UNIVERSITÉ LIBRE DE BRUXELLES

Configuration de base sécurisée pour macOS

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 Mac sécurisé

Saviez-vous que même si votre Mac 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 macOS 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 Apple Mac 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. Les utilisateurs de macOS doivent utiliser La solution fournie par l'institution « **Microsoft Defender for Endpoint** ». [1]

Sur un Apple Mac 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 macOS 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 **« Software Update »** soit actif et exécuté périodiquement :

3.1 Enable Auto Update - Activer la mise à jour automatique

Remediation - Remédiation:
Perform the following to implement the prescribed state:
Effectuez les opérations suivantes pour mettre en œuvre l'état prescrit :

[1] https://support.ulb.be/en/web/support/-/comment-telecharger-windows-defender-atp-sur-macos-/4.2

Graphical method – Méthode graphique :

1. Ouvrez les Préférences Système
2. Sélectionnez la mise à jour du logiciel
3. Sélectionnez Avancé
4. Vérifiez que Vérifier les mises à jour est sélectionné

1. Open System Preferences
2. Select Software Update
3. Select Advanced
4. Verify that Checkfor updates is selected

Alternatively - Alternativement:
Run the following command in Terminal:
Exécutez la commande suivante dans le Terminal

```
sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate
AutomaticCheckEnabled -int 1
```

Impact:
Without automatic update, updates may not be made in a timely manner and the system will be exposed to additional risk.
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

3.2 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 Apple:
https://developer.apple.com/documentation/macos-release-notes

Les versions majeures de macOS sont désormais publiées une fois par an et généralement maintenues pendant trois ans.
Major versions of macOS are released once a year now, and usually maintained for three years.

3.3 Enable system data files and security update installs – Activer les fichiers de données système et les installations de mise à jour de sécurité

Remediation - Remédiation:
Perform the following to implement the prescribed state:
Effectuez les opérations suivantes pour mettre en œuvre l'état prescrit:

Graphical method – Méthode graphique :

1. Ouvrez les Préférences Système
2. Sélectionnez Mises à jour logicielles
3. Sélectionnez Avancé
4. Vérifiez que Installer les fichiers de données système et les mises à jour de sécurité est sélectionné

1. Open System Preferences
2. Select Software Updates
3. Select Advanced
4. Verify that Install system data files and security updates is selected

Alternatively - Alternativement:
Run the following command in Terminal:
Exécutez la commande suivante dans le Terminal

```
sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate
ConfigDataInstall -bool true && sudo defaults write
/Library/Preferences/com.apple.SoftwareUpdate CriticalUpdateInstall -bool
true
```

Impact:
Unpatched software may be exploited
Un logiciel non corrigé présente des vulnérabilités qui peuvent être exploitées

3.4 Enable macOS update installs – Activer les installations de mise à jour macOS

Remediation - Remédiation:
Perform the following to implement the prescribed state:
Effectuez les opérations suivantes pour mettre en œuvre l'état prescrit:

Graphical method – Méthode graphique :

1. Ouvrez les Préférences Système
2. Sélectionnez Mises à jour logicielles
3. Sélectionnez Avancé
4. Vérifiez que Installer les mises à jour macOS est sélectionné

1. Open System Preferences
2. Select Software Updates
3. Select Advanced
4. Verify that Install macOS updates is selected

Alternatively - Alternativement:
Run the following command in Terminal:
Exécutez la commande suivante dans le Terminal

```
sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate
AutomaticallyInstallMacOSUpdates -bool true
```

Impact:
Unpatched software may be exploited.
Un logiciel non corrigé présente des vulnérabilités qui peuvent être exploitées.

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

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

Remediation - Remédiation:
Perform the following to implement the prescribed state:
Effectuez les opérations suivantes pour mettre en œuvre l'état prescrit:

```
1. Open System Preferences
1. Ouvrez les Préférences Système

2. Select Desktop & Screen Saver
2. Sélectionnez Bureau et économiseur d'écran

3. Select Screen Saver
3. Sélectionnez économiseur d'écran

4. Set Start after to 20 minutes or less
4. Réglez Démarrer après 20 minutes ou moins
```

Alternatively - Alternativement:
Run the following commands in Terminal:
Exécutez les commandes suivantes dans le Terminal

```
defaults -currentHost write com.apple.screensaver idleTime -int 600
defaults -currentHost write com.apple.screensaver idleTime -int 1200
```

Choose either 10 minutes (600) or 20 minutes (1200).
Choisissez entre 10 minutes (600) ou 20 minutes (1200).

