



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

- Introduction à la sécurité sur Internet
- Créer des mots de passe forts
- Fonctionnalité de sécurité de votre navigateur
- Éviter le spam et le phishing
- Comment éviter les logiciels malveillants
- Achats en ligne sécurisés
- Comprendre le suivi du navigateur
- Principes de base de la confidentialité des médias sociaux
- Que faire si votre ordinateur est infecté par un virus



1 - Introduction à la sécurité sur Internet

Objectif : à la découverte de la sécurité sur internet

1/ Trois articles qui parlent de sécurité sur internet.

- Article 1 = KASPERSKI – Sécurité Internet : Qu'est ce que c'est et comment vous protéger en ligne.
- Article 2 = Safety culture – Sécurité sur internet
- Article 3 = wikiHow – Comment ne pas se faire pirater (hacker) sur internet.

2 - Créer des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass

1/ Comment utiliser LastPass

Créer un compte | LastPass x

lastpass.com/create-account.php

Maps Settings - Passwo... Multimédia Réseaux sociaux Apprentissage Work Tools Culture G Tous les favoris

Un mot de passe. Zéro souci.

LastPass s'occupe du reste.

Créer un compte ou Connexion

Adresse e-mail
michael.razanakoto1996@gmail.com

Mot de passe maître
Force

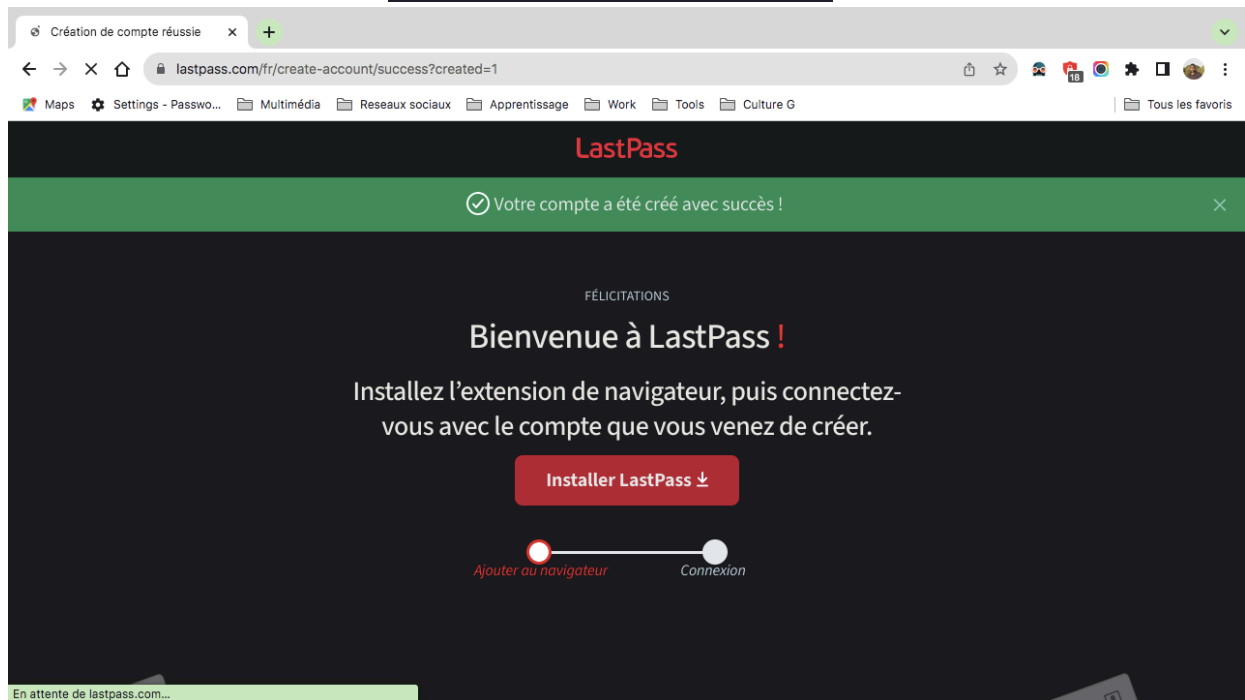
Exigences minimales:

