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

Objectif : à la découverte de la sécurité sur internet

1/ En naviguant sur le web, consulte trois articles qui parlent de sécurité sur internet :

● Article 1 = AVIRA - Sécurité sur Internet : 10 conseils pour protéger votre ordinateur personnel

https://www.avira.com/fr/blog/securite-sur-internet-10-conseils-pour-proteger-votre-ordinateur-personnel

● Article 2 = Kapersky - Confidentialité et sécurité sur Internet : 5 conseils de sécurité

https://www.kaspersky.fr/resource-center/preemptive-safety/privacy-and-security-on-the-internet

● Article 3 = cybermalveillance.gouv – Comment se protéger sur Internet ?

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-se-proteger-sur-internet

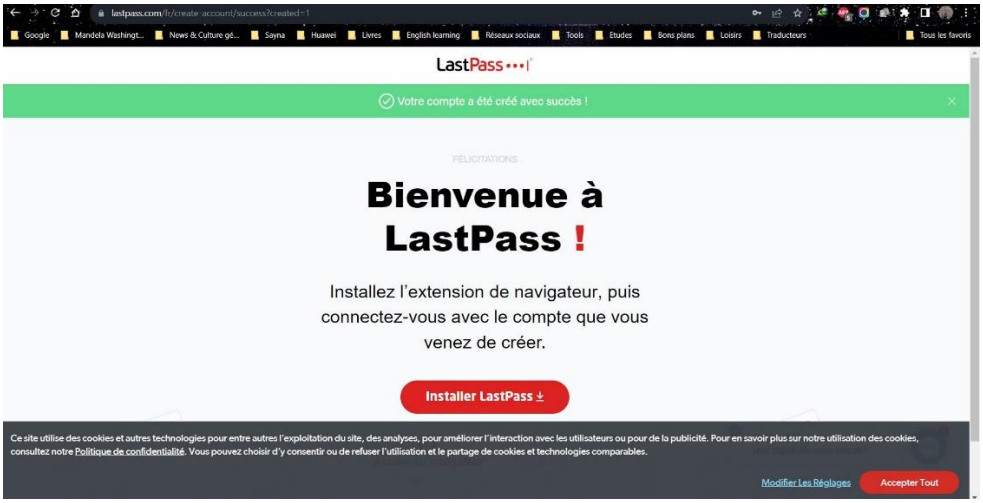
2 - Créer des mots de passe forts

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.

● Accède au site de LastPass avec le lien

● Crée un compte en remplissant le formulaire.



● Une fois la création du compte effectuée, tu arrives sur une page de validation qui propose le téléchargement de l'extension sur ton navigateur. Lance l'installation en effectuant un clic sur le bouton prévu à cet effet

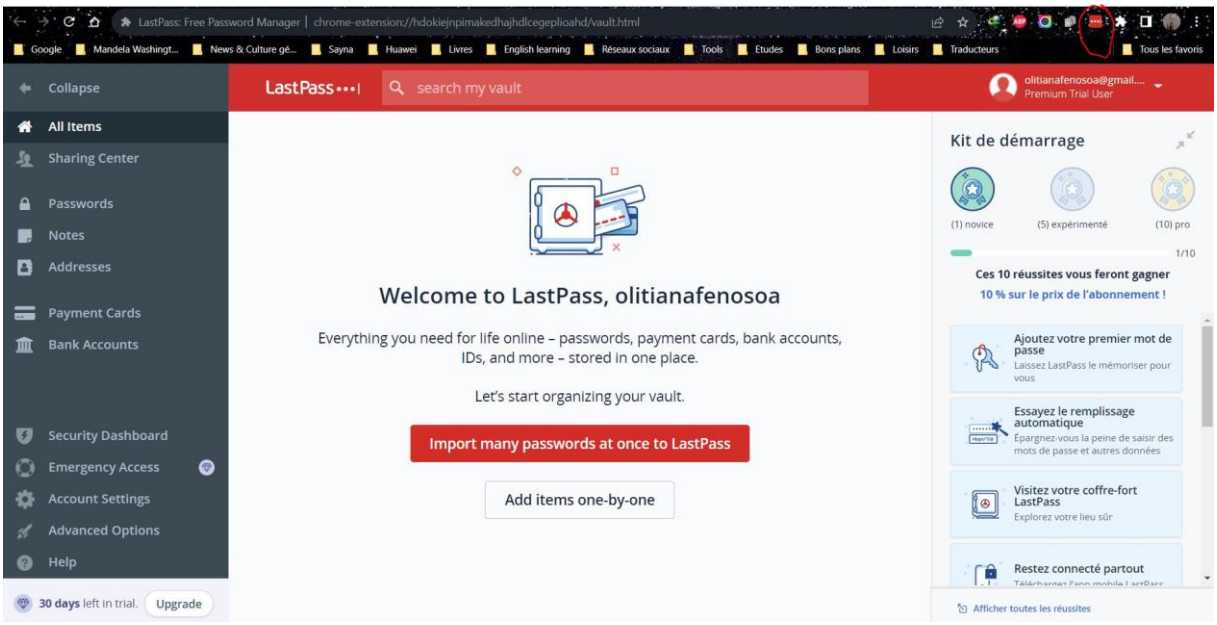
● Il te suffit de valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome"

