Parcours : DISCOVERY

MODULE : Naviguer en toute sécurité

PROJET 1 : Un peu plus de Sécurité, on n'en a jamais assez !

Sommaire

---

1 - Introduction à la sécurité sur Internet :

Objectif : à découvrir la sécurité sur internet

- ✓ En naviguant sur le web, consulte trois articles qui parlent de sécurité sur internet.

Pense à vérifier les sources des informations et essaie de consulter des articles
Voici les articles que nous avons retenus pour toi (avec les mots-clés “sécurité sur internet” et “comment être en sécurité sur internet” :

Article 1 : Kaspersky Lab. (https://www.kaspersky.com/fr) : Kaspersky est un leader mondial en matière de cyber sécurité et son site propose une multitude de ressources, y compris des articles, des analyses et des conseils sur la sécurité en ligne.

Article 2 : Norton Security (https://fr.norton.com/) : Norton propose des solutions de sécurité Internet et son site contient des guides complets sur la protection en ligne, les menaces actuelles et les meilleures pratiques.

Article 3 : Trend Micro(https://www.trendmicro.com/fr_fr/) : Trend Micro est une autre société renommée dans le domaine de la sécurité informatique. Son site propose des informations détaillées sur les dernières menaces et les moyens de se protéger.

Article 4 : Cybermalveillance.gouv.fr (https://www.cybermalveillance.gouv.fr/) : Ce site est géré par le gouvernement français et offre des conseils pratiques pour se protéger contre les cybers attaques, ainsi que des ressources pour signaler les incidents.

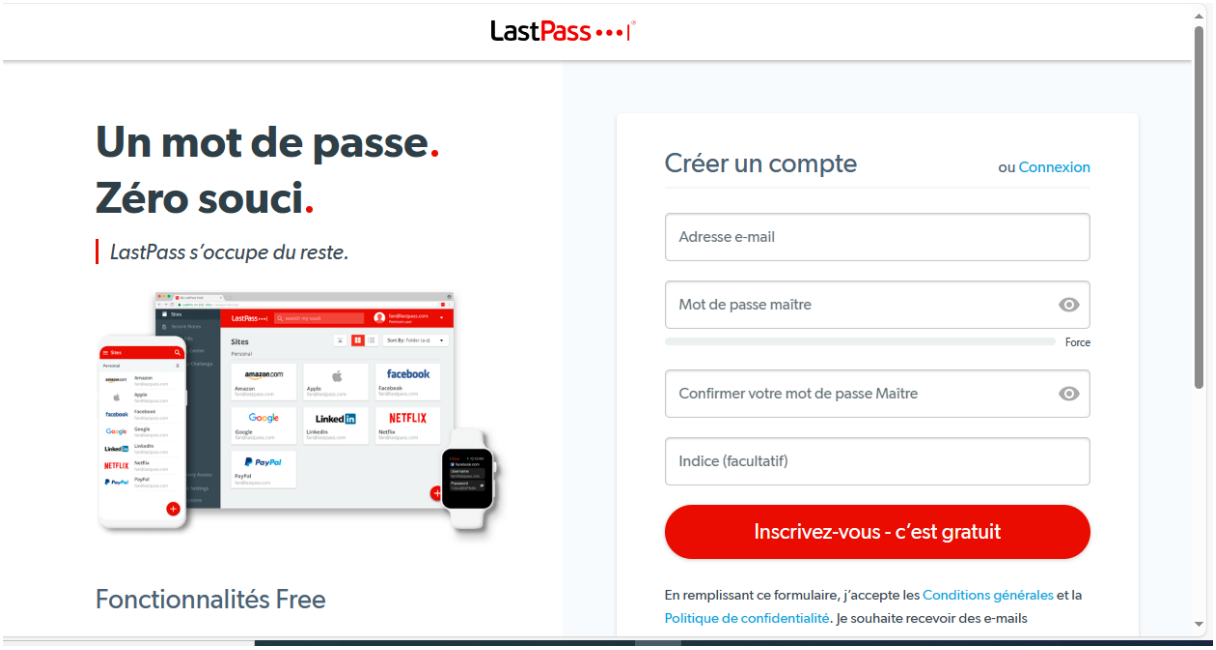
Article 5 : Cert EU (https://www.cert.europa.eu/) : Le Centre de Réponse aux Incidents de Sécurité Informatique de l'Union Européenne propose des conseils et des informations sur la sécurité des réseaux et des systèmes informatiques.

Ces sites devraient vous fournir une base solide pour comprendre et améliorer la sécurité de vos activités en ligne.