- ✓ Indicateur de force au maximum
- ✓ Au moins 12 caractères
- ✓ Au moins 1 chiffre
- ✓ Au moins 1 minuscule
- ✓ Au moins 1 majuscule
- ✓ Au moins 1 caractère spécial
- ✓ Pas votre e-mail

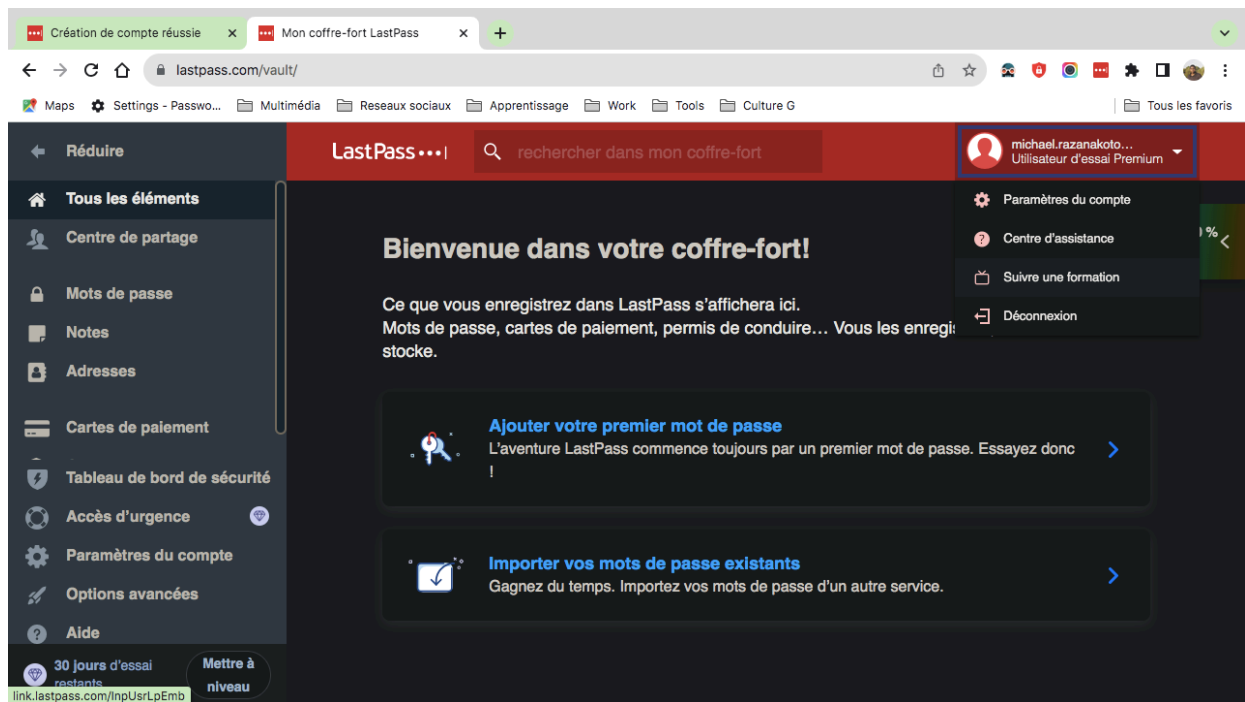
Nos conseils :

Fonctionnalités Free

✓ Coffre-fort de mots de passe sécurisé



• Connection



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.