Impact:
If the screensaver is not set users may leave the computer available for an unauthorized person to access information.
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

Si votre Mac dispose encore d'un Disque Dur (Hard Disk), nous vous recommandons de remplacer votre HDD pour Hard Drive Disk (ou disque dur mécanique) par un SSD pour Solid State Drive (ou disque à mémoire flash). Notre Atelier Informatique peut vous assister pour cette opération :

https://atelierinformatique.ulb.be/

5.1.1 Enable FileVault - Activer FileVault (natif)

Remediation- Remédiation:
Perform the following to implement the prescribed state:
Effectuez les opérations suivantes pour mettre en œuvre l'état prescrit:

```
1. Open System Preferences
1. Ouvrez les Préférences Système

2. Select Security & Privacy
2. Sélectionnez Sécurité et confidentialité

3. Select FileVault
3. Sélectionnez FileVault

4. Select Turn on FileVault
4. Sélectionnez Activer FileVault
```

Impact:
Mounting a « **FileVaulted** » volume from an alternate boot source will require a valid password to decrypt it.
Le montage d'un volume « **FileVaulted** » à partir d'une autre source de démarrage nécessitera un mot de passe valide pour le déchiffrer.

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.

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** ».

5.2 Enable Gatekeeper - Activer le Gatekeeper

Remediation - Remédiation:
Perform the following to implement the prescribed state:
Effectuez les opérations suivantes pour mettre en œuvre l'état prescrit:

```
1. Open System Preferences
1. Ouvrez les Préférences Système

2. Select Security & Privacy
2. Sélectionnez Sécurité et confidentialité

3. Sélectionnez Général
3. Select General

4. Select Allow applications downloaded from: Mac App Store and identified
developers
4. Sélectionnez Autoriser les applications téléchargées depuis: Mac App
Store et développeurs identifiés
```

Alternatively- Alternativement
Perform the following to ensure the system is configured as:
Procédez comme suit pour vous assurer que le système est configuré comme:

```
1. Run the following command in Terminal:
1. Exécutez la commande suivante dans le Terminal:

sudo spctl --master-enable
```

5.3 Enable Firewall - Activer le pare-feu

Remediation - Remédiation:
Perform the following to implement the prescribed state:
Effectuez les opérations suivantes pour mettre en œuvre l'état prescrit:

```
1. Open System Preferences
1. Ouvrez les Préférences Système

2. Select Security & Privacy
2. Sélectionnez Sécurité et confidentialité

3. Select Firewall
3. Sélectionnez Pare-feu

4. Select Turn On Firewall
4. Sélectionnez Activer le pare-feu
```

Alternatively - Alternativement:
Run the following command in Terminal:
Exécutez la commande suivante dans le Terminal

```
defaults write /Library/Preferences/com.apple.alf globalstate - int <value>
2. Where <value> is:
    • 1 = on for specific services
    • 2 = on for essential services
```

<value> = VALEUR est:

- *1 = activé pour des services spécifiques*
- *2 = activé pour les services essentiels*

Impact:
The firewall may block legitimate traffic.
Le pare-feu peut bloquer le trafic légitime.

5.4 Enable Location Services - Activer les services de localisation

Remediation - Remédiation:
Perform the following to enable location services:
Procédez comme suit pour activer les services de localisation :

Graphical Method: - Méthode graphique:

```
1. Open System Preferences
1. Ouvrez Préférences Système

2. Select Security & Privacy
2. Sélectionnez Sécurité et confidentialité

3. Select Privacy
3. Sélectionnez Confidentialité

4. Select Enable Location Services
4. Sélectionnez Activer les services de localisation
```

Terminal Method: - Méthode terminal:
Exécutez la commande suivante pour activer les services de localisation
Run the following command to enable location services

```
$ sudo launchctl load -w
/System/Library/LaunchDaemons/com.apple.locationd.plist
```

Note : - Remarque:
In some use cases organisations may not want Location Services running. To disable location services, System Integrity Protection must be disabled.
Dans certains cas d'utilisation, les organisations peuvent ne pas souhaiter que les services de localisation soient exécutés. Pour désactiver les services de localisation, la protection de l'intégrité du système doit être désactivée

6 iCloud

Préalablement à l'utilisation de iCloud, veuillez « Créer votre identifiant Apple (AppleID) »
https://support.apple.com/fr-fr/HT204316
Seule recommandation lors de la création votre identifiant, préférez votre adresse email privée plutôt que professionnelle.

