Parcours : DISCOVERY

Module : Comment internet fonctionne

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.

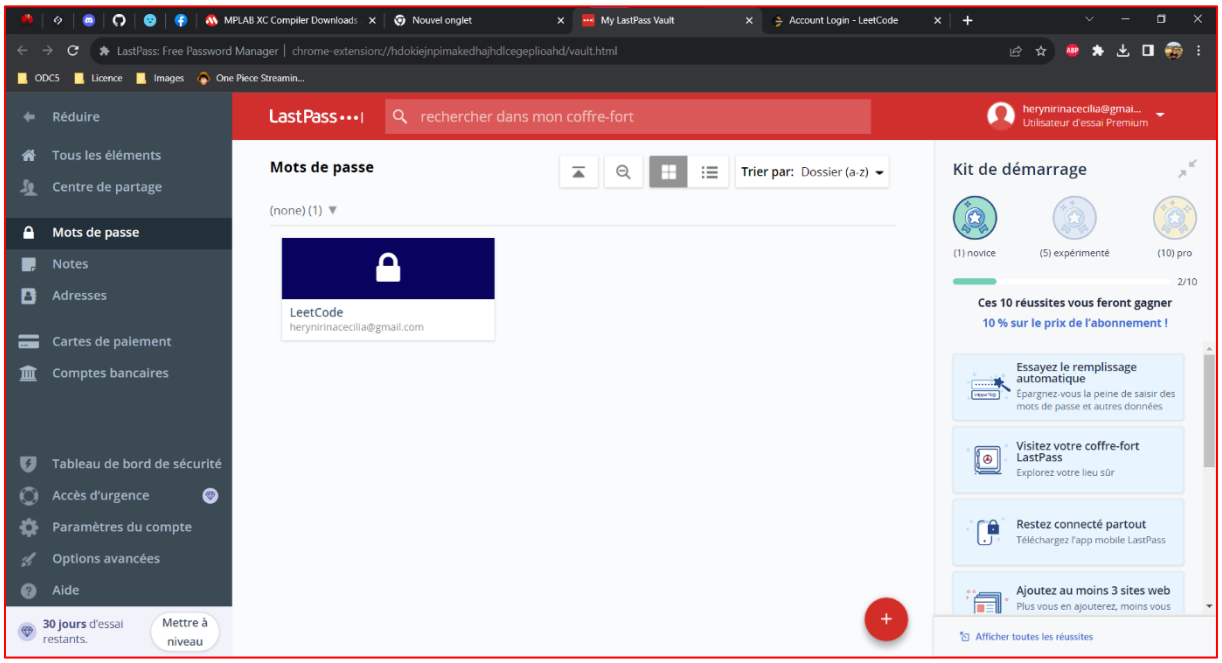
1/ Trois articles parlant de sécurité sur Internet :

- Article 1 : VPNOverview - Navigation sécurisée : restez en sécurité en ligne
- Article 2 : Site compagny - Les fondamentaux de la securite en ligne pour les debutants protegez-vous efficacement sur internet
- Article 3 : Heyme - Comment proteger sa vie privée sur internet

2 – Créer des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass.

1/ Installation et première utilisation du gestionnaire de mot de passe LastPass :



3 – Fonctionnalité de sécurité de votre navigateur

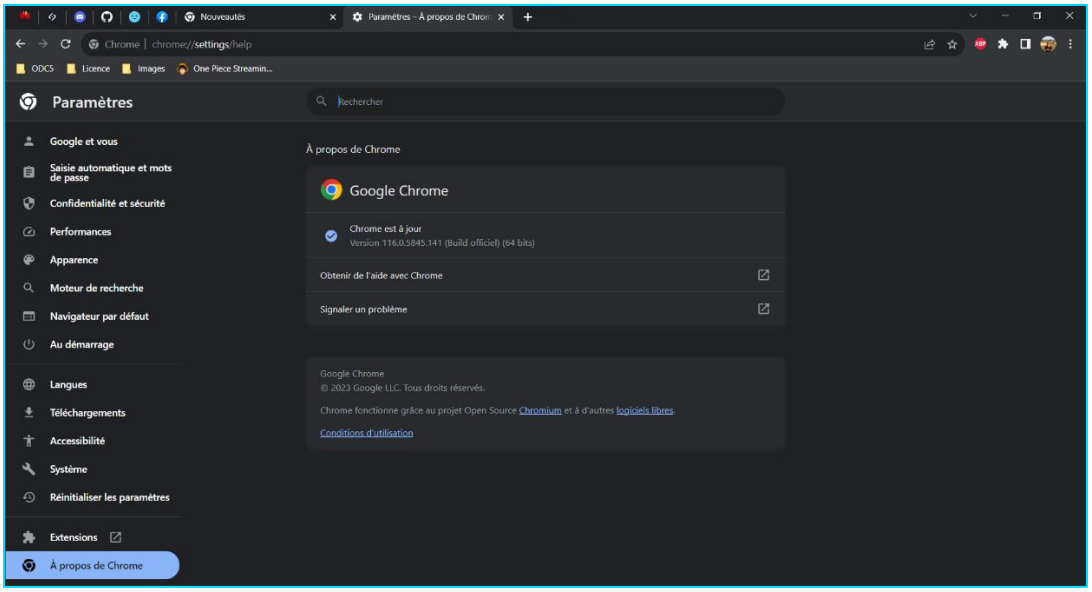
Objectif : identifier les éléments à observer pour naviguer sur le web en toute sécurité.

