SAYNA-SECURITE-PROJET1

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

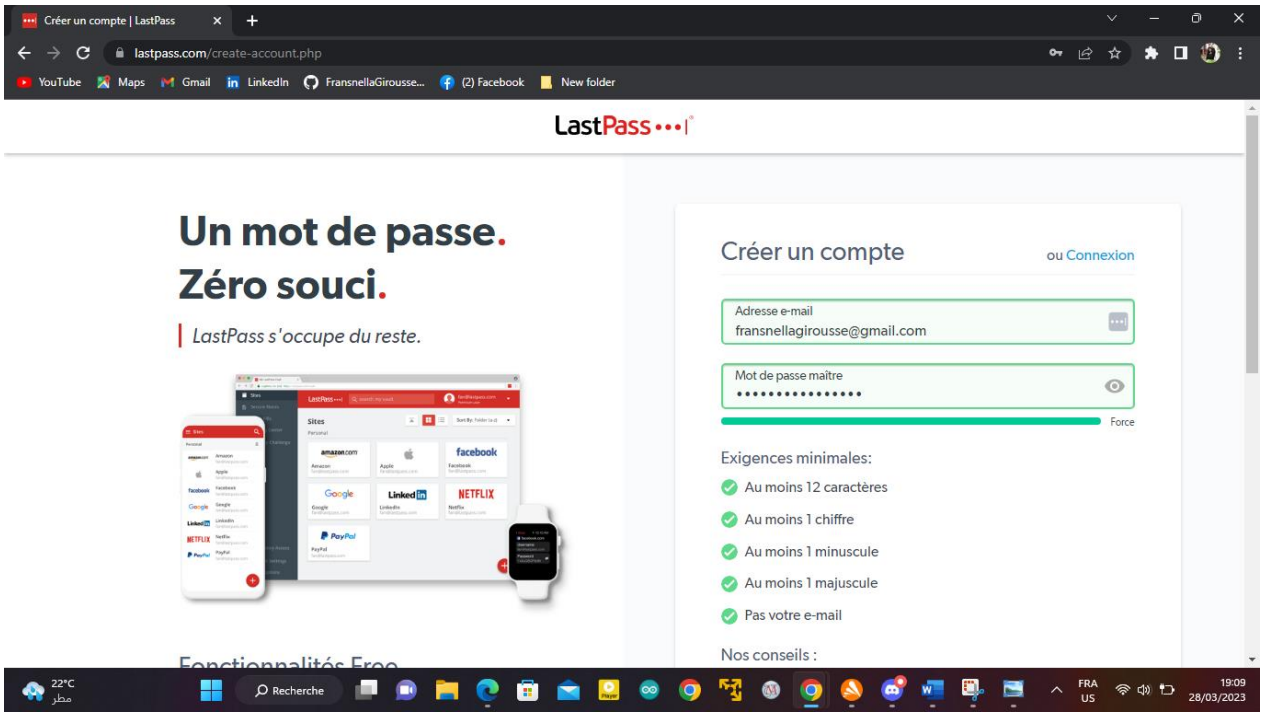
Voici trois articles qui parlent de sécurité sur internet avec lien du page :

1- Norton: https://fr.norton.com/ - Les risques du Wi-Fi public.
2- ANSSI: https://www.ssigouv.fr/ - Agir au cœur des territoires pour la sécurité numériques.
3- Le Journal du Net : https://www.journaldunet.fr/ - L'IoT, barrière aux catastrophes naturelles.

