Parcours : DISCOVERY

Module : Naviguer en toute sécurité

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

Tous vos travaux devront être déposés sur votre compte Github

---

Sommaire

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 sources 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.

Réponse 1

Voici les articles que nous avons retenus pour toi (avec les mots-clés "sécurité sur internet" et "comment être en sécurité sur internet" :

Article 1 = https://www.netsupportsoftware.com - Guide de sécurité en ligne 2024

Article 2 = https://www.cybermalveillance.gouv.fr - Comment se protéger sur Internet

Article 3 = https://www.orangecyberdefense.com- Safer Internet Day 2024

Article 4 = https://www.mesquestionsdargent.fr- Comment utiliser internet en toute sécurité ?

Beaucoup de notions traitées dans les articles sont également traitées dans le cours et des exercices y sont associés.

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)

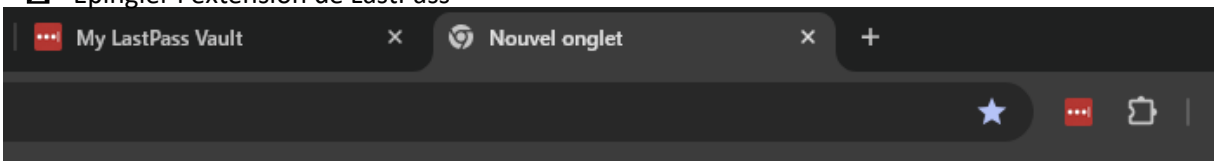
☒ Accède au site de LastPass avec ce lien

☒ Créer un compte en remplissant le formulaire

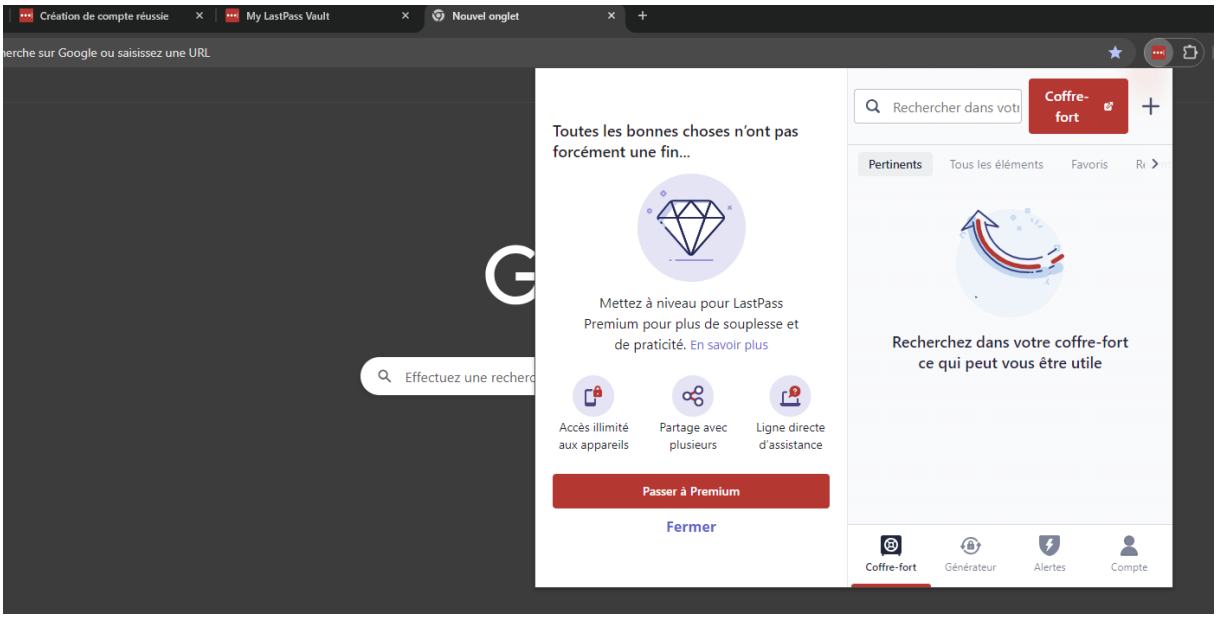
☒ Installation de Lastpass

☒ "Ajouter à Chrome"