1/ Identification des adresses internet qui semblent provenir de sites web malveillants :

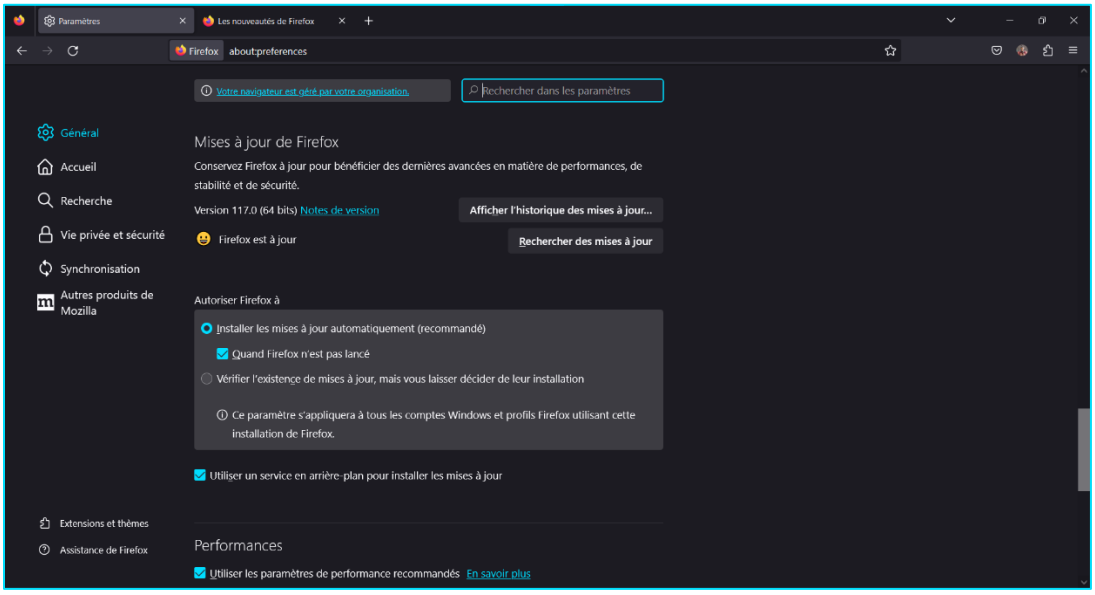
- www.morvel.com
- www.fessebook.com
- www.instagam.com

2/ Vérification des mises à jour des navigateurs Chrome et Firefox :

- Google Chrome :



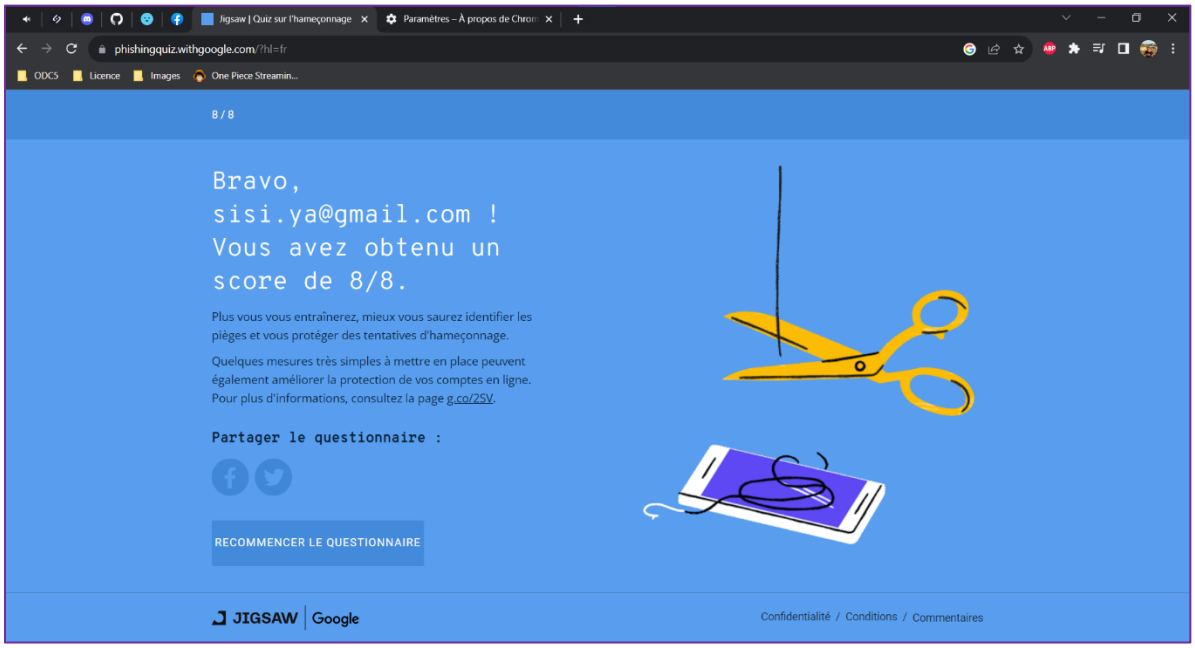
- Mozilla Firefox :



