Parcours : DISCOVERY

Module : Naviguer en toute sécurité

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

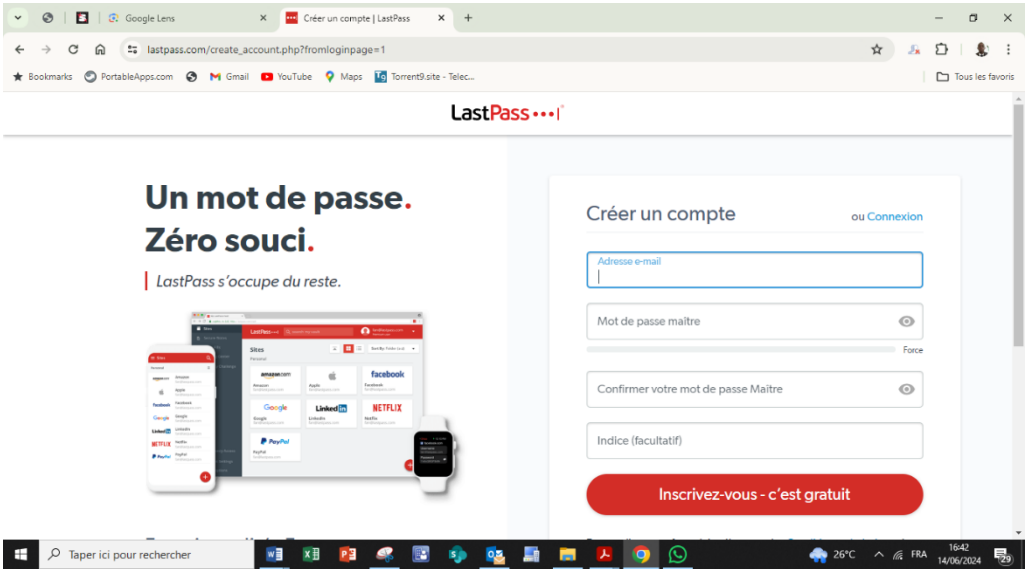
1 Introduction à la sécurité sur Internet

1/Trois articles qui parlent de sécurité sur internet

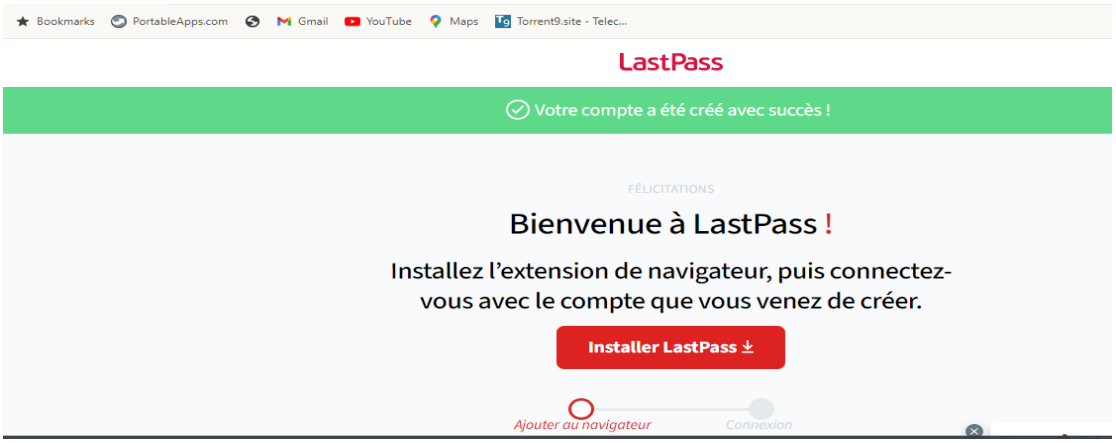
- Article1 = kaspersky- Qu'est-ce que la sécurité internet? /
- Article2 = boutique-box-internet - L'importance de la sécurité sur Internet
- Article2 = cybermalveillance - Comment se protéger sur Internet

