratuit de chiffrement de données. « **VeraCrypt** » permet de chiffrer et déchiffrer les données à la volée, c'est-à-dire de manière transparente pour l'utilisateur et le système. Vous pouvez utiliser « **VeraCrypt** » pour chiffrer un fichier, une partition de disque ou l'ensemble d'un disque dur.

- **Dépôt :** https://www.veracrypt.fr/code/VeraCrypt
- **Références** : Chiffrement du disque d'un support de stockage à l'aide de « **VeraCrypt** » https://www.veracrypt.fr/en/Home.html

Installez « **VeraCrypt** »

1. Allez sur le site officiel de et téléchargez la dernière version de « **VeraCrypt** » pour Windows.
2. Effectuez l'installation en gardant les options par défaut et choisissez *Français* pour la langue d'installation.
3. À la fin de l'installation, « **VeraCrypt** » vous propose de lire la documentation (en anglais). Cette documentation est très complète et vous pourrez l'utiliser par la suite pour aller plus loin dans l'utilisation de « **VeraCrypt** ».

5.1.4 Enable « allow apps from the Store only » - Activer « Autoriser les applications du Store uniquement »

Windows 10 est livré avec l'option d'autoriser les applications de n'importe où par défaut.

Préférer les catalogues du Store :
Si vous voulez changer cela, vous devrez ouvrir l'applet Paramètres et modifier quelques options.

- Appuyez sur « touche Windows + I » pour ouvrir l'application Paramètres.
- Ouvrez « Système » et sélectionnez « Applications et fonctionnalités » dans le volet de gauche.
- Localisez « Installation des applications » et trois options en dessous :

1. « Autoriser les applications de n'importe où »
2. « M'avertir avant d'installer des applications en dehors du Store »
3. « Autoriser les applications du Store uniquement »

La première option sera définie par défaut, alors choisissez entre les options deux et trois.

- Fermez l'application « Paramètres ».

Microsoft Store:
If applications are installed via the Microsoft Application Store, they can be set to be automatically updated
https://support.microsoft.com/en-us/help/15081/windows-turn-on-automatic-app-updates

5.2 Enable Firewall - Activer le pare-feu

Pour activer le pare-feu dans Windows 10.

1. Cliquez sur le bouton Démarrer de Windows. Le menu Démarrer de Windows s'affiche avec la barre de recherche.
2. Entrez « Windows Defender » dans la barre de recherche. Résultats de la recherche pour l'affichage « Windows Defender ».
3. Sélectionnez l'application Windows Defender. La fenêtre « Security at a Glance » s'ouvre avec l'état des zones surveillées.
4. Sélectionnez « Pare-feu & protection réseau ». La vue Protection incendie et réseau s'ouvre.
5. Assurez-vous que les pare-feux du réseau de domaine, du réseau privé et du réseau public sont activés.
6. Si l'un des trois pare-feux n'est pas activé, sélectionnez-le pour l'activer.

1. Click the Windows Start button. The Windows Start menu displays with the search bar.
2. Enter « windows defender » in the search bar. Search results for « windows defender » display.
3. Select the Windows Defender App. The « Security at a Glance» window opens with status for monitored areas.
4. Select « Firewall & network protection ». The Fire and network protection view opens.
5. Ensure that the Domain network, Private network, and Public network firewalls are set to on.
6. If any of the three firewalls are not set to on, select that firewall to enable it.

5.2.1 Configurer le pare-feu Windows

1. Bloquer toutes les connexions entrantes

En choisissant cette option, le pare-feu bloque toutes les connexions entrantes, quelles que soient les règles existantes. Cela veut dire, même pour les programmes autorisés via le pare-feu.

Utilisez cette option au cas où vous auriez besoin d'une protection maximale de votre ordinateur. (Quand vous vous connectez à un réseau Wifi public par exemple).

2. Autoriser ou bloquer un programme via le pare-feu

Vous pouvez dans les règles du pare-feu autoriser/bloquer l'accès Internet à des applications. Par exemple, si vous ne souhaitez pas qu'elles se connectent à des serveurs pour y transmettre vos données. Pour se faire, il faut aller dans :

- Paramètres > Réseaux et Internet > Pare-feu.
  Cliquez sur Autoriser une application ou une fonctionnalité via le pare-feu Windows.

Et si le programme que vous souhaitez autoriser ne figure pas dans la liste, cliquez sur l'option « Autoriser une application » plus bas et choisissez-le depuis la fenêtre qui s'ouvre.

Impact:
Le pare-feu peut bloquer le trafic légitime

6 Auto-Backup - Sauvegarde automatique

« Windows backup » permet de sauvegarder l'intégralité du contenu présent sur votre ordinateur. Il suffit de se rendre dans le panneau de configuration et de choisir un lecteur avec suffisamment d'espace libre. Idéalement, la capacité de stockage de ce disque dur externe doit être +/- 2 fois la taille de votre disque interne. Dans le cas contraire, vous allez rapidement vous retrouvez rapidement dans le rouge, en fonction de la taille de vos sauvegardes.