4 – Eviter le spam et le pishing

Objectif : Reconnaître plus facilement les messages frauduleux.

1/ Exercice : déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.



5 – Comment éviter les logiciels malveillants

Objectif : sécuriser votre ordinateur et identifier les liens suspects.

1/ Analyse des informations des sites donnés pour l'amélioration de la lecture de la sécurité d'un site internet :

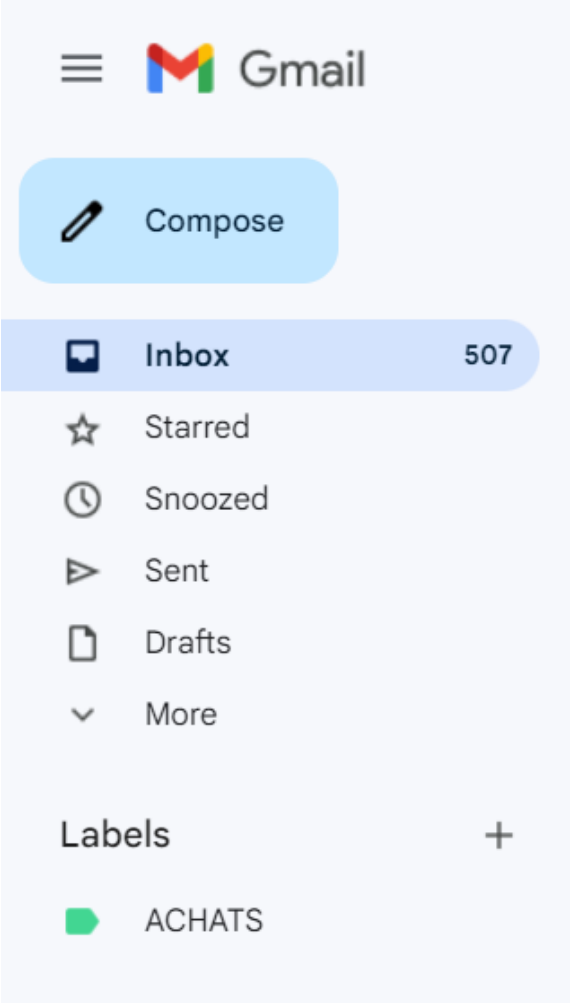
- Site n°1
  - Indicateur de sécurité :
    - HTTPS Not secure
  - Analyse Google :
    - Aucun contenu suspect
- Site n°2
  - Indicateur de sécurité :
    - HTTPS
  - Analyse Google :
    - Aucun contenu suspect
- Site n°3
  - Indicateur de sécurité :
    - Not secure
  - Analyse Google :
    - Vérifier une URL en particulier

- Site n°4 (Site non sécurisé)
    - Indicateur de sécurité :
        - Not secure
    - Analyse Google :
        - Vérifier une URL en particulier

6 – Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur interne.

1/ Création d'un registre des achats :