2/ Créer des mots de passe forts

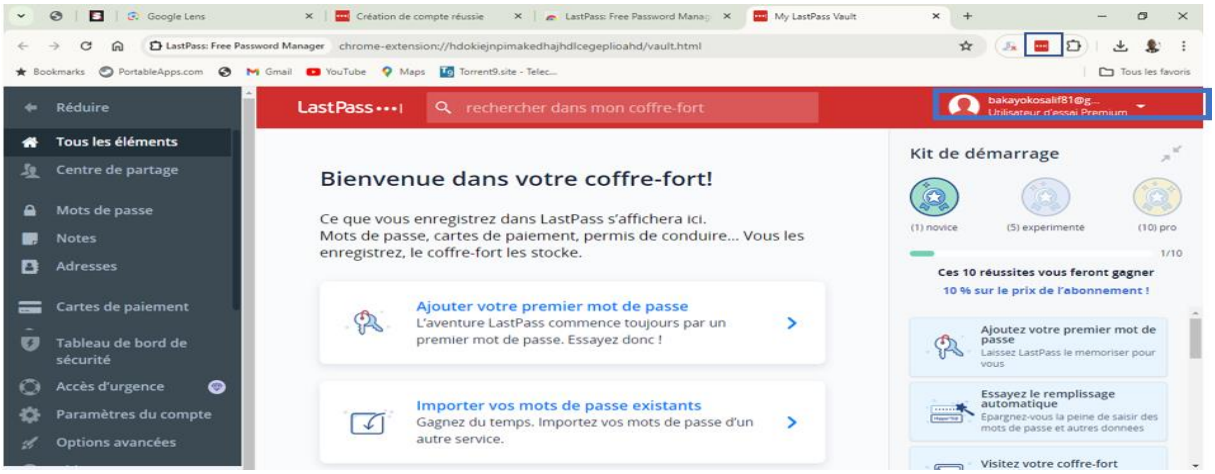
1/ Dans cet exercice, nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Ce gestionnaire prend la forme d'une application web, accessible sur tous supports (PC, Mac, mobile). Il est simple à prendre en main et propose un niveau de sécurité optimal.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



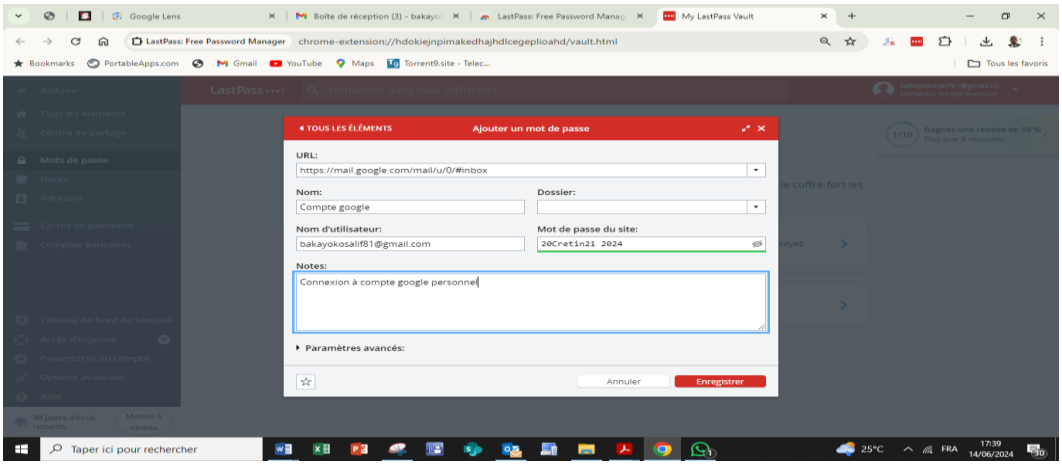
Créer un compte en remplissant le formulaire



Installation de Lastpass
"Ajouter à Chrome"
Épingler l'extension de LastPass
Connexion



Une fenêtre s'ouvre pour y insérer toutes les informations à retenir pour automatiser la prochaine connexion. LastPass demande l'URL du site en question; on conseille de mettre l'URL de la page de connexion du site. Ensuite préciser l'id et le mot de passe. On peut personnaliser le nom, un commentaire associé ou encore un dossier si besoin.