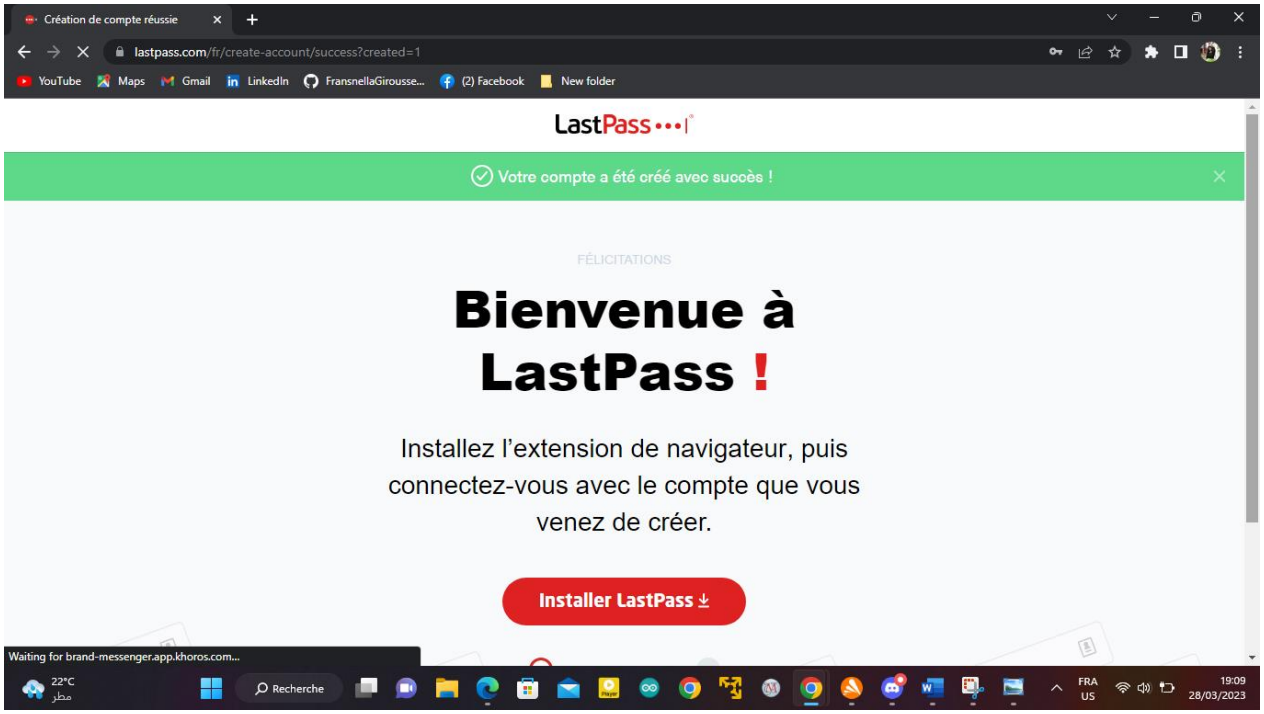
2 - Créer des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass

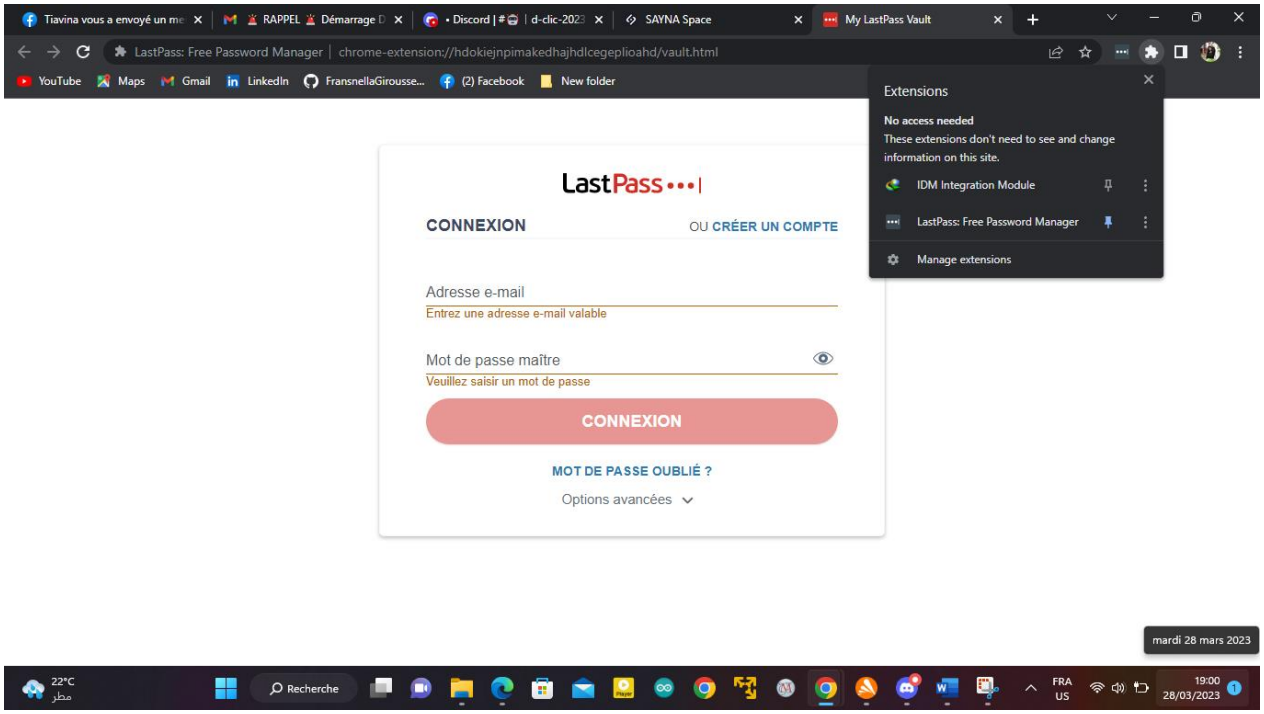
J'ai pu voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Donc J'ai suivi les étapes sur le site LastPass en remplissant le formulaire et créer mon mot de passe maître.