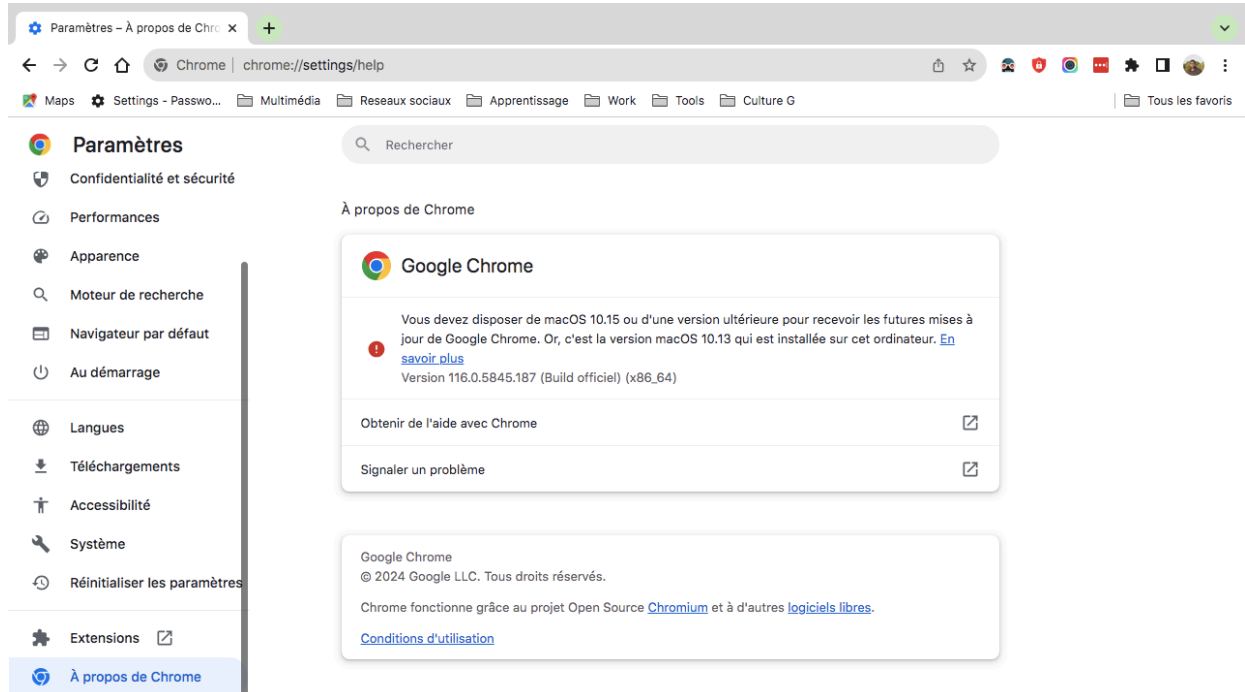
- www.morvel.com : site malveillant (à vendre), le vrai site est www.marvel.com consigner au superhéros de marvel
- www.dccomics.com : le site officiel de l'univers DC Comics
- www.ironman.com : le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)
- www.fessebook.com : site malveillant non sécurisé, faisant référence à www.facebook.com



- www.instagram.com : site malveillant non sécurisé, faisant référence à www.instagram.com

2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour.

