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

2 - Créer des mots de passe forts

3 - Fonctionnalité de sécurité de votre navigateur

4 - Éviter le spam et le phishing

5 - Comment éviter les logiciels malveillants

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 par un virus

1 - Introduction à la sécurité sur Internet

Objectif : *à la découverte de la sécurité sur internet*

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

**Pense à vérifier la source des informations et essaie de consulter des articles récents pour que les informations soient à jour. Saisis le nom du site et de l’article.**

● Article 1 = *nom du site - nom de l’article*

● Article 2 = *nom du site - nom de l’article*

● Article 3 = *nom du site - nom de l’article*

**Réponse 1**

# ● Article 1 = LA POSTE PRO - 5 conseils pour être en sécurité sur Internet

<https://www.laposte.fr/professionnel/conseils-pour-etre-en-securite-sur-internet>

# ● Article 2 = Karpersky - Confidentialité et sécurité sur Internet : 5 conseils de sécurité

<https://www.kaspersky.fr/resource-center/preemptive-safety/internet-privacy--security-5-safety-tips>

● Article 3 = SiteW - 20 Conseils pour être en sécurité sur internet

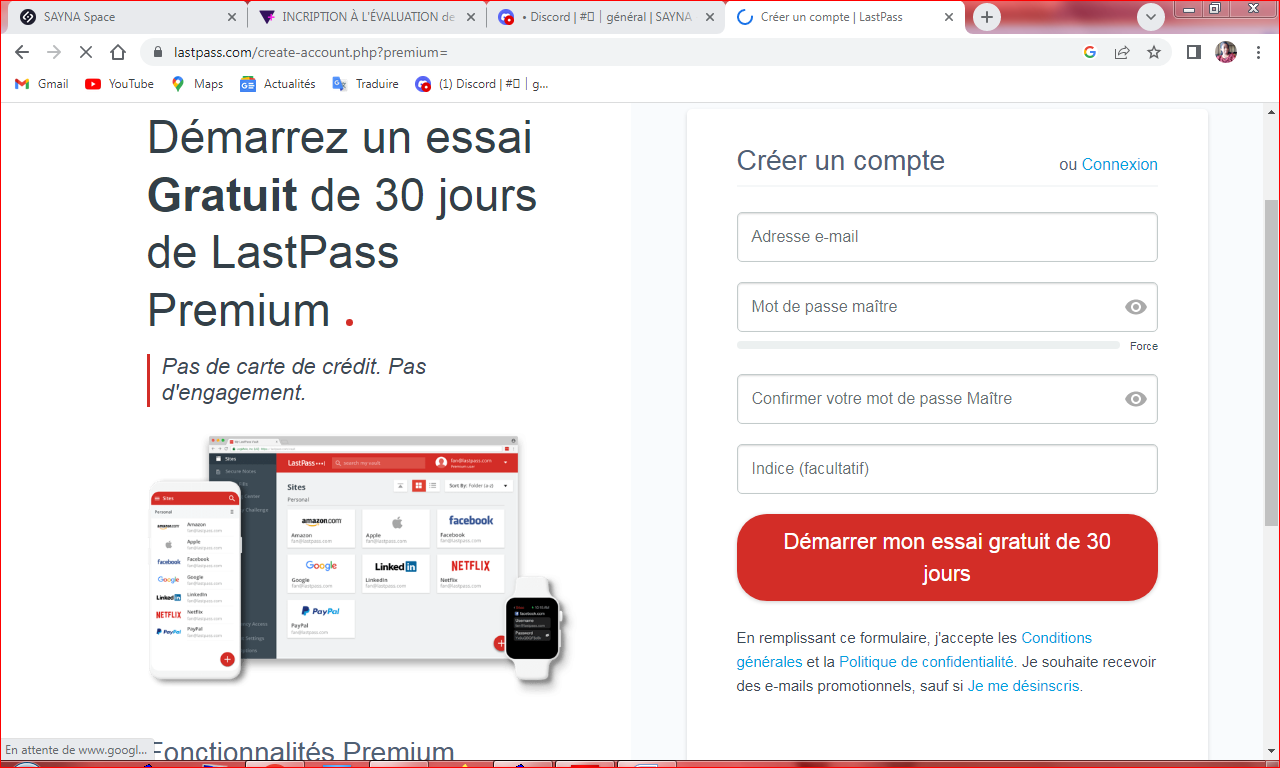
<https://www.sitew.com/Conseils-experts-en-creation-de-site/securite-informatique>

