

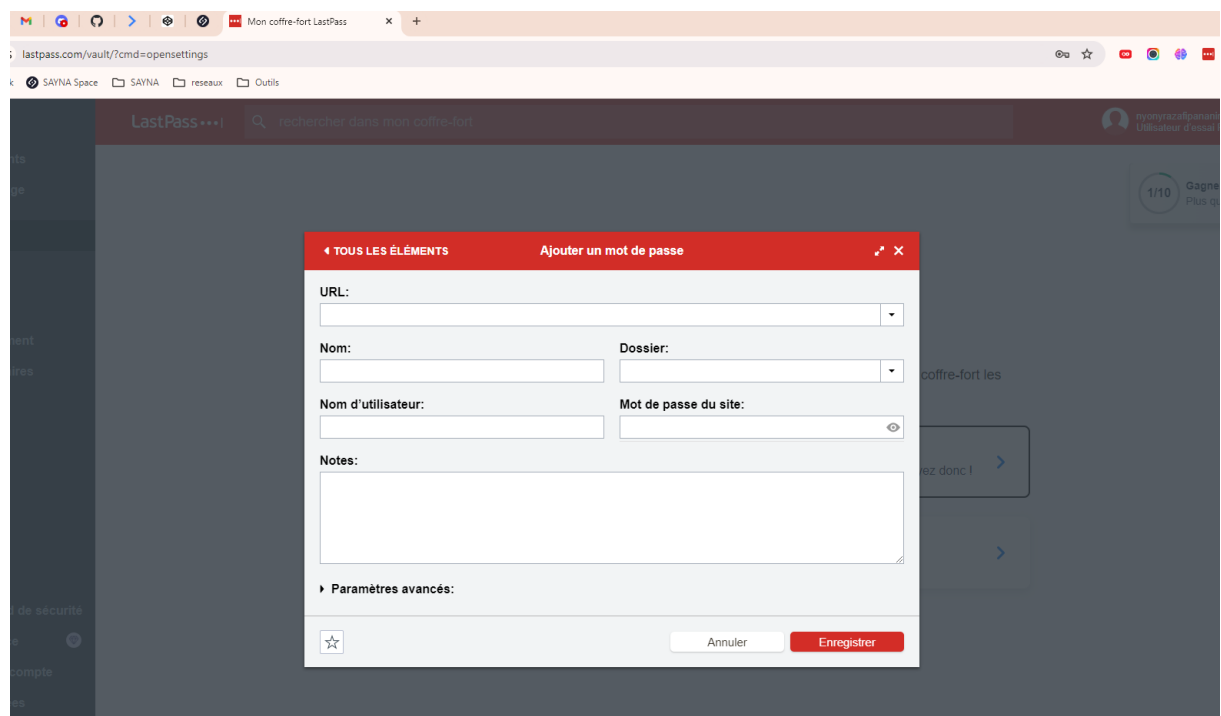
1 - Introduction à la sécurité sur Internet

1/ Voici les articles que j'ai retenu (avec les mots-clés "sécurité sur internet" et "comment être en sécurité sur internet" :

- Article 1 : cybermalveillance.gouv.fr -Les 10 règles de base pour la sécurité numérique.
- Article 2 : malwarebytes.com – Conseils de sécurité sur internet :Ce qu'il faut faire et ce qu'il ne faut pas faire
- Article 3 : safetyculture.com – Guide complet de la sécurité sur Internet

2 - Créer des mots de passe forts

*coffre LastPass



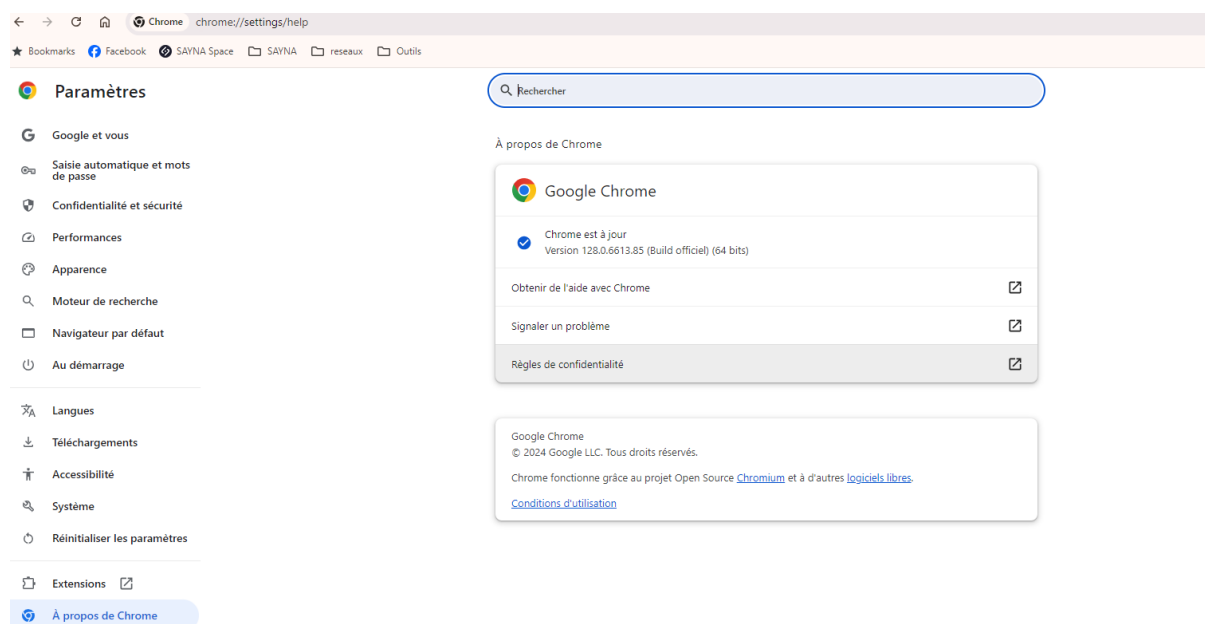
3 - Fonctionnalité de sécurité de votre navigateur

