SAYNA

Parcours : DISCOVERY

Module : Naviguer en toute sécurité

Projet 1 - Un peu plus de sécurité, on n'en a jamais assez !

1-Introduction à la sécurité sur internet

Objectif : à la découverte de la sécurité sur internet

1/ En naviguant sur le web, voici trois articles qui parlent de sécurité sur internet.

- Article 1= Kaspersky-Qu'est-ce que la sécurité internet ?
- Article 2=La Poste-5 conseils pour être en sécurité sur internet
- Article 3=Cybermalveillance.gouv-Comment se protéger sur internet

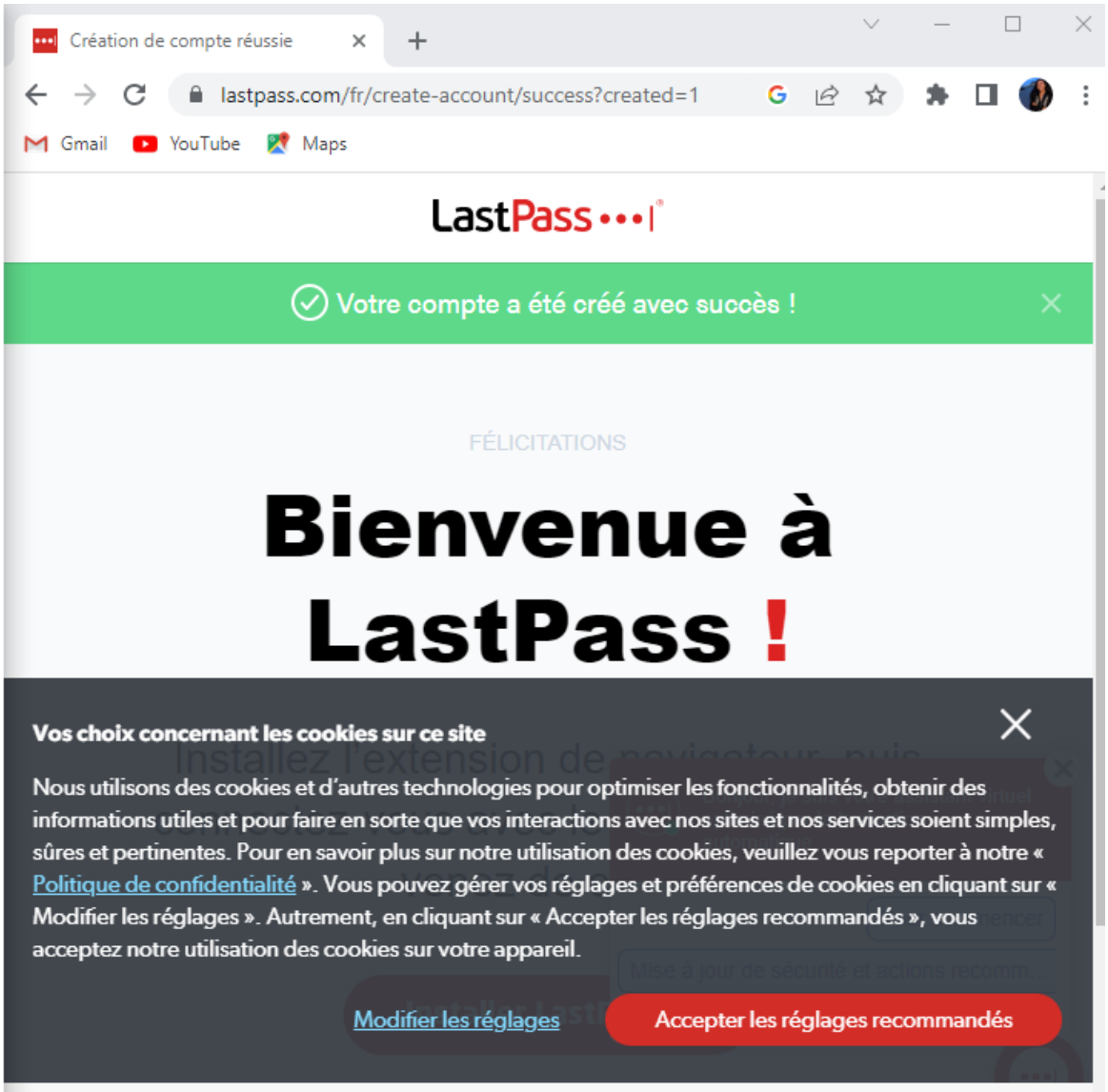
2- Création des mots de passe forts

Objectif : utilisation d'un gestionnaire de mot de passe LastPass

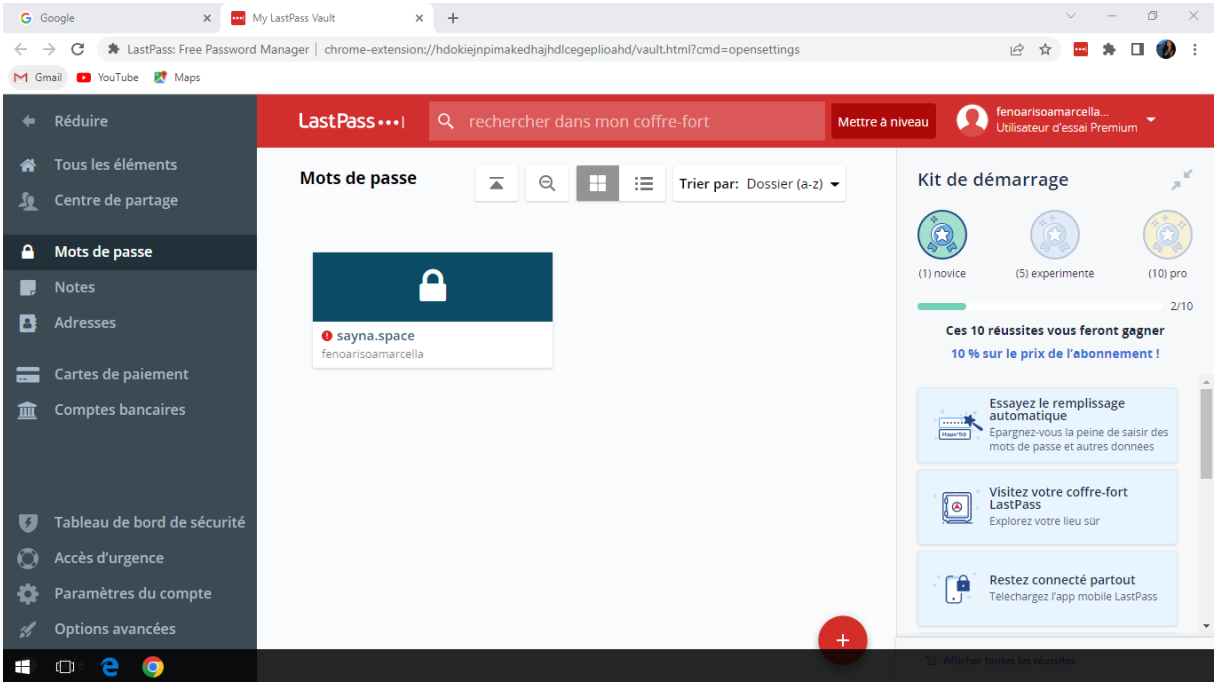
1/Utilisation d'un gestionnaire de mot de passe nommé LastPass en suivant les étapes.

Réponse 1 :