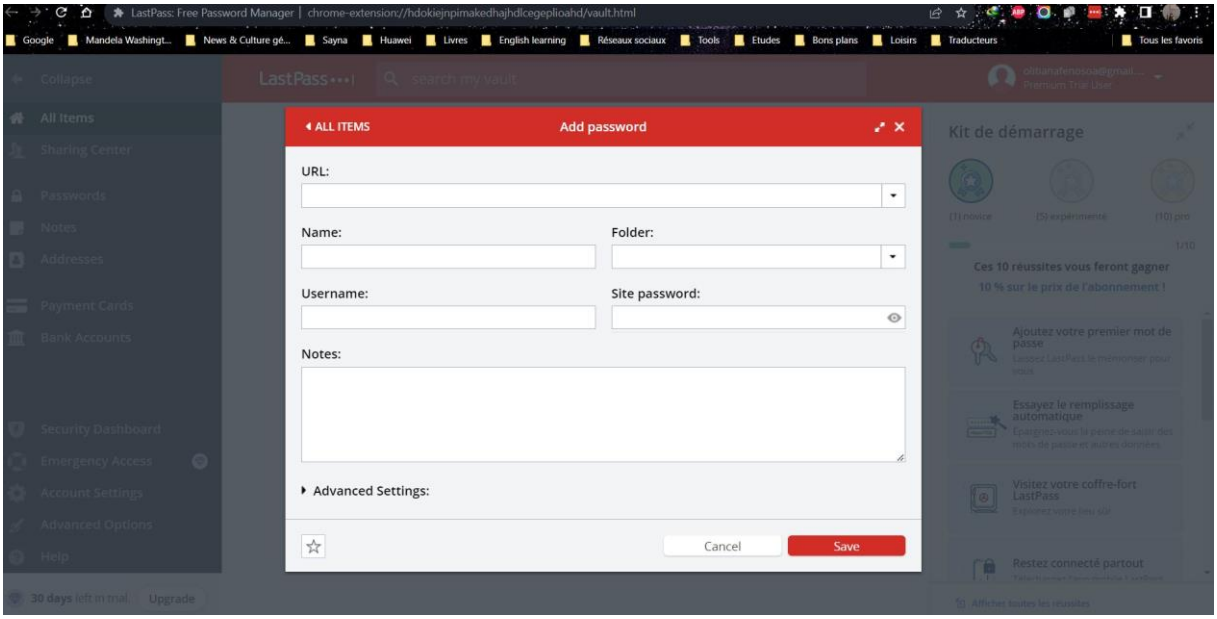
● Une fois installé, il te suffit d'accéder à cette extension et de t'y connecter

○ (1) En haut à droite du navigateur, clic sur le logo "Extensions"

○ (2) Épingle l'extension de LastPass avec l'icône

○ Il ne te reste plus qu'à te connecter en effectuant un clic sur l'icône de l'extension et en saisissant ton identifiant et 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.