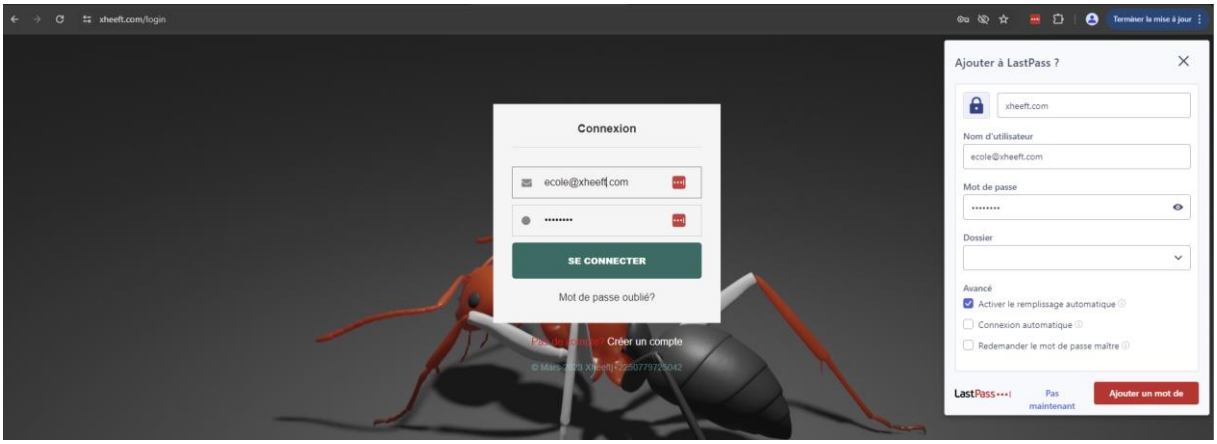
☒ Épingler l'extension de LastPass



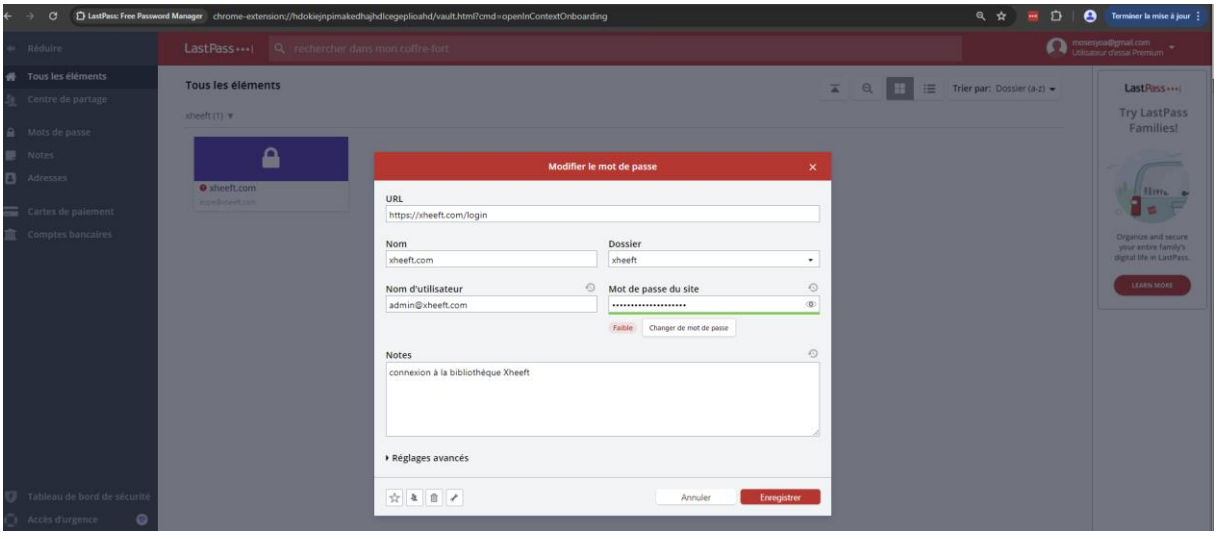
☒ Connexion



☒ Ajout de compte par connexion



☒ Ajout de compte manuel



☐ Comparatif des gestionnaires de mot de passe

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 est désormais *www.dc.com*
☐ www.ironman.com
☒ www.fessebook.com
☒ www.instagam.com

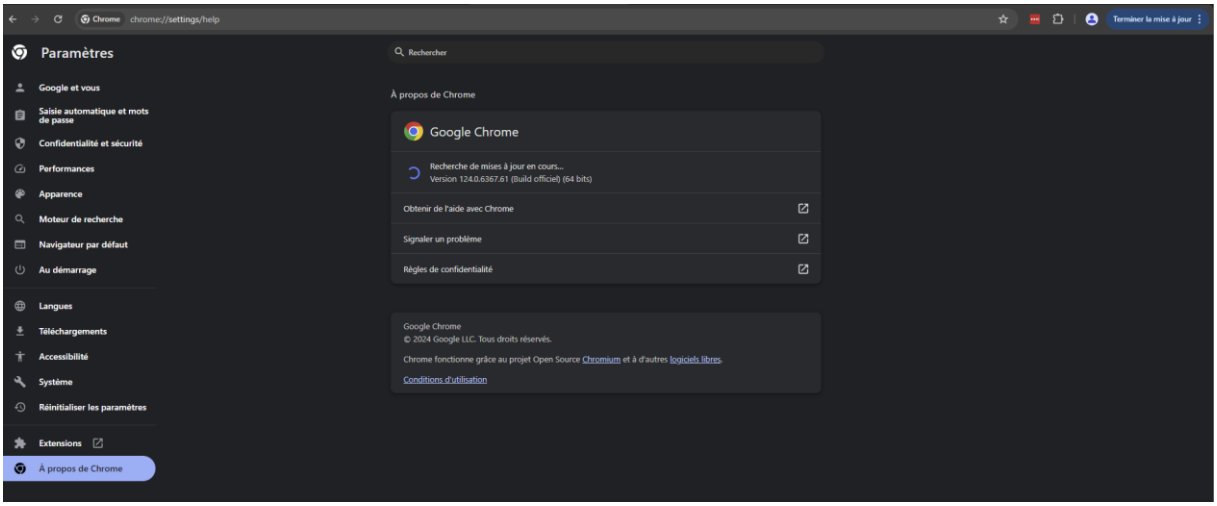
2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes. (case à cocher)

Chrome

☒ Menu -> Paramètres

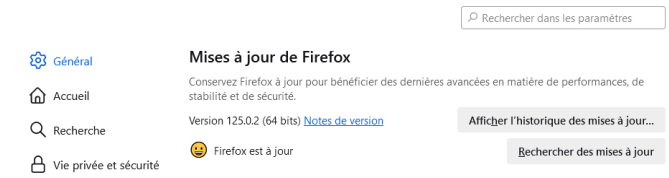
☒ A propose de Chrome

☒ Résultat : Chrome pas à jour !!