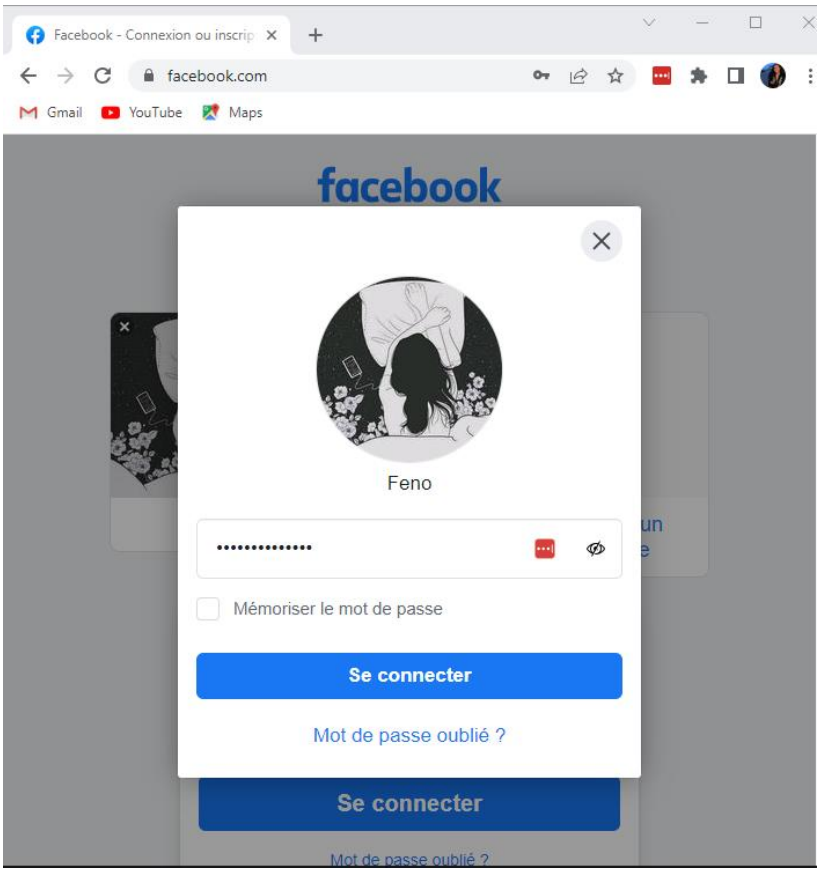
Création de mon compte LastPass :



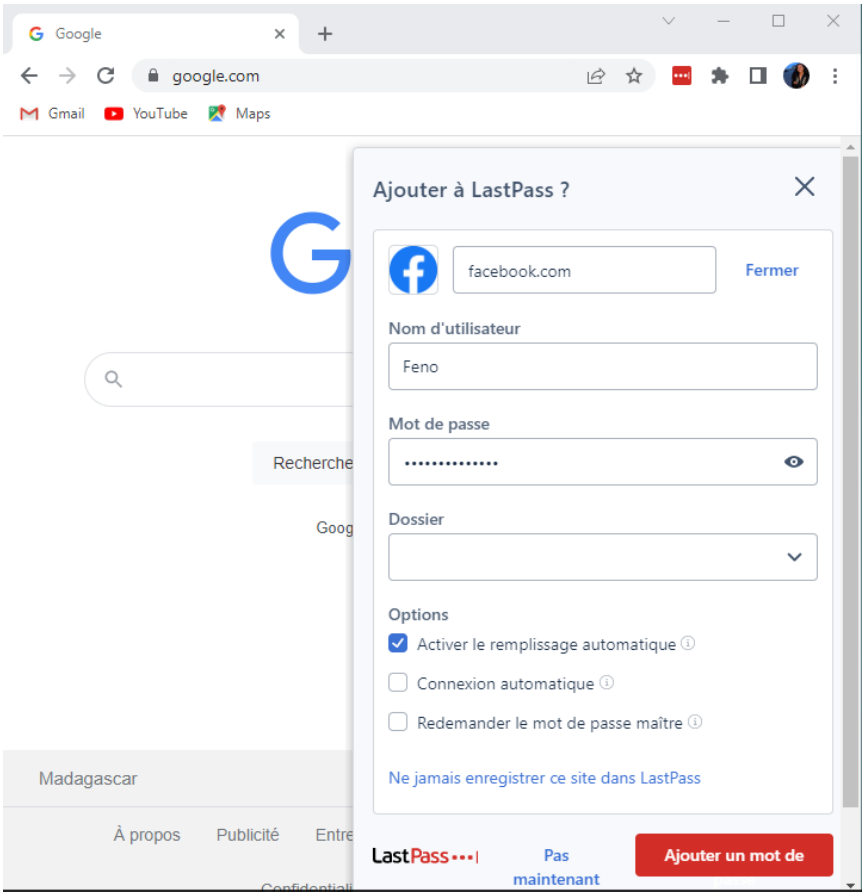
Quand j'ai accéder à la rubrique "Mot de passe" puis cliqué sur "Ajouter un élément".