6.1 Windows Auto-Backup - Sauvegarde automatique Windows

6.1.1 Ensure Regular Automated Backups – Configurer les sauvegardes automatiques

- Cliquez sur le menu Démarrer
- Allez dans « Paramètres » > « Mise à jour et sécurité »
- Cliquez sur « Sauvegarde » dans la colonne de gauche.
- Cliquez sur « Ajouter un lecteur » : une nouvelle fenêtre devrait alors apparaitre

Activez les sauvegardes automatiques :

1. Cliquez sur le bouton « Activer »
2. Une première sauvegarde sera lancée, et, par la suite, celle-ci sera refaite de telle sorte à ce qu'elle soit toujours à jour, avec plusieurs points de sauvegarde par fichier.
3. Dans « Mise à jour et sécurité » vous pouvez cliquer sur « Plus d'options » pour paramétrer vos sauvegardes automatiques. Dans la plupart des cas, vous choisirez l'option « Jusqu'à ce qu'il n'y ait plus d'espace » dans le menu déroulant « Conserver mes sauvegardes ».
4. Choisissez également une **fréquence** appropriée dans le menu « Sauvegarder mes fichiers » afin de disposer de plusieurs versions des mêmes fichiers.
5. Vous pouvez fermer toutes les fenêtres ouvertes.

Activate automated backups:

1. Click the Windows Start button. The Windows Start menu displays with the search bar.
2. Enter « backup » in the Windows search bar. Search results display for « backup ».
3. Select « Backup settings ». The Backup screen displays.
4. Select Add a drive under Back up using File History. The Backup options home screen displays. **Note:** An external hard drive or removable media (e.g., USB drive, thumb drive) must be connected to the computer to backup information onto.
5. Scroll down and select See advanced settings
6. Ensure file history is turned on.

7 File System Permissions and Access Controls Autorisations du système de fichiers et contrôles d'accès

7.1 Limiter les privilèges administrateur et le nombre d'utilisateurs autorisés à accéder au système au minimum

Nous vous recommandons d'utiliser au quotidien et en particulier pour naviguer sur internet un compte **ne possédant pas** les privilèges « **administrateur** »

Des vulnérabilités - des failles de sécurité sont découvertes avant que les patches ne soient disponibles. Avec ces vulnérabilités, le simple fait de cliquer un lien « web » avec les privilèges administrateur peut installer automatiquement un logiciel malicieux qui va infecter votre machine.

Il convient donc d'ouvrir votre session **sans les privilèges administrateur** ce qui réduit les dommages qu'un logiciel malicieux peut occasionner.

7.1.1 Implementation of administrative models according to the principle of minimum privileges – Implémentation de modèles d'administration selon le principe des privilèges minimum

https://docs.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models

De façon exceptionnelle certains utilisateurs doivent pouvoir obtenir un compte « **administrateur** » et le mot de passe associé. Dans ce cas, pour les opérations, comme des mises à jour, qui demandent les droits « **administrateur** », nous utiliserons préférentiellement les mécanismes du système d'exploitation. Ceux-ci permettent d'élever temporairement ses privilège UAC [2]ou « **Exécuter en tant qu'administrateur** » sous Windows.

https://docs.microsoft.com/en-gb/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models

Exceptionally, some users must be able to obtain an account « **administrator** » and the associated password. In this case, for operations, such as updates, which require « **administrator** » rights, we

will preferentially use the mechanisms of the operating system. These allow you to temporarily elevate your UAC or « **Run as administrator** » privileges on Windows)

8 Configure Devices to Not Auto-Run Content – Configurer pour ne pas exécuter automatiquement le contenu des périphériques

Objectif :
Les supports amovibles comprennent les clés USB, les cartes mémoire et les disques durs externes - pour ne citer que quelques exemples. Ces appareils sont souvent utilisés pour stocker des photos, des vidéos et de nombreux types de données. Les supports amovibles sont également utilisés par les attaquants pour installer des logiciels malicieux sur les systèmes informatiques. Cette méthode d'attaque peut être utilisée pour infecter les postes de travail, mais aussi les systèmes informatiques considérés comme sécurisés car dépourvus de connexion WiFi ou Internet. Si le logiciel sur un périphérique USB est autorisé à s'exécuter automatiquement, il peut être en mesure d'installer des logiciels malicieux avec une interaction limitée ou nulle de l'utilisateur.

[2] Fonctionnement du contrôle de compte d'utilisateur (UAC):
https://docs.microsoft.com/fr-be/windows/security/identity-protection/user-account-control/how-user-account-control-works

Purpose:
Removable media includes USB drives, memory cards, and external hard drives - just to name a few examples. These devices are used to store photos, videos, and many types of data. Removable media is also one method used by attackers to install malicious software on computer systems. This attack method can be used to infect workstations, but also computer systems viewed as secure since they lack a WiFi or Internet connection. If software on a USB device is allowed to automatically run, it may be able to install malware with limited to no user interaction.