1/ Les sites web qui semblent être malveillants sont :

- www.morvel.com, un dérivé de www.marvel.com
- www.fessebook.com, un dérivé de www.facebook.com
- www.instagramam.com, un dérivé de www.instagram.com

2/ Vérification de mise à jour :

*Pour Chrome :



*Pour Firefox :

Mises à jour de Firefox

Conservez Firefox à jour pour bénéficier des dernières avancées en matière de performances, de stabilité et de sécurité.

Version 129.0.2 (32 bits) [Notes de version](#)

[Afficher l'historique des mises à jour...](#)

😊 Firefox est à jour

[Rechercher des mises à jour](#)

Autoriser Firefox à

☒ Installer les mises à jour automatiquement (recommandé)

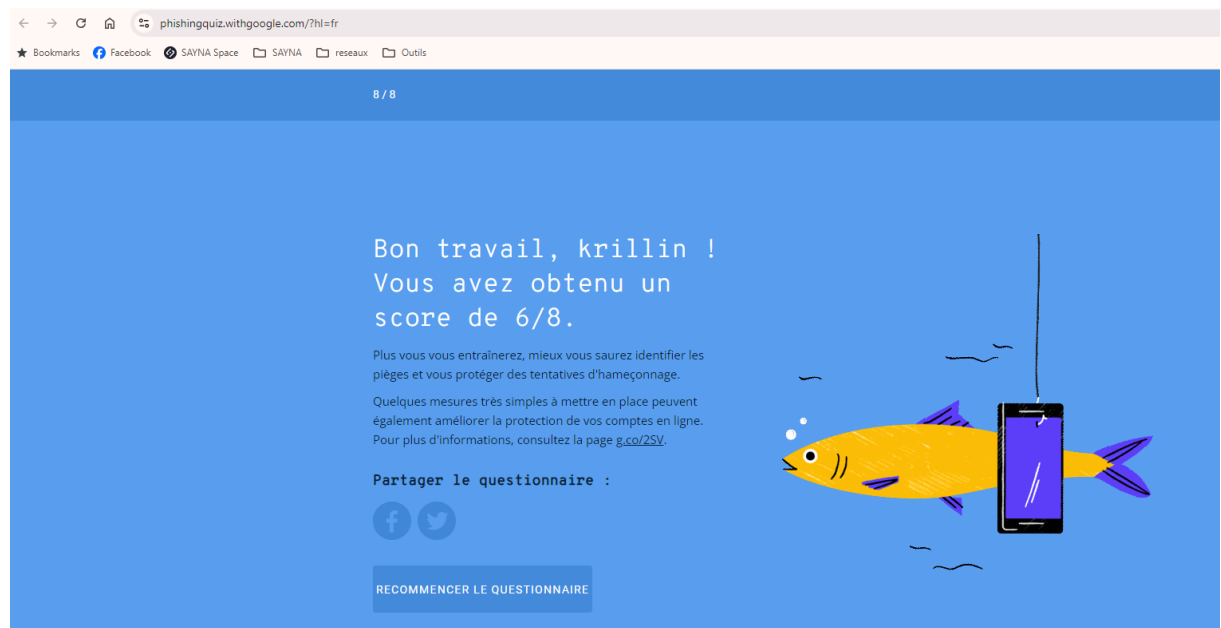
☒ Quand Firefox n'est pas lancé

☐ Vérifier l'existence de mises à jour, mais vous laisser décider de leur installation

① Ce paramètre s'appliquera à tous les comptes Windows et profils Firefox utilisant cette installation de Firefox.