On peut enregistrer les mots de passe dans LastPass



Ici j’ai ajouté à LastPass mon compte et mon mot de passe Facebook pour naviguer facilement la prochaine fois



3-Fonctionnalité de sécurité de mon navigateur

Objectif : Identification des éléments à observer pour naviguer sur le web en toute sécurité

1/Identification des adresses internet qui me semblent provenir de site web malveillants.

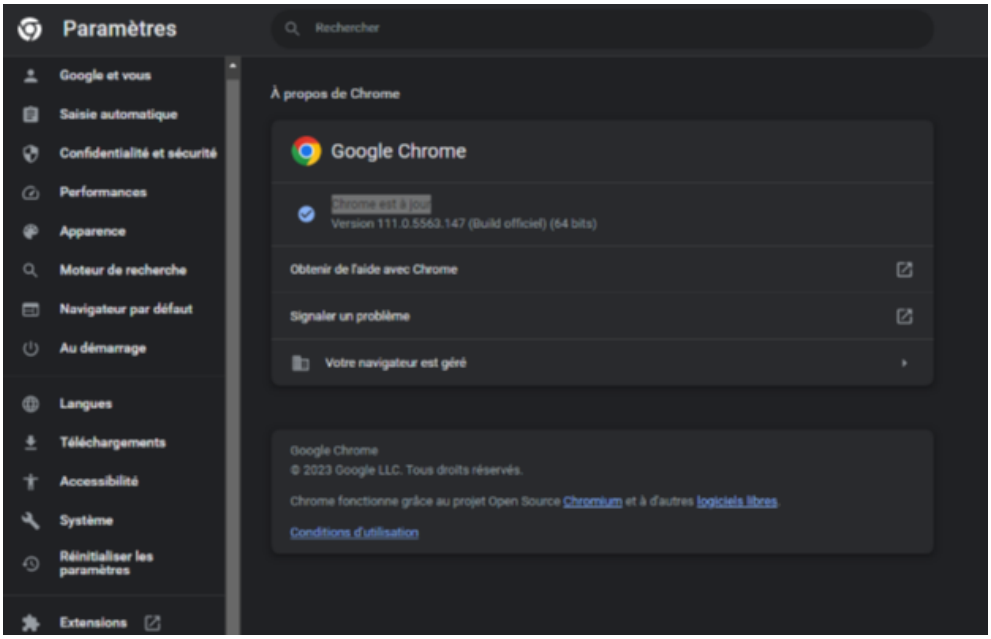
Réponse 1 :

Les sites web qui semblent être malveillants sont :