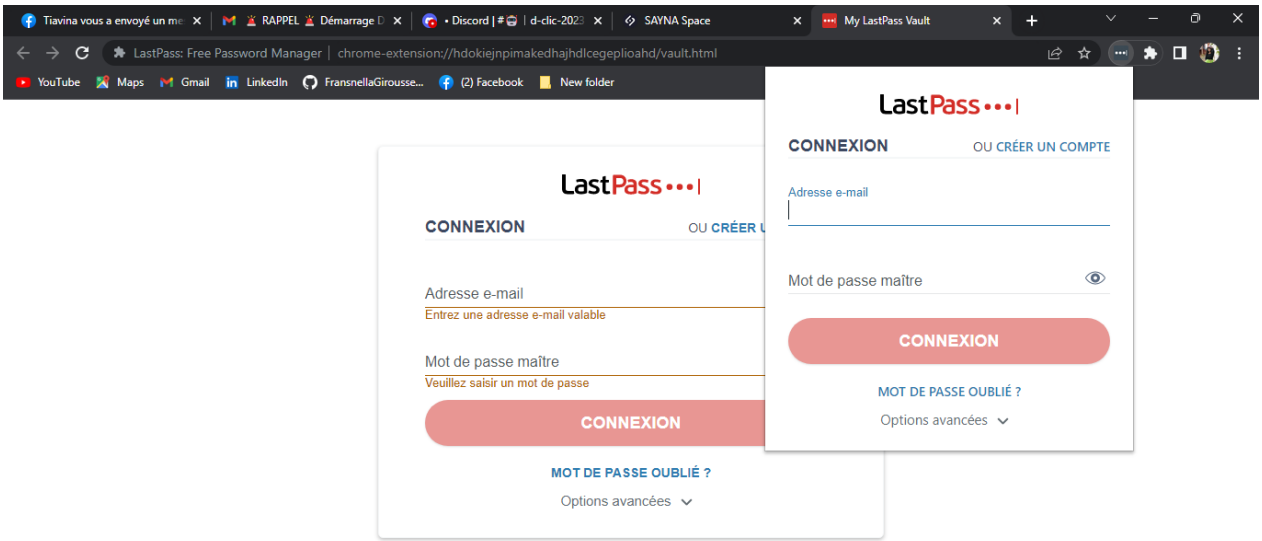


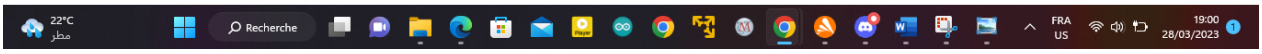
- Puis j’ai installer et ajouter l’exetension avec chrome.