- Comparatif des gestionnaires de mot de passe : https://www.clubic.com/application-web/article-854952-1-gestionnaires-mots-meilleur-logiciel -gratuit-windows.html

3/ Fonctionnalité de sécurié de votre navigateur

1/

➢ Les sites qui semblent malveillants sont:

- www.morvel.com: Le nom de domaine correct est «marvel» qui fait référence à une grande entreprise de comics
- www.fessebook.com: Le nom de domaine correct est «facebook» qui fait référence au réseau social facebook
- www.instagam.com: Il y a un «r» sur le nom de domaine du plateforme authentique (‘instagram’)

➢ 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)

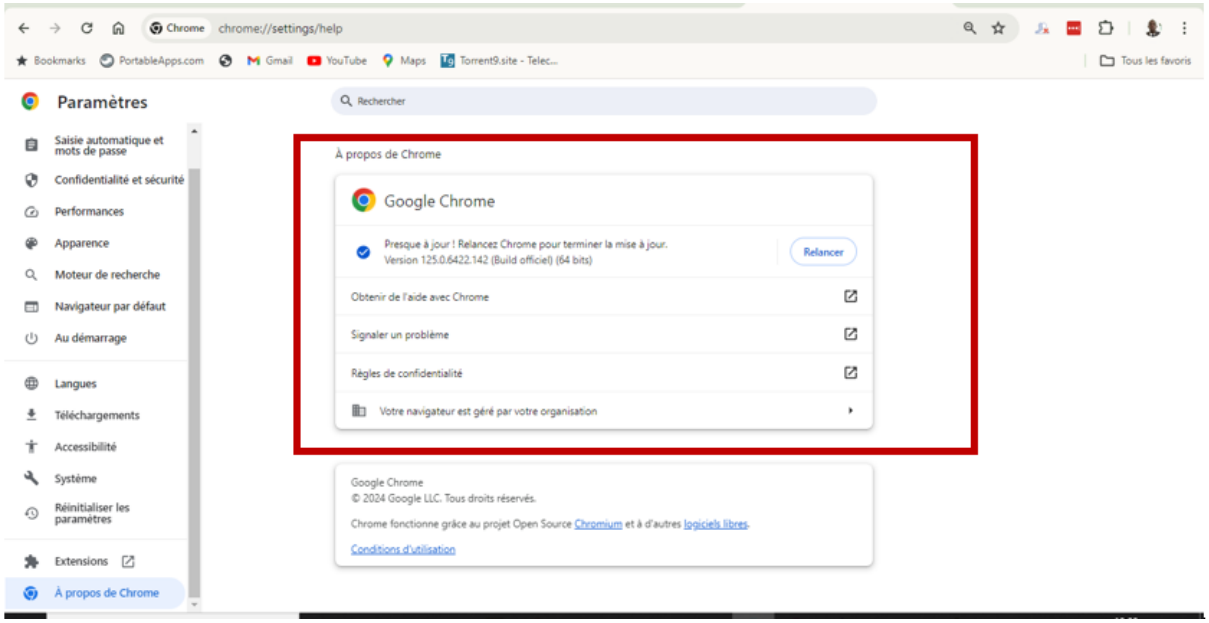
Pour Chrome

Ouvre le menu du navigateur et accède aux "Paramètres"

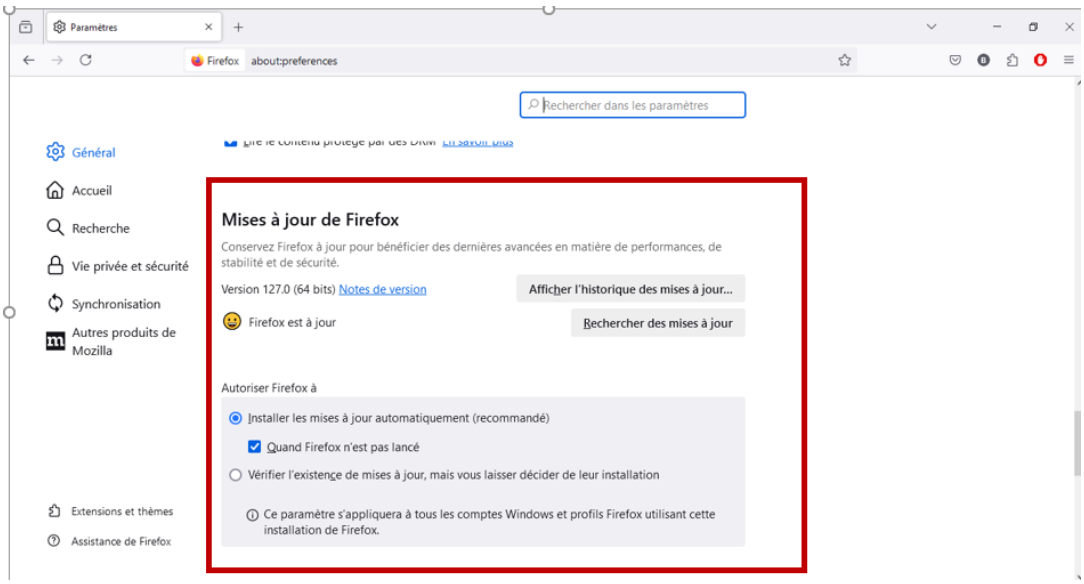
Clic sur la rubrique "A propose de Chrome"