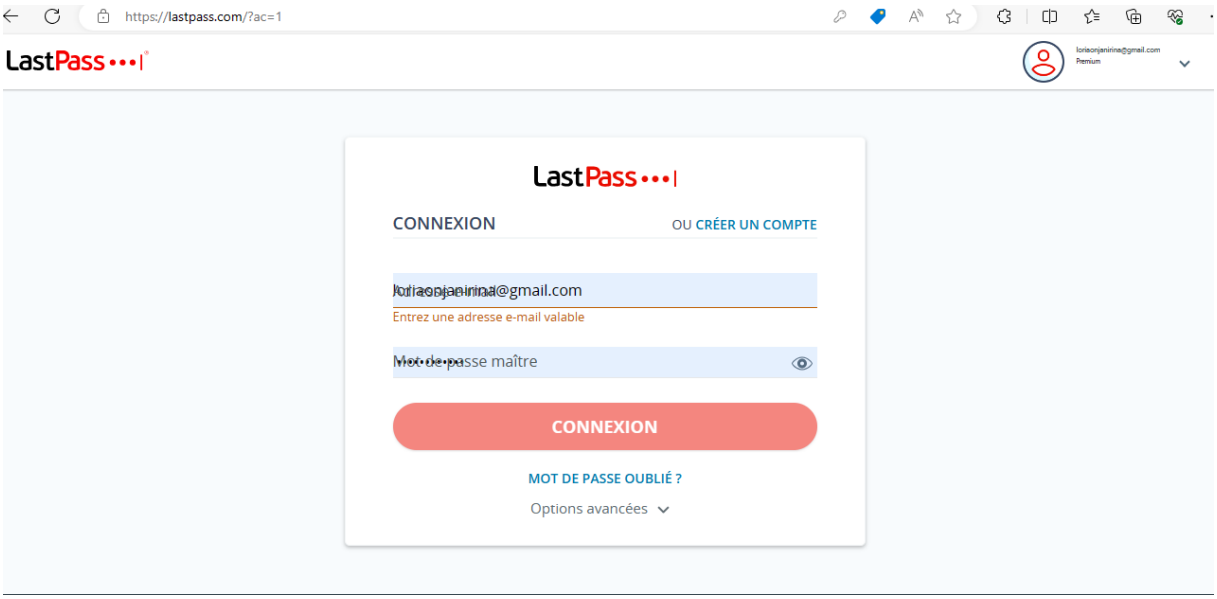
2-Creation des mots de passe fort

Objectif : utiliser un gestionnaire de mot de passe LastPass

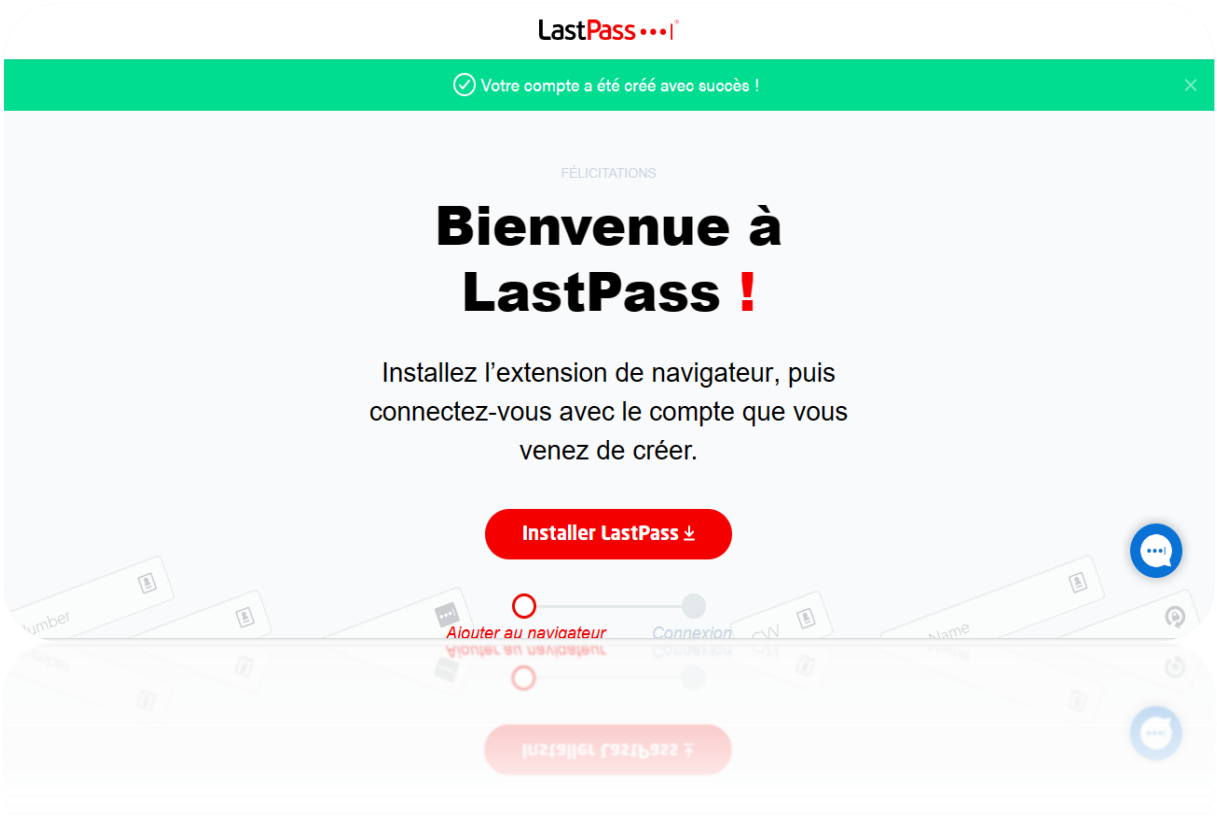
- Accès au site de LastPass