Pour Firefox

☒ Menu
☒ Paramètres
☒ Résultat : FireFox est à jour !!



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

Comment repérer un mail de phishing ?

Si les emails de phishing sont conçus pour être quasi-similaires aux mails dont ils ont usurpé l'identité, il est parfois possible de repérer les signaux d'une tentative de phishing. Bien que l'hameçonnage se présente sous diverses formes, on retrouve en effet souvent des indicateurs similaires. En voici une liste non exhaustive.

Si vous repérez un ou plusieurs de ces signaux d'alerte, et **au moindre doute, contactez l'expéditeur via un autre canal** afin de vérifier qu'il est bien à l'origine du message et qu'il ne s'agit pas d'un mail de phishing et d'une usurpation d'identité.

Quelles sont les formes les plus courantes de phishing par email ?

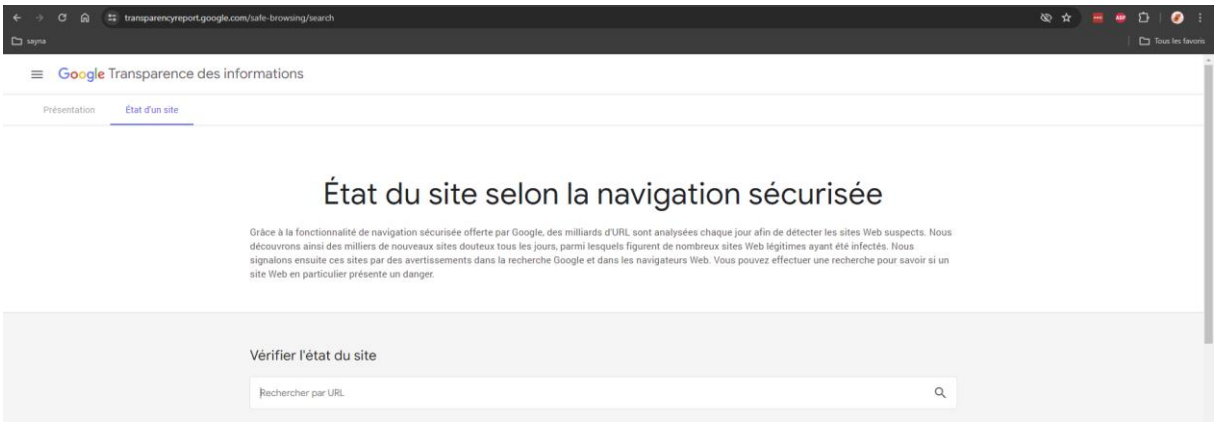
De nouveaux phishing sont créés chaque jour et les techniques employées par les cybercriminels sont de plus en plus innovantes. Il n'est donc pas possible de réaliser une liste exhaustive de toutes les formes d'arnaques par hameçonnage existantes. Cependant on peut recenser les formes de phishing par email les plus courantes et les identités les plus susceptibles d'être usurpées.

5 - Comment éviter les logiciels malveillants

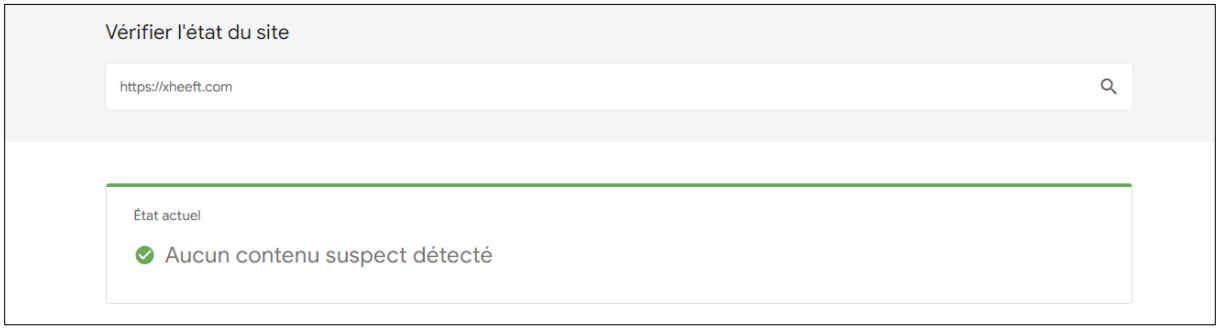
Objectif : *sécuriser votre ordinateur et identifier les liens suspects*

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)



- https://xheeft.com/
  - **Indicateur de sécurité**
    - HTTPS 🔒
  - **Analyse google**
    - Aucun contenu suspect



    - Vérifier un URL en particulier ●

https://learn.sayna.io

  - **Indicateur de sécurité**
    - HTTPS 🔒
  - **Analyse Google**
    - Aucun contenu suspect

http://referentiel.institut-agile.fr

  - **Indicateur de sécurité**
    - Not secure ○

Analyse Google

- Aucun donnée disponible

6 - Achats en ligne sécurisés

Objectif : *créer un registre des achats effectués sur internet*

1 / Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le bilan de tes dépenses du mois.