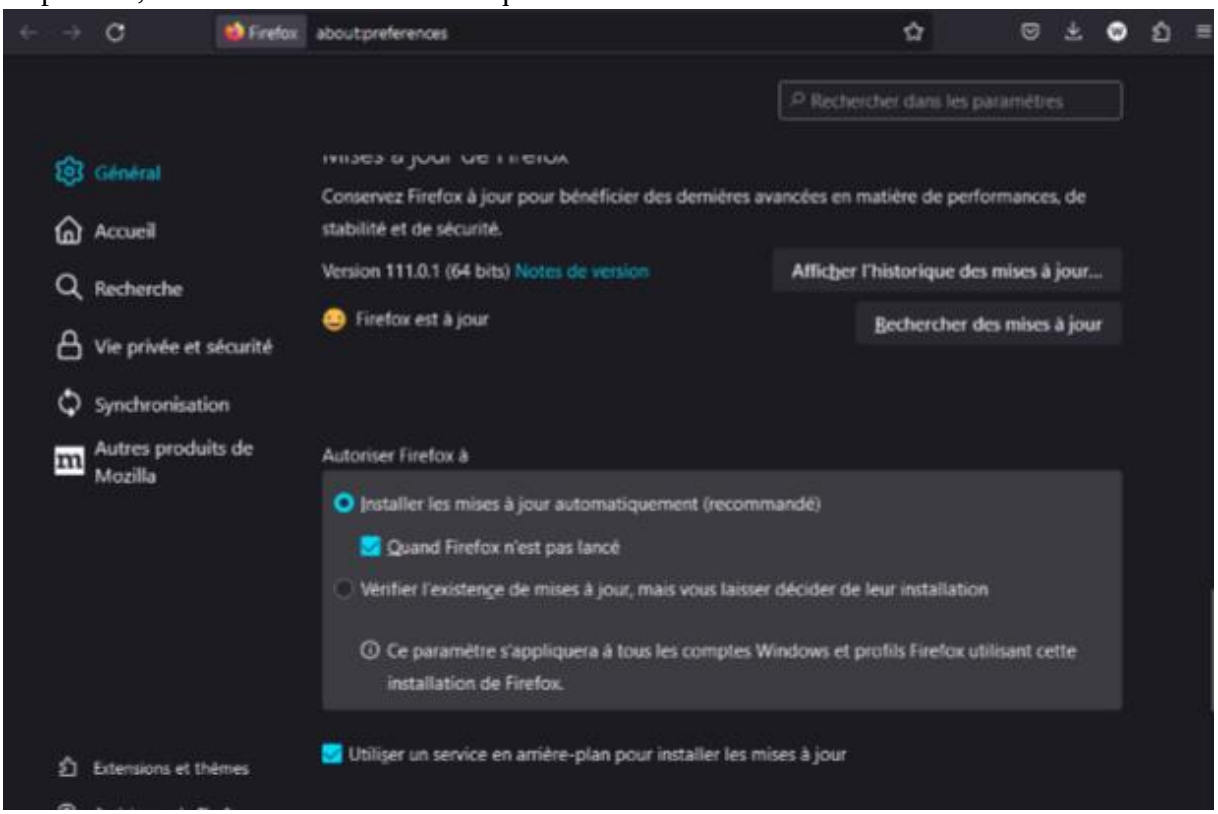
- www.morvel.com, le site web officiel est celui de l’univers Marvel (www.marvel.com)
- www.fessebook.com, le site web officiel est celui de Facebook(www.facebook.com)
- www.instagam.com, , le site web officiel est celui de l’Instagram (www.instagram.com)

2/Vérification si les navigateurs utilisés Chrome et Firefox sont à jour :

- Chrome : Il n'y a pas de mise à jour disponible pour le moment



- Firefox : il n'y a pas de mise à jour disponible pour le moment. Si une mise à jour est disponible, elle sera installée automatiquement.



4 - Éviter le spam et le phishing

Objectif : Reconnaître plus facilement les messages frauduleux

1-Exercice de capacité à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.

Réponse 1 :

En accédant au lien et en suivant les étapes qui y sont décrites. Voici le résultat du quizz que j'ai fait

5 - Comment éviter les logiciels malveillants

Objectif : sécuriser votre ordinateur et identifier les liens suspects

1/Analyse des informations de plusieurs sites en précisant pour chaque site l'indicateur de sécurité et le rapport d'analyse de l'outil Google.

Réponse 1 :

- Site n°1 : https://vostfree.ws/
  - **Indicateur de sécurité**
    - HTTPS
  - **Analyse Google**
    - Aucun contenu suspect
- Site n°2 : https://www.tv5monde.com/
  - **Indicateur de sécurité**
    - HTTPS
  - **Analyse Google**
    - Aucun contenu suspect
- Site n°3 : http://www.baidu.com/

- **Indicateur de sécurité**
  - Not secure
- **Analyse Google**
  - Vérifier un URL en particulier