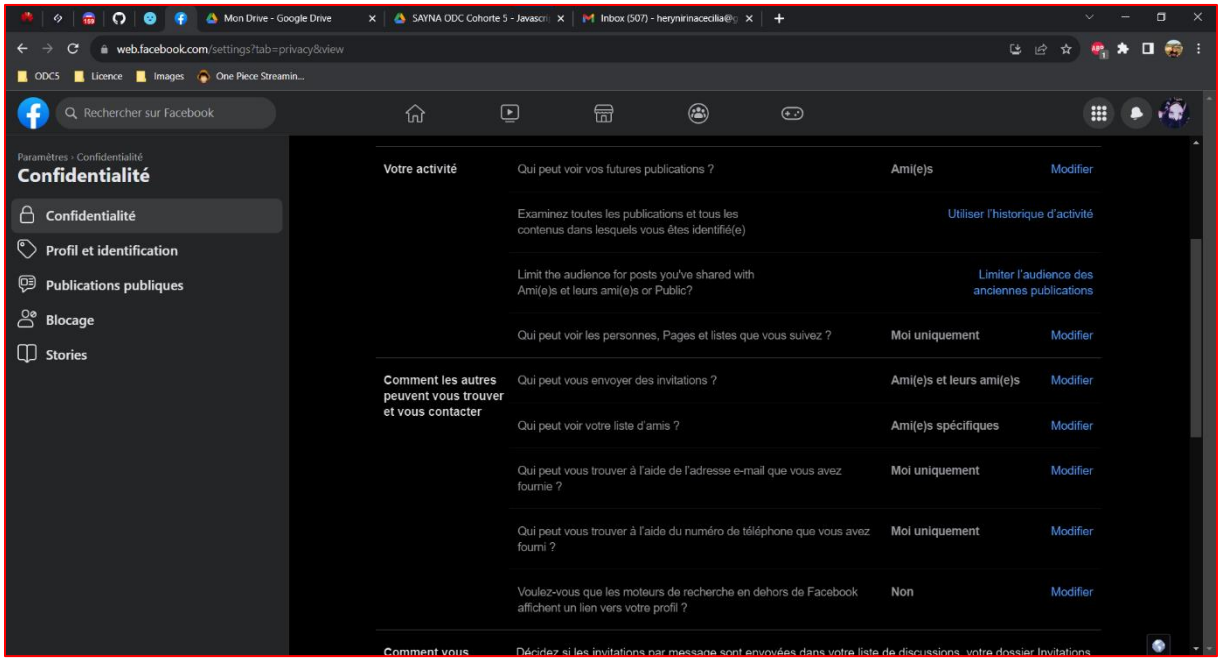
7 – Comprendre le suivi du navigateur

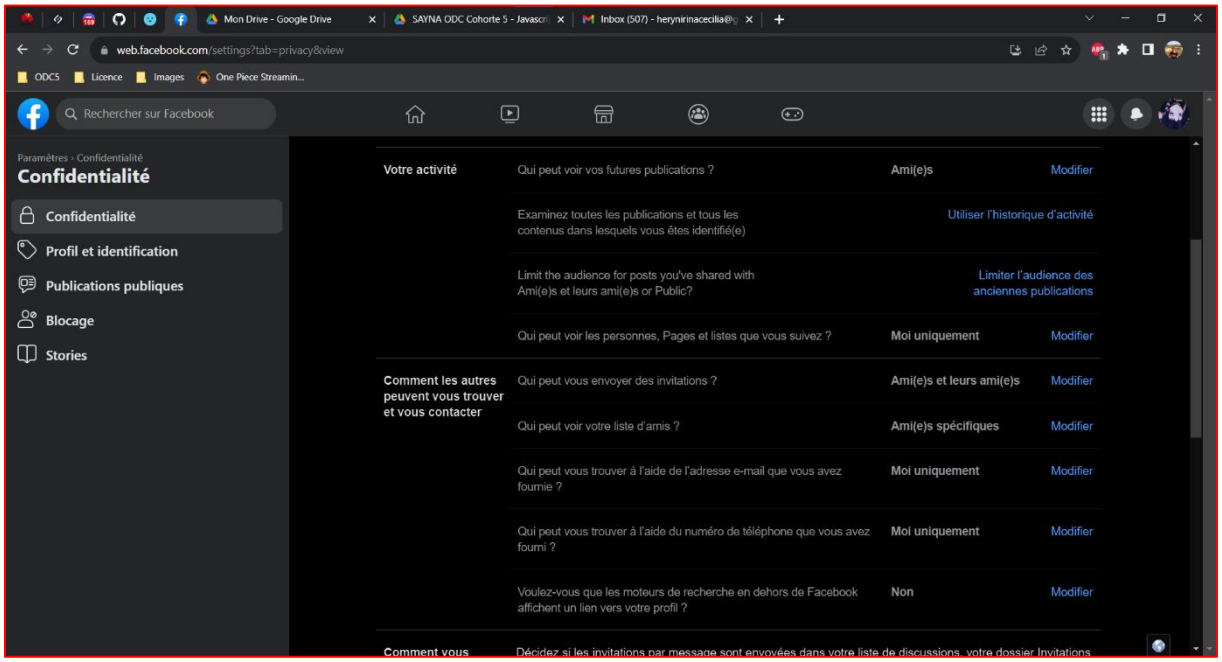
Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée.

8 – Principes de base de la confidentialité des médias sociaux

Objectif : Régler les paramètres de confidentialité de Facebook.

