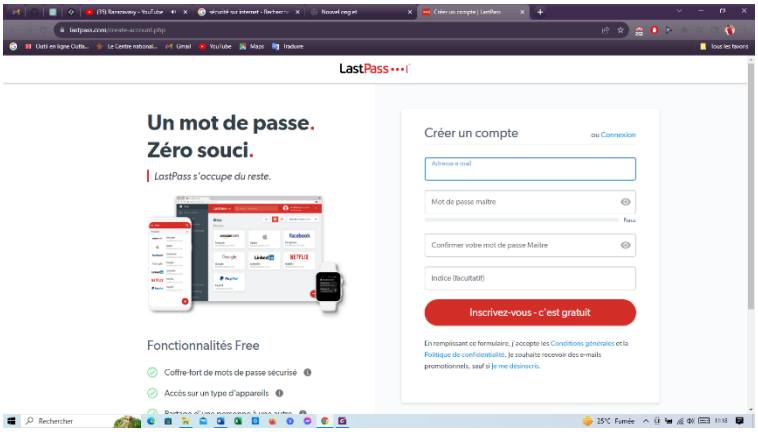
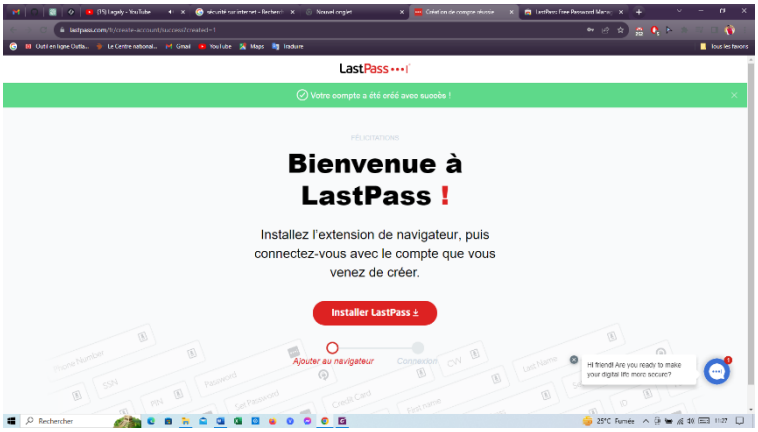
Projet 1 – Un peu plus de sécurité, on n'en a jamais assez !

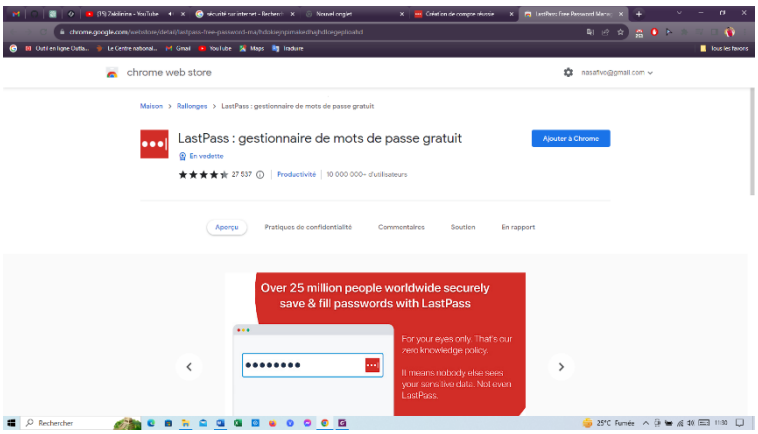
1. **Introduction à la sécurité sur internet**
    a) **Consultation de 3 articles qui parlent de sécurité sur internet**
        - Article 1 = Qu'est-ce que la sécurité Internet ? Kaspersky
        - Article 2 = L'importance de la sécurité sur Internet, Boutique-box-internet
        - Article 3 = 5 conseils pour être en sécurité sur internet, La Poste
2. **Créer des mots de passe forts**
    a) **Utilisation de LastPass**
        ✓ Accède au site de LastPass