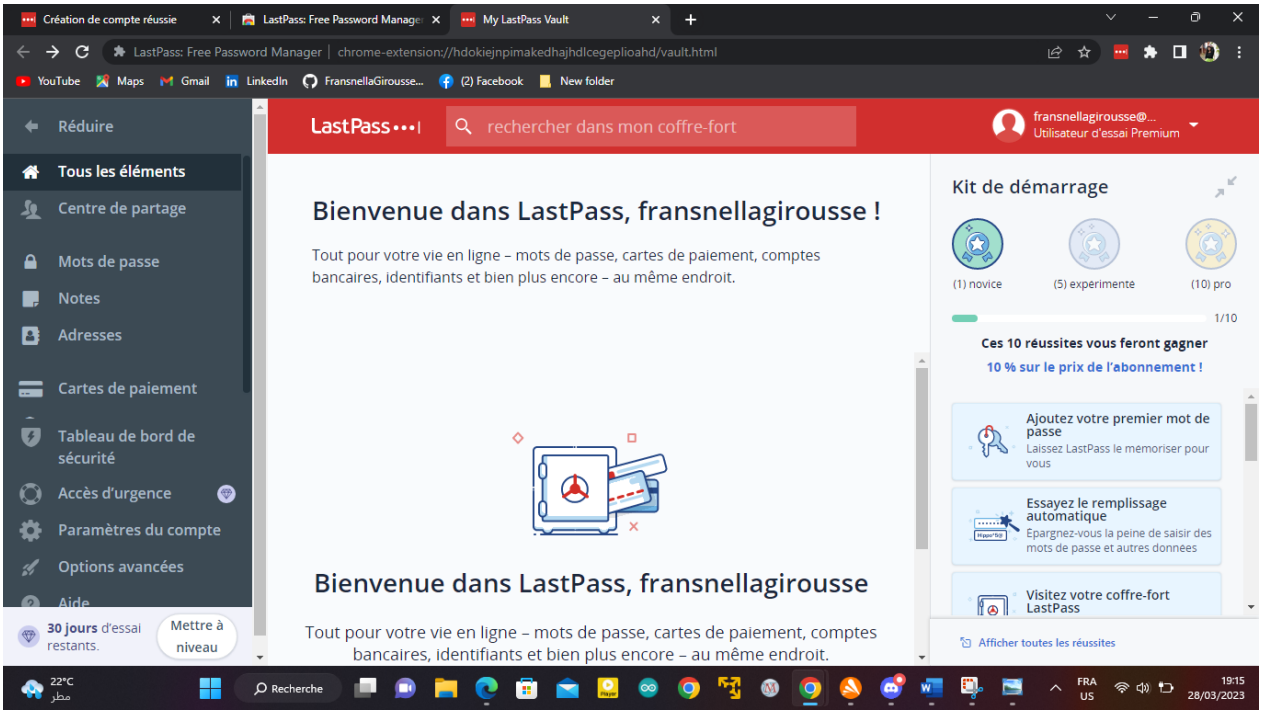
- J’ai épingle l’extension de LastPass.