Si tu constates le message "Chrome est à jour", c'est Ok

Sur Chrome



Sur FireFox



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

Ouverture du lien et exploitation d'informations

Site du gouvernement
cybermalveillance.gouv.fr

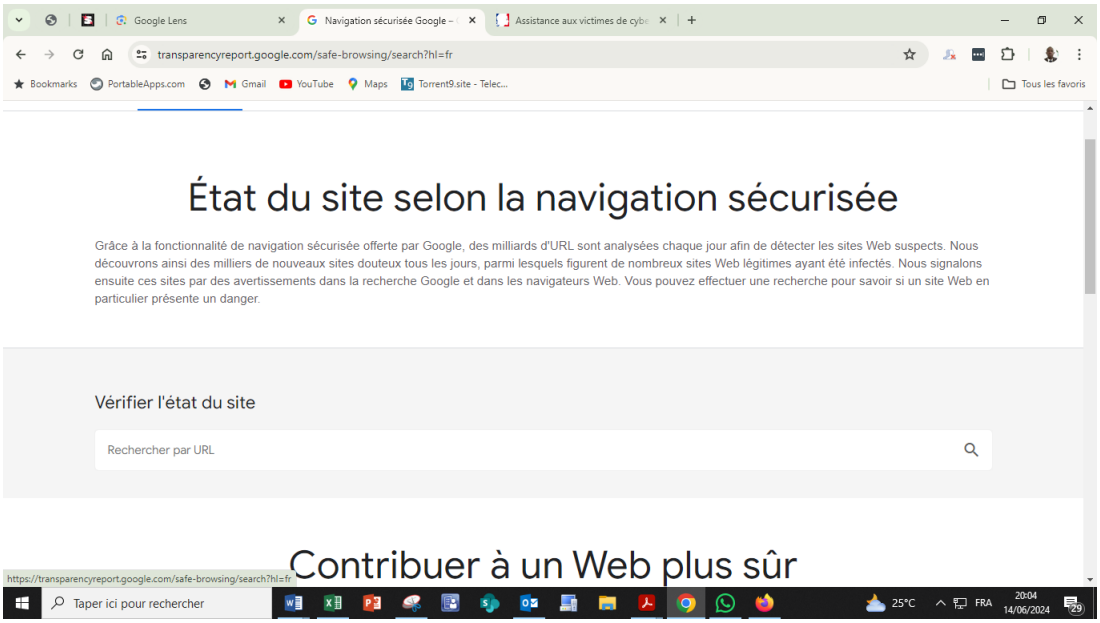
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconn aitre-un-mail-de-phishing-ou-dhameconnage

5/ Eviter les logiciels malveillants

Objectif: sécuriser votre ordinateur et identifier les liens suspects

3/ 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 affichent des indicateurs de sécurité pour donner une information sur la protection d'un site internet.