7 Time Machine

Time Machine permet de sauvegarder l'intégralité du contenu présent sur votre Mac : les photos, vidéos, fichiers texte, applications, logiciels, fichiers systèmes, et même vos préférences. Time Machine effectue une sauvegarde selon une fréquence prédéfinie, sans engendrer de charge supplémentaire. Avant toute chose, sachez qu'il est vivement recommandé d'investir dans un disque dur externe compatible pour MacOS.
Idéalement, la capacité de stockage de ce disque dur externe doit être +/- 2 fois la taille de votre disque interne.

7.1 Time Machine Auto-Backup – Sauvegarde automatique Time Machine

Remediation - Remédiation:
Perform the following to enable Time Machine:
Procédez comme suit pour activer Time Machine:

Graphical Method: - Méthode graphique:

```
1. Open System Preferences
1. Ouvrez les Préférences Système

2. Select Time Machine
2. Sélectionnez Time Machine

3. Select Back Up Automatically
3. Sélectionnez Sauvegarder automatiquement

4. Select the drive to use for Time Machine
4. Sélectionnez le lecteur à utiliser pour Time Machine
```

Terminal Method: - Méthode terminal:
Run the following enable Time Machine:
Exécutez l'activation suivante de Time Machine:

```
$ sudo sudo tmutil setdestination -a /Volumes/<volumename>
$ sudo tmutil enable

example:
$ sudo tmutil setdestination -a /Volumes/TimeMachineDrive/
$ sudo tmutil enable
```

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

8.1 Secure Home Folders - Dossiers personnels sécurisés

Remediation - Remédiation:
For each user, run the following command to secure all home folders:
Pour chaque utilisateur, exécutez la commande suivante pour sécuriser tous les dossiers personnels:

```
$ sudo chmod -R og-rwx /Users/<username>
```

Alternately, run the following command if there needs to be executable access for a home folder:
Sinon, exécutez la commande suivante si un accès « exécutable » pour un dossier personnel est nécessaire:

```
$ sudo chmod -R og-rw /Users/<username>
```

example - Exemple:

```
$ sudo chmod -R og-rw /Users/thirduser/
$ sudo chmod -R og-rwx /Users/fourthuser/
# ls -l /Users/
total 0
drwxr-xr-x+ 12 Guest _guest 384 24 Jul 13:42 Guest
drwxrwxrwt 4 root wheel 128 22 Jul 11:00 Shared
drwx--x--x+ 18 firstuser staff 576 10 Aug 14:36 firstuser
drwx--x--x+ 15 seconduser staff 480 10 Aug 09:16 seconduser
drwx--x--x+ 11 thirduser staff 352 10 Aug 14:53 thirduser
drwx------+ 11 fourthuser staff 352 10 Aug 14:53 fourthuser
```

9 Password Management - Gestion mots de passe

9.1 Complex passwords must uppercase and lowercase letters - Les mots de passe complexes doivent être majuscules et minuscules

Remediation - Remédiation:
Run the following command to set passwords to require at upper and lower case letter:
Exécutez la commande suivante pour définir les mots de passe à exiger en majuscules et minuscules

```
$ sudo pwpolicy -n /Local/Default -setglobalpolicy
"requiresMixedCase=<value≥1>"
```

example - Exemple:

```
$ sudo pwpolicy -n /Local/Default -setglobalpolicy "requiresMixedCase=1"
```

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.)

9.2 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.