2 - Créer des mots de passe forts

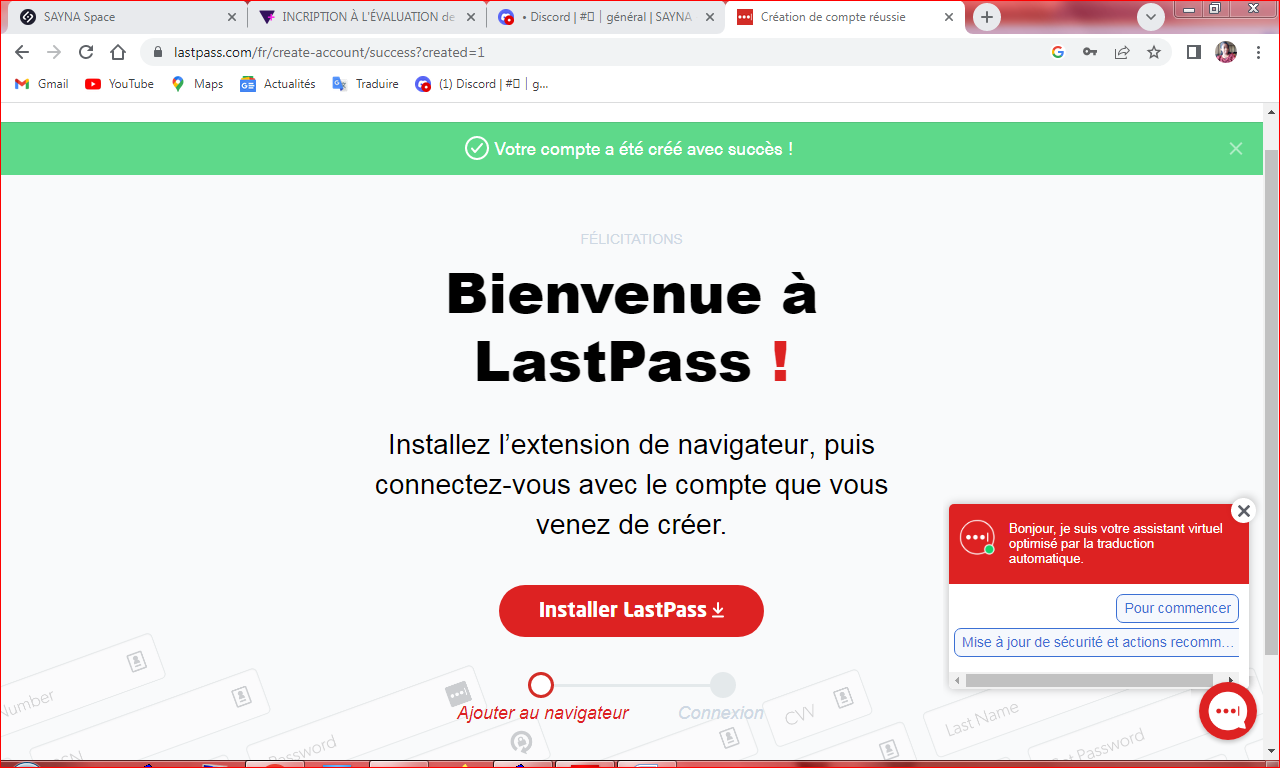
Objectif : *utiliser un gestionnaire de mot de passe LastPass*

**1/ Dans cet exercice, nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Ce gestionnaire prend la forme d’une application web, accessible sur tous supports (PC, Mac, mobile). Il est simple à prendre en main et propose un niveau de sécurité optimal. Suis les étapes suivantes. (case à cocher)**