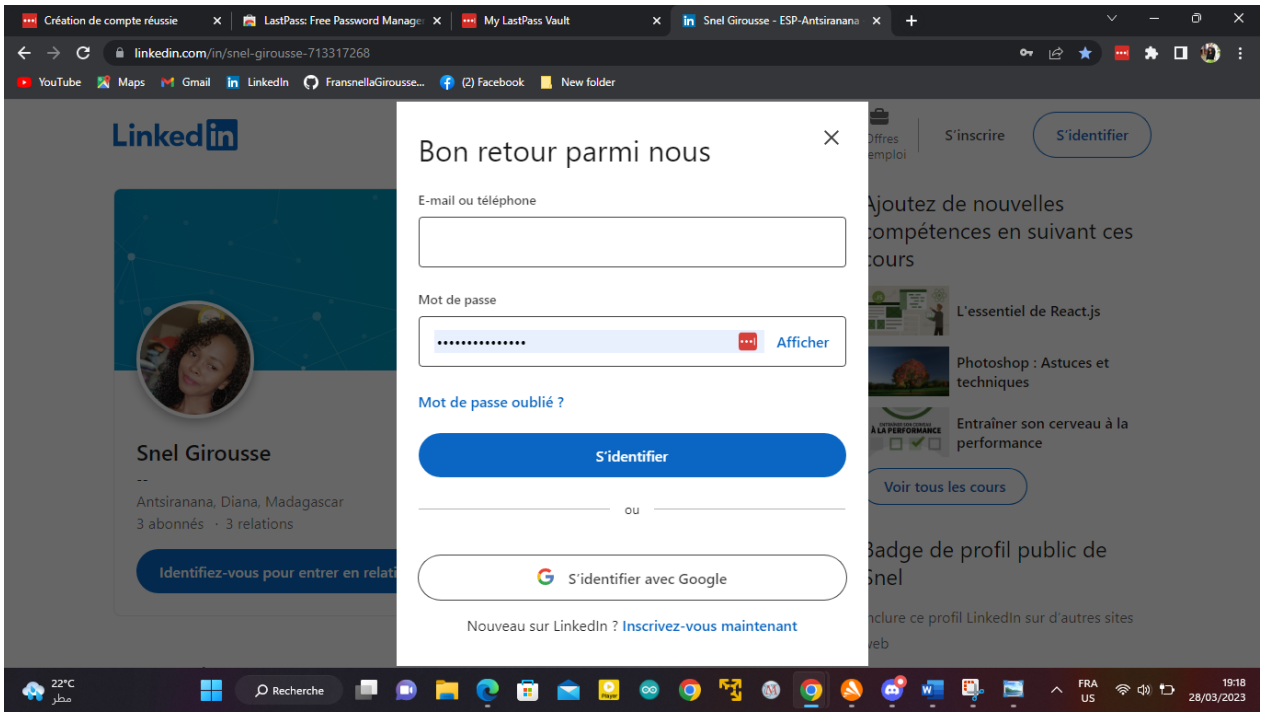




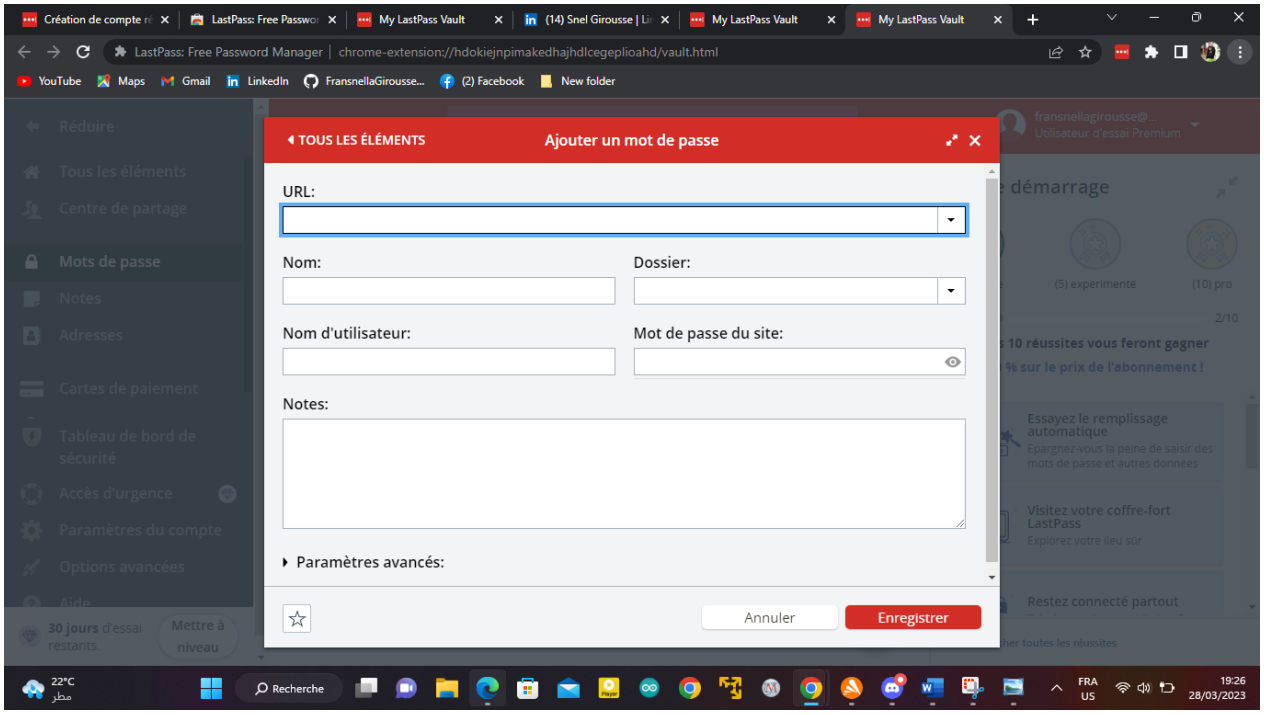
➢ Ensuite je me suis connecté avec mon compte sur Lastpass.