Les sites web qui semblent être malveillants sont :

● www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel

● www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde

● www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très utilisé

Les seuls sites qui semblaient être cohérents sont donc :

● www.dccomics.com, le site officiel de l'univers DC Comics

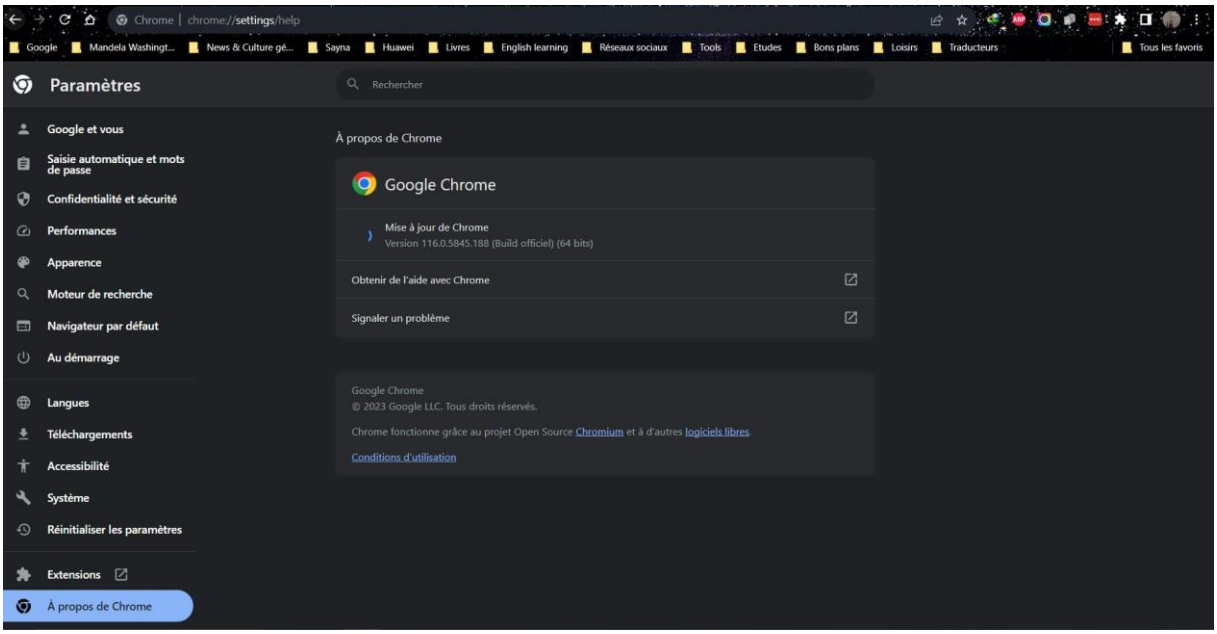
● www.ironman.com, le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

2/ Dans cet exercice, nous allons vérifier si le navigateur Chrome est à jour.