8.1 Configure Devices to Not Auto-Run Content – Configurer les périphériques pour ne pas exécuter automatiquement leur contenu.

1. Cliquez sur le bouton Démarrer de Windows. (la barre de recherche)
2. Saisissez « Paramètres » dans le champ de recherche.
3. Cliquez sur l'icône de recherche. Options de recherche Windows pour les « Paramètres ».
4. Sélectionnez l'application « Paramètres ». La fenêtre « Paramètres » Windows s'ouvre.
5. Sélectionnez Périphériques. L'écran Bluetooth et autres périphériques s'ouvrent.
6. Sélectionnez **Exécution automatique**. L'écran **AutoPlay** (Exécution automatique) s'ouvre.
7. Assurez-vous que la lecture automatique est désactivée.

1. Click the Windows Start button. (displays with the search bar)
2. Enter «settings» in the search field.
3. Click the search icon. Windows search options for «settings».
4. Select the Settings app. The Windows Settings window opens.
5. Select Devices. The Bluetooth and Other Devices screen opens.
6. Select **AutoPlay**. The **AutoPlay** screen opens.
7. Ensure that AutoPlay is turned off.

9 Password Management - Gestion mots de passe

Les bonnes pratiques :

- Votre mot de passe doit rester personnel, pas de mot de passe partagé entre plusieurs utilisateurs.
- Votre mot de passe doit être suffisamment complexe (utilisation d'un mélange de lettres, ***majuscules, minuscules, chiffres*** et idéalement des caractères de ponctuation) d'une longueur ***minimum de 15 caractères***.
- Votre mot de passe doit être changé assez régulièrement
- Votre mot de passe doit être changé dès que vous en soupçonnez sa compromission (vol ou perte du PC, divulgation à un tiers, etc.)

9.1 Conservez vos mots de passe en lieu sûr

Mémoriser plusieurs mots de passe peut être difficile. Afin d'éviter de les oublier, conservez la liste de vos mots de passe hors connexion en un lieu sûr, secret et verrouillé. Ne la conservez pas dans votre boîte de messagerie ou ailleurs en ligne.

9.1.1 Gestionnaire de phrases et mots de passe

Si vous êtes dépassé par le nombre de mots de passe que vous devez retenir, vous pouvez utiliser un gestionnaire de mots de passe pour les générer et les conserver. Les mesures suivantes peuvent vous aider à protéger les mots de passe stockés dans un gestionnaire de phrases et mots de passe :

- Stockez uniquement les mots de passe associés à vos comptes qui ne nécessitent pas des privilèges administratifs ou des justificatifs d'identité liés à des comptes bancaires.
- Utilisez un mot de passe robuste et une authentification à deux facteurs pour sécuriser votre gestionnaire de mots de passe.

Nous vous recommandons le gestionnaire de mot de passe suivant :

« **Bitwarden** »: https://bitwarden.com/

10 Ne téléchargez pas, n'installez pas et n'exécutez pas de logiciels depuis des sources « non sures »

Parmi ces sources exposées au danger :

- Internet,
- les clés USB,
- CDs, DVDs,
- etc. ...

Un nombre croissant d'incidents de sécurité informatique détectés à l'ULB est dû à des logiciels téléchargés, installés ou exécutés depuis des sources douteuses. Les virus sont souvent cachés au sein de ces fichiers. Lorsque vous copiez et exécutez un fichier contenant un virus, vous pouvez non seulement infecter votre propre ordinateur, mais également commencer à propager un virus à l'intérieur du réseau ULB en contournant le pare-feu (firewall).

Les « **Logiciels gratuits** » populaires disponibles sur le Web peuvent introduire des problèmes de sécurité, soit lorsque le logiciel est installé (par exemple en installant des logiciels espions (« spyware ») ou plus tard, à cause du manque de mises à jour servant à éliminer les failles de sécurité. De plus l'installation d'un module d'extension (en anglais « plug-in ») peut aussi télécharger un logiciel malicieux que l'extension peut contenir. Si un site web nécessite un « plug-in » pour être visualisé, il vaut mieux ne pas l'activer.

En plus des problèmes de sécurité, les logiciels installés pour une utilisation personnelle créent souvent des problèmes de support. Les logiciels additionnels peuvent rendre l'analyse des problèmes plus difficile (temps de résolution plus grand).

Pour télécharger/installer vos logiciels, veuillez-vous référer à nos recommandations :

- L'application **Store** de votre **Windows**
- Simplifiez l'installation et maintenez vos applications à jour :
  - https://patchmypc.com/home-updater
  - https://chocolatey.org/

11 Références

CIS - Center For Internet Security - CIS Microsoft Windows 10 Enterprise Release 21H1 v1.11.0
https://downloads.cisecurity.org/?bypassToken=zrcxFuY5xcKHFXEhL6ffC5hNpKnOlj6f#/

ANSSI - Agence nationale de la sécurité des systèmes d'information
https://www.ssi.gouv.fr/administration/bonnes-pratiques/