➢ Désormais, lorsque je me connecte à mes comptes, je peux enregistrer le mot de passe grâce à LastPass , je prends un exemple par mon compte LinkedIn.



- Je peux également ajouter des informations supplémentaires, telles que l'URL du site web et des notes.



3 - Fonctionnalité de sécurité de votre navigateur

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

1- Parmi les sites internet mentionnées, Les sites web qui semblent être malveillants sont :

- www.fessebook.com
- www.instagam.com

Elles sont peut-être des fautes d'orthographe intentionnelles des sites populaires comme « www.facebook.com » et « www.instagram.com » . Et les cybercriminalités peuvent utiliser des noms de domaine similaires pour piéger les utilisateurs en leur faisant croire qu'ils visitent un site de confiance.

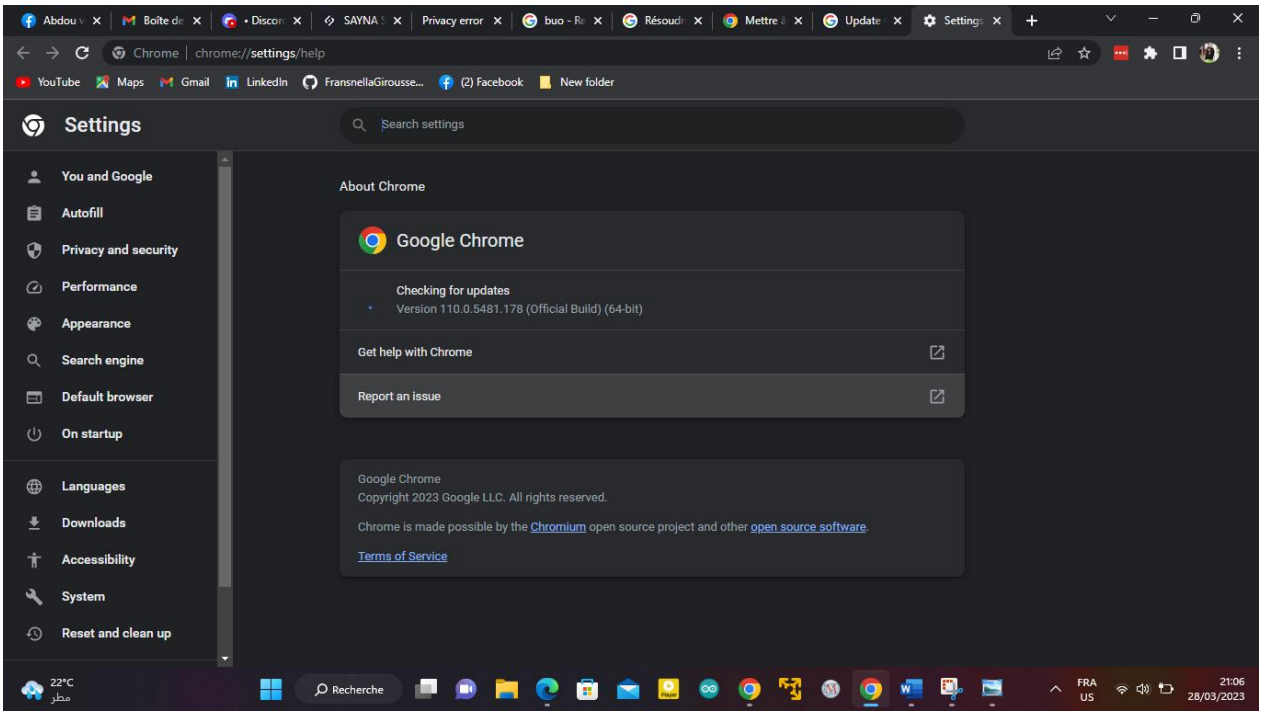
Les sites qui sont cohérents sont donc :

- www.morvel.com
- www.dccomics.com
- www.ironman.com

Ce sont des adresses de site web légitimes.

