SAYNA SECURITE PROJET 1

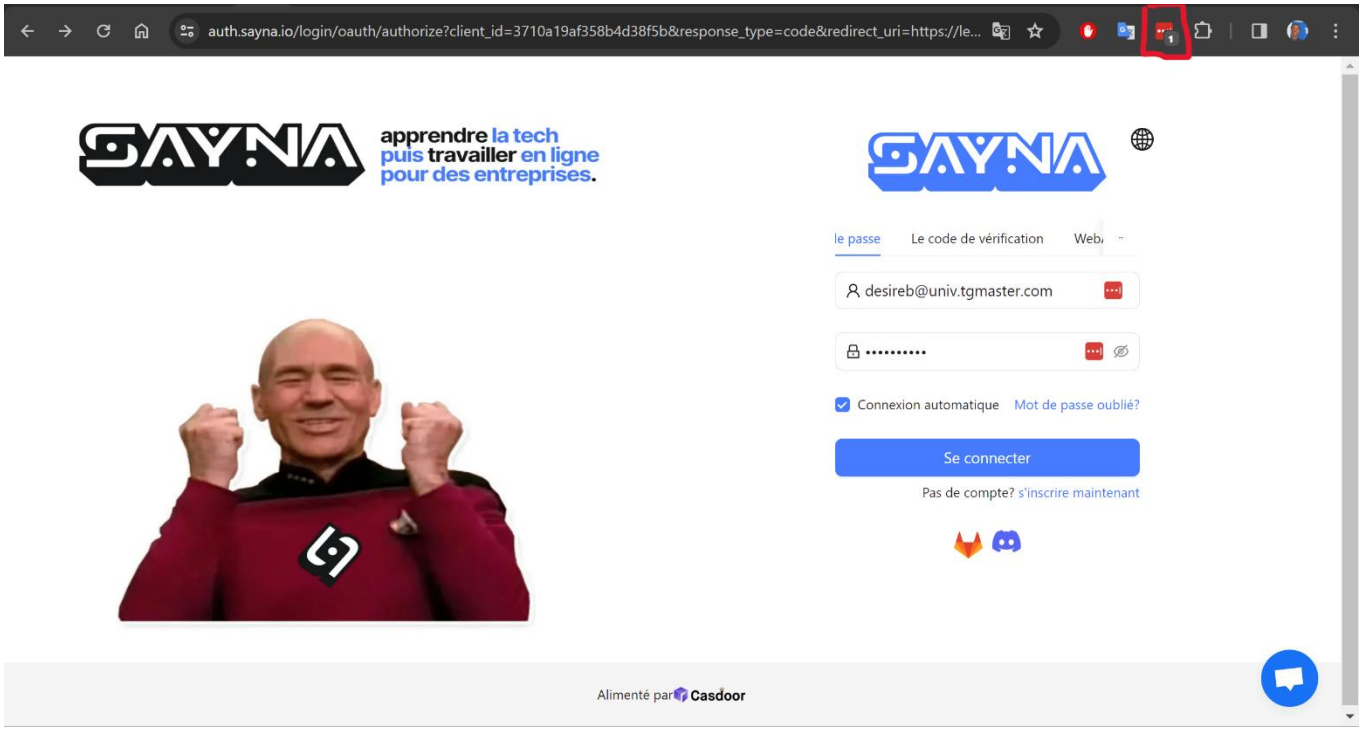
1- Introduction à la sécurité sur internet