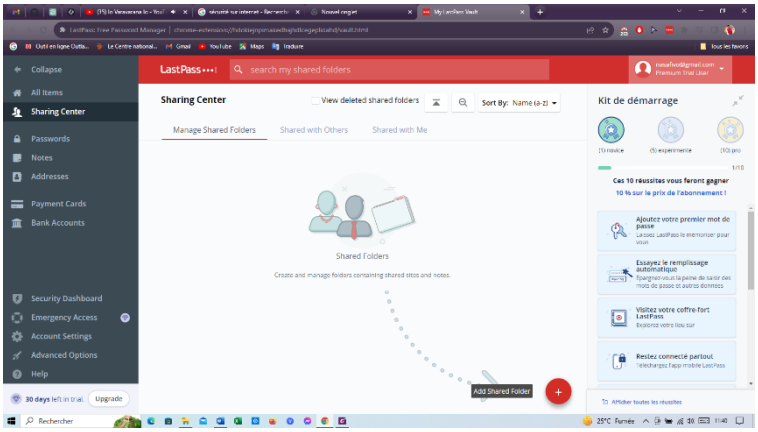
✓ Crée un compte en remplissant le formulaire
✓ Installation de LastPass



✓ Validation de l'opération sur le Chrome Web Store

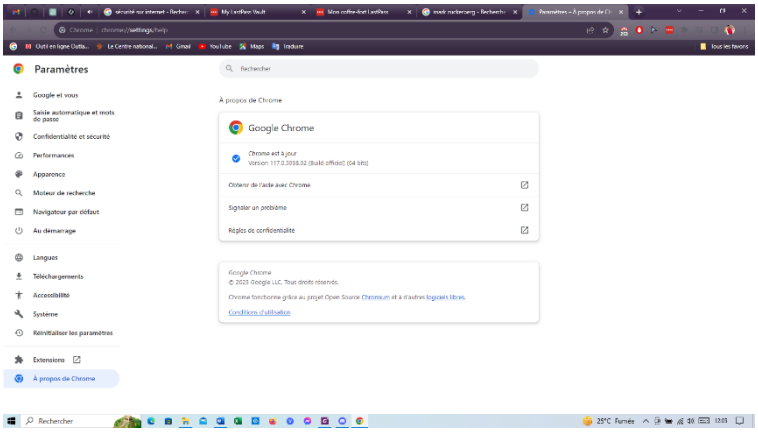


✓ Accès à cette extension et connexion

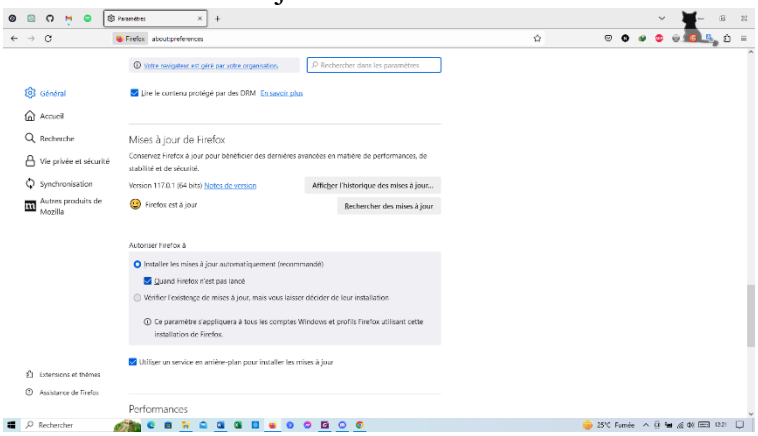


3. **Fonctionnalité de sécurité de votre navigateur**
   a) **Identification des adresses internet qui semblent provenir de sites malveillants.**
      - www.morvel.com, c'est dérivé du site web officiel de Marvel
      - www.fessebook.com, c'est un dérivé du réseau social créé par Mark Zuckerberg
      - www.instagam.com, c'est un dérivé du réseau social créé par Kevin Systrom et Mike Krieger

   b) **Vérification des mises à jour de Chrome et Firefox**
      - Pour Chrome
        ✓ Ouvre le menu du navigateur et accède aux « Paramètres »
        ✓ Clic sur la rubrique « A propos de Chrome »
        ✓ Si tu constates le message « Chrome est à jour », c'est OK