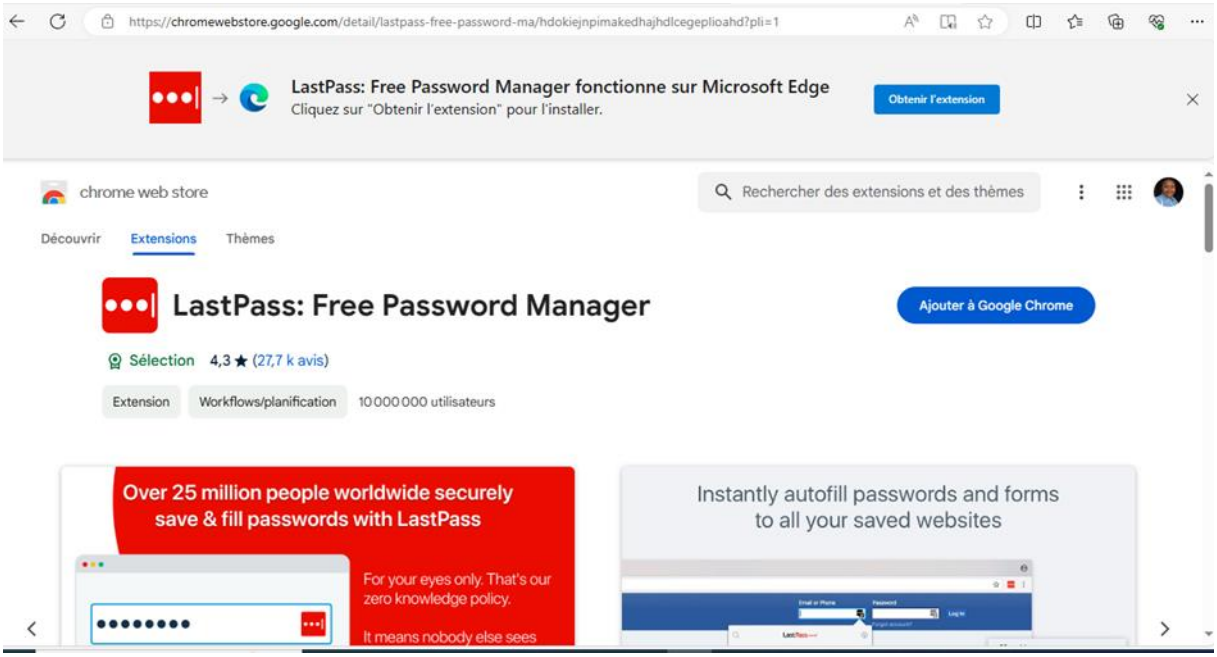
- Création d'un compte



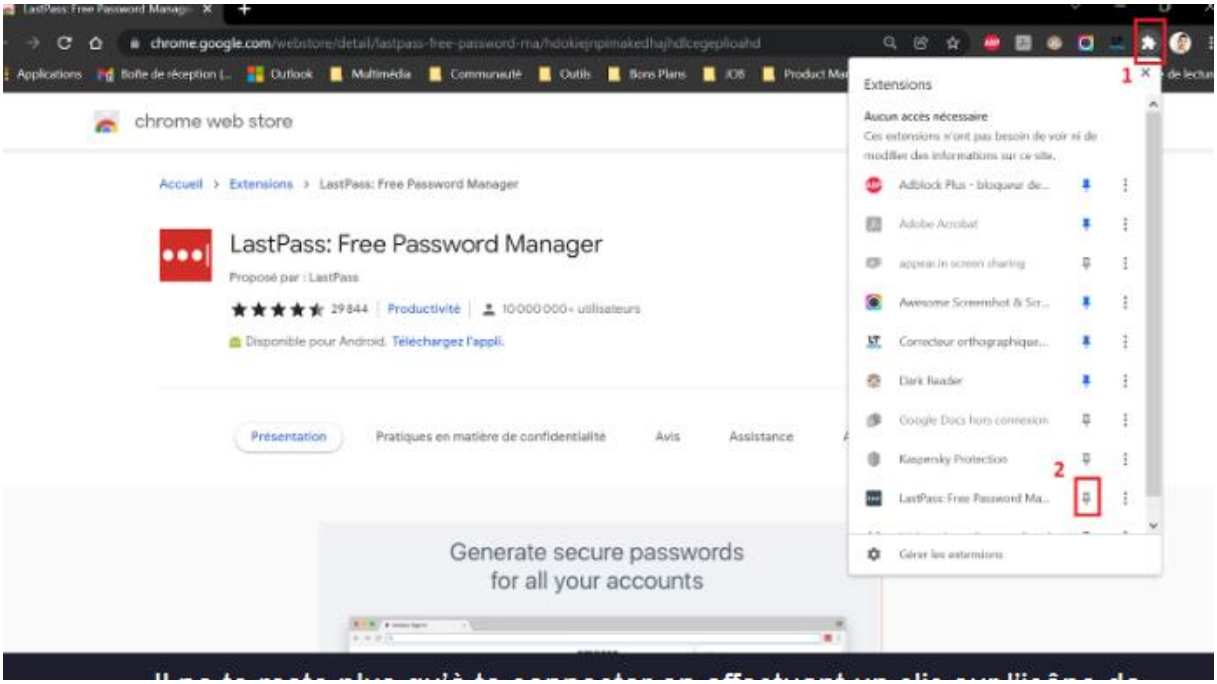
- Validation du compte



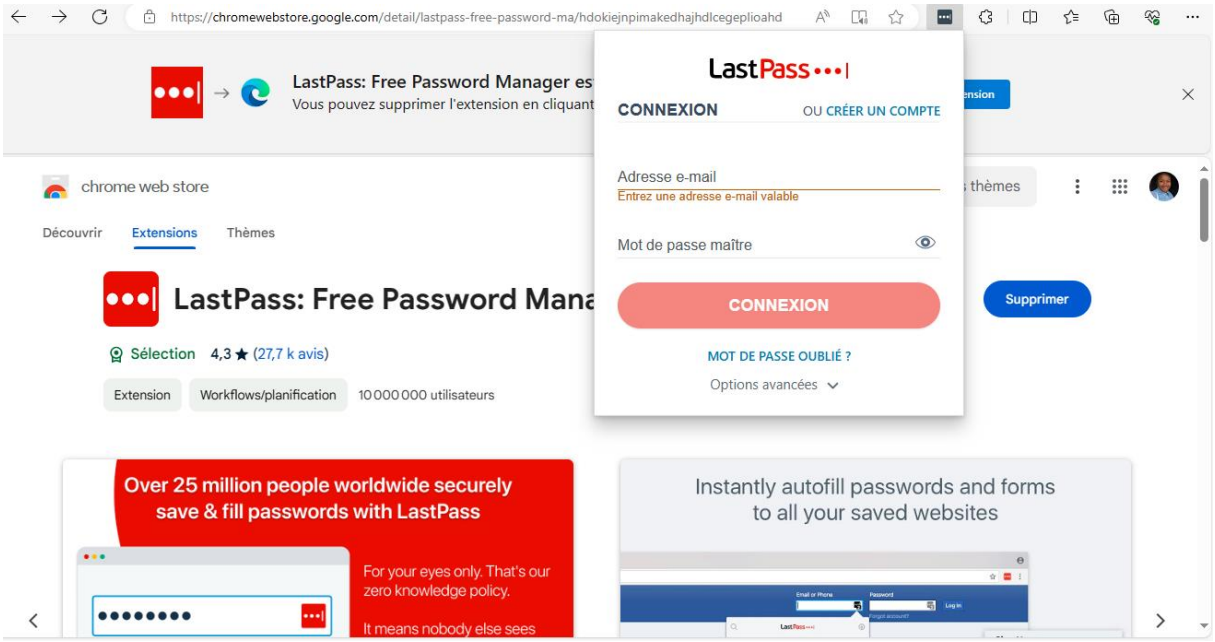
Validation l'opération sur le Chrome Web Store