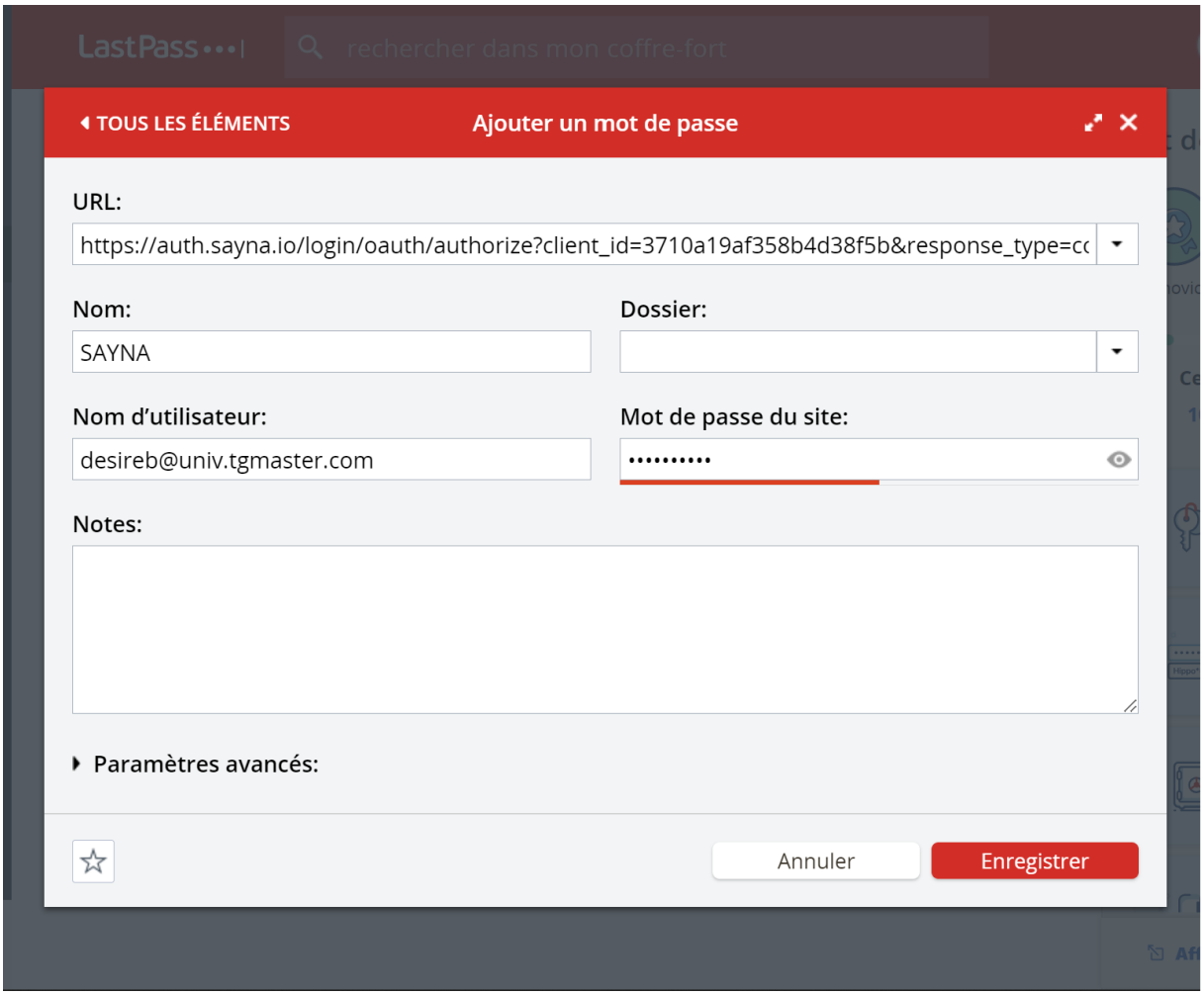
Article 1 : 1jour1actu - C'est quoi, les dangers d'Internet ?

Article 2 : Vaadata - Comment renforcer la sécurité de vos applications web pour contrer les attaques les plus courantes ?

Article 3 : La Jaune et la Rouge - Une introduction à la sécurité sur Internet

2- Créer des mots de passes fort





3- Fonctionnalité de sécurité de votre navigateur

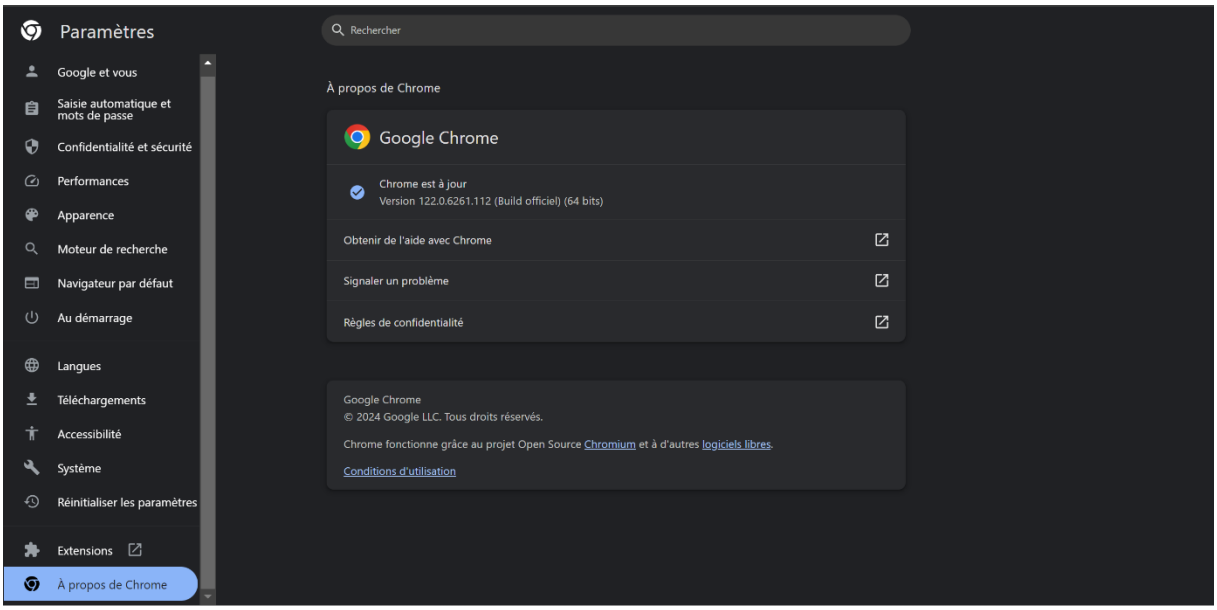
3-1 Les adresses malveillants sont :

