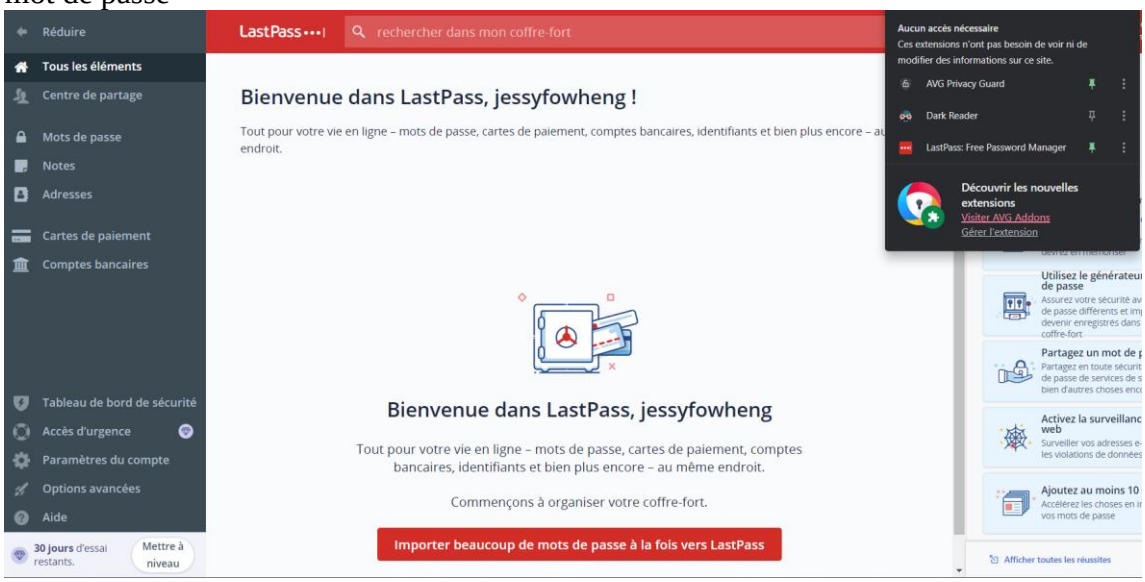
1- Introduction à la sécurité sur Internet

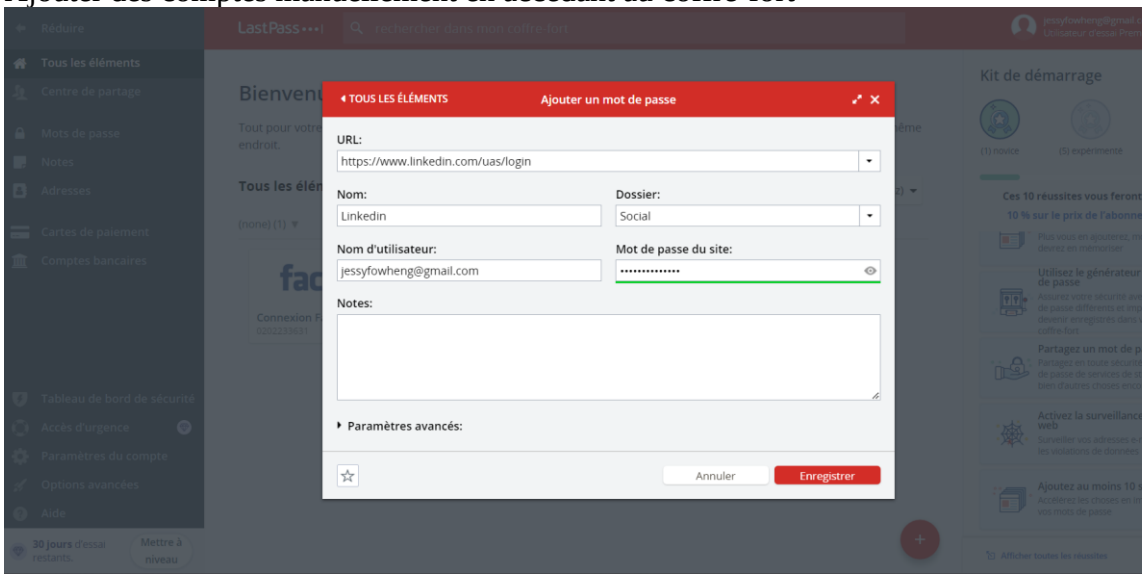
☑ Consulter 3 articles qui parlent de sécurité sur internet
-Article 1 : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-se-proteger-sur-internet
-Article 2 : https://www.laposte.fr/professionnel/conseils-pour-etre-en-securite-sur-internet
-Article 3 : https://www.kaspersky.fr/resource-center/preemptive-safety/internet-privacy--security-5-safety-tips