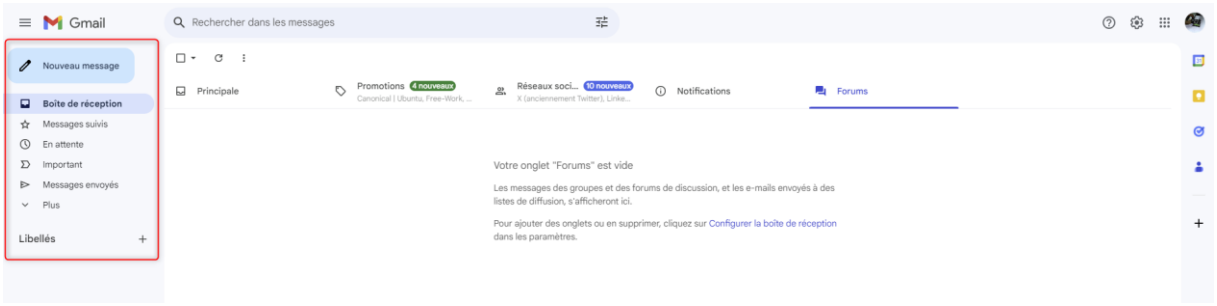
Deux possibilités s'offrent à toi pour organiser ce registre :

Créer un dossier sur ta messagerie électronique

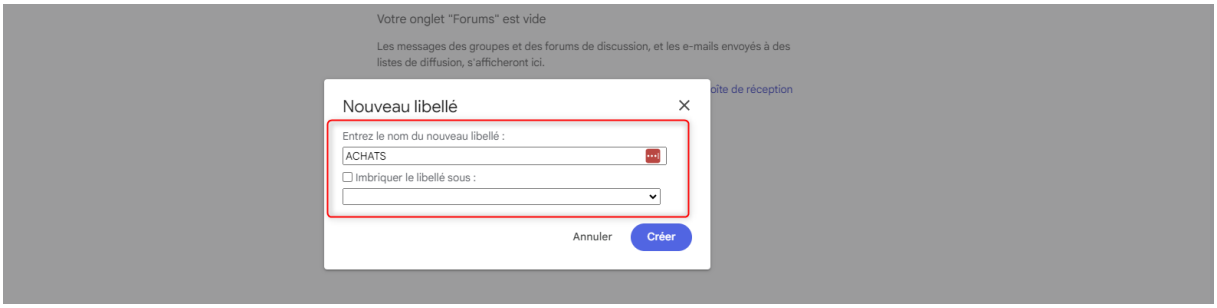
Créer un dossier sur ton espace de stockage personnel (en local ou sur le cloud)

La première est la plus pratique à utiliser et la plus facile à mettre en place. Nous prendrons pour exemple la messagerie de Google (les autres messageries fonctionnent sensiblement de la même manière). Suis les étapes suivantes pour créer un registre des achats sur ta messagerie électronique. (case à cocher)

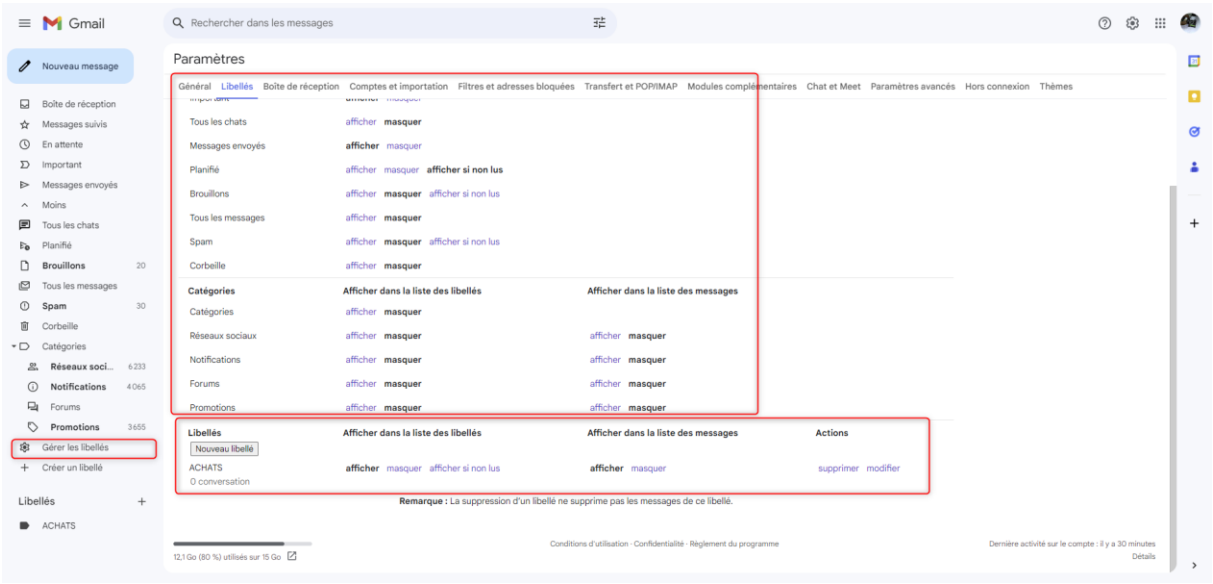
- Libellés Gmail



- Création du Libellé « ACHATS »