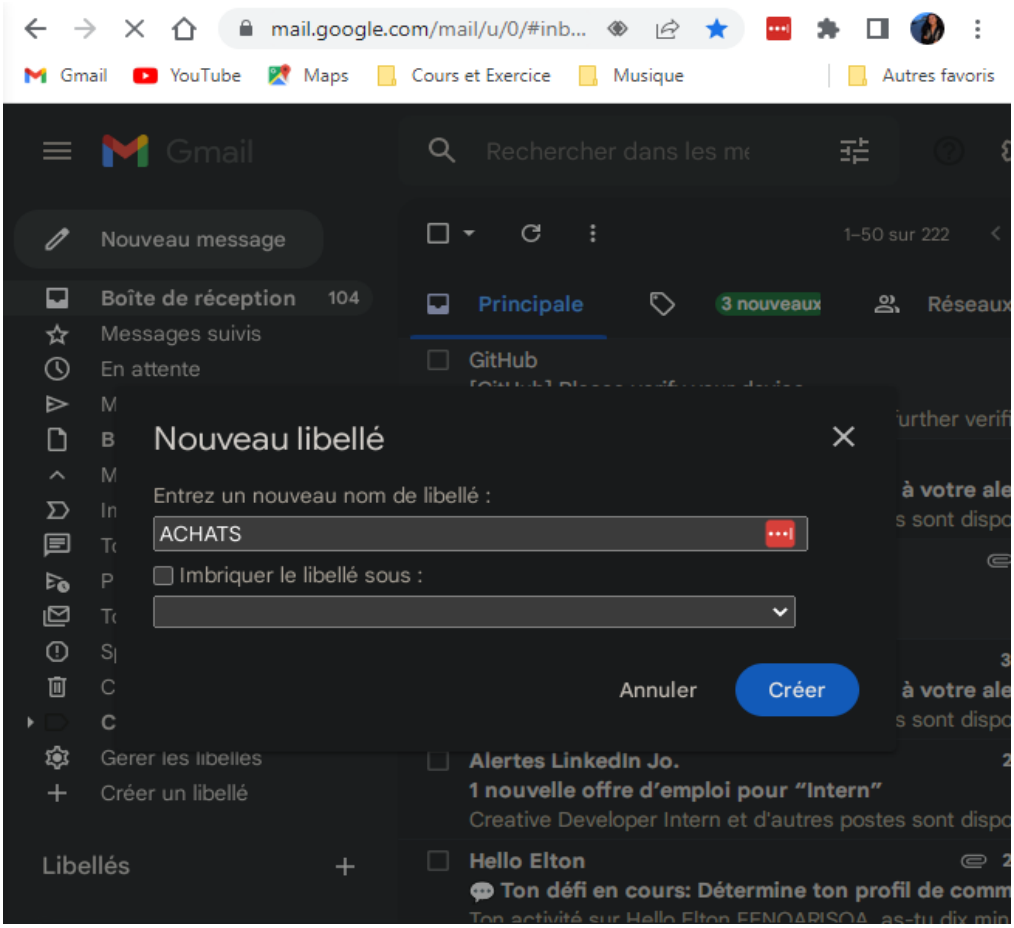
6 - Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

1/Création d'un registre des achats.

Réponse 1 :

Pour commencer, j'ai accéder à ma messagerie électronique en ouvrant un onglet dans la barre des favoris, puis sur la page d'accueil, j'ai cliqué sur « plus » ensuite sur le libellé j'ai créé un nouveau libellé nommer « ACHATS » et enfin sur le bouton « créer » pour valider l'opération. Voici l'image qui le montre :



Pour mes études :

Je vais utiliser des libellés pour organiser mes cours en ligne, mes projets en cours, mes devoirs à rendre.

Pour la formation : Je vais utiliser des libellés pour suivre mes sessions de formation, définir mes objectifs de formation et mes programmes de certification

Pour les informations personnelles : Je vais créer des libellés pour gérer la liste de tous mes messages personnels.

7 - Comprendre le suivi du navigateur

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

- Les cookies peuvent également être utilisés pour suivre votre comportement en ligne et collecter des informations sur vous, y compris des données sensibles comme les identifiants de connexion ou les informations de carte de crédit. Par conséquent, la gestion des cookies est essentielle pour garantir la protection de votre vie privée en ligne
- L'utilisation de la navigation privée est une autre pratique importante pour protéger votre vie privée en ligne. La navigation privée est un mode de navigation qui ne conserve pas l'historique de navigation, les cookies ou les données de formulaire. Cela signifie que les sites web que vous visitez ne pourront pas collecter d'informations sur vous pendant que vous naviguez en mode privé.
- La gestion des cookies et l'utilisation de la navigation privée sont des pratiques importantes pour protéger la vie privée en ligne. Cependant, elles ne garantissent pas une sécurité totale et doivent être utilisées en complément d'autres mesures de sécurité en ligne, comme l'utilisation de logiciels antivirus et le choix de mots de passe forts et uniques.