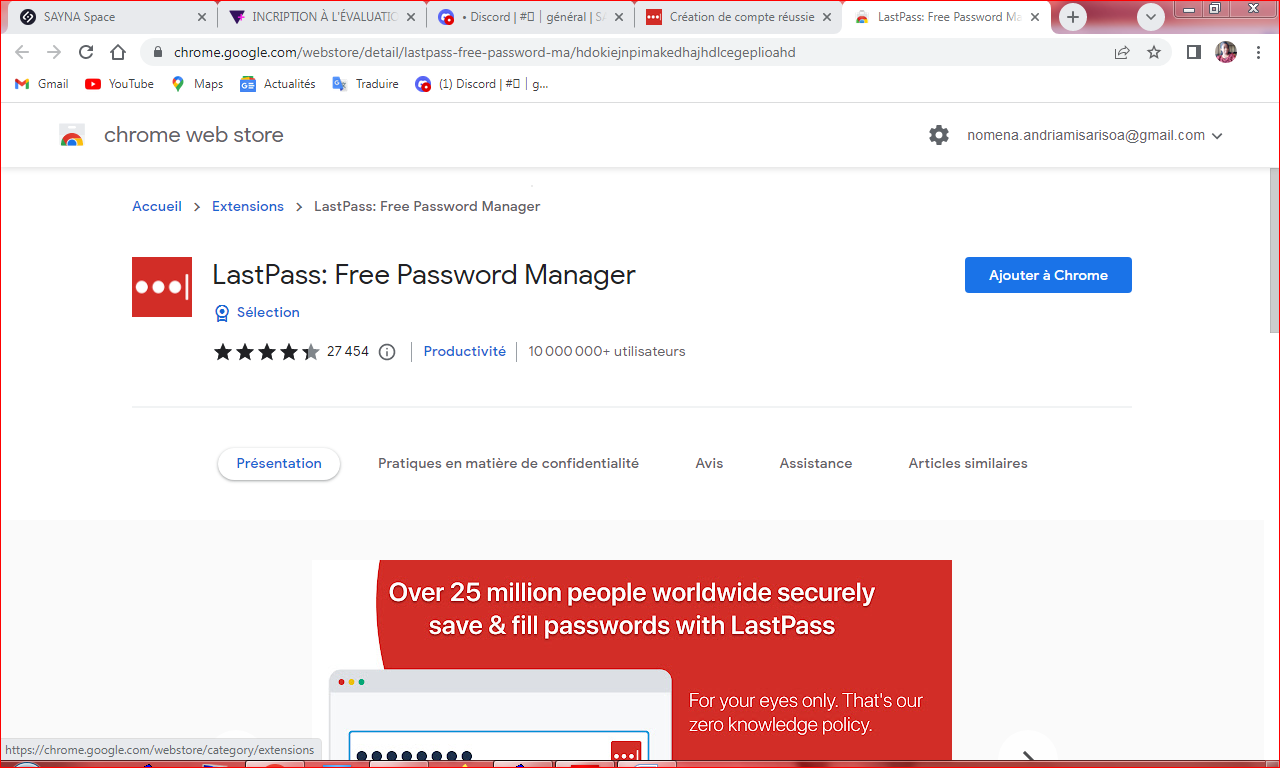
● Accède au site de LastPass



● Une fois la création du compte effectuée, j’arrive sur une page de validation qui propose le téléchargement de l’extension sur mon navigateur. Lance l’installation en effectuant un clic sur le bouton prévu à cet effet.