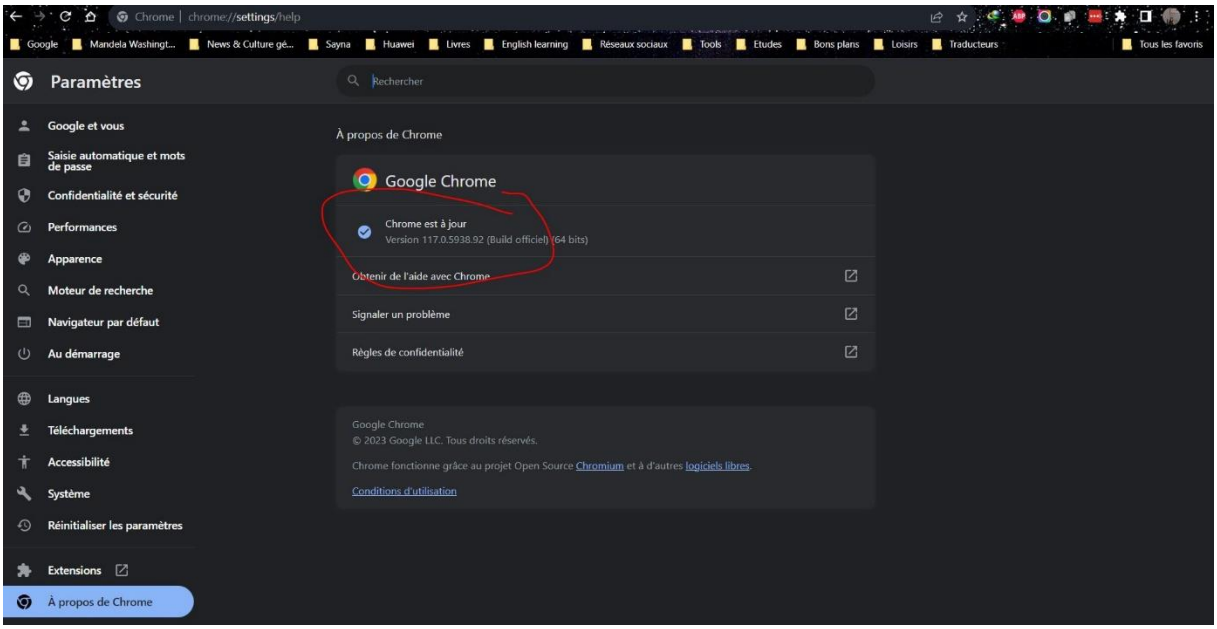
● Pour Chrome

○ 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



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

5 - Comment éviter les logiciels malveillants

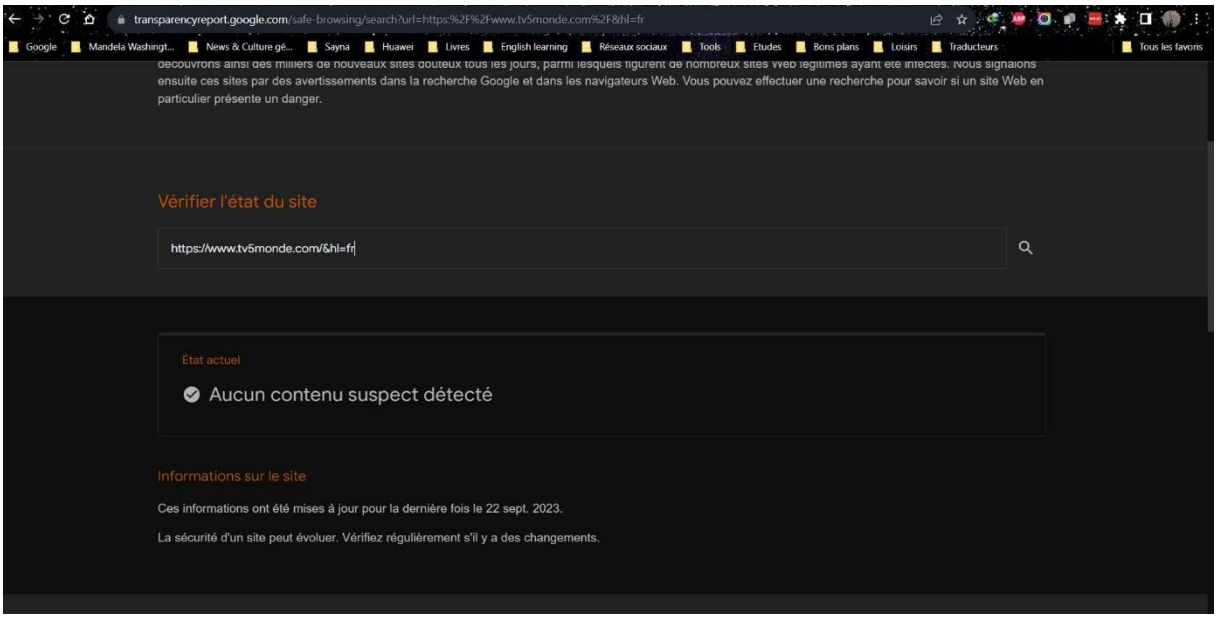
Objectif : sécuriser votre ordinateur et identifier les liens suspects

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.