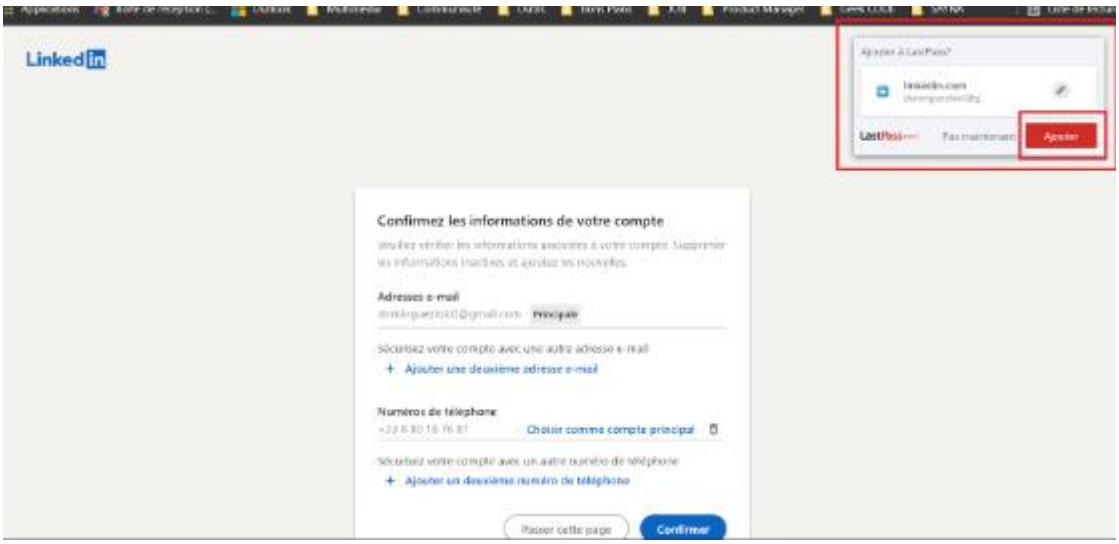
- Accès à l'extension



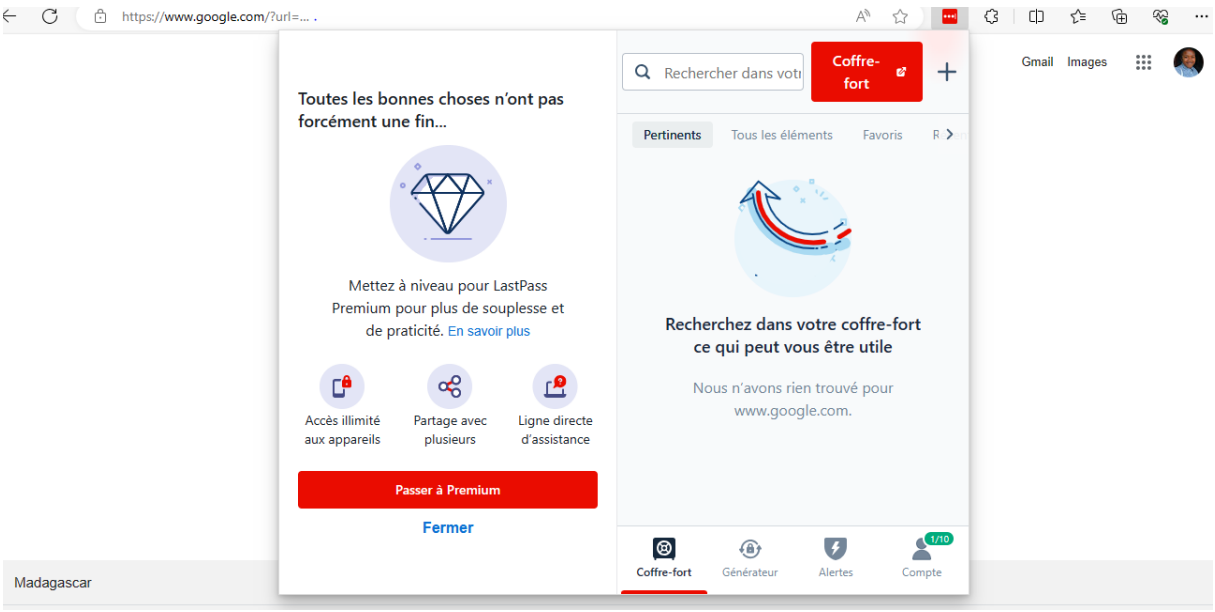
- Connexion à Lastpass



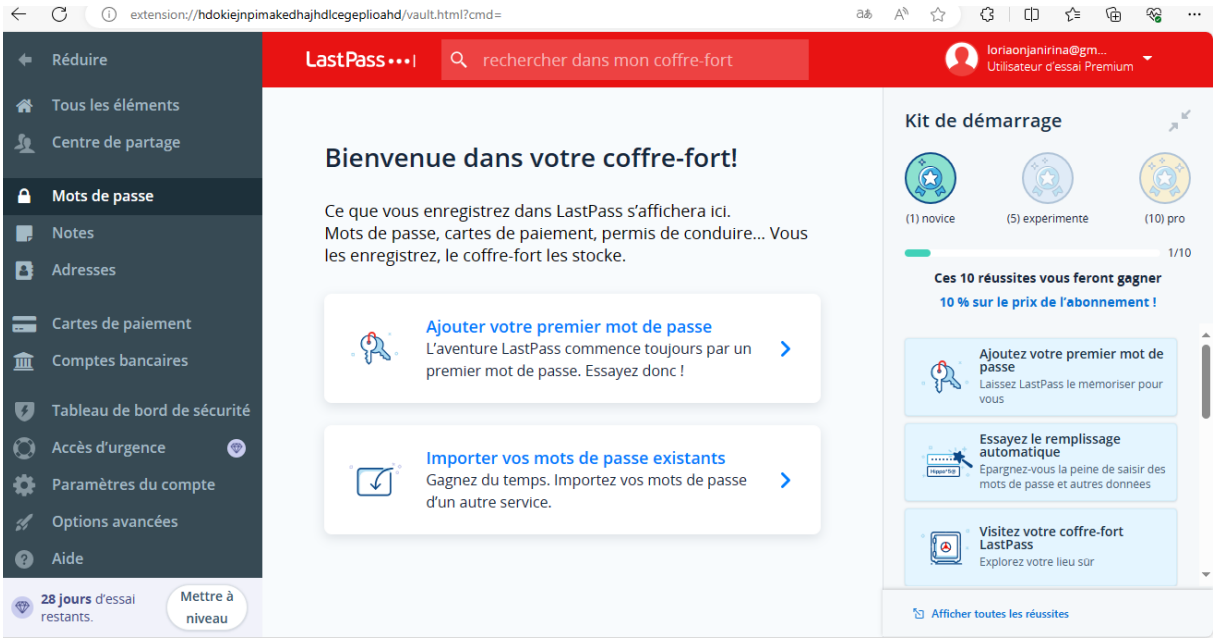
- Enregistrement du mot de passe sur Lastpass



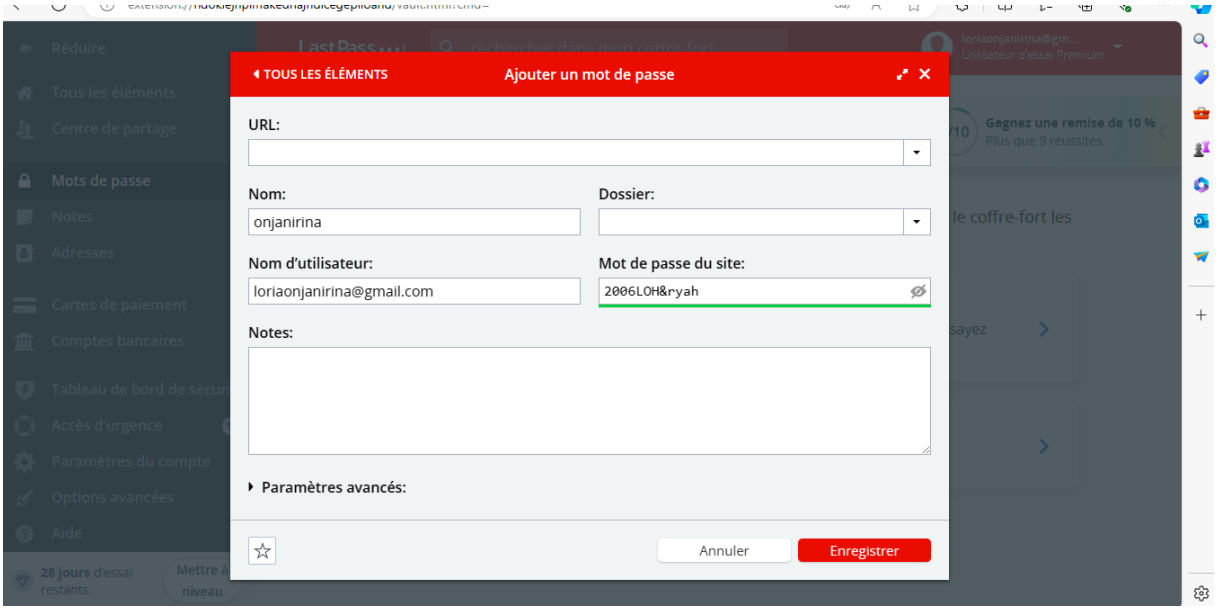
- Accès au coffre-fort



- Accès à la rubrique “Mot de passe”