1/ Réglage des paramètres de confidentialité :





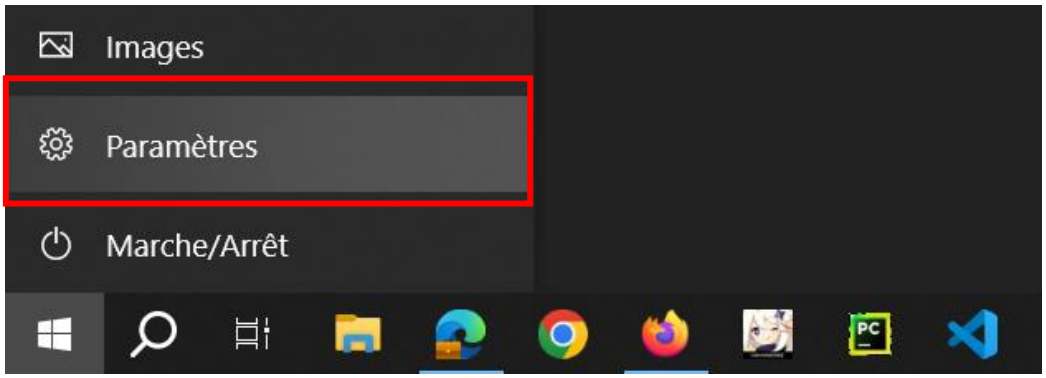
9 – Que faire si votre ordinateur est infecté par un virus

Objectif : Savoir quoi faire lorsque notre ordinateur est infecté par un virus

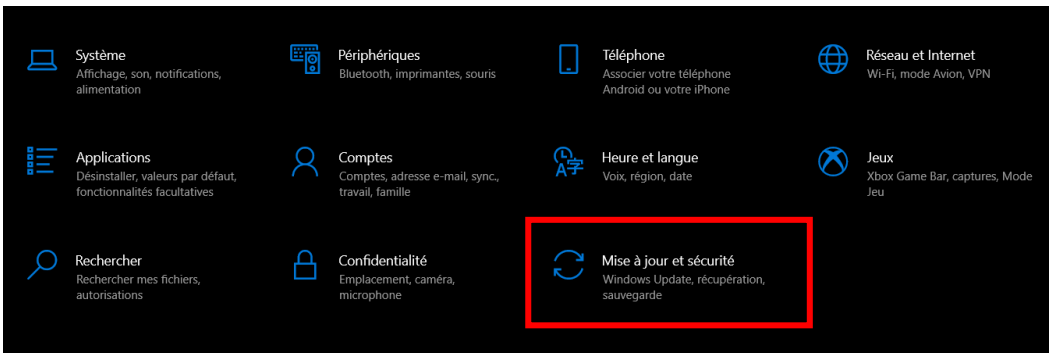
1/ Exercice pour vérifier la sécurité en fonction de l'appareil utilisé :

- Si vous êtes sur Windows 10, vous pouvez suivre les étapes suivantes pour accéder à Microsoft Defender :
  - ✦ Ouvrir le menu Démarrer, en bas à gauche de votre écran.

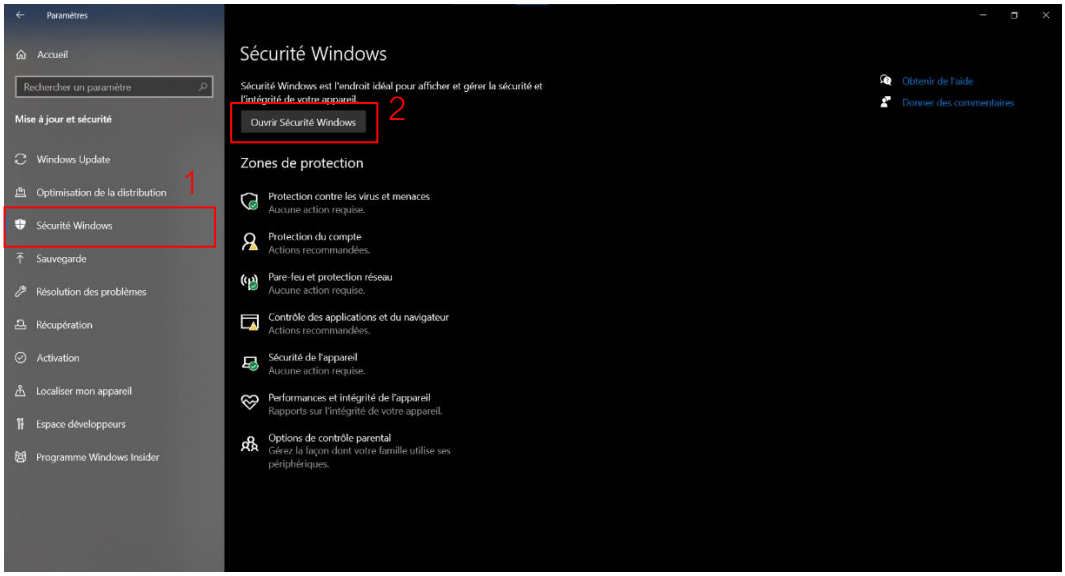
  - ✦ Ensuite, sélectionnez « Paramètres »