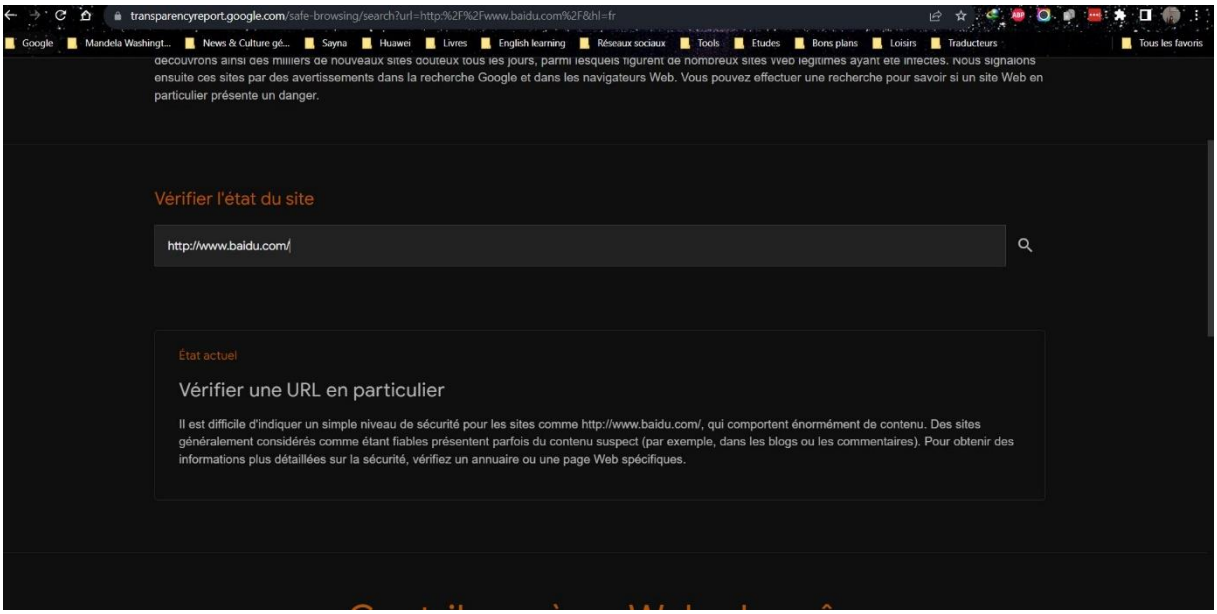
Lorsque le doute persiste tu peux t'appuyer sur un outil proposé par Google : Google Transparency Report (en anglais) ou Google Transparence des Informations (en français).

- Site n°1 : https://vostfree.tv/
  - Indicateur de sécurité
    - HTTPS
  - Analyse Google

- Site n°2 : https://www.tv5monde.com/
  - Indicateur de sécurité
    - HTTPS
  - Analyse Google
    - Aucun contenu suspect



- Site n°3 : http://www.baidu.com/
  - Indicateur de sécurité
    - Not secure
  - Analyse Google
    - Vérifier un URL en particulier



- Site n°4 (site non sécurisé)

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 :

1. Créer un dossier sur ta messagerie électronique

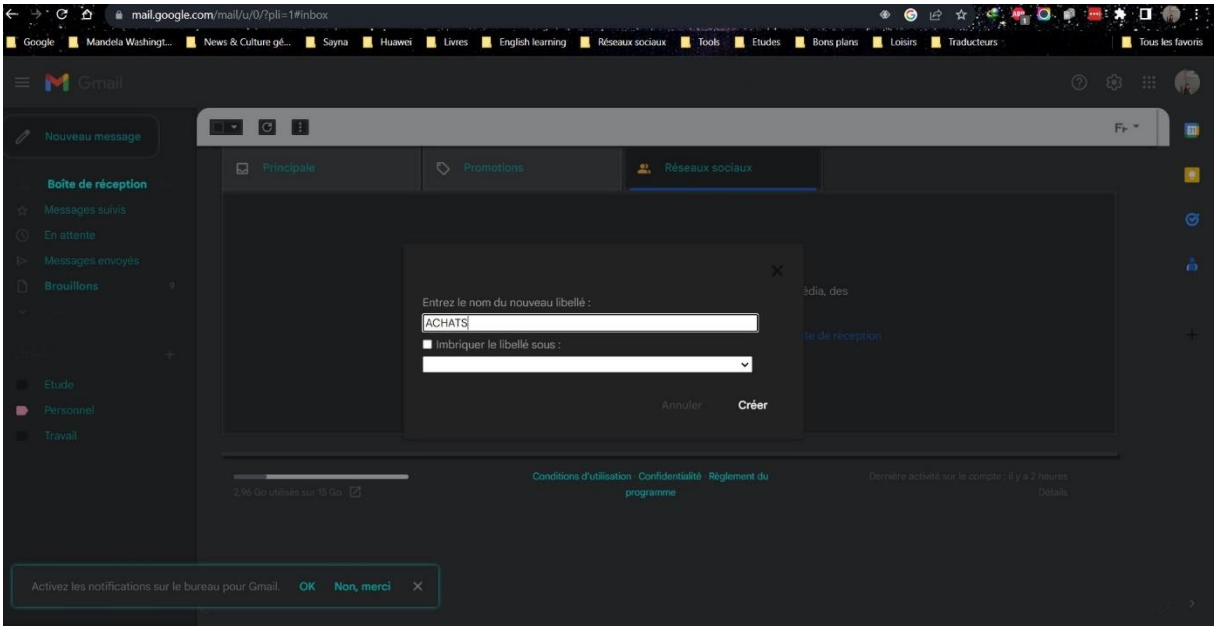
2. Créer un dossier sur ton espace de stockage personnel (en local ou sur le cloud)