2- Création de mots de passe forts

☑ Créer un compte sur le gestionnaire de mot de passe LastPass
☑ Télécharger l'extension sur mon navigateur
☑ Lancer l'installation
☑ Epingler l'extension de LastPass
☑ Se connecter en cliquant sur l'icône de l'extension et en saisissant mon identifiant et mot de passe



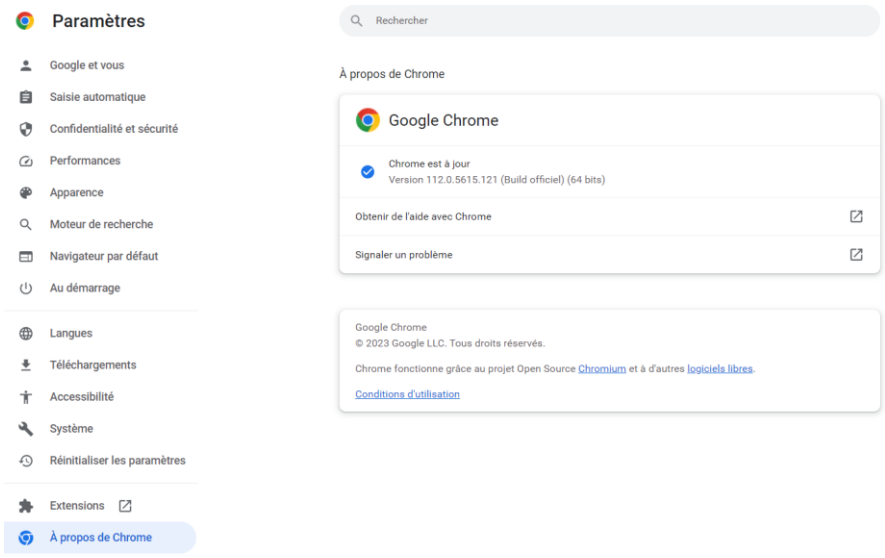
☑ Ajouter des comptes manuellement en accédant au coffre-fort



3- Fonctionnalité de sécurité de votre navigateur

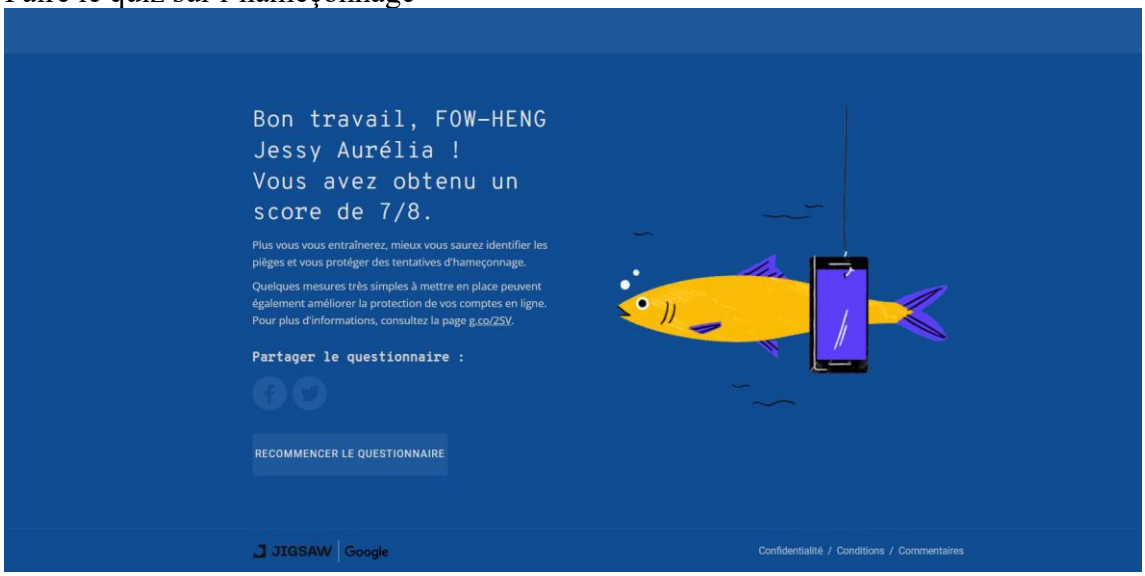
☑ Identifier les adresses internet qui proviennent de sites web malveillants
Exemples :
www.linkedon.com
www.canvan.com
www.amaizon.com