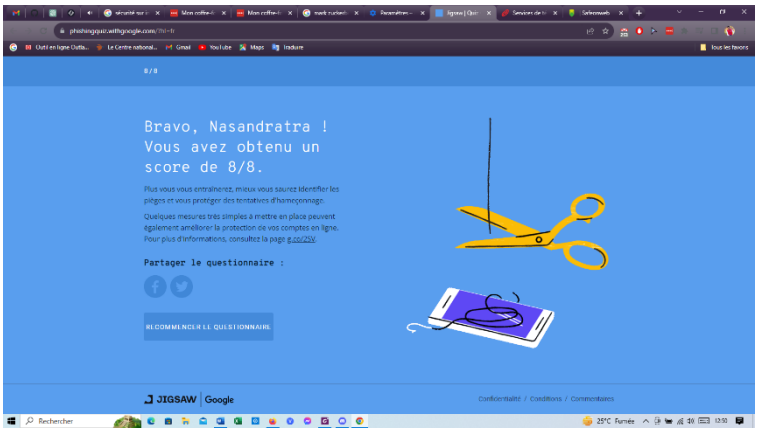


- Pour Firefox
  - ✓ Ouvre le menu du navigateur et accède aux « Paramètres »
  - ✓ Dans la rubrique « Général », fais défiler jusqu'à voir la section « Mise à jour de Firefox »



4. Eviter le spam et le phishing

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



5. Comment éviter les logiciels malveillants

a) Utilisation de Google Transparence des informations

- Site n°1 :

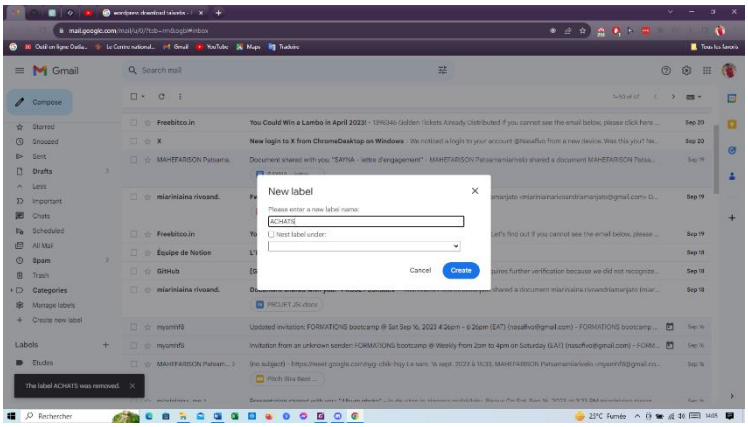
- ✓ Indicateur de sécurité : HTTPS, cadenas
- ✓ Analyse Google : Aucun contenu suspect détecté

- Site n°2 :
  - ✓ Indicateur de sécurité : HTTPS, cadenas
  - ✓ Analyse de Google : Aucune donnée disponible
- Site n°3 :
  - ✓ Indicateur de sécurité : Non sécurisé
  - ✓ Analyse de Google : Vérifier une URL en particulier

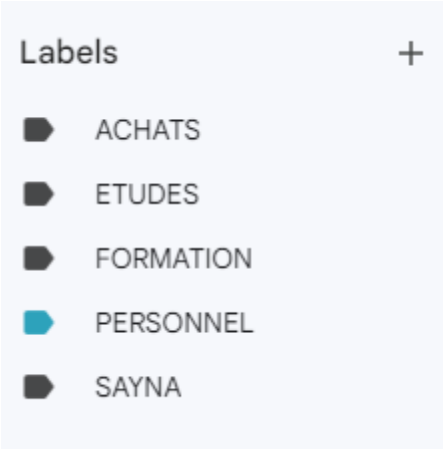
6. Achats en ligne sécurisés

a) Registre des achats

- Création d'un registre d'achat sur la messagerie de Google



- Organisation de libellé



7. Comprendre le suivi du navigateur

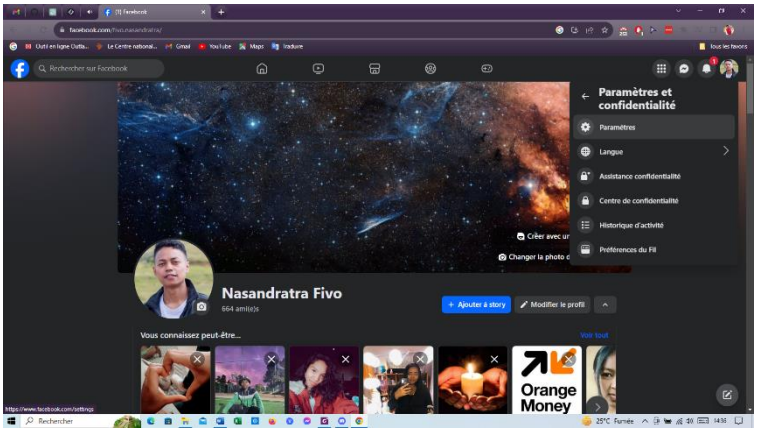
La gestion des cookies et la navigation privée sont des fonctionnalités cruciales des navigateurs web pour la confidentialité et la sécurité en ligne. Les cookies sont de petits fichiers textes utilisés par les sites web pour stocker des informations sur votre appareil, mais vous pouvez les accepter, bloquer les cookies tiers et les supprimer à partir des paramètres de votre navigateur. La navigation privée, aussi appelée "mode

incognito", vous permet de naviguer sans que les cookies soient stockés après la session, sans historique, et avec une réduction du suivi publicitaire.