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)

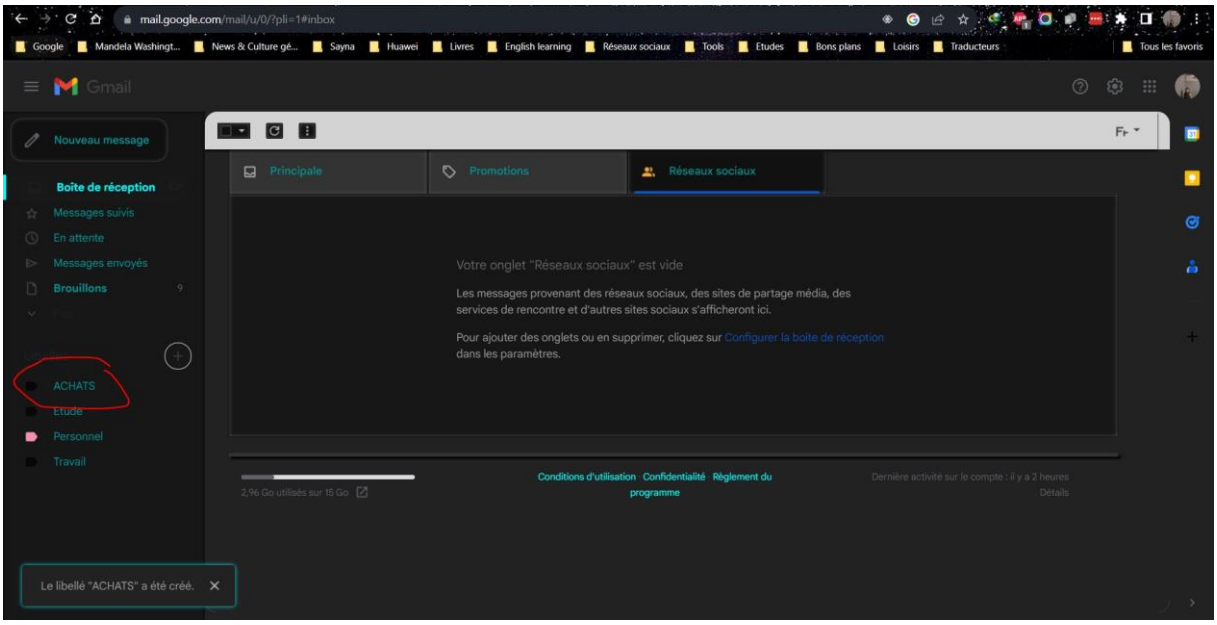
● Pour commencer, accède à ta messagerie électronique. Pour rappel, tu peux y accéder rapidement en ouvrant un nouvel onglet

● Sur la page d'accueil de ta messagerie, tu trouveras sur la gauche les libellés initialement prévus (boite de réception, messages envoyés, etc.)

● C'est dans cette partie que tu vas créer ta rubrique des achats. Pour ce faire, clic sur "Plus" et va tout en bas des libellés. Pour créer un libellé rapidement il te suffit d'effectuer un clic sur "Créer un libellé" et de le nommer "ACHATS" (pour notre exercice)



● Effectuer un clic sur le bouton "Créer" pour valider l'opération



● Tu peux également gérer les libellés en effectuant un clic sur “Gérer les libellés”(1). Sur cette page, tu peux gérer l’affichage des libellés initiaux (2) et gérer les libellés personnels (3)

● Tu as maintenant un libellé pour stocker tous tes messages électroniques relatifs aux achats effectués sur internet : confirmation de l’achat, détail de la commande, modalités de livraison