☑ Mettre à jour mes navigateurs



4- Eviter le spam et le phishing

☑ Faire le quiz sur l'hameçonnage



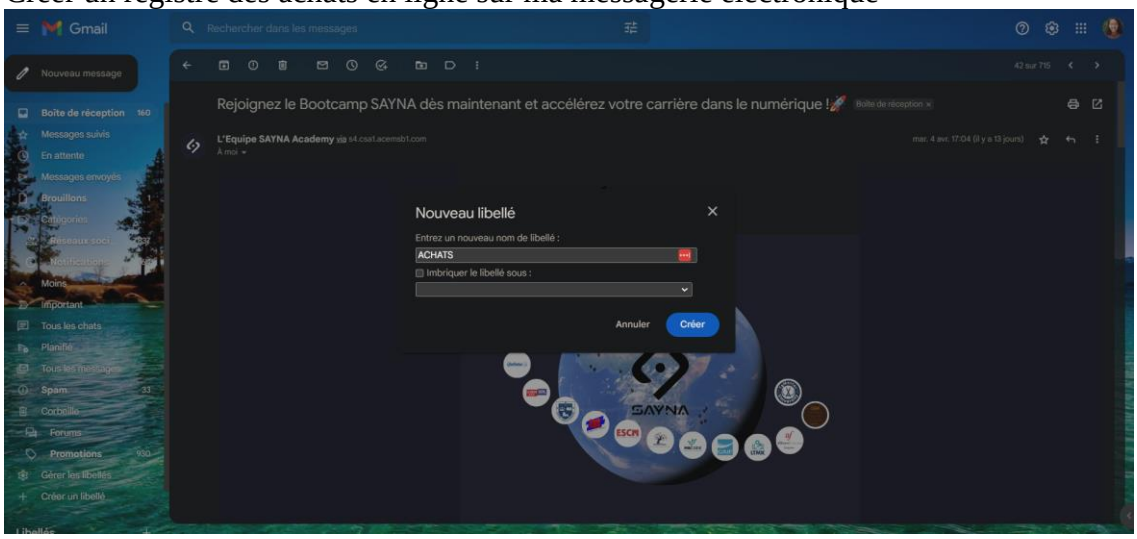
☑ Consulter les ressources annexes pour m'exercer

5- Comment éviter les logiciels malveillants

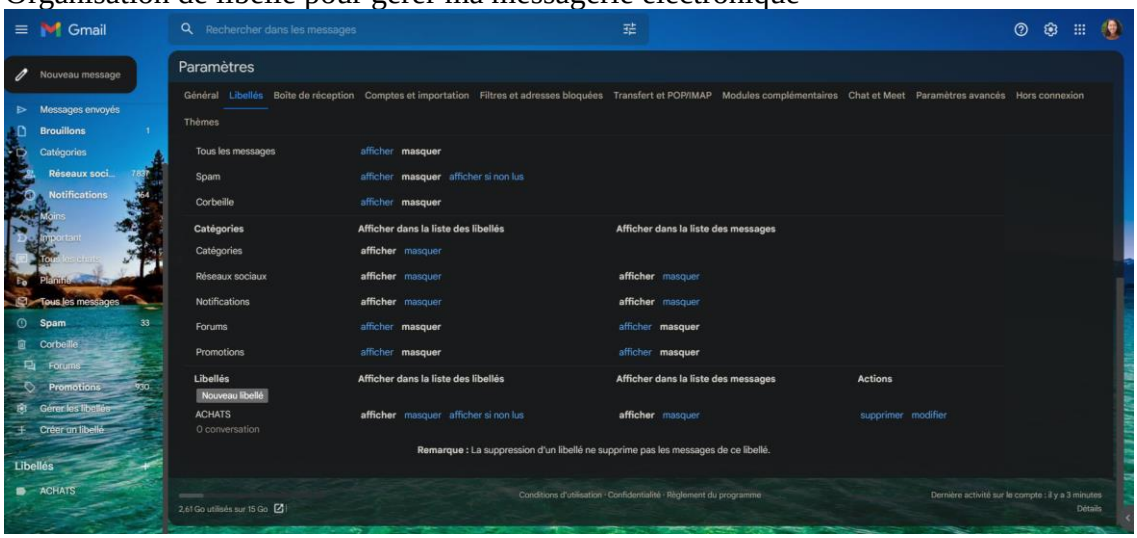
☑ Observer l'indicateur de sécurité des sites internet avec Google Transparency Report