4 - Éviter le spam et le phishing

1/ Exercice de détection de Spam et Phishing :

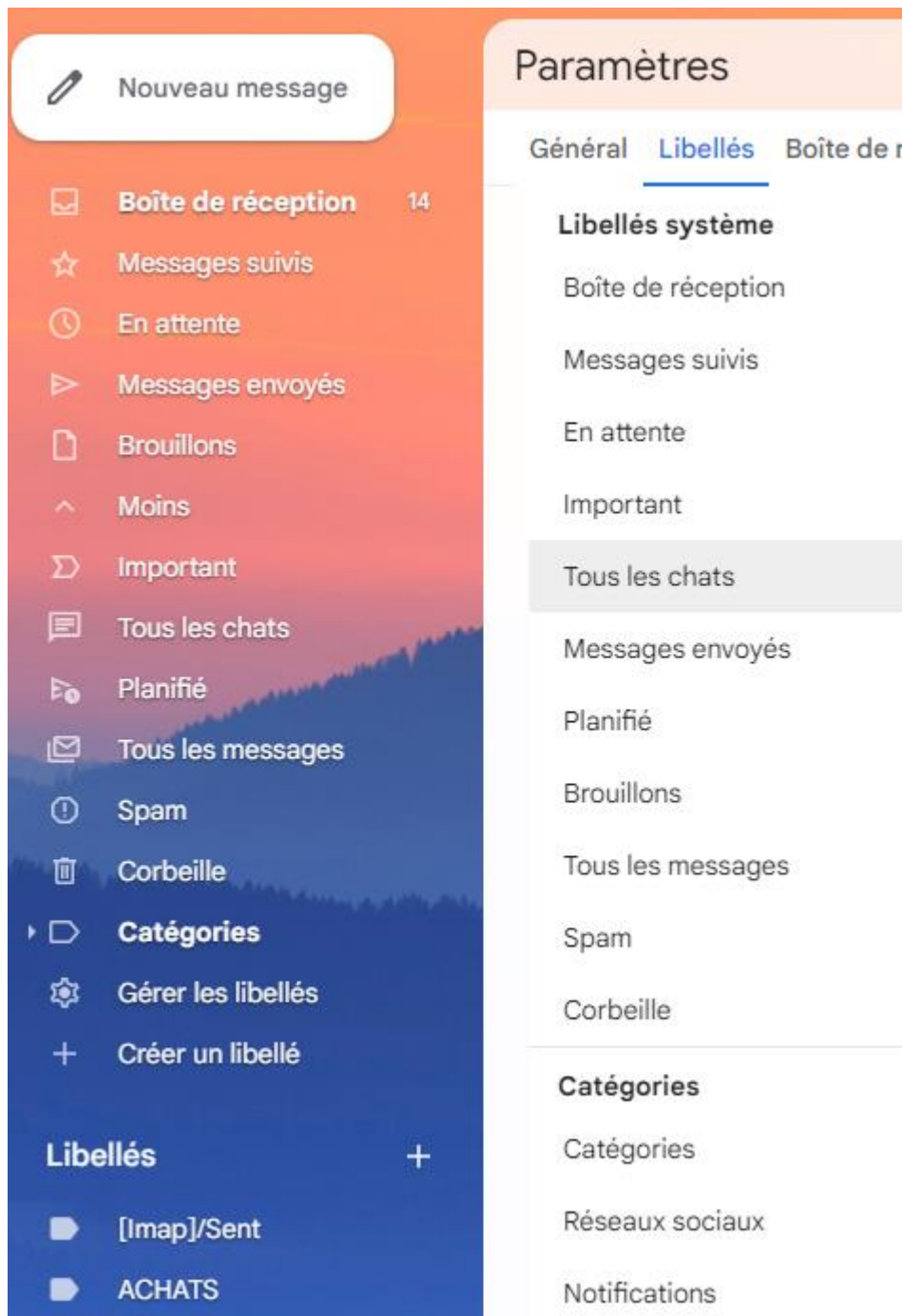


5 - Comment éviter les logiciels malveillants

3/ indicateur de sécurité et outil Google :

- Site 1 : <https://ww1.vostfree.tv/?usid=17&utid=34214388612>
 - Indicateur de sécurité :HTTPS
 - Analyse Google : Aucun contenu suspect
- Site 2 : <https://www.tv5monde.com/>
 - Indicateur de sécurité :HTTPS
 - Analyse Google : Aucun contenu suspect
- Site 3 : <https://www.baidu.com/>
 - Indicateur de sécurité :HTTPS
 - Analyse Google : Vérifier une URL en particulier

6 - Achats en ligne sécurisés



7 - Comprendre le suivi du navigateur

8 - Principes de base de la confidentialité des médias sociaux

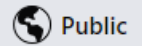
*publication publiques :

Followers et contenu public

Qui peut me suivre

Vos followers voient vos publications, reels et stories dans le Fil. Vos ami(e)s suivent vos publications, reels et stories par défaut, mais vous pouvez aussi autoriser quiconque ne faisant pas partie de vos ami(e)s à suivre vos publications, reels et stories publics. Utilisez ce paramètre pour choisir qui peut vous suivre.