www.morvel.com

www.dccomics.com

www.fessebook.com

3-2 Mise à jour de mon navigateur



4- Eviter le spam et le phising

5- Comment éviter les logiciels malveillants

Site 1 : Indicateur de sécurité : HTTPS

Analyse Google : Aucun contenu suspect

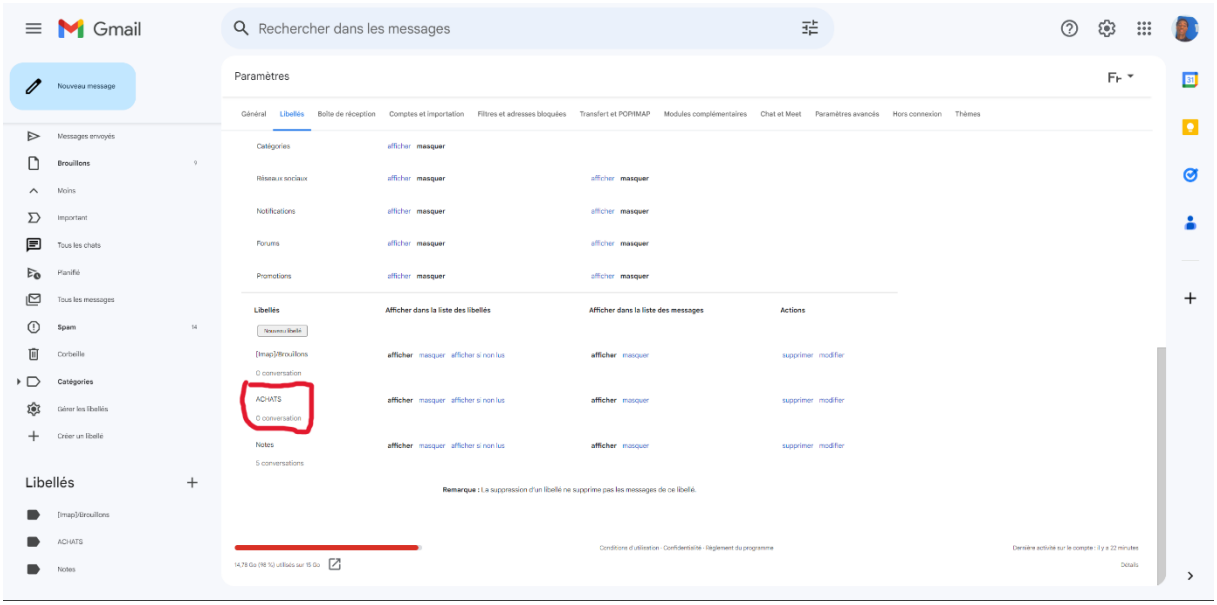
Site 2 : Indicateur de sécurité : Not secure

Analyse Google : Aucun contenu suspect

Site 3 : 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

9- Que faire si votre ordinateur est infecté.

9-1- Exercices pour vérifier la sécurité

❖ **POUR ORDINATEUR**

- **Vérification de l'antivirus** :

Assurez-vous que vous avez un antivirus installé et actif. Si vous utilisez Windows, vérifiez si Windows Defender est activé. Sinon, installez un antivirus tiers fiable.

Pour Windows 11, ouvrez le Centre de sécurité en cliquant sur l'icône dans la zone d'accès rapide. Vérifiez l'état de protection antivirus1.