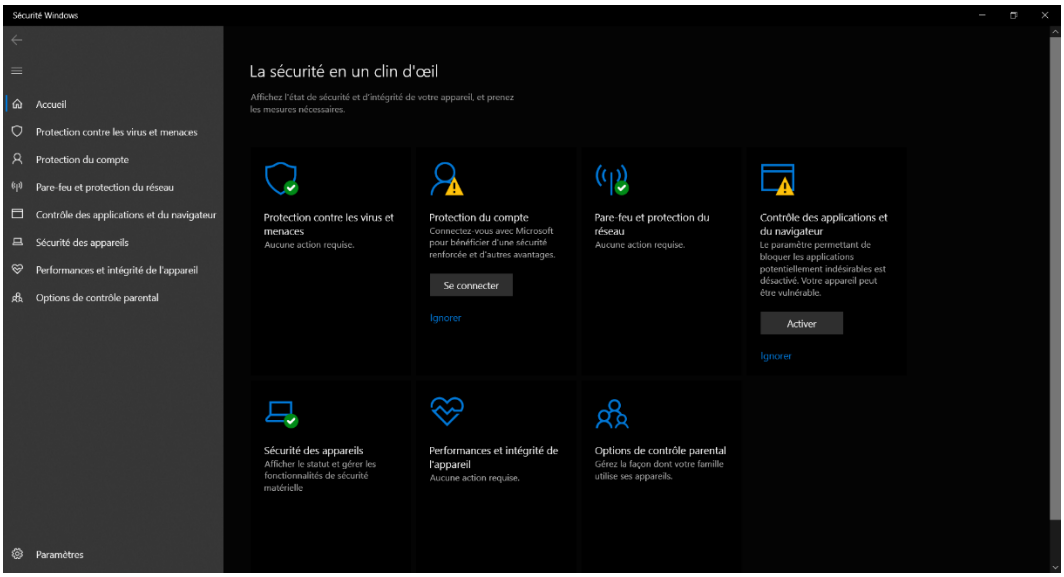
  - ✦ Après, choisissez « Mise à jour et sécurité »



✦ Enfin, allez dans « Sécurité Windows »

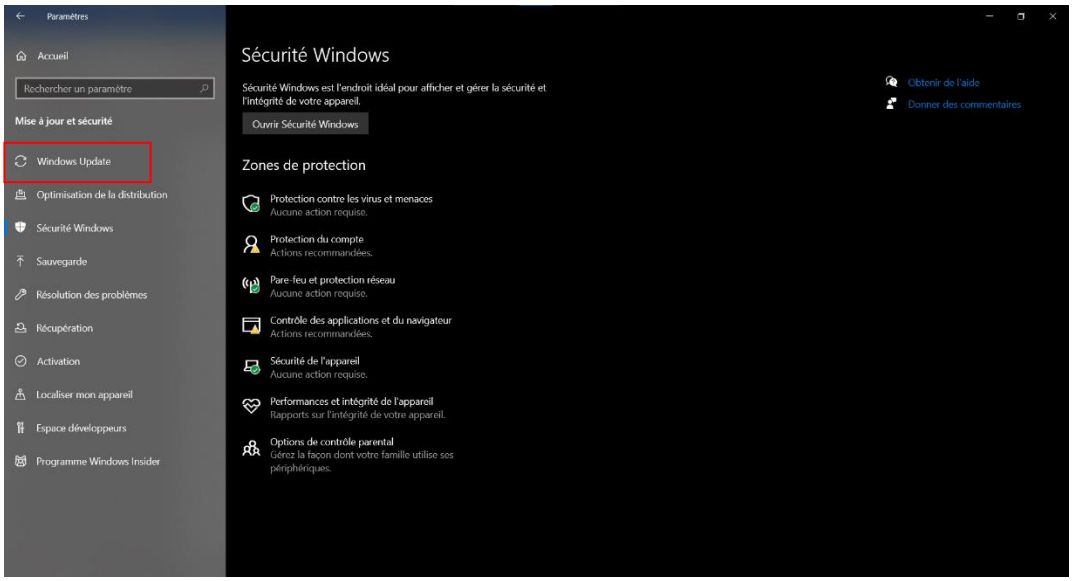


Plusieurs actions peuvent être effectué à partir de là, comme la protection contre les virus et les menaces, le contrôle des applications et du navigateur ou encore la sécurité des appareils.



N'hésitez pas à regarder et à essayer un par un les fonctionnalités proposées.

Il est également important de vérifier que Windows Defender soit bien mis à jour. Pour cela il vous suffit de voir les mises à jour disponibles dans Windows Updates.