6- Achats en ligne sécurisés

☑ Créer un registre des achats en ligne sur ma messagerie électronique



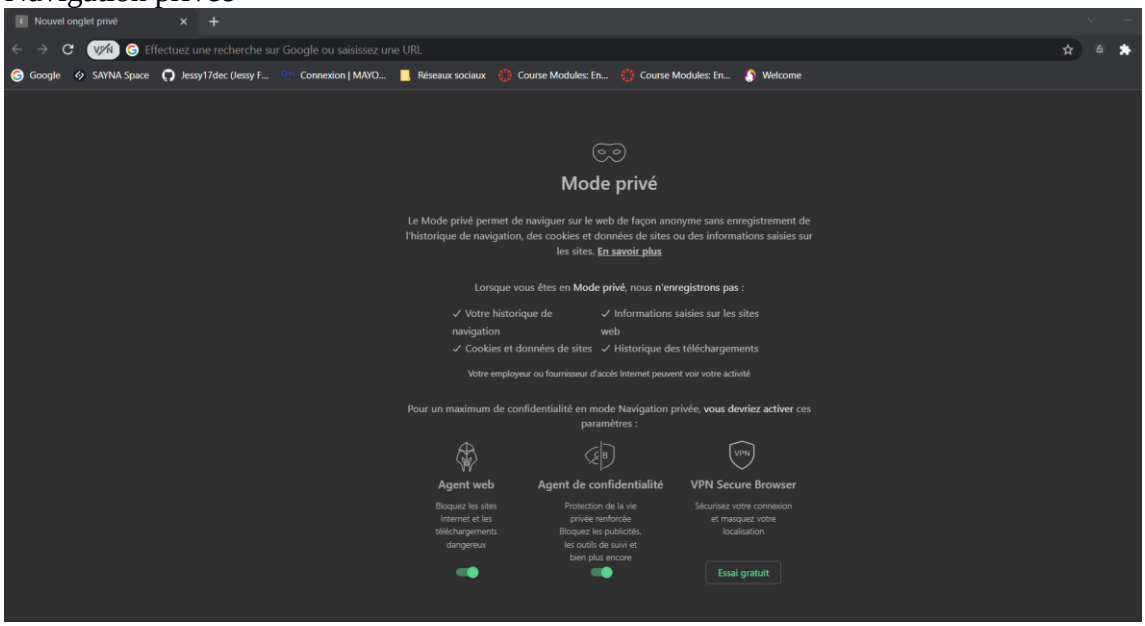
☑ Organisation de libellé pour gérer ma messagerie électronique



7- Comprendre le suivi du navigateur

☑ Gestion des cookies

☑ Navigation privée



8- Principes de base de la confidentialité des médias sociaux

☑ Régler les paramètres de confidentialité de Facebook

9- Que faire si l'ordinateur est infecté par un virus

☑ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé

- **Déconnecter l'ordinateur de l'internet** : si l'ordinateur est connecté à l'internet, le virus peut être en mesure de communiquer avec d'autres ordinateurs et se propager davantage. La déconnexion aide à éviter cela.

- **Installer et exécuter un logiciel antivirus** : installez un logiciel antivirus de bonne réputation sur l'ordinateur et exécuter une analyse complète du système. Cela aidera à détecter et à éliminer les virus qui peuvent être présents.