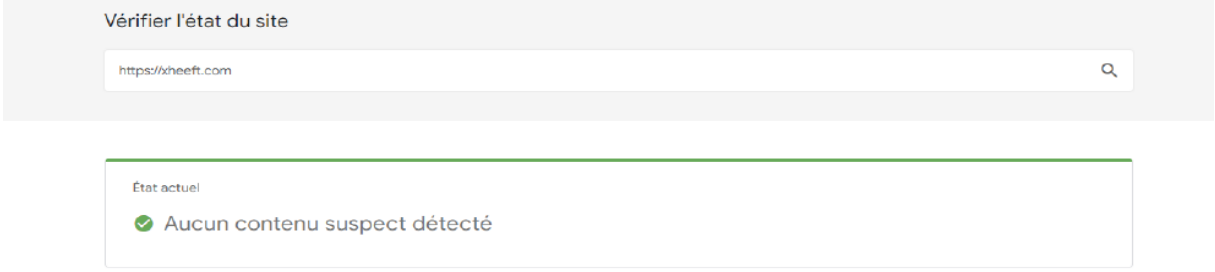
Lorsque le doute persiste tu peux t'appuyer sur un outil proposé par Google: Google Transparency Report (en anglais) ou Google Transparence des Informations (en français). Afin d'améliorer ta lecture de la sécurité sur internet, tu vas devoir analyser les informations de plusieurs sites. Pour chaque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

