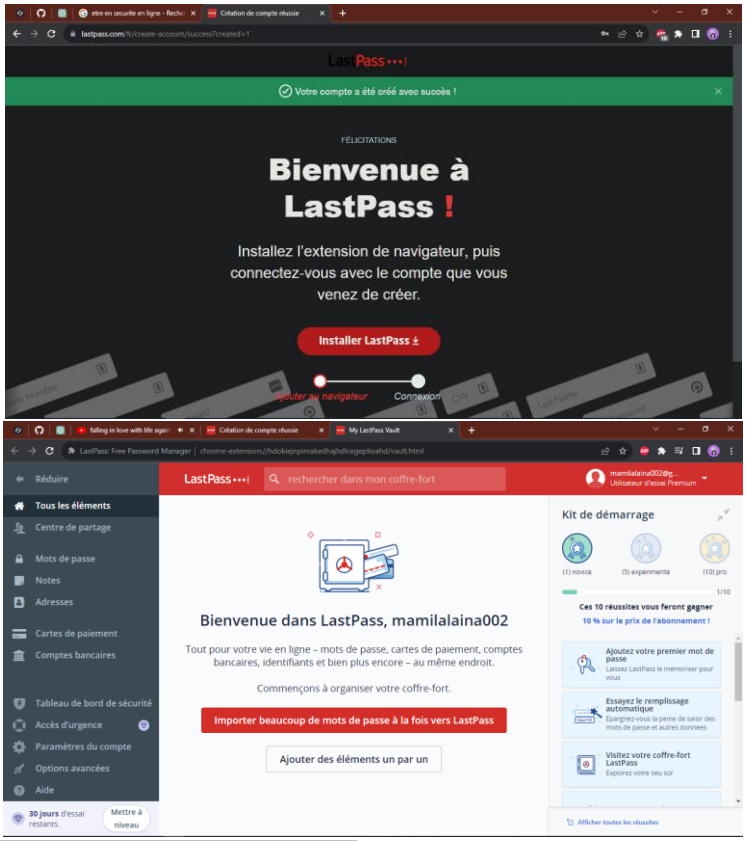
1- Introduction à la sécurité sur internet

a) Les trois articles qui parlent de sécurité sur Internet :

- Article 1 = Qu'est-ce que la sécurité Internet ? – Définition et signification : https://www.kaspersky.fr/resource-center/definitions/what-is-internet-security
- Article 2 = La sécurité numérique : https://www.oecd.org/fr/numerique/securite-numerique/
- Article 3 = 12 choses simples pour être plus en sécurité en ligne : https://www.maison-et-domotique.com/137132-12-choses-simples-pour-etre-plus-en-securite-en-ligne/

2- Créer des mots de passes forts

a) Utilisation du gestionnaire de mot de passe LastPast

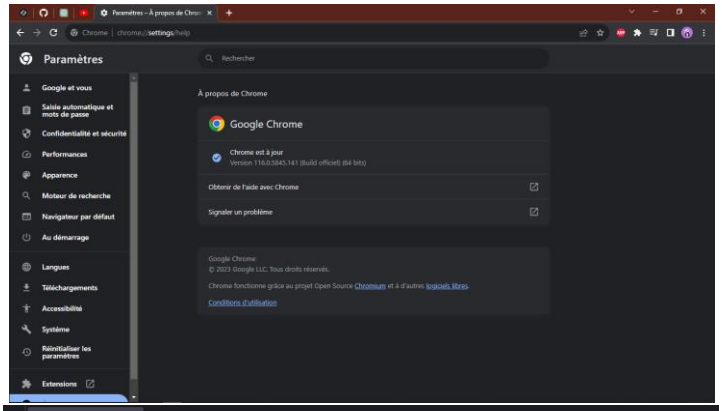


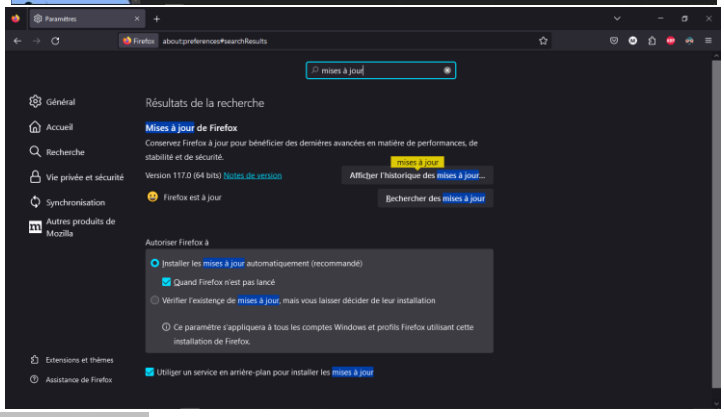
3- Fonctionnalité de sécurité de votre navigateur

a) Identification des sites Web malveillants :

Sites semblant être malveillants	Sites semblant être cohérents
- www.morvel.com , c'est un dérivé de www.marvel.com - www.fessebook.com qui semble être un dérivé de www.facebook.com - www.instagam.com qui est le dérivé de www.instagram.com	- www.docomics.com, le site officiel de DC Comics - www.ironman.com