2- Les mis à jour des navigateurs (Chrome et Firefox).

J'ai comme navigateur Chrome et voilà :



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

j'ai utilisé ce lien « https://transparencyreport.google.com/ » pour l'analyse google :

- Site n°1

Indicateur de sécurité

- HTTPS

Analyse Google

- Aucun contenu suspect

- Site n°2

Indicateur de sécurité

- HTTPS

Analyse Google

- Aucun contenu suspect

- Site n°3

Indicateur de sécurité

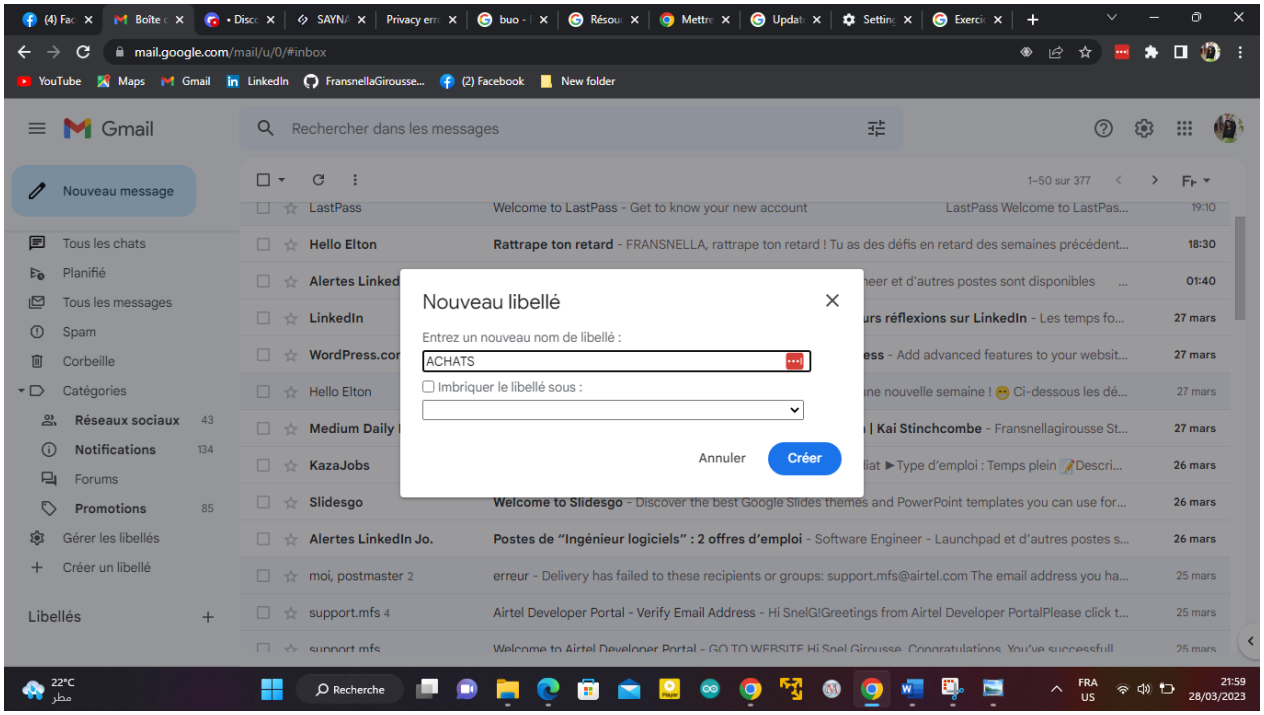
- Not secure

Analyse Google

- Vérifier un URL en particulier

6 - Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

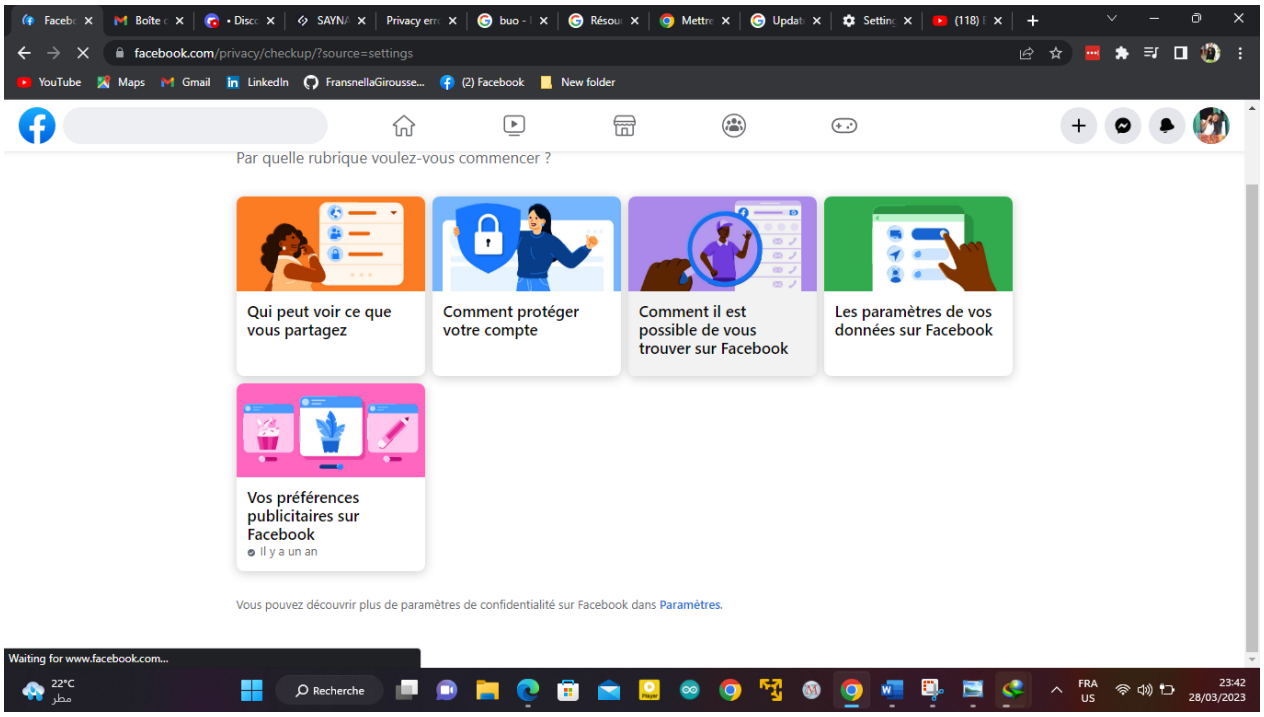


J’ai créé mon registre d’achet et maintenant je sais créer un libellé et suis de près sur mon mail les historiques des achats.

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



Grace aux paramètres je peux gérer mon compte facebooka et faire de ne pas mélanger la vie professionnelle et le personnel et mon compte sera en sécurité. Donc quand on utilise les réseaux sociaux il faut bien différencier la vie personnelle et la professionnelle.

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

1- un exercice pour vérifier la sécurité sur Windows