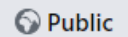
Chaque fois que vous créez ou publiez un reel ou une story, vous choisissez l'audience avec laquelle vous voulez les partager.



Ce paramètre ne s'applique pas aux personnes qui vous suivent sur Marketplace et dans les groupes d'achat et de vente. Vous pouvez gérer ces paramètres sur Marketplace.

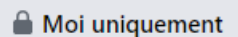
Les profils en mode professionnel sont configurés sur Public afin que tout le monde puisse vous suivre. Pour modifier ce paramètre, vous devrez désactiver le mode professionnel.

Qui peut voir vos followers sur votre journal ?



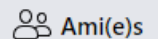
Qui peut voir les personnes, Pages et listes que vous suivez ?

N'oubliez pas que les personnes que vous suivez le savent.



Qui peut commenter vos publications publiques ?

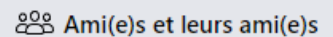
Choisissez qui est autorisé à commenter vos publications publiques. Il se peut que les personnes identifiées dedans et leurs ami(e)s puissent toujours les commenter. **En savoir plus**



Vous pouvez mettre à jour cette option sur chaque publication sans affecter les paramètres de votre compte.

Notifications de publications publiques

Vous pouvez recevoir des notifications lorsque des personnes qui ne font pas partie de vos ami(e)s commencent à vous suivre et partagent, aiment ou commentent vos publications publiques.



*Confidentialité :

Paramètres personnalisés



Qui peut voir vos futures publications ?

Ami(e)s

Qui peut voir vos stories ?

Ami(e)s sauf...

Qui peut voir vos reels ?

Ami(e)s

Qui peut commenter vos publications publiques ?

Ami(e)s

Informations de profil publiques

Ami(e)s et leurs ami(e)s

Qui peut voir les personnes, Pages et listes que vous suivez ?

Moi uniquement

9 - Que faire si votre ordinateur est infecté par un virus

Objectif :

1/Exercices pour vérifier la sécurité et comment procéder :

1. Faire l'Analyse Antivirus :

But : Détecter et supprimer les virus existants.

Process : Téléchargez et installez un logiciel antivirus réputé (comme Avast, Bitdefender, ou Kaspersky). Suivre les instructions puis exécutez une analyse complète du système.

2. Vérifier les Mises à Jour :

Assurer que votre appareil est protégé contre les vulnérabilités connues.

Etapes : Vérifiez que votre système d'exploitation et tous vos logiciels sont à jour dans les paramètres . Activez les mises à jour automatiques.

3. Vérification des Permissions des Applications

Identifier les applications qui pourraient avoir des permissions excessives.

Passez en revue les logiciels installés et désinstallez ceux que vous n'utilisez pas ou qui semblent suspects.

4. Faire des exercices de Phishing

Tester votre capacité à identifier les tentatives de phishing.

Utilisez des outils en ligne comme PhishMe ou des simulateurs de phishing pour vous entraîner à reconnaître les emails et les liens suspects.

5. Vérification des Réseaux Wi-Fi

Assurer que votre connexion réseau est sécurisée.

Utilisez des outils comme Wireshark pour analyser le trafic réseau et vérifier qu'il n'y a pas d'activités suspectes. Assurez-vous que votre réseau Wi-Fi est protégé par un mot de passe fort et utilisez le chiffrement WPA3 si possible.

6. Faites des Sauvegardes Régulières

Cela est utile pour Protéger vos données en cas d'infection.

Configurez des sauvegardes automatiques de vos données importantes sur un support externe ou un service de cloud sécurisé.

2/ Exercice pour installer et utiliser un antivirus + antimalware :

1. Tout d'abord Téléchargez « Malwarebytes » depuis le site officiel

[Malwarebytes](<https://www.malwarebytes.com/fr/mwb-download>).

- Ensuite ,ouvrez le fichier téléchargé (`mbsetup.exe`) et suivez les instructions à l'écran pour installer le logiciel.

- Acceptez les termes et conditions, puis cliquez sur « Installer ».

2. Pour la Configuration et Utilisation

- Lancez Malwarebytes après l'installation.

- Cliquez sur « Scan » pour effectuer une analyse complète de votre système.

- Examinez les résultats : Une fois l'analyse terminée, Malwarebytes affichera une liste des menaces détectées.

- Supprimez les menaces: Cliquez sur « Quarantine » pour mettre en quarantaine les menaces détectées, puis redémarrez votre ordinateur si nécessaire.