- https://xheeft.com/
- Indicateur de sécurité
  HTTPS
- Analyse google

Aucun contenu suspect



site n°2
https://learn.sayna.io

• Indicateur de sécurité

HTTPS

• Analyse Google

Aucun contenu suspect

site n°3

http://referentiel.institut-agile.fr

• Indicateur de sécurité

Not secure O

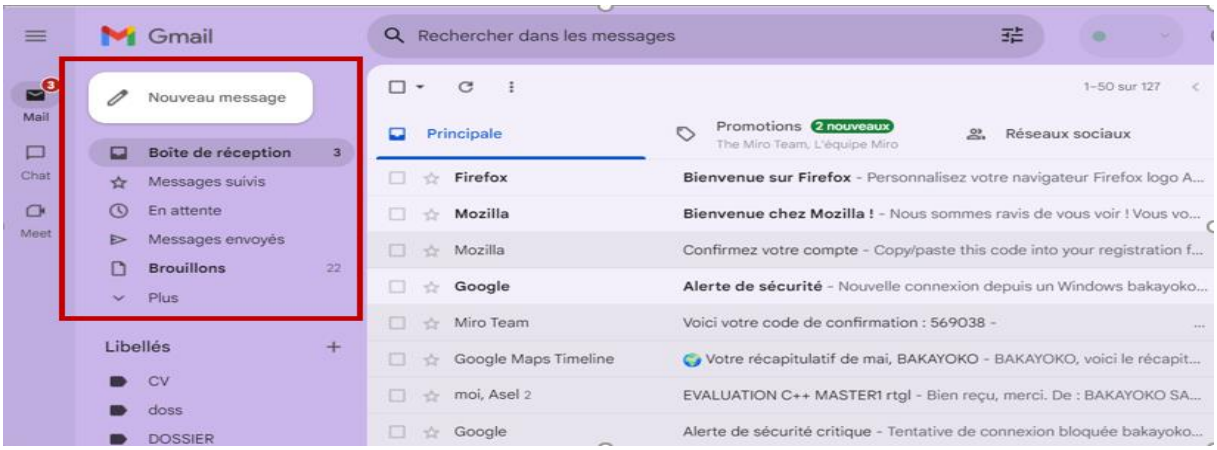
Analyse Google

Aucun donnée disponible

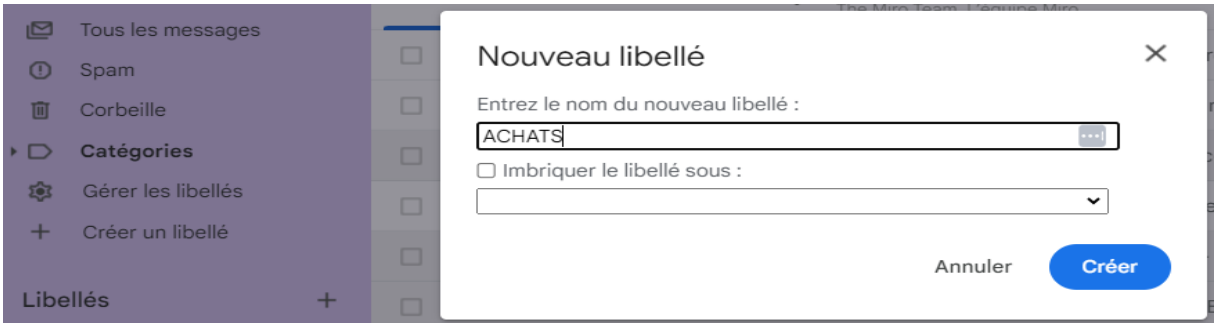
6/ Achats en ligne sécurisés

Objectif: créer un registre des achats effectués sur internet

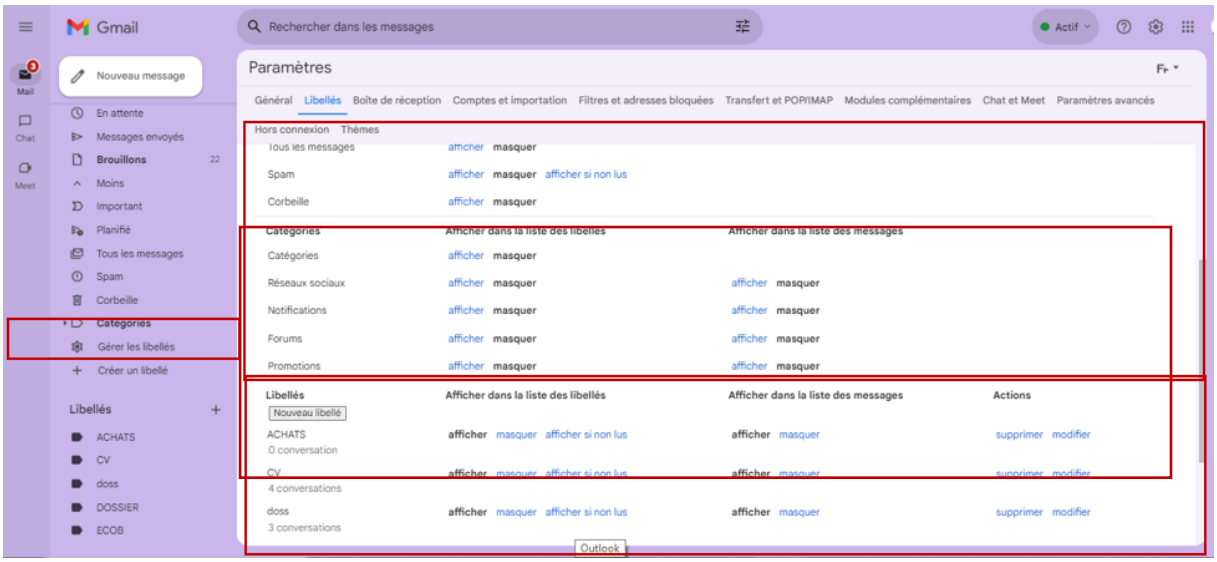
Sur la page d'accueil de ta messagerie, tu trouveras sur la gauche les libellés initialement prévus (boite de réception, messages envoyés, etc.)
MBoîte de réception (2) - cloudors x +