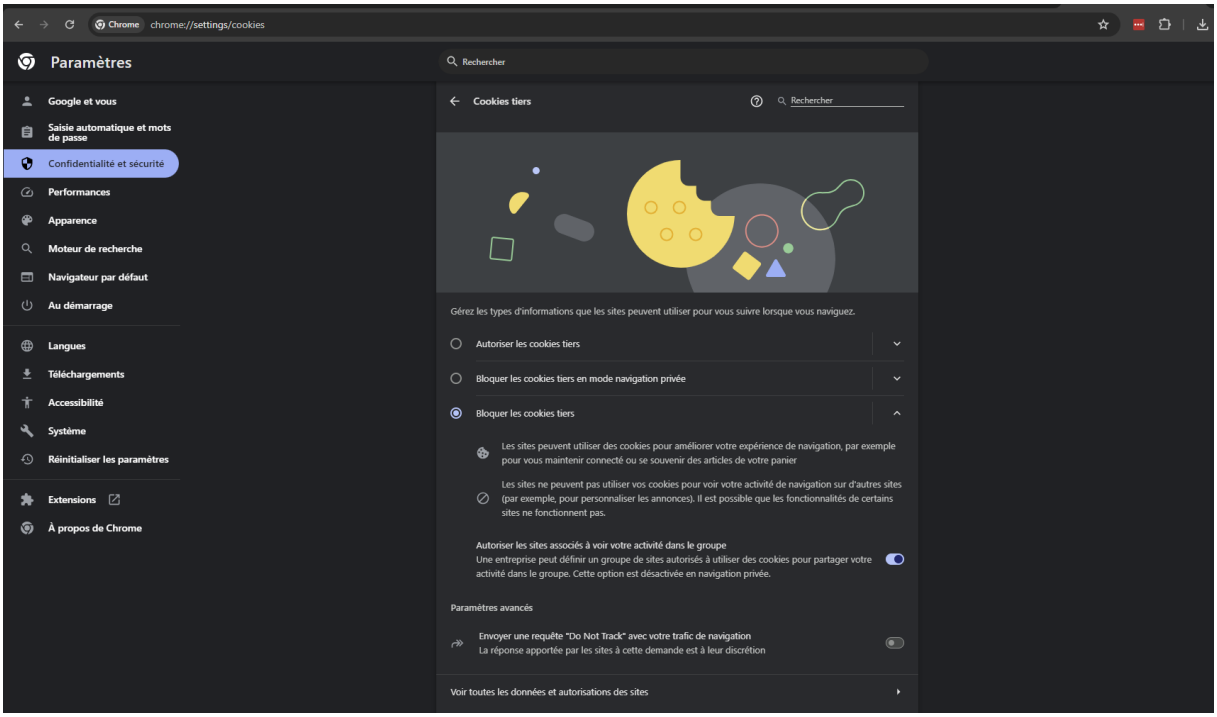
- Gestion des Libellés



7 - Comprendre le suivi du navigateur

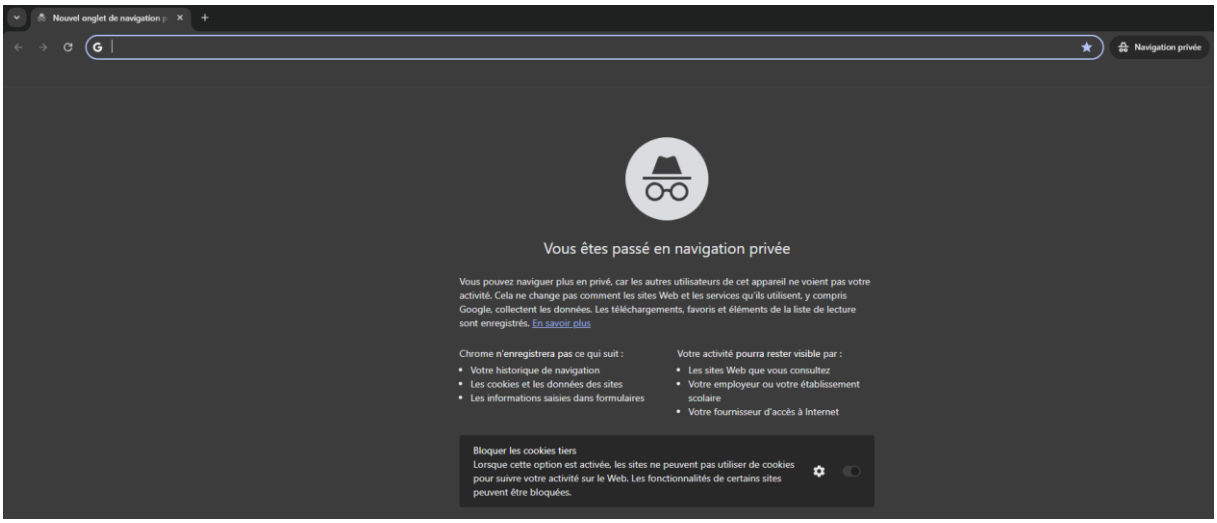
Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée