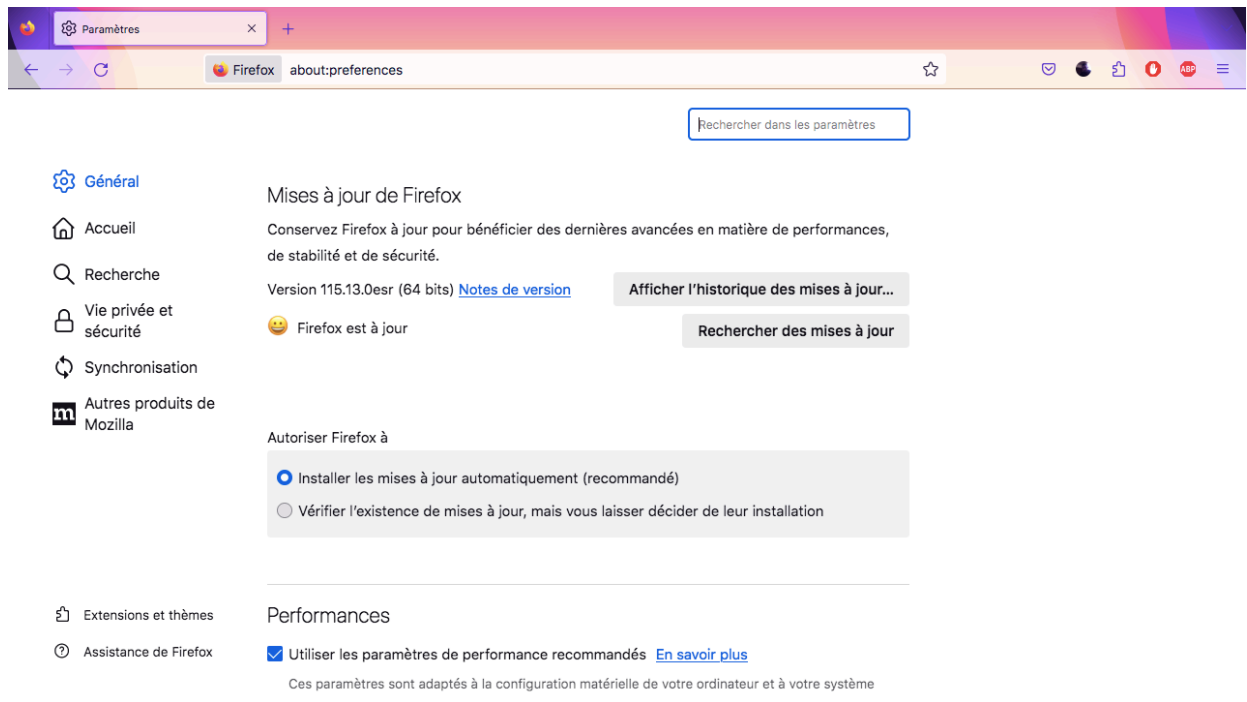
- Pour Chrome



Chrome n'est pas à jour, je ne peux pas télécharger le nouveau MAJ car je possède une ancien version de MacBook air et je ne peux pas télécharger la nouvelle MAJ du système sans changer de MacBook.