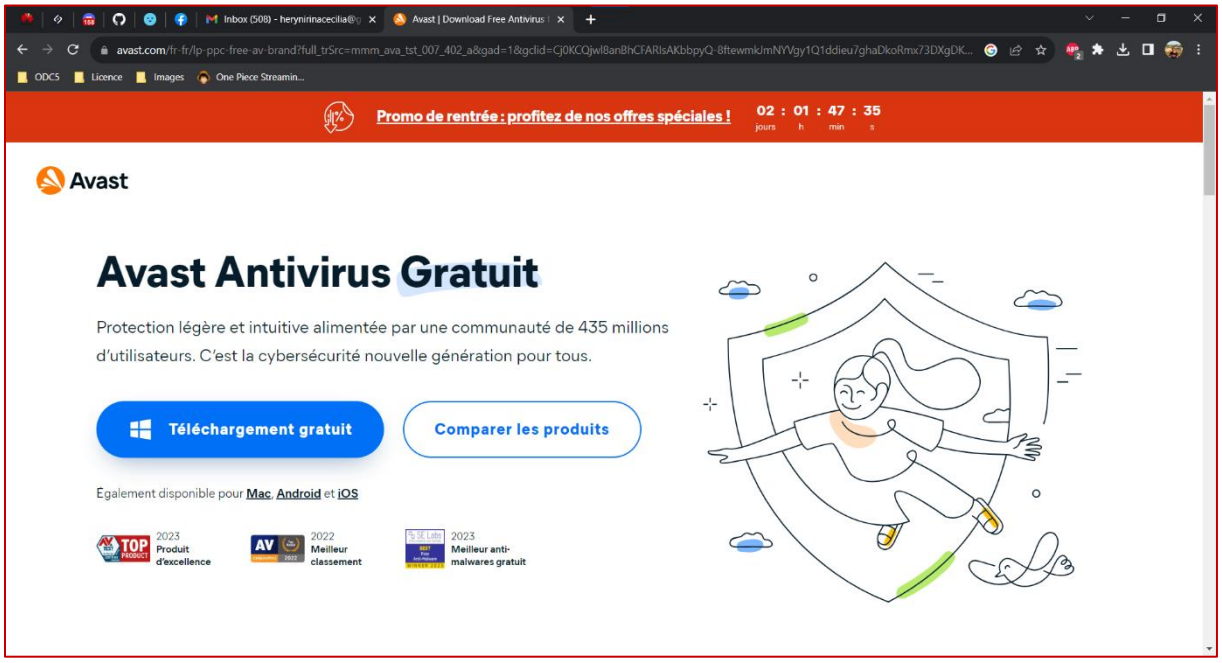
Il y a également beaucoup d'autres alternatives, si vous voulez en savoir plus, cliquez sur le lien suivant pour y accéder : Meilleur antivirus gratuit (2023) : liste des logiciels à fuir.

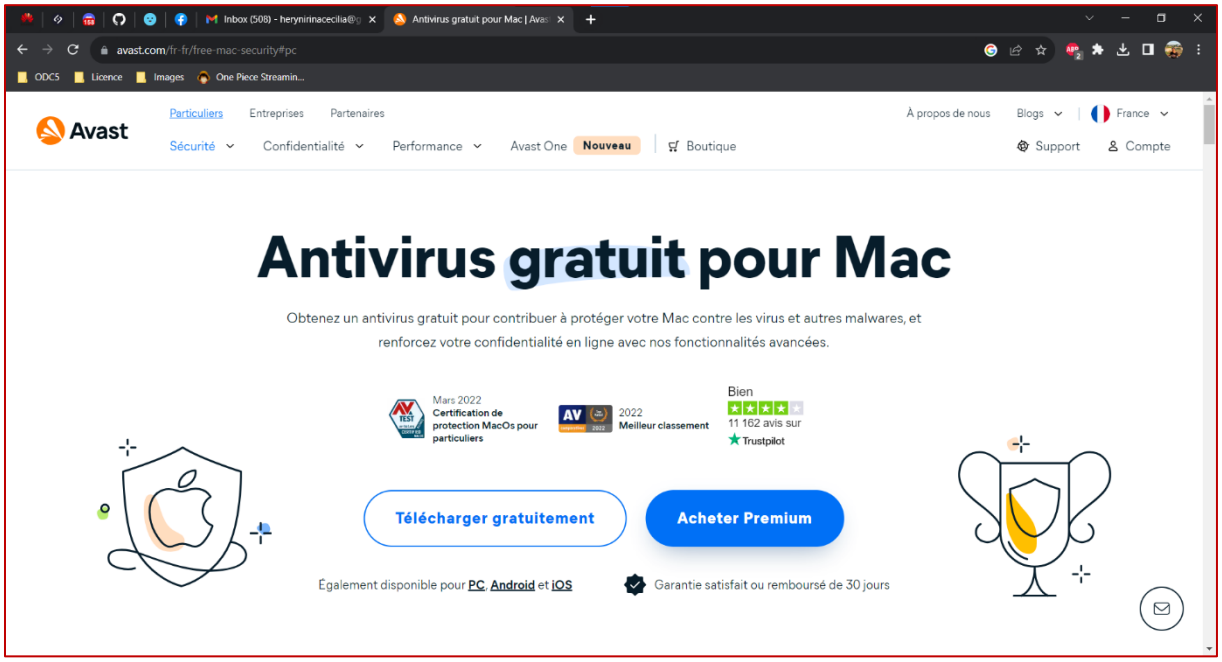
- Bien que vous seriez moins susceptible d'héberger un virus ou un logiciel malveillant sur Mac que sur Windows, vous n'êtes cependant pas totalement à l'abris de quelques désagréments. La prudence est donc un allié dont vous ne devriez pas vous séparer. Il est donc toujours recommandé de bien mettre à jour vos logiciels et d'appliquer toutes les procédures de *sécurité en ligne* tel que : Ne pas cliquer sur des liens suspects. Si toutefois vous vous retrouviez avec un virus voici quelques consignes que vous pourriez appliquer : Retirer des virus sur Mac. Pour plus de prudence il serait également nécessaire de vérifier Antivirus pour Mac.

