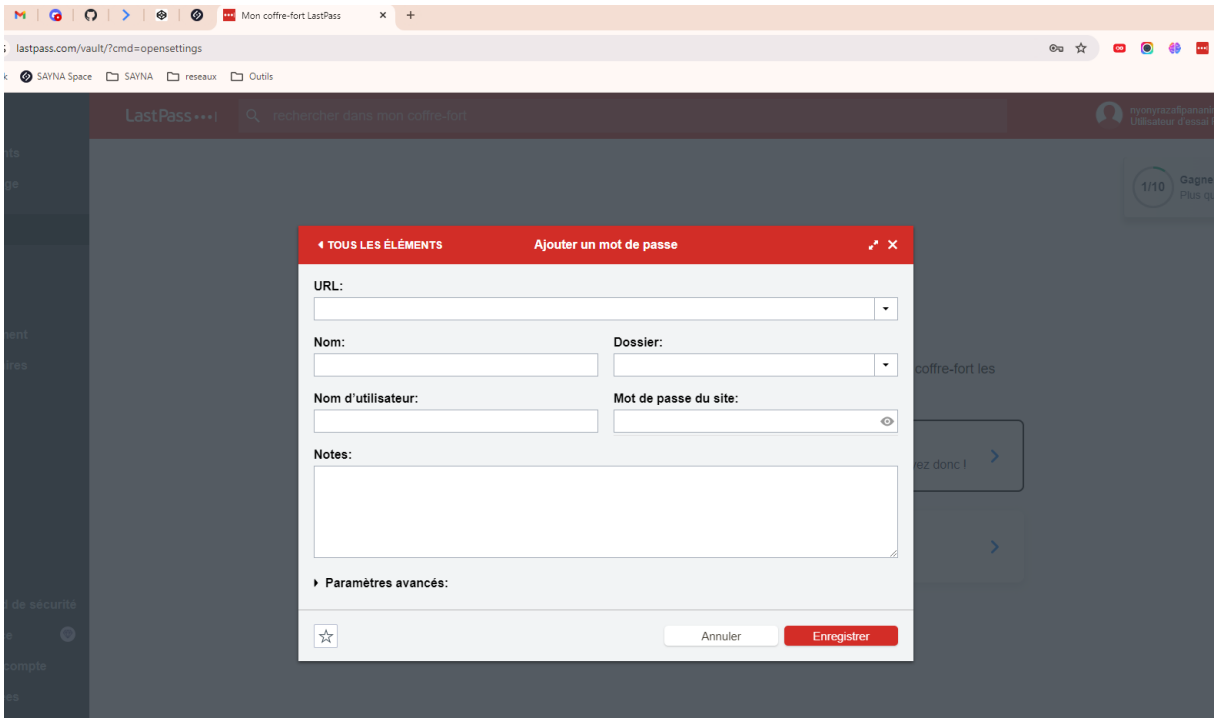
1 - Introduction à la sécurité sur Internet

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



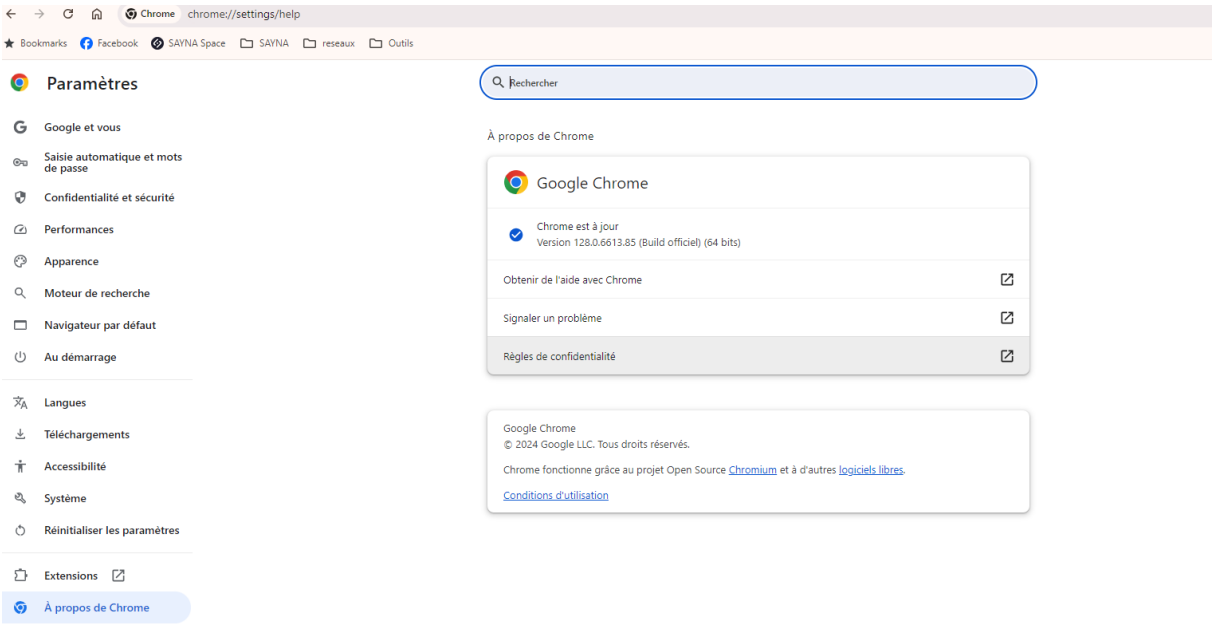
3 - Fonctionnalité de sécurité de votre navigateur