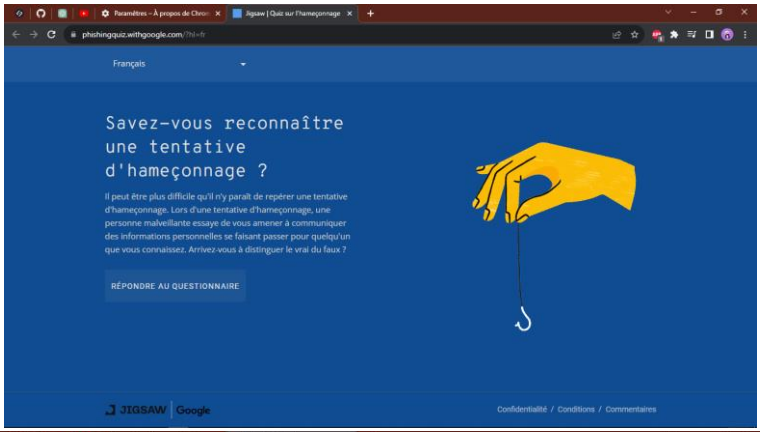
b) Mise à jour de Chrome et Firefox :

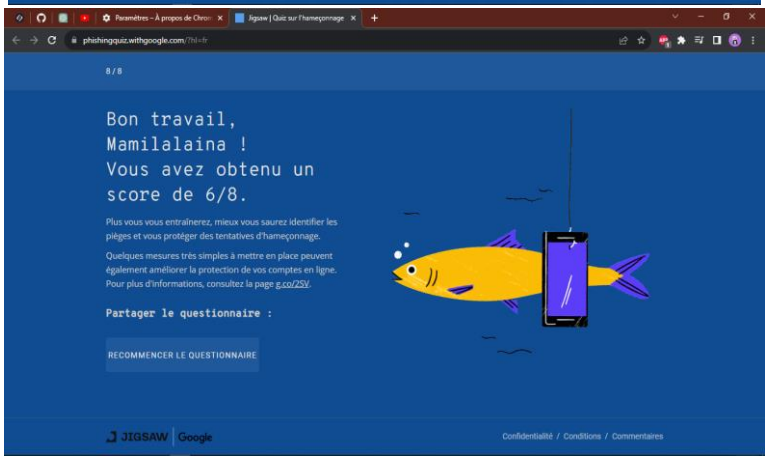




4- Eviter le spam et le phishing

a) Exercice 4 – Spam et phishing





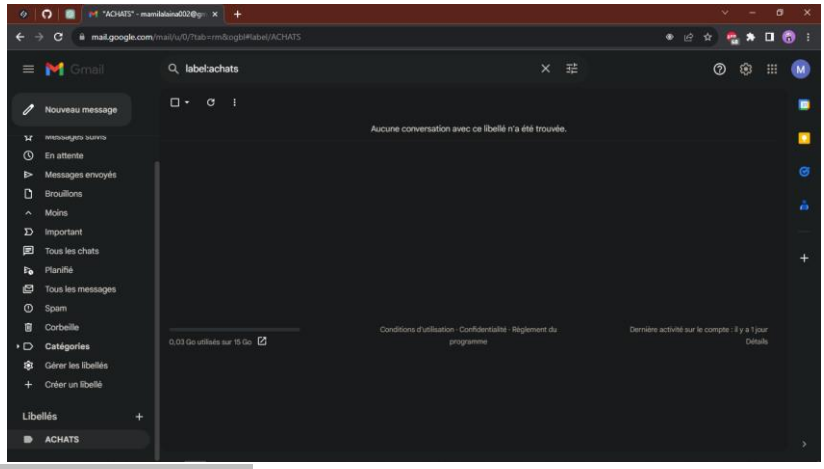
5- Comment éviter les logiciels malveillants

a) Vérification de la sécurité des sites

	Indicateur de sécurité	Analyse Google
https://vostfree.tv/	HTTPS	Aucun contenu suspect
http://www.tv5monde.com/	Not Secure	Aucun contenu suspect
http://www.baidu.com/	Not Secure	Vérifier un URL en particulier (analyse trop générale)

6- Achat en ligne sécurisé

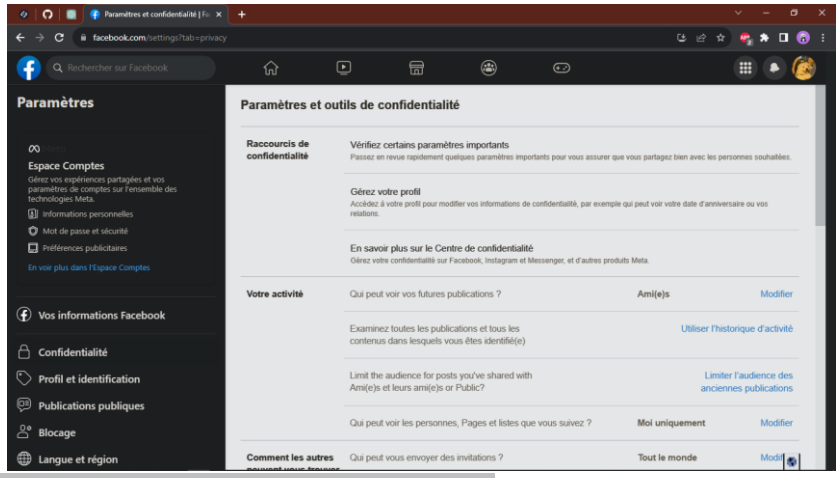
a) Création d'un registre d'achat



7- Comprendre le suivi du navigateur

8- Principes de base de la confidentialité des medias sociaux

a) Réglage des paramètres de confidentialité sur Facebook



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

a) Comment vérifier la sécurité en fonction de l'appareil utilisé :