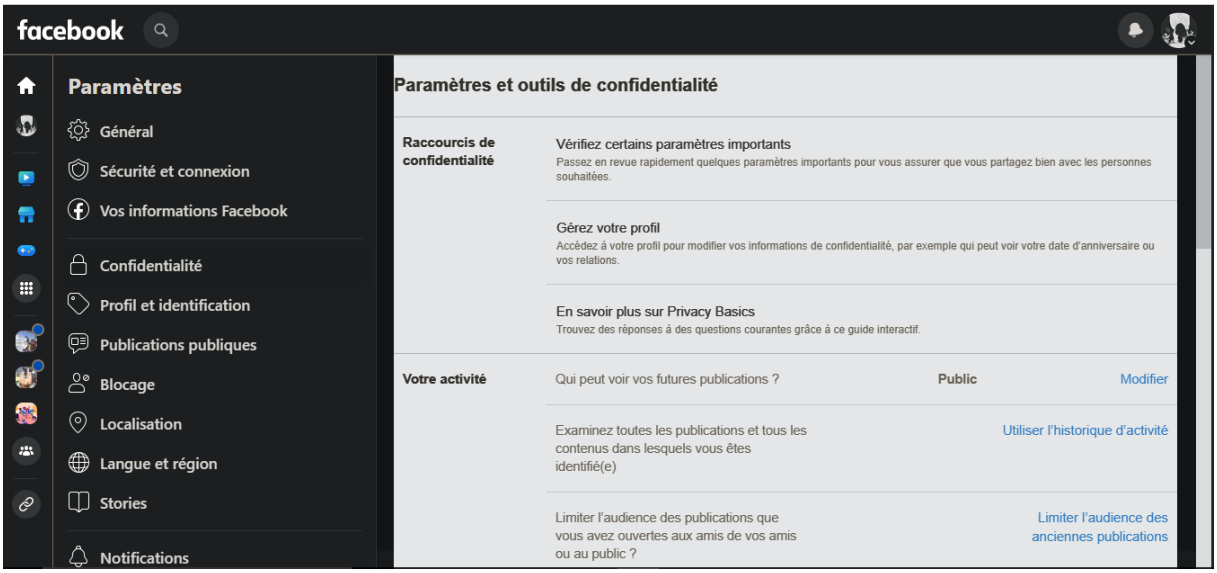
8 - Principes de base de la confidentialité des médias sociaux

Objectif : Régler les paramètres de confidentialité de Facebook

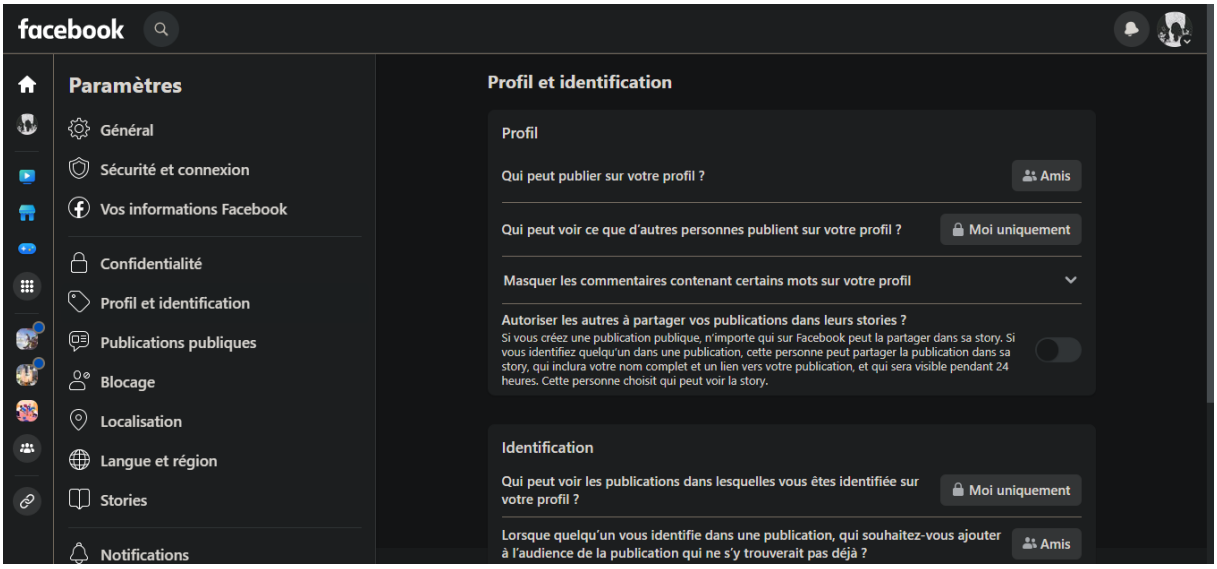
Réponse 1 :