Si mon ordinateur est infecté par un virus donc je dois m'en débarrasser , alors voici quelques étapes à suivre pour le débarrassement :

Etape 1 : Téléchargera et installer un scanner antivirus comme Kaspersky Internet Security

Etape 2 : Se déconnecter d'internet

Etape 3 : Redémarrer l'ordinateur en mode sans échec

Etape 4 :Supprimer les fichiers temporaires

- Cliquez sur « Démarrer ».
- Sélectionnez « Tous les programmes ».
- Cliquez sur « Accessoires ».
- Choisissez « Outils système ».
- Choisissez « Nettoyage du disque ».
- Recherchez « Fichiers temporaires » dans la liste « Fichiers à supprimer ».
- Sélectionnez « Fichiers temporaires » pour les supprimer.

Etape 5 :Lancer une analyse antivirus

Etape 6 : Supprimer ou mettre en quarantaine

Etape 7 :Redémarrer l'ordinateur

Etape 8 :Modifier tous les mots de passe

Etape 9 ; Mettre à jour tous les logiciels, les navigateurs, et le système d'exploitation.

Un exercice pour installer et utiliser un antivirus + antimalware sur Windows

- Télécharger un antivirus et antimalware comme Avast AVG, Malwarebytes.
- Ensuite suivez les instructions de l'installation
- Une fois installer on effectue l'analyse complète de l'ordinateur pour détecter et de supprimer tout virus ou malware présent sur l'ordinateur.