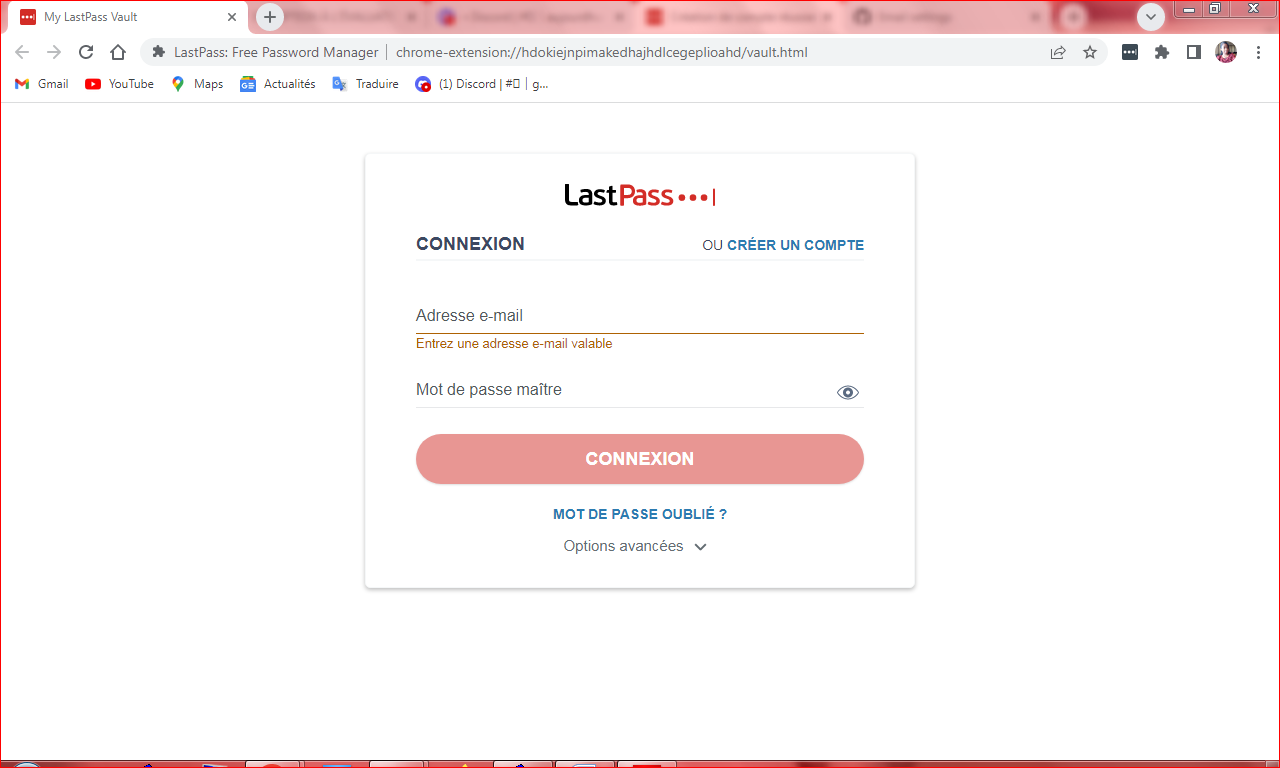
● Il me suffit de valider l’opération sur le Chrome Web Store en effectuant un clic sur le bouton “Ajouter à Chrome”.



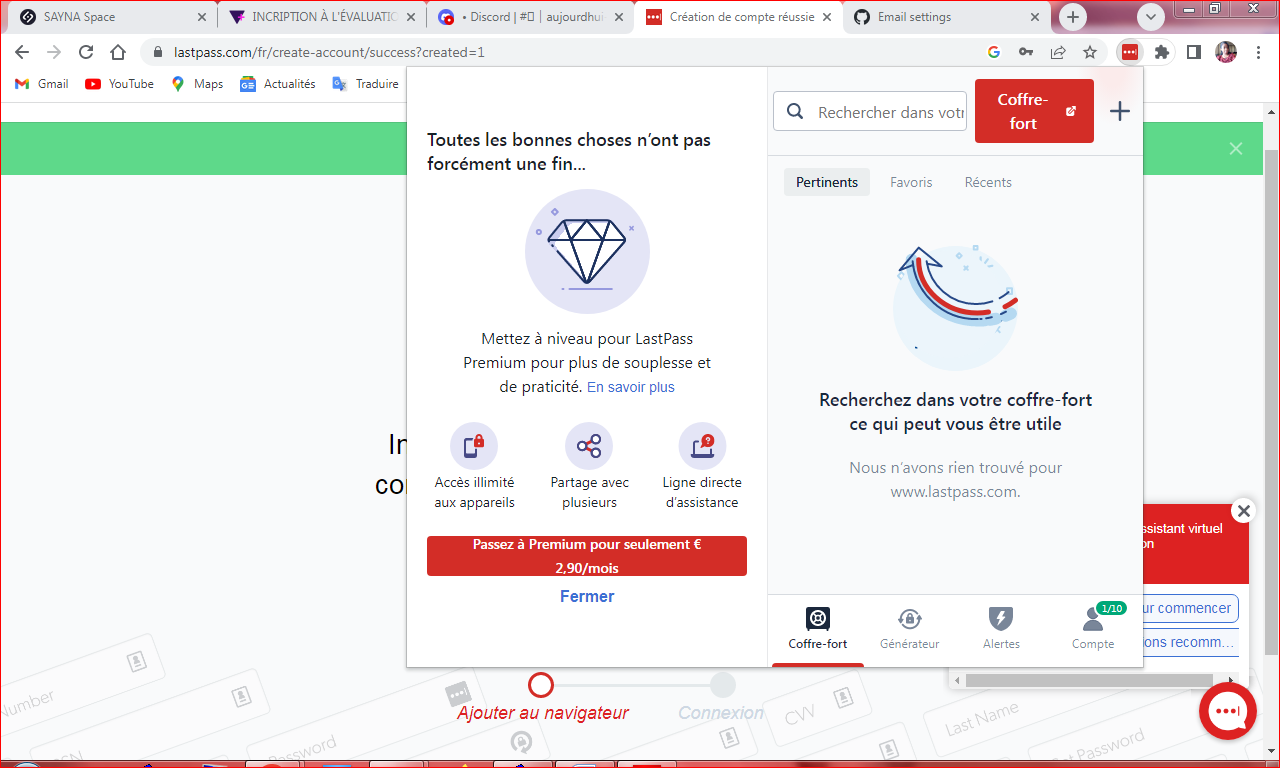
● Une fois installé, il me suffit d’accéder à cette extension et de m’y connecter