☒ Paramètre des cookies : chrome://settings/cookies

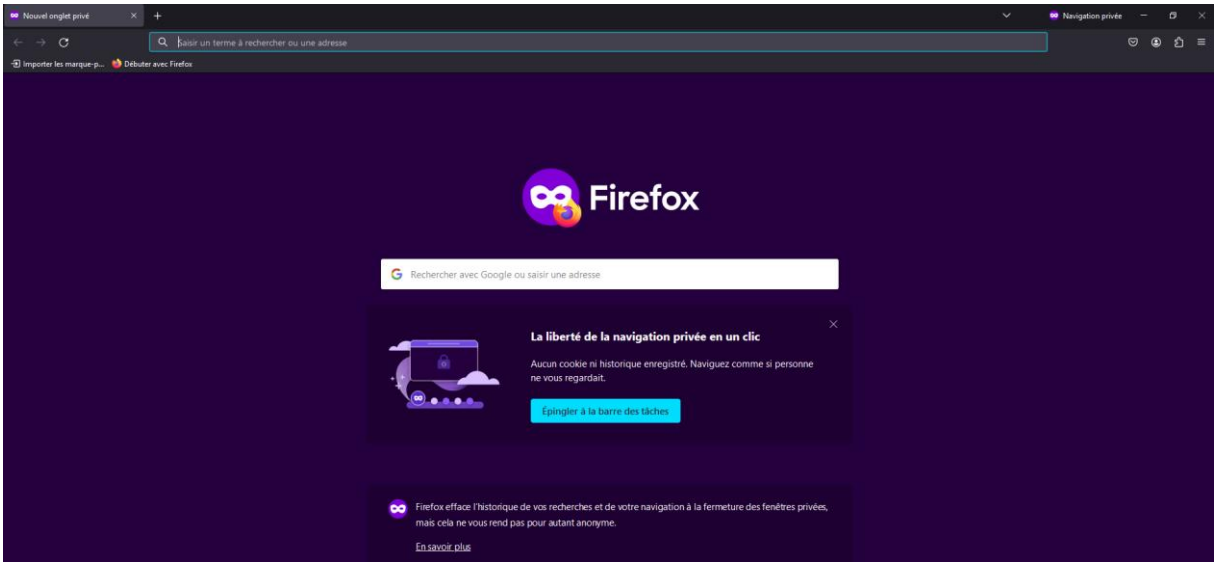


☒ Navigation privée

☒ Chrome: CTRL + SHIFT + N



☒ Firefox: CTRL + SHIFT + P



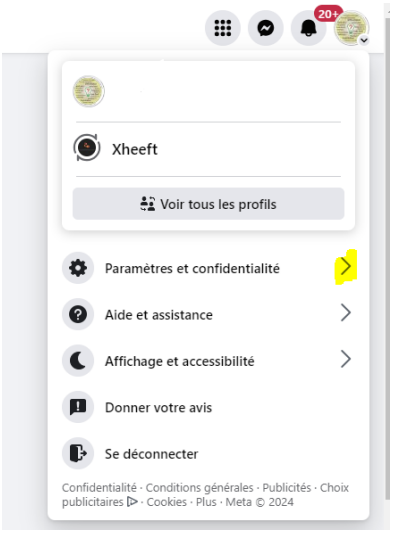
8 - Principes de base de la confidentialité des médias sociaux

Objectif : *Régler les paramètres de confidentialité de Facebook*

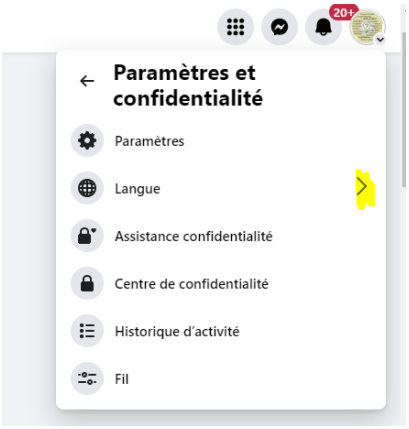
1 / Plus tôt dans le cours (Internet de base) tu as déjà été amené à utiliser ce réseau social en partageant une publication. Dans cet exercice on va te montrer le réglage des paramètres de confidentialité pour Facebook. Suis les étapes suivantes. (case à cocher)