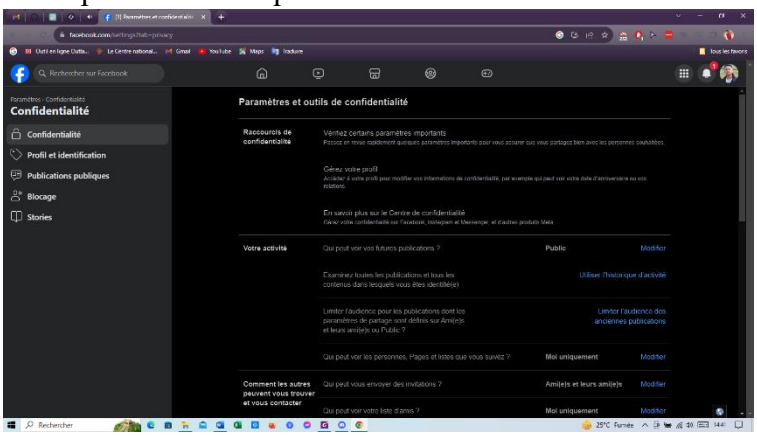
8. Principes de bases de la confidentialité des médias sociaux

a) Réglage des paramètres de confidentialité pour Facebook

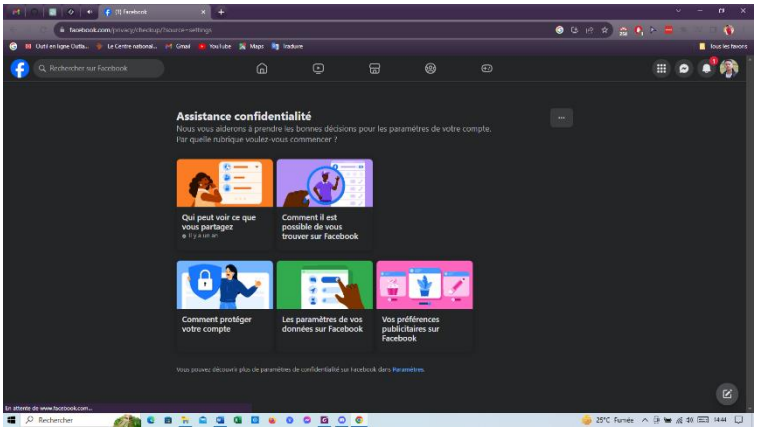
- Connecte-toi à ton compte Facebook
- Une fois sur la page d'accueil, ouvre le menu Facebook, puis effectue un clic sur « Paramètres et confidentialité ». Pour finir, clic sur « Paramètres »



- Ce sont les onglets « Confidentialité » et « Publications publiques » qui nous intéressent. Accède à « Confidentialité » pour commencer et clic sur la première rubrique



- Cette rubrique résume les grandes lignes de la confidentialité sur Facebook



- Dans les paramètres de Facebook tu as également un onglet « Cookies ». Maintenant que tu sais comment sont utilisées tes données, tu es capable de choisir en pleine conscience ce que tu souhaites partager.

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

a) Vérification de la sécurité de mon ordinateur

Les étapes à suivre pour savoir si mon ordinateur est infecté par un virus :

- Analyse antivirus : Faire une analyse complète de l'ordinateur à l'aide d'un logiciel antivirus fiable et à jour.
- Mises à jour du logiciel : faire des mises à jour du système d'exploitation, du navigateur web et des autres logiciels obsolète pour bénéficier des correctifs de sécurité.
- Surveillance des performances : si l'ordinateur est lent, affiche des comportements inhabituels ou des publicités intempestives, cela peut indiquer une infection.
- Gestionnaire des tâches : bloquer les processus suspects.
- Contrôle des extensions du navigateur : identifier les extensions dont on n'a pas installé mais qui sont présent dans notre navigateur.
- Anti-malware : faire un scan complet de l'ordinateur avec un logiciel anti-malware pour trouver de logiciels malveillants.
- Changements inexpliqués : faire attention aux modification inexpliquées dans notre fichier, dossiers et paramètres.