Création de libellé ACHATS



Gestion des libellés



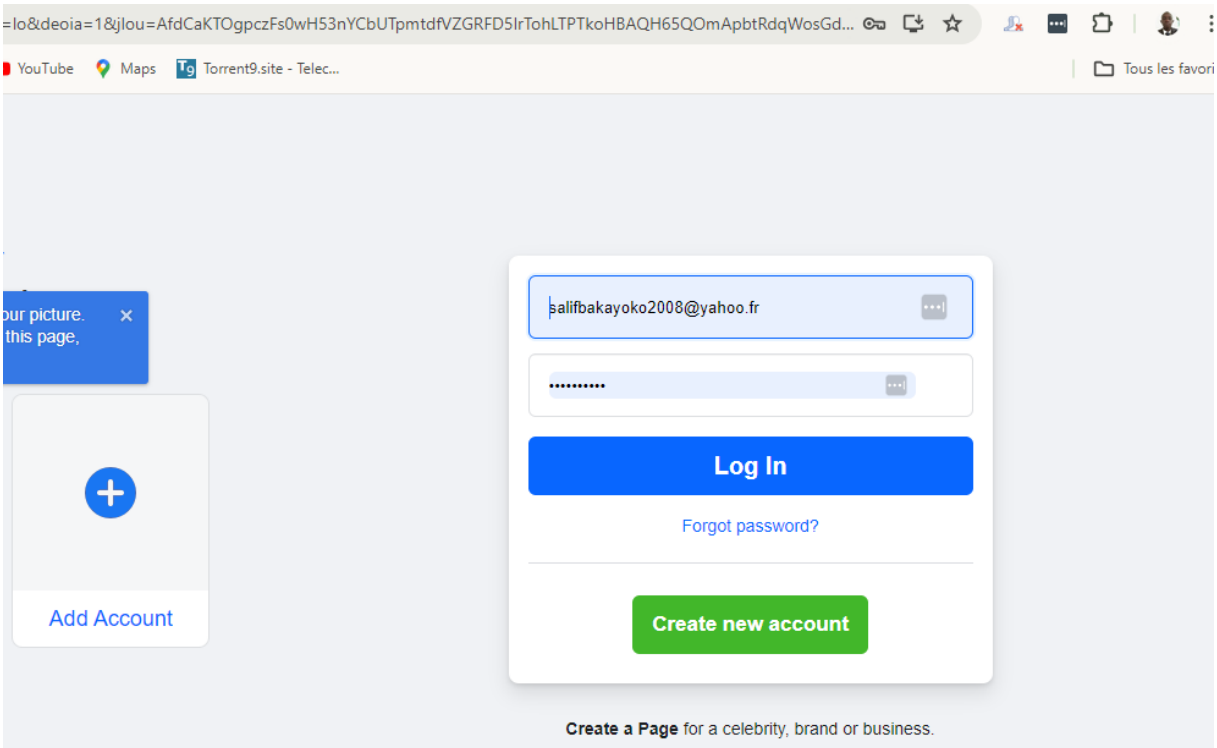
7/ Comprendre le suivi du navigateur

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

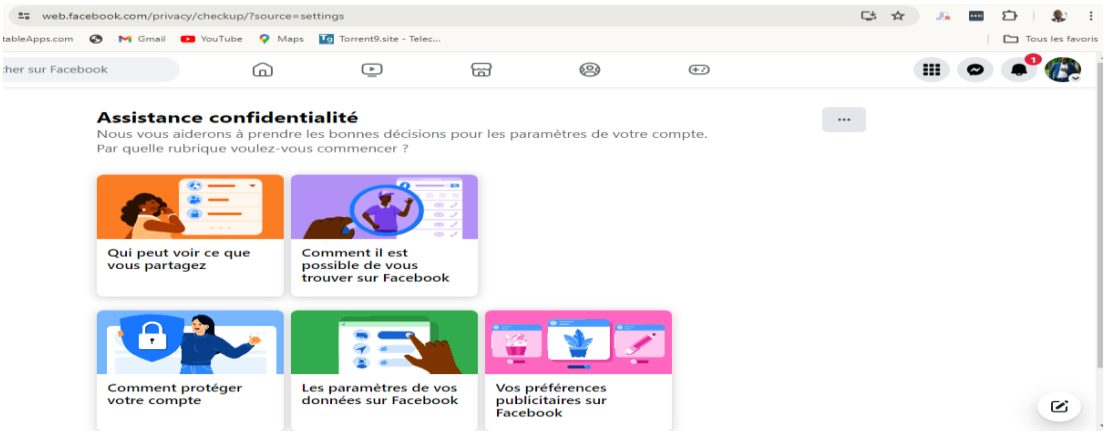
8/ Principe de base de la confidentialité des médias sociaux