Pour Windows 10, cliquez sur l'icône du Centre de sécurité dans la barre des tâches et vérifiez l'état de protection1.

- **Analyse en ligne** :

Utilisez des services en ligne pour vérifier la présence de virus ou de logiciels malveillants sur votre PC. Par exemple, 01net propose un outil pour vérifier la sécurité de votre ordinateur en ligne2.

- **Vérification des performances et de l'intégrité** :

Dans Sécurité Windows, consultez le rapport d'intégrité de votre appareil. Recherchez "Sécurité Windows" dans la barre des tâches et sélectionnez "Performances et intégrité de l'appareil" pour afficher le rapport3.

- **Optimisation de la confidentialité** :

Utilisez des outils comme O&O Shutup10 pour préserver votre confidentialité.

Sauvegardez automatiquement vos fichiers avec Windows File History.

- **Surveillance continue** :

Mettez à jour régulièrement votre système d'exploitation et vos logiciels.

Soyez vigilant face aux emails suspects, aux liens inconnus et aux pièces jointes.

❖ POUR TELEPHONE

- **Mises à jour du système :**

Assurez-vous que votre téléphone fonctionne avec la dernière version du système d'exploitation. Les mises à jour corrigent les vulnérabilités de sécurité.

Allez dans les paramètres de votre téléphone, puis recherchez la section "Mise à jour du logiciel". Téléchargez et installez les mises à jour disponibles1.

- **Applications et autorisations :**

Passez en revue les applications installées sur votre téléphone. Désinstallez celles que vous n'utilisez plus.

Vérifiez les autorisations accordées à chaque application. Limitez l'accès aux données personnelles uniquement aux applications de confiance.

- **Sécurité des réseaux Wi-Fi :**

Évitez de vous connecter à des réseaux Wi-Fi publics non sécurisés. Si nécessaire, utilisez un réseau privé virtuel (VPN) pour chiffrer votre connexion.

- **Verrouillage de l'écran :**

Activez un mot de passe, un schéma ou une empreinte digitale pour verrouiller l'écran de votre téléphone. Cela protège vos données en cas de perte ou de vol.

- **Vérification des applications tierces :**

Téléchargez uniquement des applications depuis le Google Play Store ou l'App Store (pour les iPhones).

Méfiez-vous des applications provenant de sources inconnues ou non vérifiées.

- **Double authentification :**

Activez la double authentification pour vos comptes importants (comme les comptes de messagerie ou les services bancaires). Cela ajoute une couche de sécurité supplémentaire.

- **Sauvegarde régulière :**

Effectuez des sauvegardes de vos données importantes (photos, contacts, etc.) sur un service cloud sécurisé ou un ordinateur.

9-2- Exercice pour installer et utiliser un antivirus

❖ POUR ORDINATEUR :

- **Installer un Antivirus :**

Pour Windows, vous pouvez utiliser Windows Defender, qui est inclus dans le système d'exploitation. Assurez-vous qu'il est activé.

Si vous préférez un antivirus tiers, téléchargez et installez un logiciel fiable comme Avast, AVG, ou Bitdefender12.

Pour Mac, vous pouvez utiliser Avira Free Antivirus ou d'autres solutions tierces3.

- **Mettre à jour régulièrement :**

Assurez-vous que votre système d'exploitation et vos logiciels sont à jour. Les mises à jour corrigent les vulnérabilités de sécurité.

- **Analyse en ligne :**

Utilisez des services en ligne pour vérifier la présence de virus ou de logiciels malveillants sur votre PC. Par exemple, AVG propose une analyse gratuite en ligne4.

- **Optimisation de la confidentialité :**

Utilisez des outils comme O&O Shutup10 pour préserver votre confidentialité.

Sauvegardez automatiquement vos fichiers avec Windows File History.

❖ POUR TELEPHONE :

- **Installer un Antivirus :**

Pour Android, téléchargez un antivirus gratuit comme AVG Antivirus ou Avast Mobile Security depuis le Google Play Store54.

Mettez à jour régulièrement les applications sur votre téléphone.

- **Éviter les risques :**

Soyez prudent avec les réseaux Wi-Fi publics. Évitez de vous connecter à des réseaux non sécurisés.

Méfiez-vous des emails suspects et des liens inconnus.

Téléchargez uniquement des applications depuis le Google Play Store.

- **Mises à jour du système :**

Mettez à jour votre téléphone avec les dernières versions du système d'exploitation.

Activez les mises à jour automatiques pour les applications.