9.2.1 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 Do not enable the « root » account – Ne pas activer le compte « root »

Remediation - Remédiation:
Perform the following to ensure that the root user is disabled:
Procédez comme suit pour vous assurer que l'utilisateur « root » est désactivé

Graphical Method - Méthode graphique:

```
1. Open /System/Library/CoreServices/Applications/Directory Utility
1. Ouvrez /System/Library/CoreServices/Applications/Directory Utility

2. Click the lock icon to unlock the service
2. Cliquez sur l'icône de verrouillage pour déverrouiller le service

3. Click Edit
3. Cliquez sur Modifier

4. Click Disable root User
4. Cliquez sur Désactiver l'utilisateur root
```

Terminal Method - Méthode terminal:
Run the following command to disable the « root » user:
Exécutez la commande suivante pour désactiver l'utilisateur « root »

```
$ sudo dsenableroot -d
username = root
user password:
```

10.1 Disable automatic login - Désactiver la connexion automatique

Remediation - Remédiation:
Perform the following to set automatic login to off:
Procédez comme suit pour désactiver la connexion automatique:

Graphical Method - Méthode graphique:

```
1. Open System Preferences
1. Ouvrez les Préférences Système

2. Select Users & Groups
2. Sélectionnez Utilisateurs et groupes

3. Click the lock to authenticate
3. Cliquez sur le verrou pour vous authentifier

4. Select Login Options
4. Sélectionnez les options de connexion

5. Select Automatic login and set it to Off
5. Sélectionnez Connexion automatique et réglez-le sur Désactivé
```

Terminal Method - Méthode terminal:

Run the following command to disable automatic login:
Exécutez la commande suivante pour désactiver la connexion automatique:

```
$ sudo defaults delete /Library/Preferences/com.apple.loginwindow
autoLoginUser
```

10.2 Require a password to wake the computer from sleep or screen saver – Exiger un mot de passe pour sortir l'ordinateur du mode veille ou de l'économiseur d'écran

Remediation - Remédiation:
Perform the following enable a password for unlock after a screen saver begins:
Procédez comme suit pour activer un mot de passe pour le déverrouillage lors d'un économiseur d'écran:

```
1. Open System Preferences    1. Ouvrez les Préférences Système

2. Select Security & Privacy  2. Sélectionnez Sécurité et confidentialité

3. Select General             3. Sélectionnez Général

4. Set Require password after or screensaver begins with a time of ≤5
minutes (immediately or 5 seconds is recommended)
4. Définissez Exiger un mot de passe après ou l'économiseur d'écran
commence avec une durée ≤5 minutes (immédiatement ou 5 secondes est
recommandé)
```

10.3 Do not enter a password-related hint Ne saisissez pas d'indication relative au mot de passe

Remediation – Remédiation :
Perform the following to remove users' password hint:
Procédez comme suit pour supprimer l'indice de mot de passe des utilisateurs :

Graphical Method - Méthode graphique:

```
1. Open System Preferences
1. Ouvrez les Préférences Système

2. Select Users & Groups
2. Sélectionnez Utilisateurs et groupes

3. Select the Current User
3. Sélectionnez l'utilisateur actuel

4. Select Change Password
4. Sélectionnez Modifier le mot de passe

5. Change the password and ensure that no text is entered in the Password
hint box
5. Modifiez le mot de passe et assurez-vous qu'aucun texte n'est entré dans
la zone Indice de mot de passe
```

Terminal Method - Méthode terminal:
Run the following command to remove a user's password hint:
Exécutez la commande suivante pour supprimer l'indice de mot de passe d'un utilisateur :

```
$ sudo dscl . -delete /Users/<username> hint
```

Example - Exemple:

```
$ sudo dscl . -delete /Users/firstuser hint
$ sudo dscl . -delete /Users/seconduser hint
```

11 Disable « Show password hints » - Désactiver « Afficher les indices de mot de passe »

Remediation – Remédiation :
Perform the to disable password hints from being shown:
Exécutez la pour désactiver l'affichage des conseils de mot de passe :

Graphical Method - Méthode graphique:

```
1. Open System Preferences
1. Ouvrez les Préférences Système

2. Select Users & Groups
2. Sélectionnez Utilisateurs et groupes

3. Select Login Options
3. Sélectionnez les options de connexion

4. Uncheck Show password hints
4. Décochez Afficher les indices de mot de passe
```

Terminal Method - Méthode terminal:
Run the following command to disable password hints:
Exécutez la commande suivante pour désactiver les indices de mot de passe:

```
$ sudo defaults write
/Library/Preferences/com.apple.loginwindowRetriesUntilHint -int 0
```

11.1 Disable guest account login – Désactiver la connexion au compte invité

Remediation - Remédiation:
Perform the following to disable guest account availability:
Procédez comme suit pour désactiver la disponibilité du compte invité:

Graphical Method - Méthode graphique:

```
1. Open System Preferences
1. Ouvrez les Préférences Système

2. Select Users & Groups
2. Sélectionnez Utilisateurs et groupes

3. Select Guest User
3. Sélectionnez l'utilisateur invité

4. Uncheck Allow guests to log in to this computer
4. Décochez Autoriser les invités à se connecter à cet ordinateur.
```

Terminal Method - Méthode terminal:
Run the following command to disable the guest account:
Exécutez la commande suivante pour désactiver le compte invité :

```
$ sudo defaults write /Library/Preferences/com.apple.loginwindow
GuestEnabled -bool false
```

11.2 Disable « Allow guests to connect to shared folders » - Désactiver « Autoriser les invités à se connecter aux dossiers partagés »

Remediation - Remédiation:
Perform the following to no longer allow guest user access to shared folders:
Procédez comme suit pour ne plus autoriser l'accès des utilisateurs invités aux dossiers partagés:

Graphical Method - Méthode graphique:

```
1. Open System Preferences
1. Ouvrez les Préférences Système

2. Select Users & Groups
2. Sélectionnez Utilisateurs et groupes

3. Select Guest User
3. Sélectionnez l'utilisateur invité

4. Uncheck Allow guests to connect to shared folders
4. Décochez Autoriser les invités à se connecter aux dossiers partagés
```

Terminal Method - Méthode terminal:
Run the following commands to verify that shared folders are not accessible to guest users:
Exécutez les commandes suivantes pour vérifier que les dossiers partagés ne sont pas accessibles aux utilisateurs invités:

```
$ sudo defaults write /Library/Preferences/com.apple.AppleFileServer
guestAccess -bool false
$ sudo defaults write
/Library/Preferences/SystemConfiguration/com.apple.smb.server
AllowGuestAccess -bool false
```

11.3 Disable the automatic run of safe files in Safari – Désactiver l'exécution automatique des fichiers sécurisés dans Safari

Remediation - Remédiation:
Perform the following to set safe files to not open after downloading in Safari:
Procédez comme suit pour que les fichiers sécurisés ne s'ouvrent pas après le téléchargement dans Safari:

Graphical Method - Méthode graphique:

```
1. Open Safari
1. Ouvrez Safari

2. Select Safari from the menu bar
2. Sélectionnez Safari dans la barre de menus

3. Select Preferences
3. Sélectionnez Préférences

4. Select General
4. Sélectionnez Général

5. Uncheck Open "safe" files after downloading
5. Décochez Ouvrir les fichiers «sûrs» après le téléchargement
```

Terminal Method - Méthode terminal:
Run the following command to disable safe files from not opening in Safari:
Exécutez la commande suivante pour empêcher les fichiers sécurisés de ne pas s'ouvrir dans Safari:

```
$ sudo -u <username> defaults write
/Users/<username>/Library/Preferences/com.apple.Safari
AutoOpenSafeDownloads -bool false
```

```
Example - Exemple:
$ sudo -u firstuser defaults write
/Users/firstuser/Library/Preferences/com.apple.Safari AutoOpenSafeDownloads
-bool false
```

12 FileVault and Local Account Password Reset using AppleID FileVault – Réinitialisation du mot de passe du compte local à l'aide de l'identifiant Apple

Apple propose depuis plusieurs années des services permettant à un utilisateur de réinitialiser un compte local et son mot de passe en utilisant leur identifiant Apple et un service pour stocker le Mot de passe Maître « **FileVault** » qui serait contrôlé par l'accès à un identifiant Apple.

12.1 Chiffrement du disque de démarrage d'un Mac à l'aide de « FileVault »

https://support.apple.com/fr-be/HT204837
https://support.apple.com/en-us/HT204837

13 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. Lorsque vous copiez et exécutez un fichier contenant un virus, vous pouvez non seulement infecter votre propre Mac, 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 **App Store** de votre macOS
- Installez vos apps de Mac automatiquement! https://macapps.link/
- List of Macintosh software: https://www.wikiwand.com/en/List_of_Macintosh_software
- Pour les plus expérimentés **Brew** : https://brew.sh/index_fr

14 Références

CIS - Center For Internet Security CIS Apple macOS 11.0 Benchmark v1.1.0
https://downloads.cisecurity.org/?bypassToken=zrcxFuY5xcKHFXEhL6ffC5hNpKn0Ij6f#/

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