Voici le paramétrage de mon compte Facebook :

- Confidentialité :



- Profil et identification :



On peut trouver le même type de paramétrage sur les autres médias.

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

1-Vérification de la sécurité en fonction de l'appareil utilisé :

Voici quelques étapes que vous pouvez suivre pour assurer la sécurité de vos appareils :

1. Mettez à jour vos logiciels et systèmes d'exploitation : les mises à jour de sécurité sont importantes pour corriger les vulnérabilités et les failles de sécurité dans vos logiciels et systèmes d'exploitation.
2. Utilisez un logiciel antivirus : un logiciel antivirus est essentiel pour protéger votre ordinateur et votre téléphone contre les virus, les malwares et autres menaces en ligne.

3. Utilisez des mots de passe forts et uniques : utilisez des mots de passe différents pour chaque compte et utilisez des combinaisons de chiffres, de lettres et de caractères spéciaux pour rendre les mots de passe plus difficiles à deviner.
4. Vérifiez les paramètres de confidentialité : vérifiez les paramètres de confidentialité de votre ordinateur et de votre téléphone pour vous assurer que vos informations personnelles sont protégées.
5. Utilisez des connexions sécurisées : évitez de vous connecter à des réseaux Wi-Fi publics non sécurisés, car ils peuvent être utilisés pour intercepter vos données.
6. Vérifiez régulièrement vos comptes en ligne : vérifiez régulièrement l'activité de vos comptes en ligne pour détecter toute activité suspecte ou non autorisée.
7. Utilisez des outils de sécurité supplémentaires : en fonction de vos besoins et de votre utilisation d'Internet, vous pouvez utiliser des outils de sécurité supplémentaires tels que des VPN (réseau privé virtuel) ou des extensions de navigateur pour bloquer les publicités et les trackers.

   En suivant ces étapes, vous pouvez réduire les risques de sécurité et assurer la protection de vos appareils.

2/ Je propose un exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé.

Alors je choisis McAfee pour faire une exemple :

- Tout d'abord, rendez-vous sur le site officiel de McAfee pour télécharger le logiciel d'installation : https://www.mcafee.com/enus/downloads/. Assurez-vous de télécharger la version compatible avec votre système d'exploitation.
- Une fois le téléchargement terminé, double-cliquez sur le fichier d'installation pour lancer le processus d'installation. Suivez les instructions à l'écran pour installer le logiciel.
- Une fois l'installation terminée, ouvrez McAfee et suivez les instructions pour configurer le programme. Vous pouvez choisir les paramètres de numérisation et les options de sécurité en fonction de vos préférences.
- Pour lancer une numérisation, cliquez sur le bouton "Analyser" dans l'interface de McAfee. Vous pouvez choisir de numériser tout votre système ou des fichiers spécifiques.
- En cas de détection de menaces, McAfee vous avertira et vous proposera des options pour supprimer ou mettre en quarantaine les fichiers infectés.
- Vous pouvez également configurer des paramètres de planification pour que McAfee effectue des numérisations régulières de votre système, ou exécuter manuellement une numérisation à tout moment.
- Pour finir, il est important de garder McAfee à jour en téléchargeant les dernières mises à jour de sécurité pour vous protéger contre les nouvelles menaces.