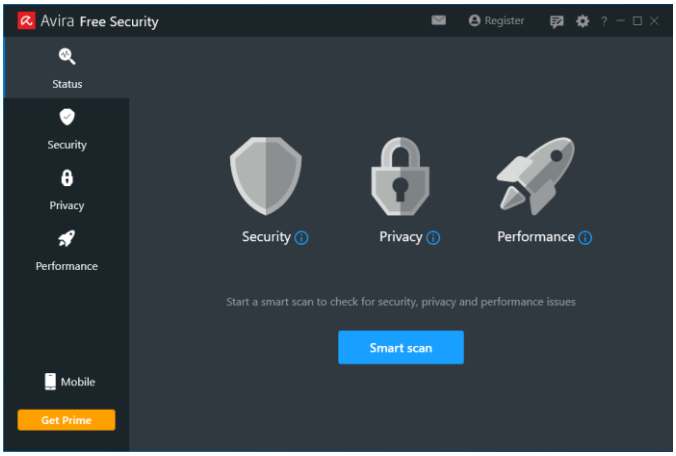
b) Installation et utilisation d'un antivirus et d'un antimalware

Etapes d'installation d'Avira Free Antivirus (l'antivirus que j'utilise) :

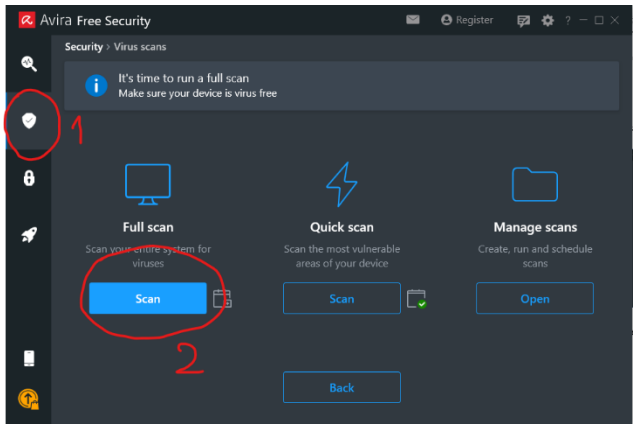
- Télécharger le dans le lien : https://www.avira.com/fr/free-antivirus-windows
- Une fois le téléchargement terminé, lancer l'installateur en double-cliquant sur le fichier téléchargé
- Cliquez sur « Oui » dans la boîte de dialogue pour démarrer l'installation
- Suivez les instructions affichées à l'écran (l'installation ne devrait prendre que quelques minutes)

Utilisation d'Avira :

- Quand l'installation est terminée, la fenêtre d'Avira se présente comme suit :



- Pour faire un scan complet, il faut cliquer sur « Security » (1) et lancer le scan en cliquant sur « Scan » (2)

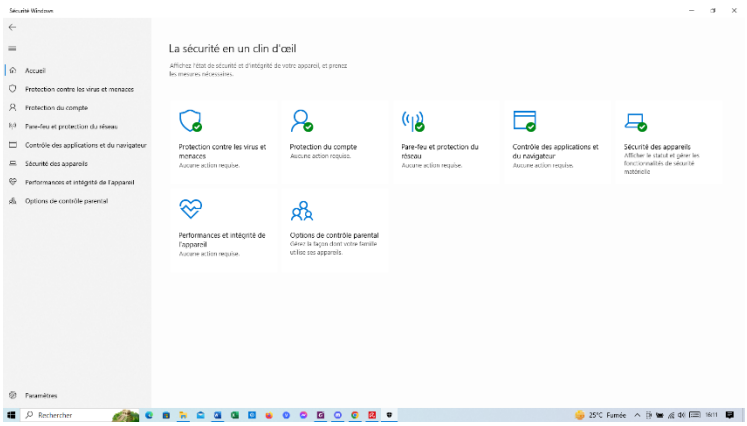


Etape d'installation d'antimalware (Windows Defender)

- Comme Windows Defender est un outil antivirus et antimalware intégré de Microsoft donc on n'a pas besoin faire une installation

Utilisation de Windows Defender :

- La fenêtre de Windows Defender se présente comme suit :



- Pour voir la sécurité de l'ordinateur, il faut aller sur la rubrique « Protection contre les virus et menaces » et activer les fonctions suivantes :

- ✓ Protection en temps réel
- ✓ Protection dans le cloud
- ✓ Envoi automatique d’échantillon