- **Mettre à jour le système d'exploitation et le logiciel** : s'assurer que le système d'exploitation et le logiciel sont à jour avec les derniers correctifs et mises à jour de sécurité. Cela peut aider à prévenir les futures attaques de virus.

- **Changer les mots de passe** : s'il existe des mots de passe enregistrés sur l'ordinateur, il faut les changer immédiatement. Cela peut aider à empêcher les pirates d'accéder aux comptes et à aux renseignements personnels.

- **Sauvegardez vos données** : si l'ordinateur est infecté par un virus, les données personnelles risquent d'être perdues ou compromises. La sauvegarde des données peut aider à la protéger en cas d'attaque de virus.

- **Vérifiez les comptes en ligne** se connecter aux comptes en ligne et vérifier s'il y a des activités inhabituelles, comme des ouvertures de session non autorisées ou des transactions. Si vous remarquez quelque chose de suspect, changez votre mot de passe et contactez l'entreprise immédiatement.

- **Considérer l'aide professionnelle** : Si vous êtes incapable de supprimer le virus ou soupçonnez que vos renseignements personnels ont été compromis, envisagez de demander l'aide d'un expert en sécurité informatique. Ils peuvent vous aider à vérifier votre sécurité Internet et à protéger vos renseignements personnels.

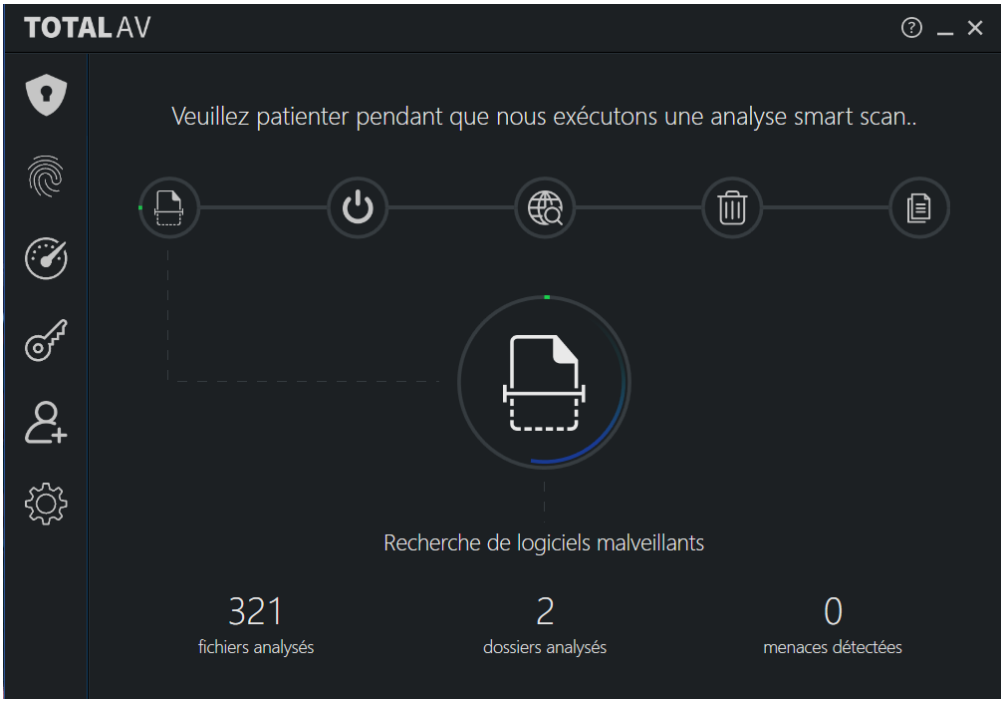
☑ Proposer un exercice pour installer et utiliser un antivirus + antimalware ne fonction de l'appareil utilisé

- **Effectuer des recherches et choisir un logiciel antivirus et antimalware de bonne réputation** : il existe de nombreuses options disponibles, il est donc important d'effectuer vos recherches et de choisir un programme qui est bien examiné et a fait ses preuves dans la détection et la suppression des virus et des logiciels malveillants. (exemple : TotalAV)