1/ Les sites web qui semblent être malveillants sont :

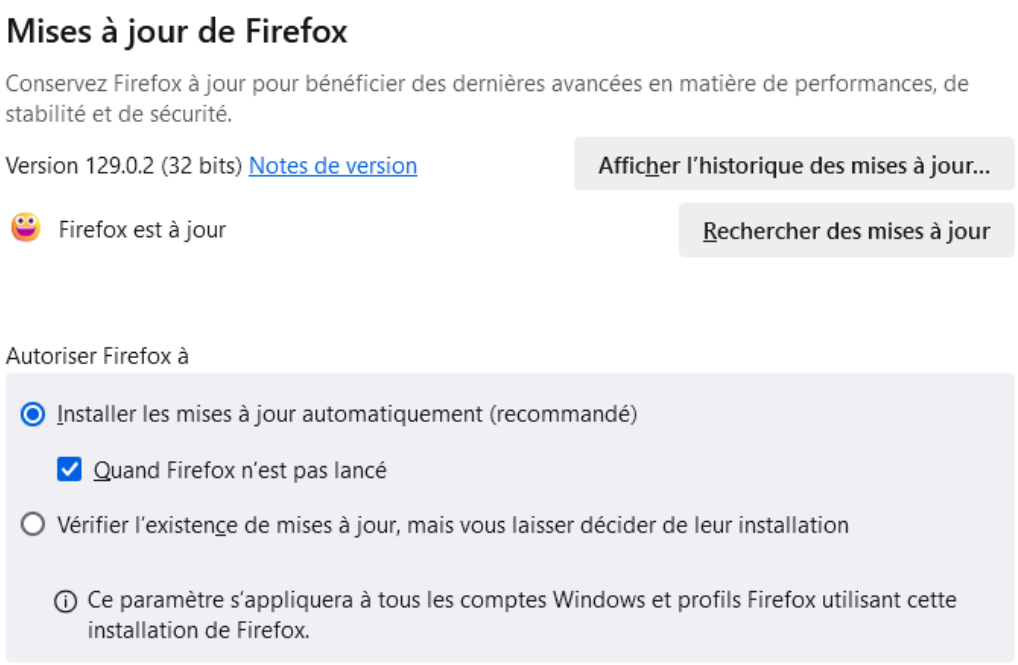
- www.morvel.com, un dérivé de www.marvel.com
- www.fessebook.com, un dérivé de www.facebook.com
- www.instagam.com, un dérivé de www.instagram.com

2/ Vérification de mise à jour :

*Pour Chrome :