2/ Installation d'antivirus + antimalware :

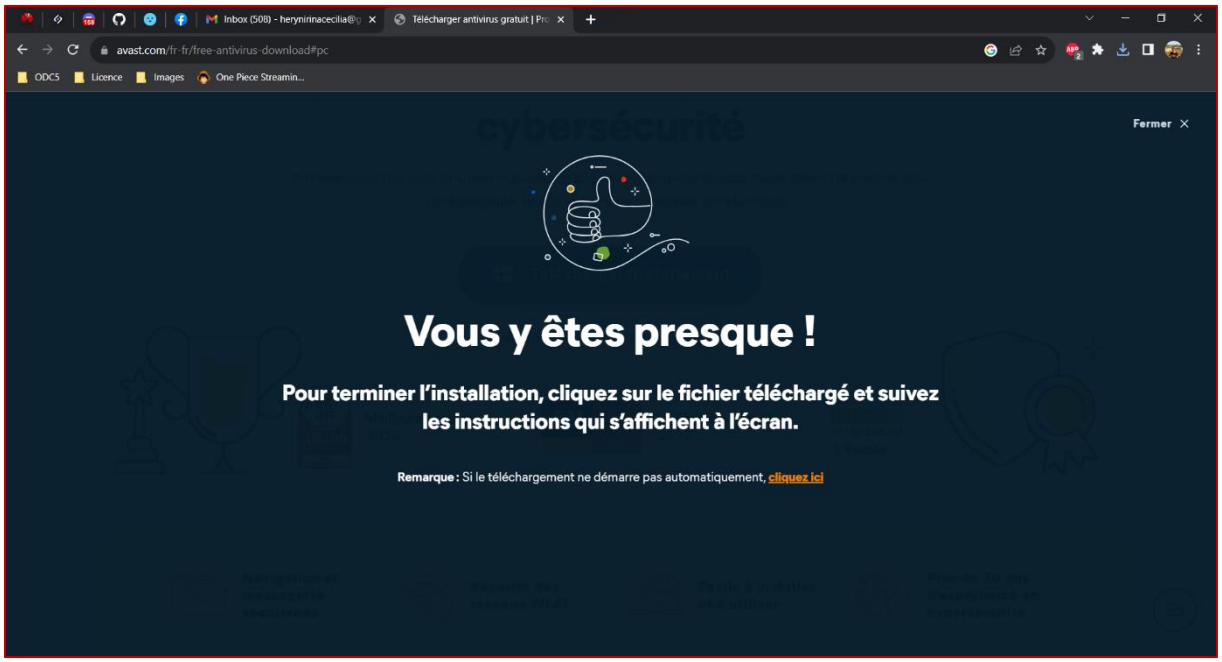
Pour cet exercice, nous avons décidé d'installer Avast. Ce logiciel possède une version gratuite mais si l'envie vous prend, il vous est également possible d'essayer la version premium pendant 30j garantie ou remboursé.

Pour commencer, il faut tout d'abord télécharger Avast. Bien que les liens diffèrent un peu, il vous est possible de basculer du téléchargement pour Windows vers les autres systèmes d'exploitation supportés.





Il suffit par la suite de cliquer sur « Télécharger gratuitement » et le téléchargement devrait se lancer de lui-même. Vous serez face à l'onglet suivant :



**Si votre téléchargement ne démarre pas directement, vous aurez la possibilité de le relancer grâce au lien donné.

Une fois le fichier télécharger, vous pourrez installer l'application en cliquant sur « Ouvrir ». Notez que l'installation se fera en ligne, il vous sera nécessaire d'être connecté à internet pour que le processus se déroule sans encombre. Une fois installé, il ne vous restera plus qu'à tester les fonctionnalités que vous aurez sous la main !