☒ Connexion Facebook

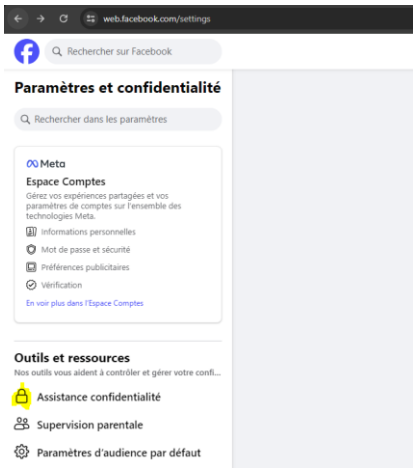
☒ Paramètres et confidentialité

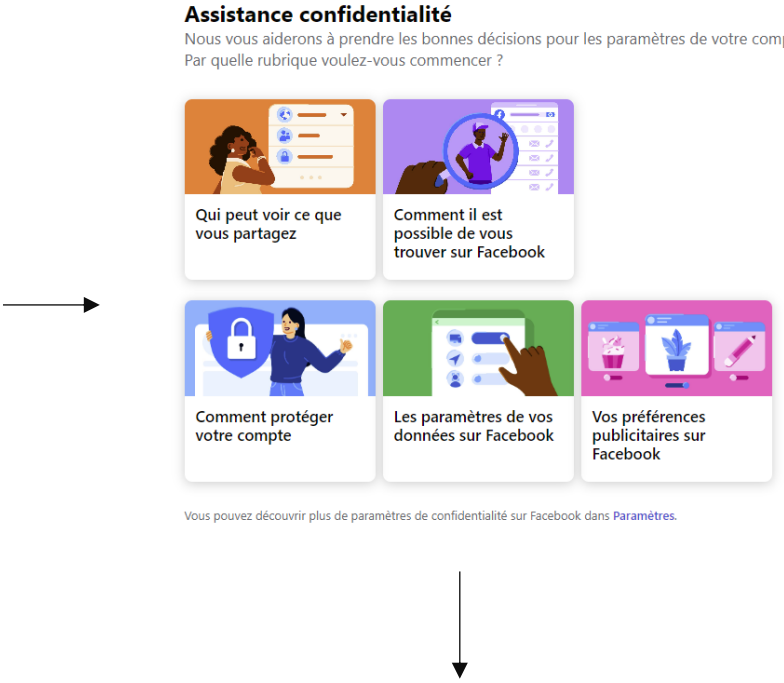


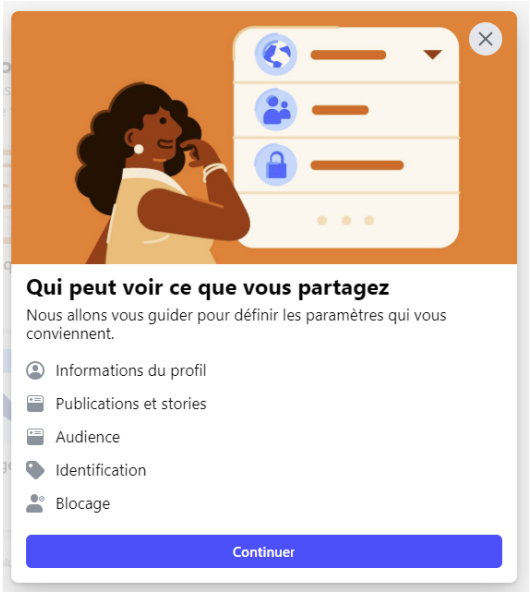
☒ Paramètres : https://web.facebook.com/settings