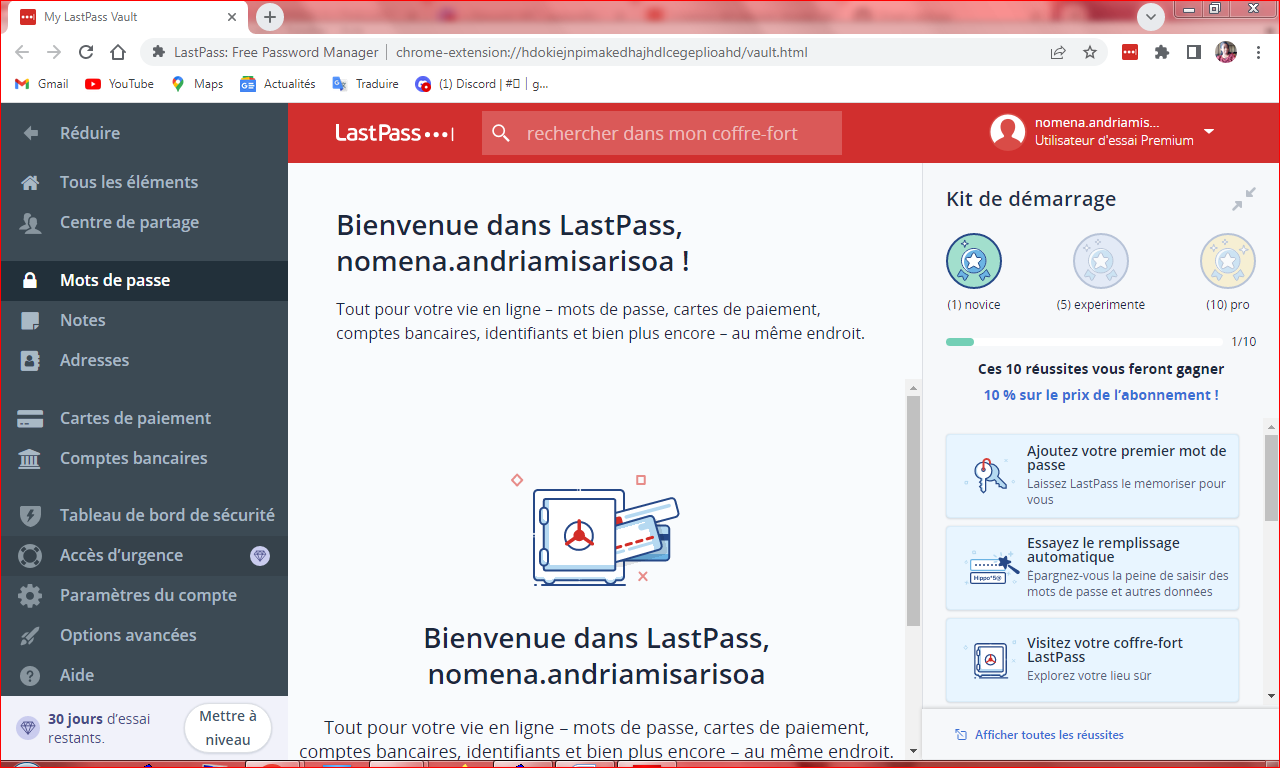
○ (1) En haut à droite du navigateur, clic sur le logo “Extensions”

○ (2) Épingle l’extension de LastPass avec l’icône



○ Il ne me reste plus qu’à me connecter en effectuant un clic sur l’icône de l’extension et en saisissant mon identifiant et mot de passe



Je connais maintenant les grandes lignes de l’utilisation du gestionnaire de mot de passe

LastPass.