- Insertion de toutes les informations à retenir pour automatiser la prochaine connexion



3 - Fonctionnalité de sécurité de votre navigateur

Objectif : identifier les éléments à observer pour naviguer sur le web en toute sécurité

1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants :
Les sites web qui semblent être malveillants sont :

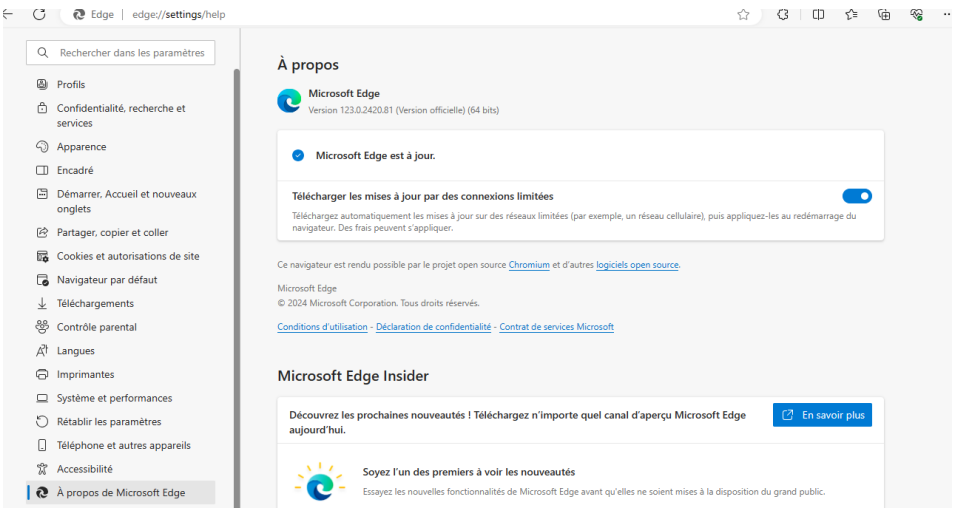
- www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel
- www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde
- www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très utilisé

Les seuls sites qui semblaient être cohérents sont donc :

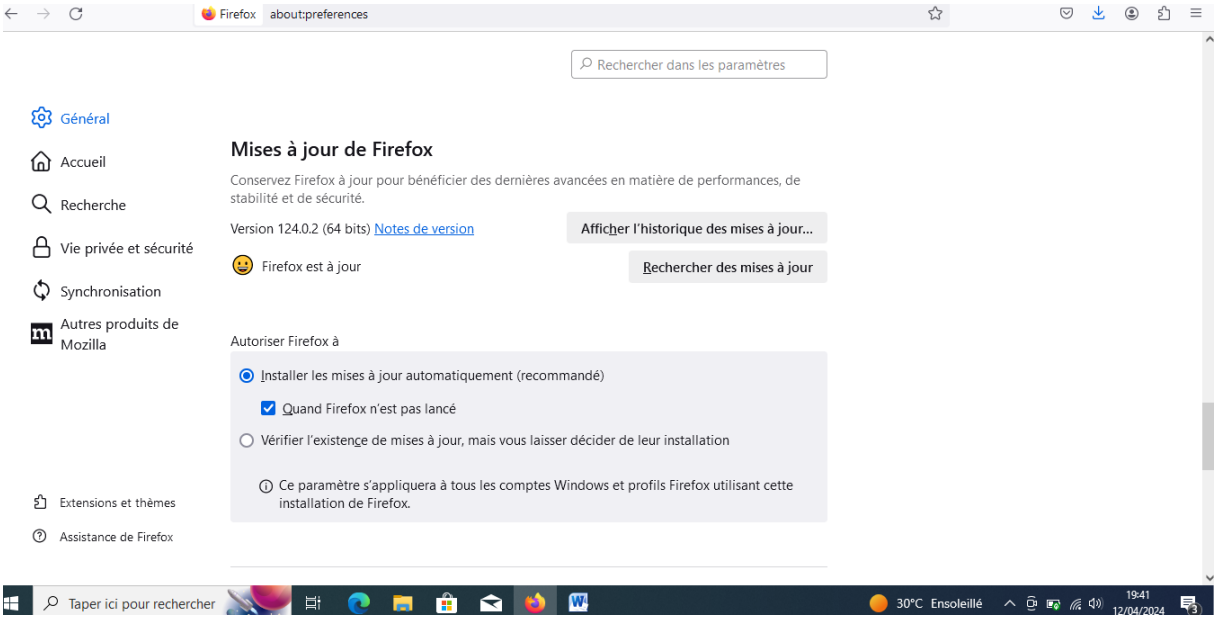
- www.dccomics.com, le site officiel de l'univers DC Comics
- www.ironman.com, le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

➢ Vérification si les navigateurs utilisés, Microsoft edge et Firefox sont à jour :

- Pour Microsoft edge



- Pour Chrome



4- Éviter le spam et le phishing

Objectif : Reconnaître plus facilement les messages frauduleux

5 - Comment éviter les logiciels malveillants

Objectif : sécuriser votre ordinateur et identifier les liens suspects

Lors de la navigation sur le web, il arrive d'avoir des doutes sur la sécurité de certains sites. Comme tu as pu le voir précédemment, le premier de niveau de vigilance à avoir se trouve dans la barre d'adresse des navigateurs web. La plupart affiche des indicateurs de sécurité pour donner une information sur la protection d'un site internet.

Lorsque le doute persiste tu peux t'appuyer sur un outil proposé par Google : Google Lorsque le doute persiste tu peux t'appuyer sur un outil proposé par Google : Google Transparency Report (en anglais) ou Google Transparence des Informations (en français). Afin d'améliorer ta lecture de la sécurité sur internet, tu vas devoir analyser les informations de plusieurs sites. Pour chaque site tu devras préciser l'indicateur de sécurité et le rapport d'analyse de l'outil

Google. Il te suffit d’accéder aux liens proposés ci-dessous pour observer l’indicateur de sécurité et de copier-coller l’URL du site dans l’outil Google. (Choix multiples)