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

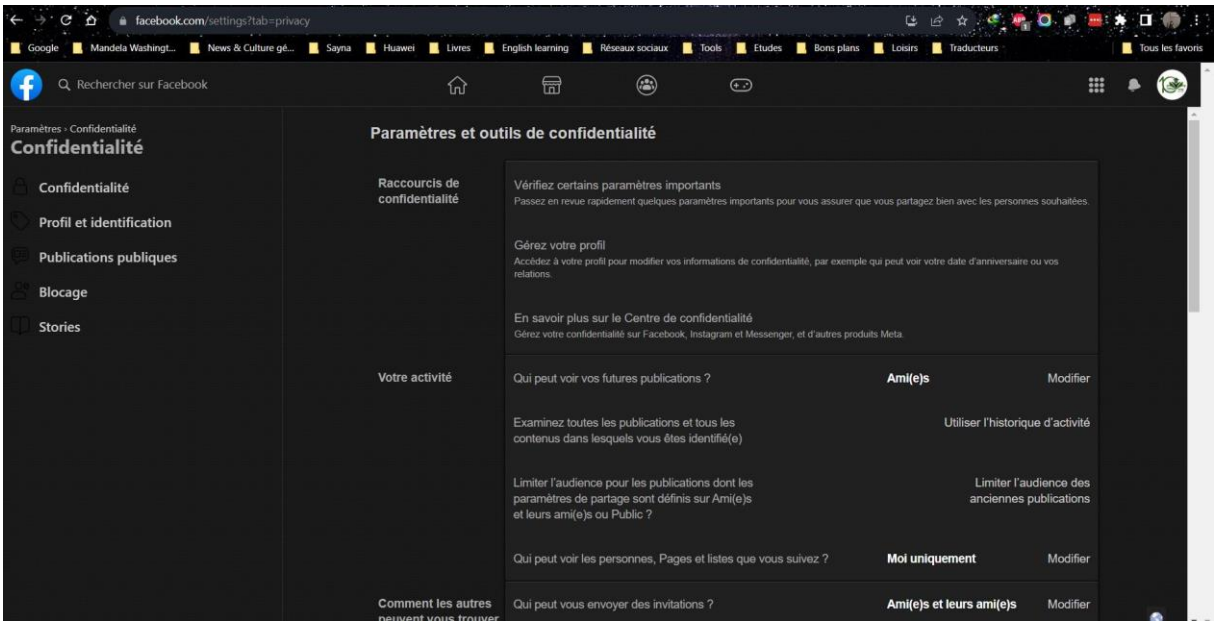
Objectif : Régler les paramètres de confidentialité de Facebook

1/ 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.

● 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

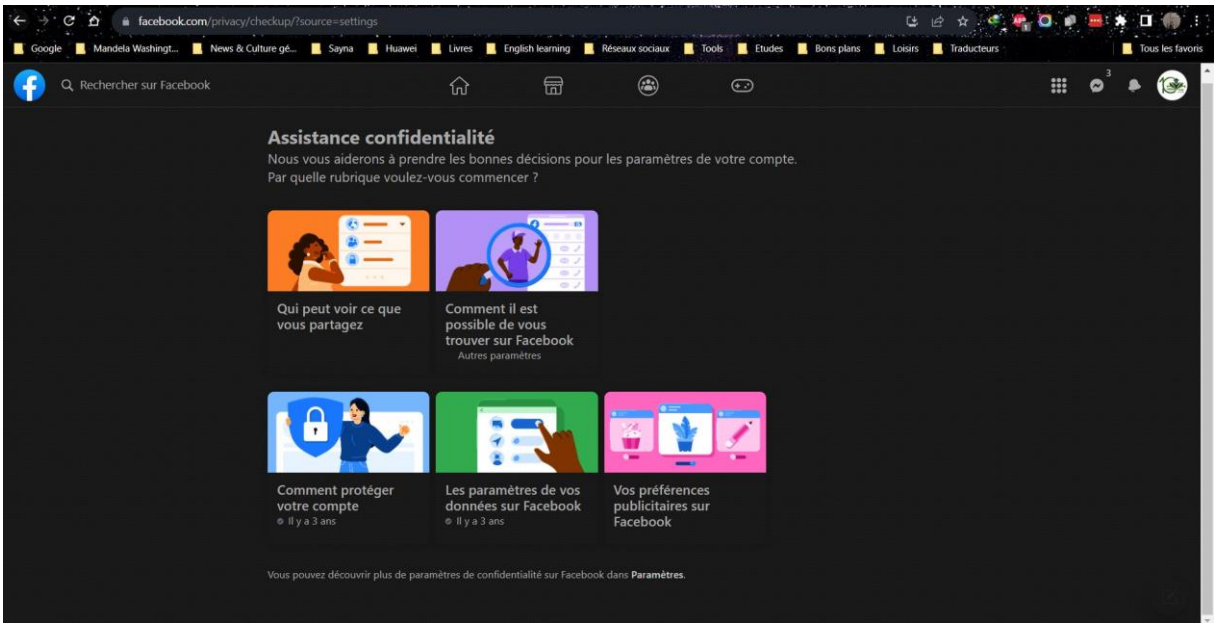
○ La première rubrique (orange) te permettra de régler la visibilité de tes informations personnelles