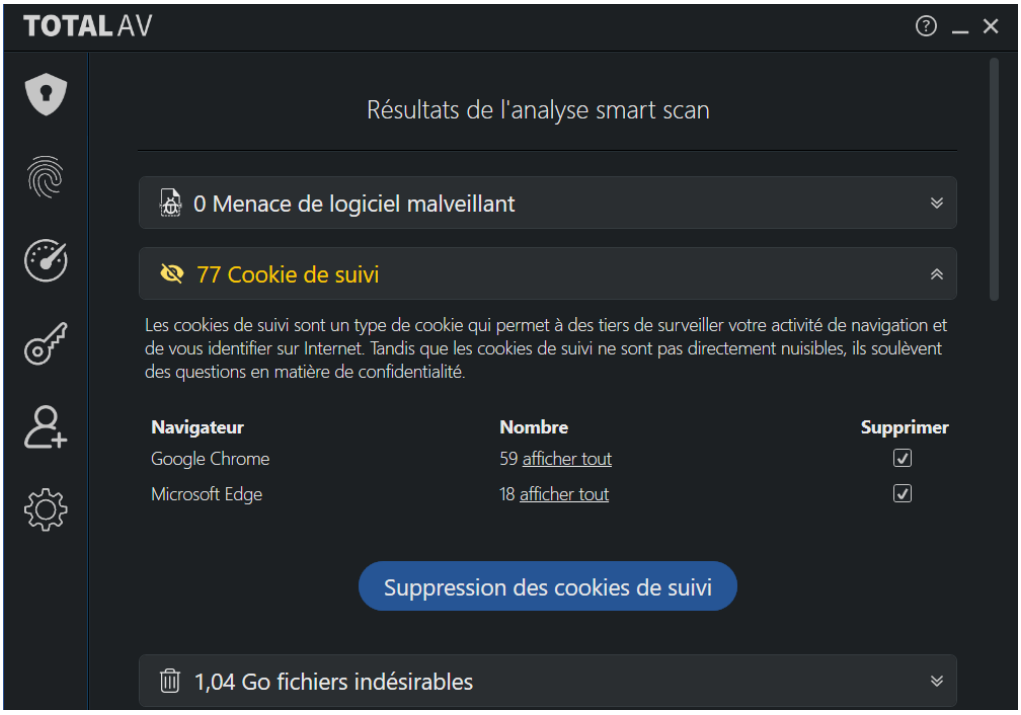
- **Télécharger et installer le logiciel** : Une fois que vous avez choisi votre logiciel, téléchargez-le à partir du site Web du fournisseur et exécutez l'installateur. Suivre les instructions pour terminer le processus d'installation.

- **Mettre à jour le logiciel** : Une fois le logiciel installé, assurez-vous de le mettre à jour vers la dernière version. Cela permettra de s'assurer que le logiciel a les définitions de virus et de logiciels malveillants les plus à jour.

- **Exécuter une analyse** : une fois le logiciel installé et mis à jour, exécuter une analyse complète du système. Cela va analyser votre ordinateur entier pour les virus et les logiciels malveillants et supprimer toutes les menaces qui sont trouvés.



- **Programmer des scans réguliers** : Il est conseillé de programmer des scans réguliers, par exemple une fois par semaine ou une fois par mois, pour s'assurer que votre ordinateur reste exempt de virus et de logiciels malveillants.



- **Activer la protection en temps réel** : La plupart des logiciels antivirus et antimalware comprend une protection en temps réel, qui surveille votre ordinateur en temps réel pour toute menace. Assurez-vous d'activer cette fonctionnalité pour une protection supplémentaire.

- **Méfiez-vous des pièces jointes aux courriels et des téléchargements** : Même avec un logiciel antivirus et antimalware installé, il est important de faire attention aux pièces jointes aux courriels et aux téléchargements provenant de sources inconnues. Assurez-vous de ne télécharger que des fichiers de sources fiables et évitez d'ouvrir des pièces jointes de sources inconnues.

- **Gardez votre logiciel à jour** : Enfin, il est important de garder votre antivirus et antimalware à jour. De nouveaux virus et logiciels malveillants sont constamment créés, il est donc important de s'assurer que votre logiciel est en mesure de les détecter et de les supprimer.