● Site n°1

○ Indicateur de sécurité

■ HTTPS

■ HTTPS Not secured

■ Not secured

○ Analyse Google

■ Aucun contenu suspect

■ Vérifier un URL en particulier

● Site n°2

○ Indicateur de sécurité

■ HTTPS

■ HTTPS Not secured

■ Not secured

○ Analyse Google

■ Aucun contenu suspect

■ Vérifier un URL en particulier

● Site n°3

○ Indicateur de sécurité

■ HTTPS

■ HTTPS Not secured

■ Not secured

○ Analyse Google

■ Aucun contenu suspect

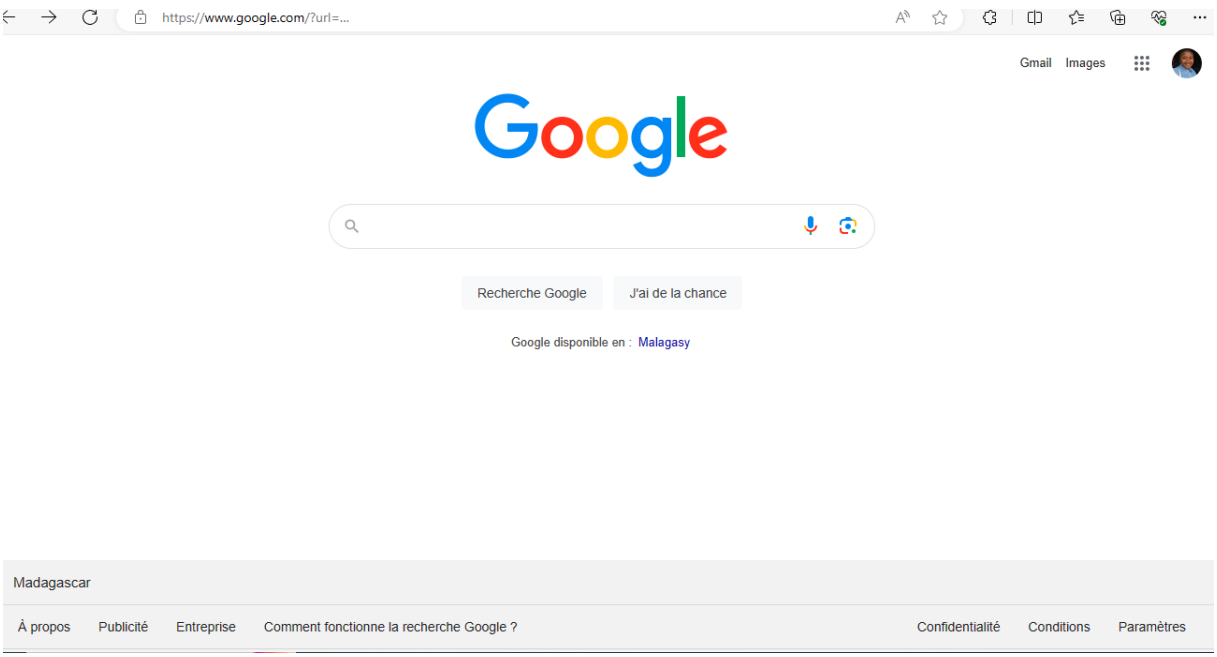
■ Vérifier un URL en particulier

● Site n°4 (site non sécurisé)

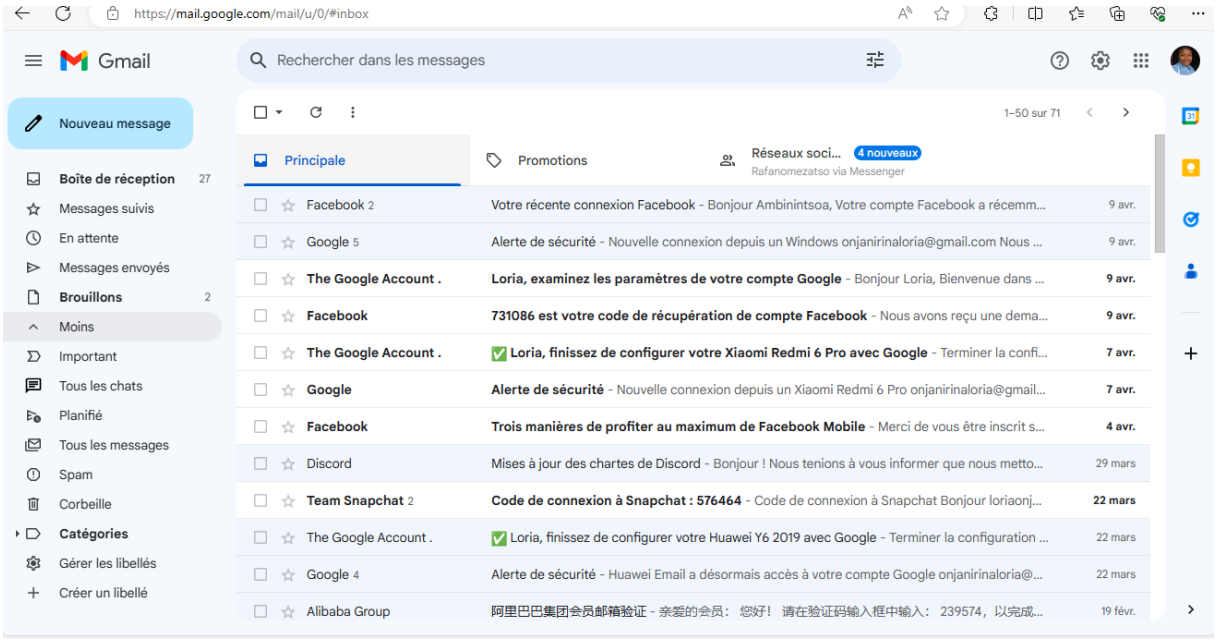
6 - Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