○ La deuxième rubrique (bleu) te permet de changer ton mot de passe

○ La troisième rubrique (violet) te permet de gérer la visibilité de ton profil pour la gestion des invitations

○ La quatrième rubrique (vert) permet de gérer la connexion simplifiée sur des applications ou des sites utilisés qui permettent cela

○ La dernière rubrique (rose) permet de gérer les informations récoltées par Facebook utiles pour les annonceurs



● Retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à gauche. Tu peux continuer à explorer les rubriques pour personnaliser tes paramètres. On ne peut pas te dire ce que tu dois faire. C'est à toi de choisir les informations que tu souhaites partager et celles que tu veux garder privées. Voici tout de même quelques conseils :

○ Si tu utilises ton compte Facebook uniquement pour communiquer avec tes amis, règles les paramètres en conséquence en choisissant une visibilité "Amis" ou "Amis de leurs amis".

○ Beaucoup de personnes utilisent Facebook en mêlant réseau professionnel et réseau personnel. Il n'y a pas vraiment de contre-indication, mais on te conseille tout de même de ne pas trop mélanger les deux. Il existe LinkedIn pour utiliser un média social pour le réseau professionnel

○ Pour limiter les haters et les commentaires malveillants, tu peux restreindre les commentaires de tes publications. Ça se passe dans l'onglet "Publications publiques"

● Dans les paramètres de Facebook tu as également un onglet "Cookies". On t'en a parlé dans le cours précédent (Comprendre le suivi du navigateur). 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

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

• Vérifier l'état de protection antivirus de mon PC.

Pour vérifier l'état de protection antivirus de votre ordinateur, ouvrez le centre de sécurité de Windows. Cible : Zone d'accès rapide -> Centre de sécurité Windows -> Pare-feu et protection du réseau

Un PC ralenti et qui a tendance à « ramer » plus que d'habitude, Des dossiers manquants ou déplacés sur votre bureau ; La page d'accueil de votre navigateur a changé ; Des bugs et messages d'erreurs (impossible d'ouvrir certains programmes, d'autres se ferment subitement ou s'exécutent sans votre accord…) et il y a aussi des redémarrages non désirés. Que faire ? Nous allons en premier lieu installer un antivirus pour analyser le système, s'il y a de quelconque alarme, nous allons formater le PC et réinstaller son système d'exploitation.

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

• Si vous n'avez pas installé d'antivirus par vous-même, qu'il soit gratuit (Avast, AVG…) ou payant (Norton, McAfee, BitDefender…), c'est l'antivirus intégré de Windows, appelé Windows Defender, qui doit s'occuper de protéger votre PC contre différentes menaces (virus, malwares, ransomwares…).

Si vous installez un antivirus tiers, Windows Defender va alors automatiquement se désactiver. En revanche, si vous installez plusieurs antivirus tiers, ils seront tous activés par Windows, ce qui peut être problématique (ralentissements de votre PC, voir instabilité). Je vous conseille donc de n'activer qu'un seul antivirus en désinstallant les autres antivirus présents sur votre PC.

-Il faut mettre à jour le Windows Defender ; lui aussi il peut protéger contre des virus

-Choisir un antivirus. Voici le classement des 7 meilleurs antivirus en 2023 selon 01net.com
Bitdefender Antivirus
Intego
Norton
NordVPN Antivirus
Avast Antivirus
McAfee
AVG Ultimate
-Choisir parmi ces antivirus et l'installer.

-Regarder un tutoriel sur l'utilisation de ce dernier.