Pour un ordinateur (Windows, MacOs, Linux) :

1. Mises à jour du système : Assurez-vous que votre système d'exploitation et vos logiciels sont régulièrement mis à jour avec les derniers correctifs de sécurité. Activez les mises à jour automatiques si possibles.
2. Logiciel antivirus et antimalware : Installez un logiciel antivirus ou antimalware fiable et assurez-vous qu'il est toujours à jour.
3. Pare-feu : Activez ou installez un pare-feu pour surveiller les connexions entrantes et sortantes de votre ordinateur.

4. Prudence en ligne : Soyez vigilant lorsque vous naviguez sur Internet, évitez les téléchargements à partir de sources non fiables et ne cliquez pas sur des liens suspects ou des pièces jointes inconnues.
5. Mots de passe forts : Utilisez des mots de passe forts et un gestionnaire de mots de passe pour gérer vos identifiants en ligne.
6. Chiffrement : Si vous stockez des données sensibles sur votre ordinateur, envisagez de les chiffrer pour les protéger en cas de vol ou d'accès non autorisé.

Pour un smartphone ou une tablette (iOS, Android) :

1. Mises à jour : Mettez à jour régulièrement votre système d'exploitation et les applications installées sur votre appareil.
2. Téléchargements d'applications : Téléchargez uniquement des applications à partir de sources officielles comme l'App Store d'Apple ou Google Play Store, et lisez les avis avant de télécharger une application.
3. Autorisations d'application : Vérifiez les autorisations demandées par les applications et n'accordez que celles qui sont nécessaires.
4. Sécurité du réseau : Utilisez des réseaux Wi-Fi sécurisés et évitez les réseaux Wi-Fi publics non sécurisés.
5. Verrouillage de l'appareil : Activez un code PIN, un mot de passe, ou une méthode de déverrouillage biométrique (comme l'empreinte digitale ou la reconnaissance faciale) pour sécuriser votre appareil.
6. Effacement à distance : Activez la fonctionnalité "Effacement à distance" pour pouvoir effacer les données de votre appareil en cas de perte ou de vol.
7. Sécurité des comptes : Activez la vérification en deux étapes sur vos comptes en ligne, notamment sur les comptes de messagerie et les médias sociaux.

Pour d'autres appareils connectés :

1. Mises à jour : Assurez-vous que le firmware ou le logiciel de l'appareil est régulièrement mis à jour, surtout s'il s'agit d'appareils IoT (Internet des objets).
2. Changement des mots de passe par défaut : Changez les mots de passe par défaut sur les appareils connectés et utilisez des mots de passe forts.
3. Réseau sécurisé : Intégrez ces appareils dans un réseau Wi-Fi sécurisé et configurez correctement les paramètres de sécurité de votre routeur.
4. Évaluation de la sécurité : Recherchez des vulnérabilités potentielles et des correctifs pour les appareils IoT, en particulier ceux qui peuvent être exploités à distance.

Enfin, il est important de rester informé sur les dernières menaces et pratiques de sécurité en ligne en suivant les actualités technologiques et en restant vigilant. La sécurité en ligne est un processus continu qui nécessite une attention constante.

b) Comment installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé :

Les logiciels antivirus et antimalware ne sont pas tous fiables. Pour éviter de prendre des risques je propose plutôt de se fier à l'antivirus préinstallé dans le système d'exploitation utilisé, de les entretenir et de les mettre à jour régulièrement.
Pour Windows, c'est « Microsoft Defender » et pour MacOs c'est « XProtect », également connu sous le nom de « File Quarantine ».

Sur Linux, il n'y a généralement pas d'antivirus préinstallé de manière native, car Linux est souvent considéré comme plus sûr en raison de sa structure de sécurité et de son modèle de gestion des autorisations. Les utilisateurs de Linux ont tendance à se fier à des pratiques de sécurité telles que la mise à jour régulière de leur système, l'utilisation de pare-feu et la prudence lors du téléchargement de logiciels depuis des sources non fiables pour maintenir leur système sûr.

Cependant, il existe des solutions antivirus pour Linux que vous pouvez installer si vous le souhaitez, notamment ClamAV, Sophos pour Linux, et d'autres logiciels tiers. Ces solutions sont souvent utilisées pour analyser des fichiers spécifiques ou des serveurs Linux qui interagissent avec des systèmes Windows pour détecter et supprimer les menaces potentielles lors de l'utilisation de Linux dans un environnement mixte.