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.**

**(case à cocher)**

● www.morvel.com

● www.dccomics.com

● www.ironman.com

● www.fessebook.com

● www.instagam.com

**Réponse 1**

Les sites web qui semblent être malveillants sont :

● www.morvel.com, un dérivé de [www.marvel.com](http://www.marvel.com) , le site web officiel de l’univers Marvel

● www.fessebook.com, un dérivé de [www.facebook.com](http://www.facebook.com) , le plus grand réseau social du monde

● www.instagam.com, un dérivé de [www.instagram.com](http://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)

**2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox**

**dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes. (case à**

**cocher)**

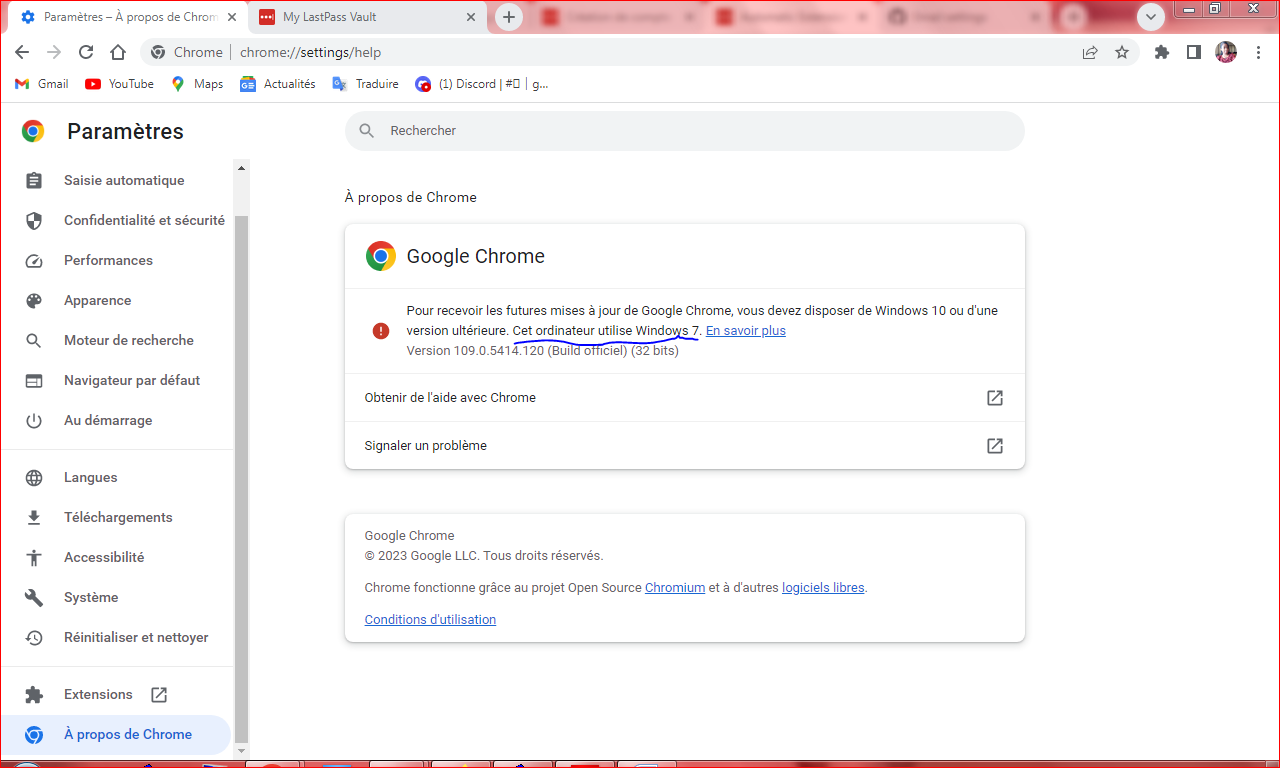
● Pour Chrome

○ Ouvre le menu du navigateur et accède aux “Paramètres”