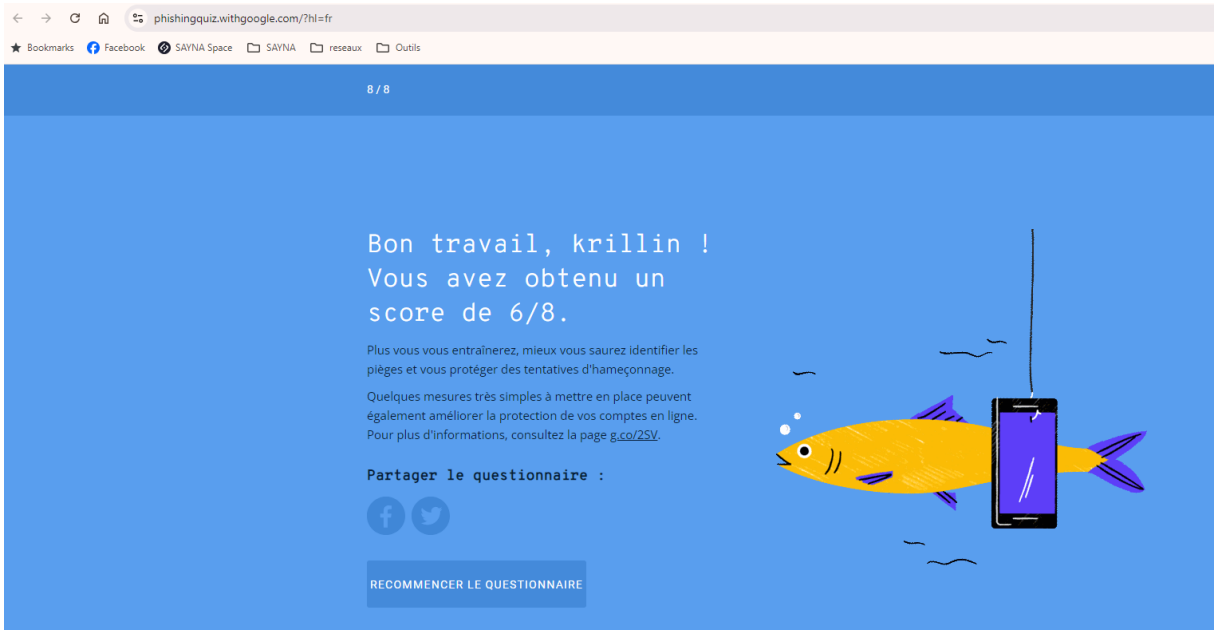


*Pour Firefox :



4 - Éviter le spam et le phishing

1/ Exercice de détection de Spam et Phishing :

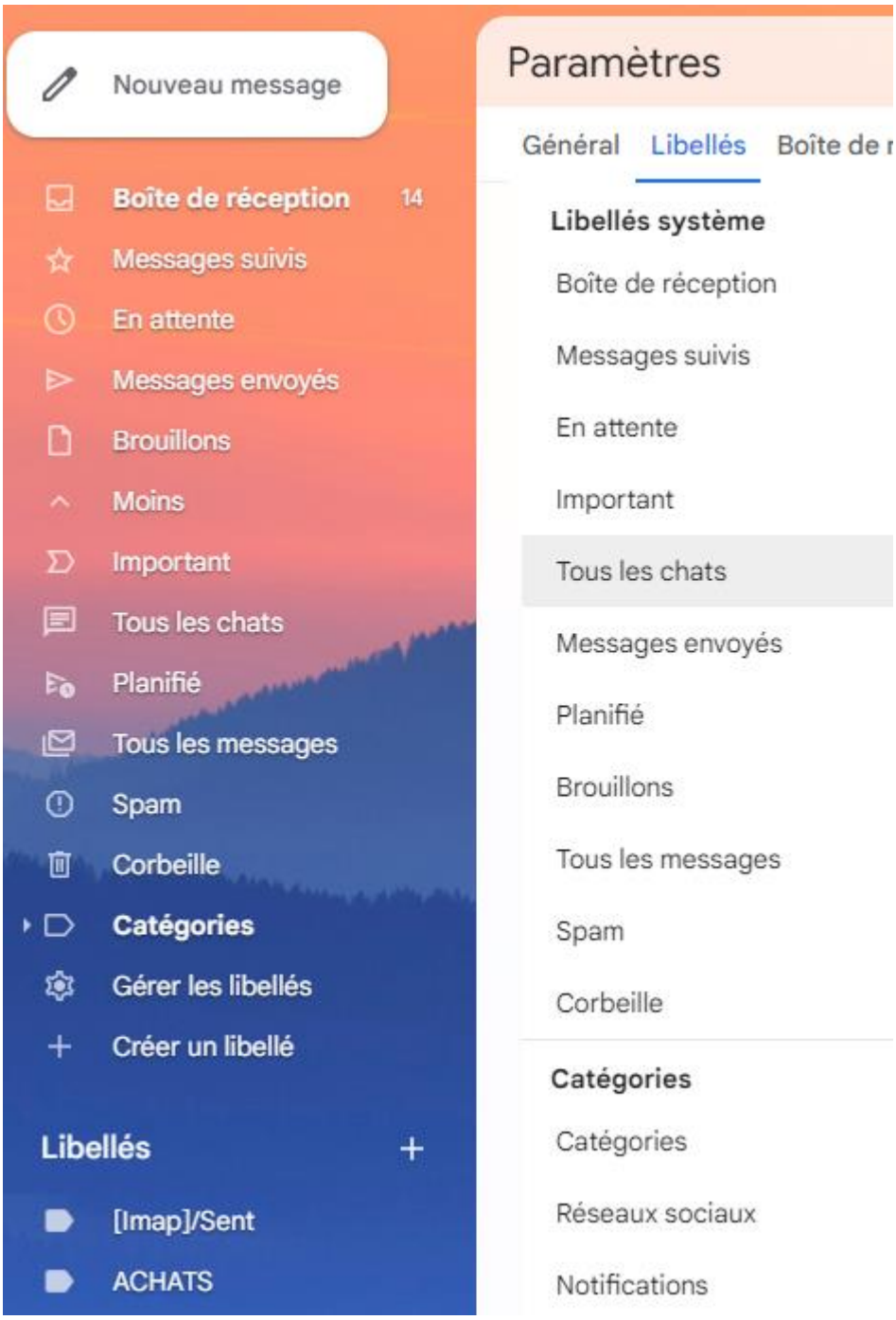


5 - Comment éviter les logiciels malveillants

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 **<u>- Comprendre le suivi du navigateur</u>**

8 **<u>- Principes de base de la confidentialité des médias sociaux</u>**

*publication publiques :

*Confidentialité :

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.