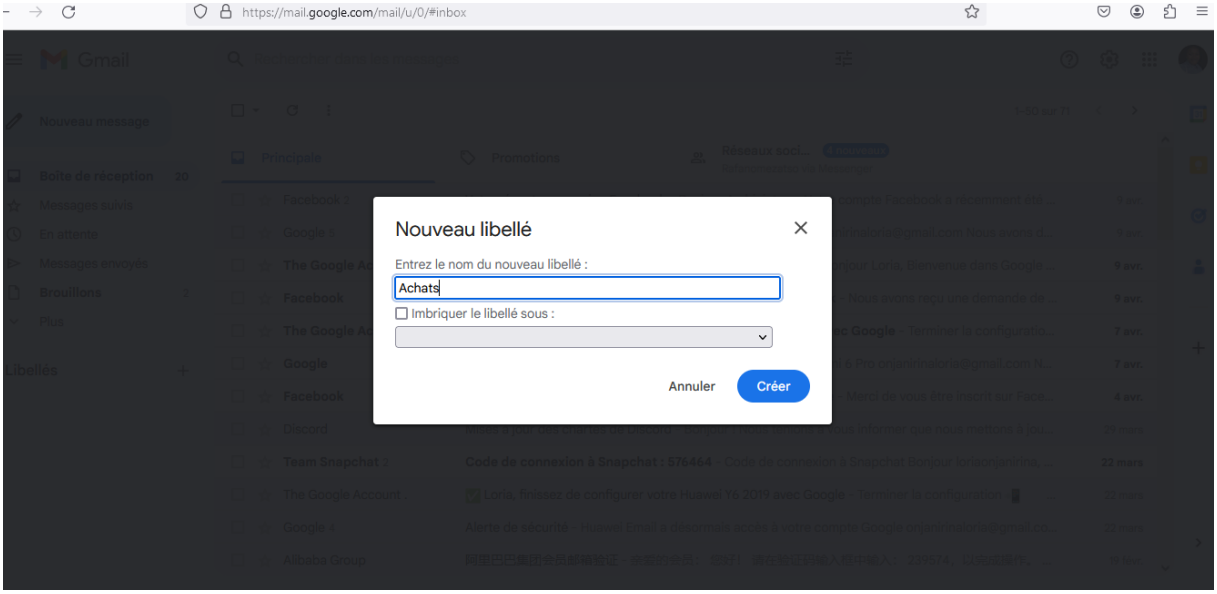
- Accès à la messagerie électronique



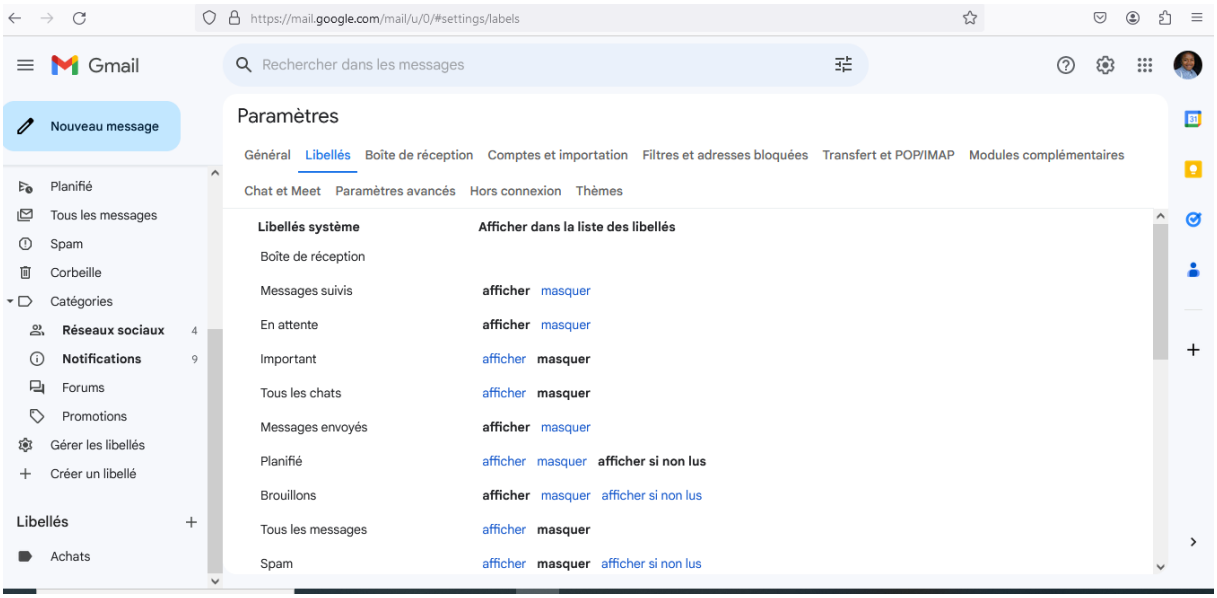
- Page d'accueil de la messagerie



- Création ta rubrique des achats



- Gestion des libellés



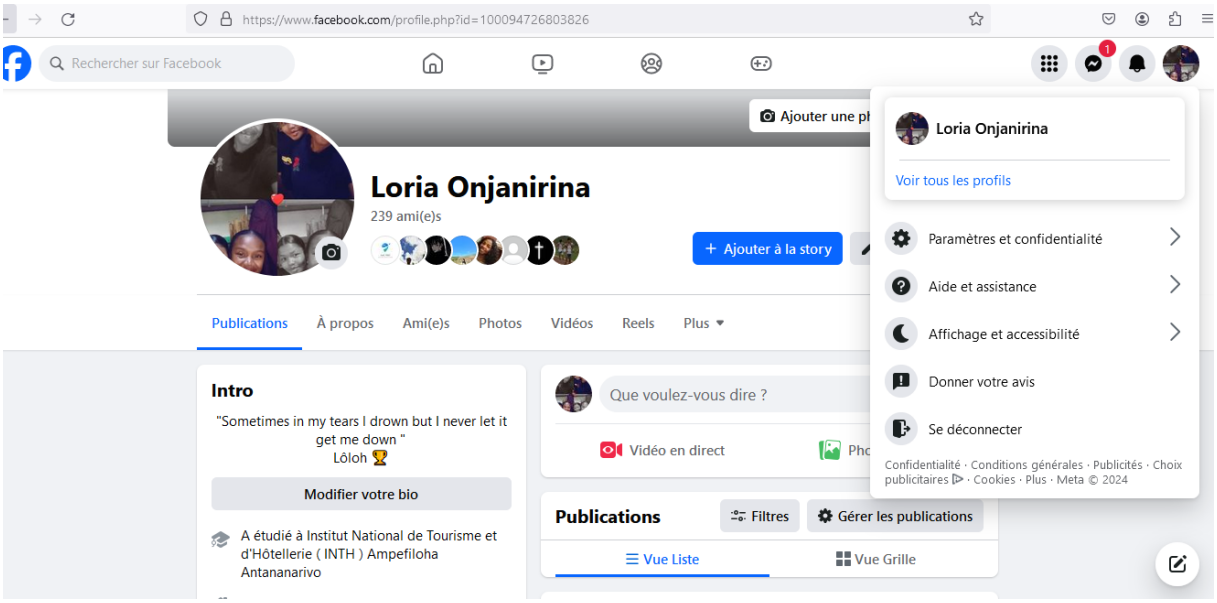
7 - Comprendre le suivi du navigateur

Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée

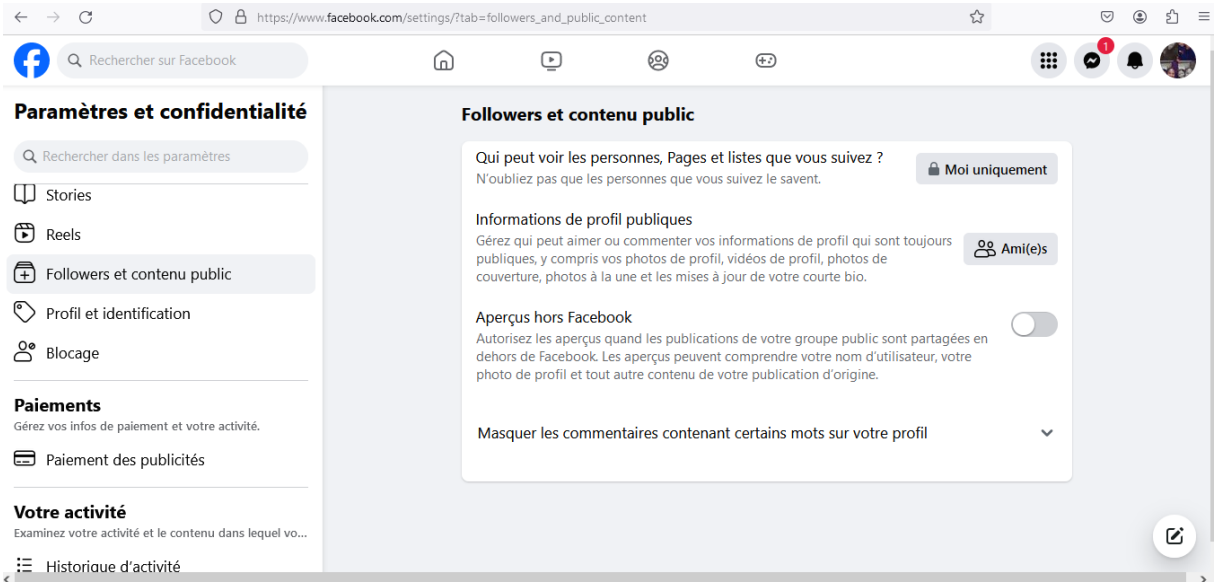
8 - Principes de base de la confidentialité des médias sociaux