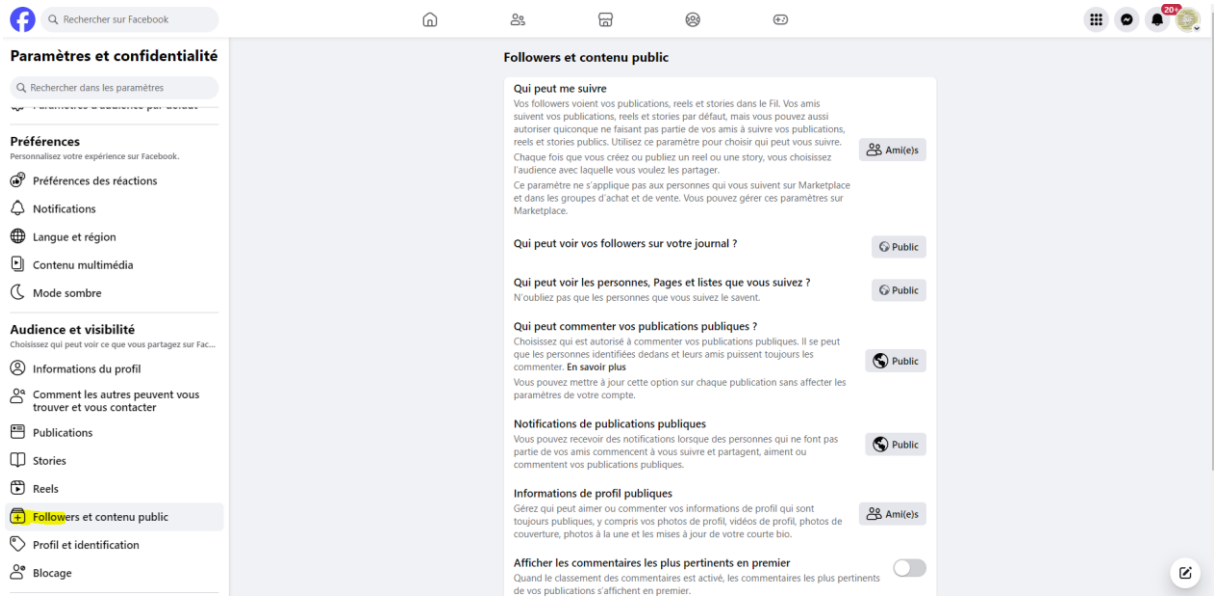
☒ Assistance confidentialité







☒ Followers et contenu public



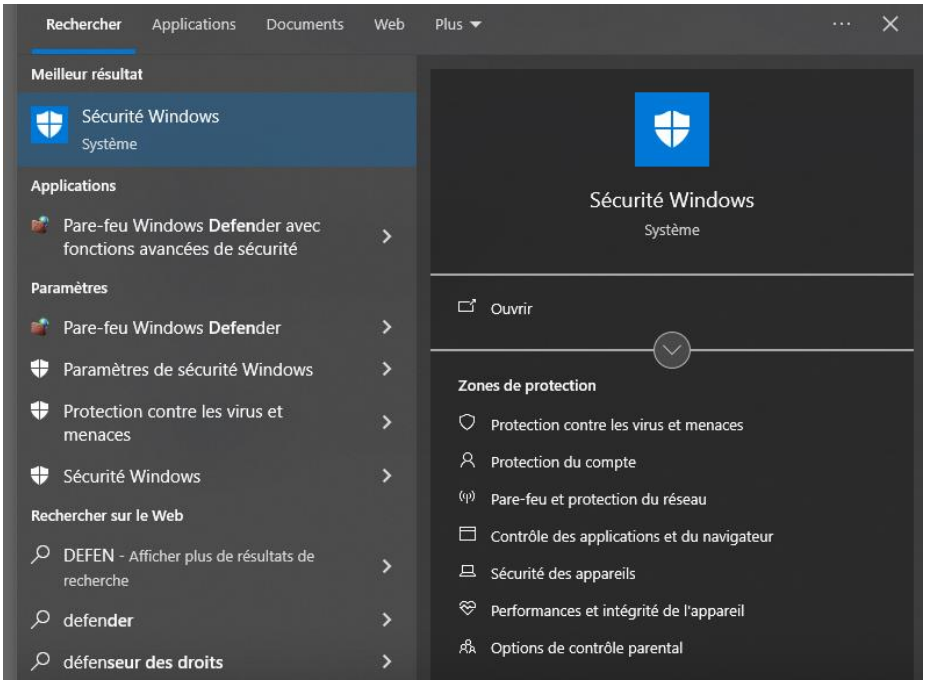
9 - Que faire si votre ordinateur est infecté par un virus

Objectif :

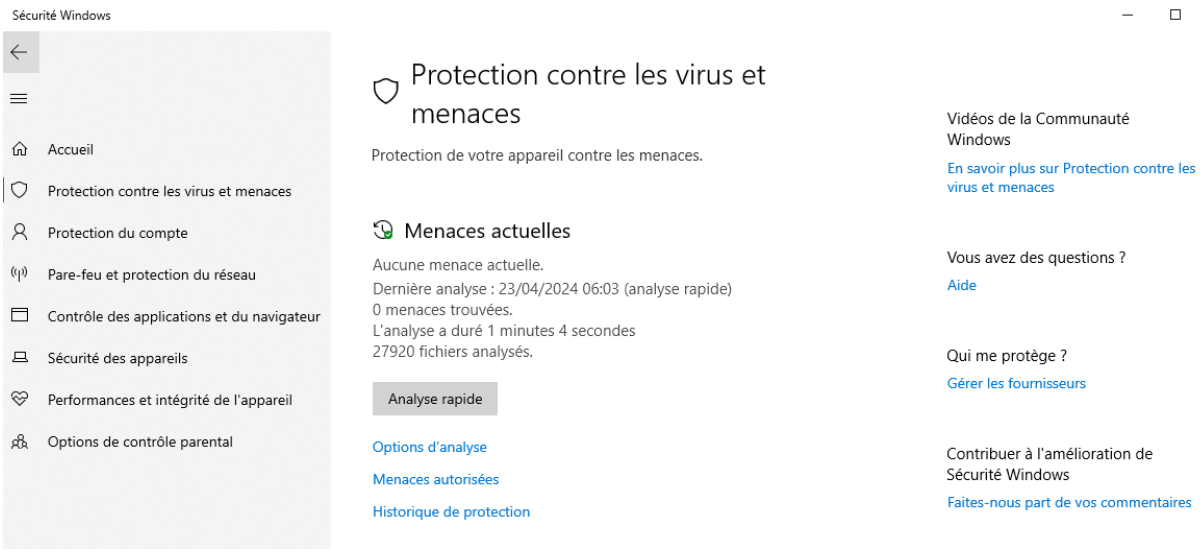
1/ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé.

Cas de l'ordinateur PC WINDOWS

☒ Paramètres de sécurité windows



☒ Comment faire : Faire une analyse rapide pour détection des ménaces



2/ Proposer un exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé.

Cas de l'ordinateur PC WINDOWS pour installation et utilisation antivirus et antiMalware

☒ installation et utilisation d'antimalware et antivirus : Malwarebytes