○ Clic sur la rubrique “A propose de Chrome”

○ Si tu constates le message “Chrome est à jour”, c’est Ok

Dans mon navigateur Chrome, il indique cela : « Pour recevoir les futures mises à jour de Google Chrome, vous devez disposer de Windows 10 ou d'une version ultérieure. Cet ordinateur utilise Windows 7. »

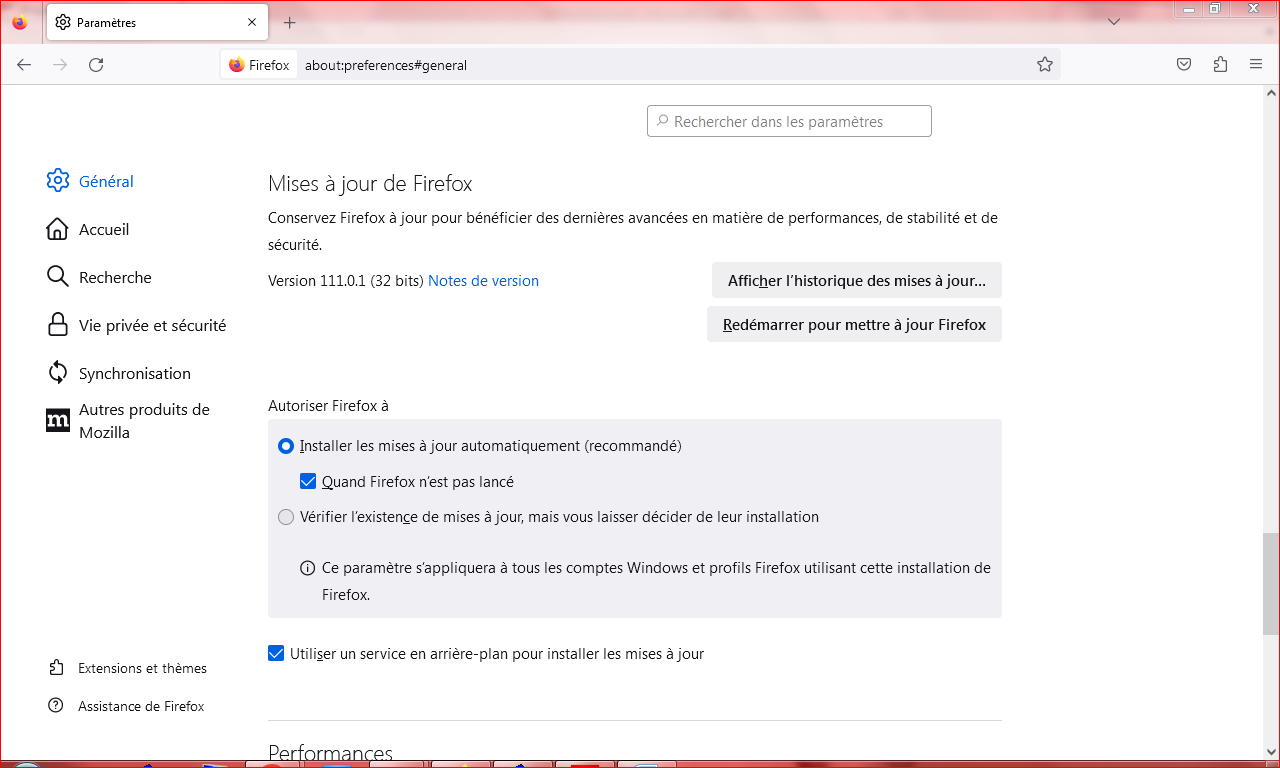


● Pour Firefox

○ Ouvre le menu du navigateur et accède aux “Paramètres”

○ Dans la rubrique “Général”, fais défiler jusqu’à voir la section “Mise à jour de Firefox (astuce : tu peux également saisir dans la barre de recherche (2) “mises à jour” pour tomber directement dessus)

Pour mon ordinateur, c’est encore Windows 7 et j’ai déjà fait une mise à jour alors le résultat est comme ça :



4 - Éviter le spam et le phishing

Objectif : *Reconnaître plus facilement les messages frauduleux*

**1/ Dans cet exercice, on va exercer ta capacité à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.**

Pour ce faire accède au lien suivant et suis les étapes qui y sont décrites : Exercice 4 - Spam et Phishing