Objectif : Régler les paramètres de confidentialité de Facebook

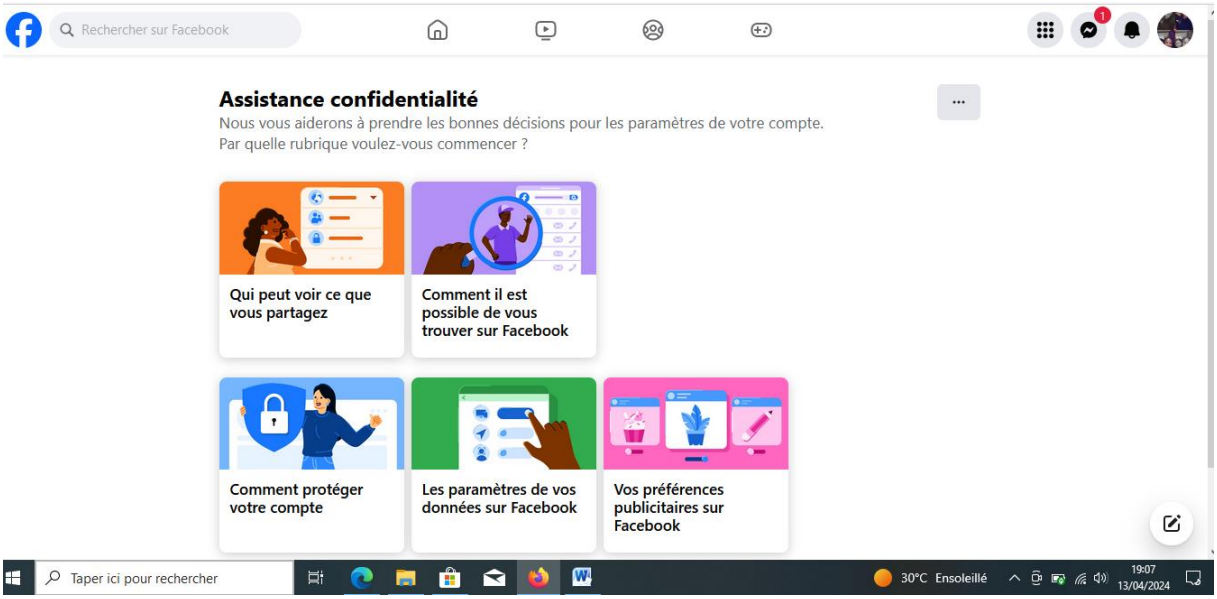
● Paramètres sur Facebook



●Paramètre et Confidentialité



● Assistance de confidentialité



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

Objectif :

- ✓ Exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé

Pour un ordinateur (PC/Mac) :

- ➢ Vérification des mises à jour :
  -Assurer que le système d'exploitation, les navigateurs web et les logiciels de sécurité sont tous à jour.
- ➢ Scan antivirus /antimalware :
  -Effectuer régulièrement des scans antivirus pour détecter d'éventuelles menaces.
- ➢ Vérification des paramètres de pare-feu :
  -Assurer que le pare-feu est activé et configuré correctement pour bloquer les connexions non autorisées.
- ➢ Test de phishing : Faire un test pour voir si vous pouvez repérer les e-mails de phishing ou les sites web frauduleux.
- ➢ Utilisation d'un VPN : Si possible, utiliser un VPN pour sécuriser la connexion internet, surtout sur des réseaux publics.
  Pour un Smartphone ou une tablette :
- ➢ Mises à jour système et application :
  -Assurer que le système d'exploitation et les applications sont à jour pour bénéficier des derniers correctifs de sécurité.

- Activation du verrouillage :
  -Utiliser un code PIN, un schéma ou une reconnaissance faciale /empreinte digitale pour verrouiller l'appareil.

- Autorisations des applications :
  -Vérifier régulièrement les autorisations accordées aux applications et révoquer celles qui semblent excessives ou suspectes.

- Test de sécurité des réseaux Wi-Fi :
  -Utiliser une application de test de sécurité des réseaux auxquels nous nous connectons.

- Chiffrement des données : Activer le chiffrement des données sur l'appareil pour protéger les informations personnelles en cas de perte ou de vol.

    - ✓ Exercices pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé :

Sur un ordinateur Windows :

- Installation de l'antivirus :

- Téléchargez l'antivirus de votre choix depuis le site officiel.

- Exécutez le fichier téléchargé et suivez les instructions pour installer le logiciel.

- Une fois installé, effectuez une mise à jour de la base de données de virus.

- Configuration de l'antivirus :

- Ouvrez l'interface de l'antivirus et explorez les paramètres de protection.

- Activez les fonctions de protection en temps réel, de balayage complet et de mise en quarantaine des fichiers suspects.

- Planifiez des analyses régulières de votre système.

- Exercice pratique :

- Lancez une analyse complète de votre ordinateur.

- Après l'analyse, vérifiez les résultats pour voir s'il y a des menaces détectées.

- Mettez en quarantaine ou supprimez les fichiers infectés, le cas échéant.

Sur un Smartphone Android :

- Installation de l'antivirus :

- Accédez au Google Play Store et téléchargez une application antivirus réputée.

- Installez l'application et suivez les étapes d'inscription si nécessaire.

- Mettez à jour la base de données de virus après l'installation.

- Configuration de l'antivirus :

- Ouvrez l'application antivirus et explorez les options de sécurité.

- Activez les fonctions telles que la protection en temps réel, le balayage automatique des nouvelles applications, etc.

- Configurez les paramètres de navigation sécurisée et de protection contre les logiciels malveillants.

- Exercice pratique :

- Lancez un balayage complet de votre Smartphone.

- Après le balayage, examinez les résultats pour identifier les menaces éventuelles.

- Supprimez ou mettez en quarantaine les applications ou fichiers suspects détectés