Objectif: Régler les paramètres de confidentialité de Facebook

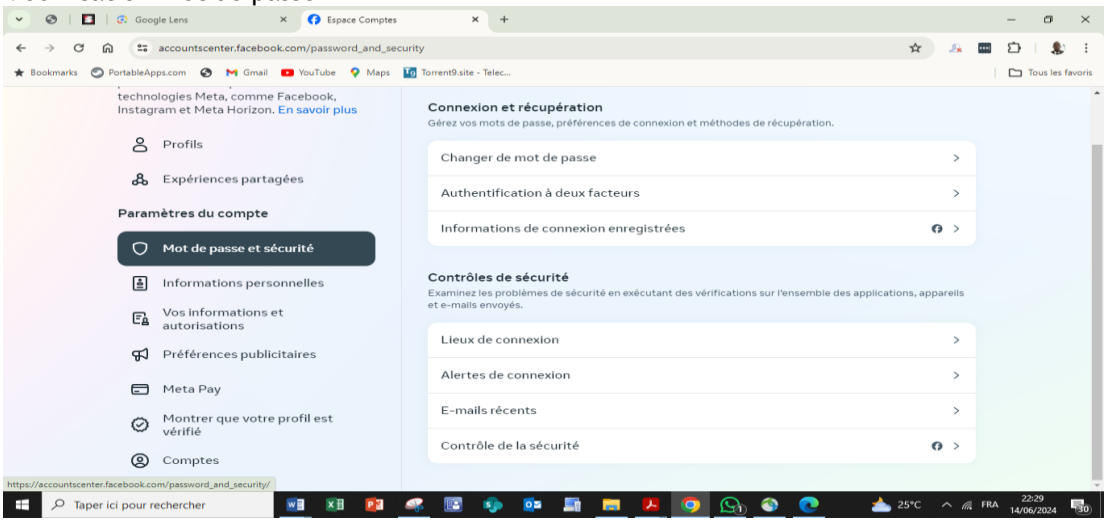
Connexion à facebook



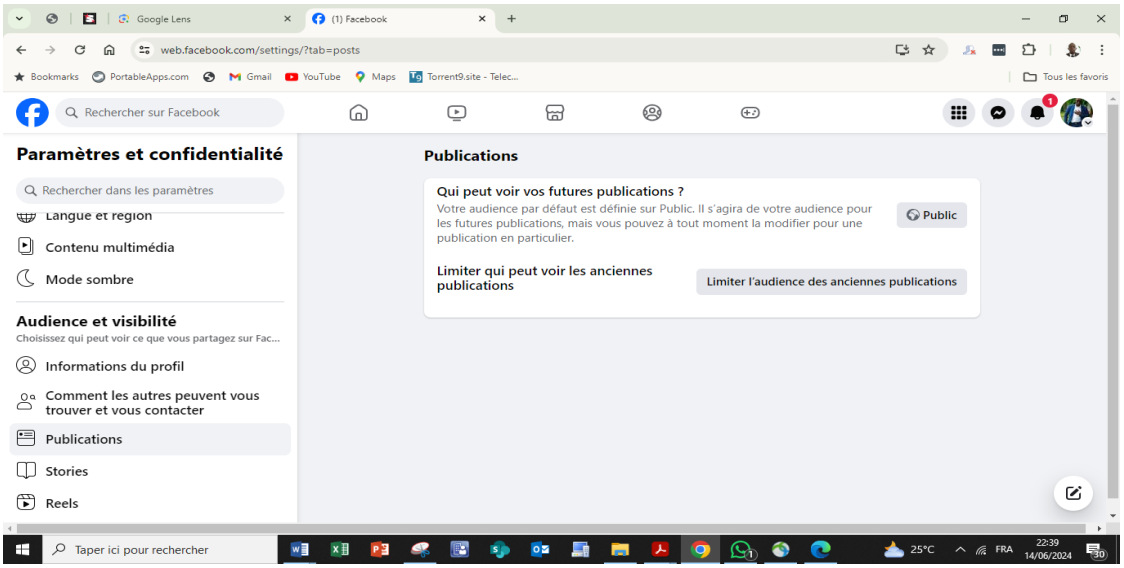
Assistance et confidentialité



Modification mot de passe



Publications



9/Que faire si mon ordianteur est infecté par un virus

Objectif :
1/ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé.

- ❖ Mises à Jour du Système :

- Assurer que mon système est à jour en termes de correctifs de sécurité et de mises à jour logicielles.
- Mettez à jour tous les logiciels et bibliothèques tiers utilisés.

- ❖ Pare-feu et Filtres :

- Vérifier la configuration du pare-feu pour vous assurer que seules les connexions nécessaires sont autorisées.

- ❖ Audits de Sécurité :

- Utiliser des outils comme «Lynis» pour effectuer des audits de sécurité automatisés sur mon système.

- ❖ Sauvegardes Régulières :

- Assurer que des sauvegardes régulières sont effectuées et testées pour pouvoir restaurer rapidement le système en cas d'incident de sécurité.

- ❖ Voici un exercice pour installer et utiliser un antivirus appelé Kaspersky