• Pour Firefox

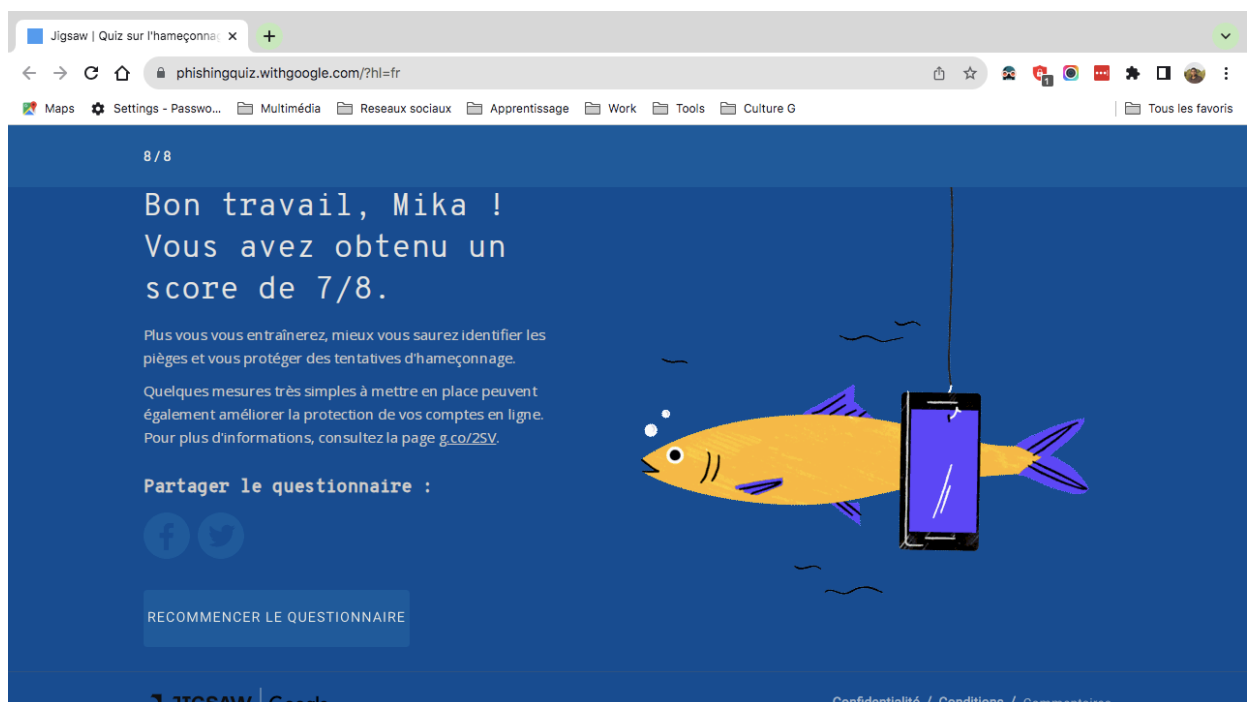


Firefox est à jour

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.





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.

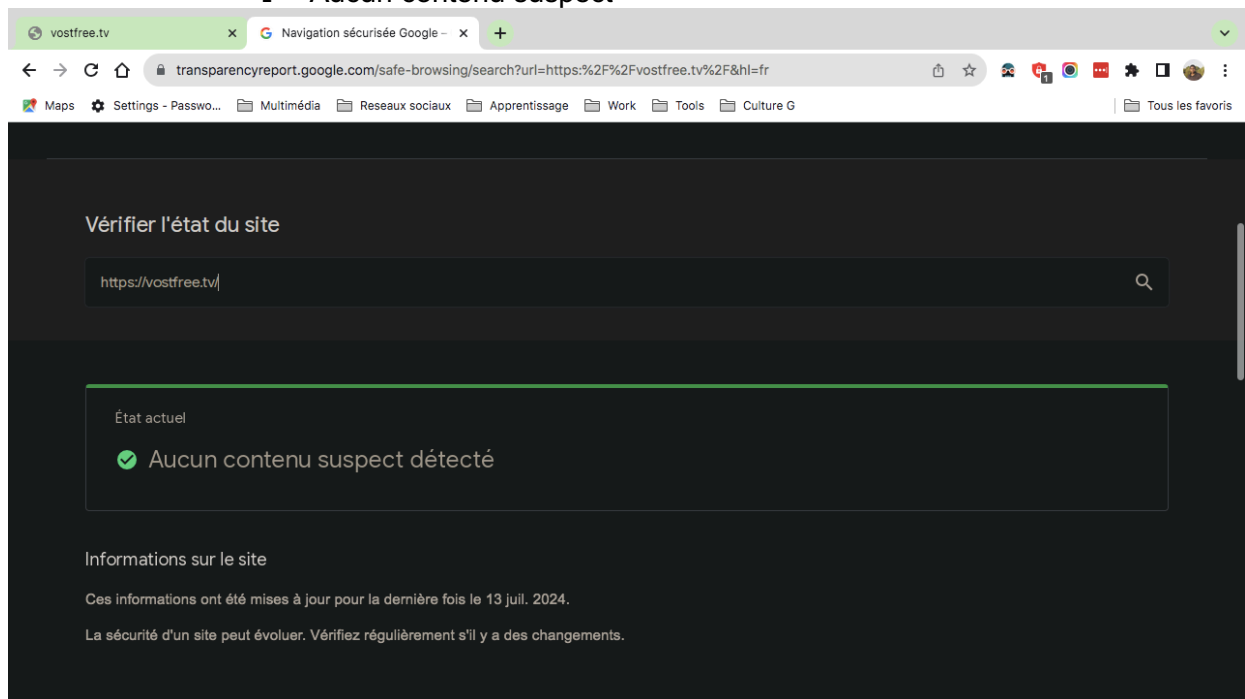
- Site n°1

Indicateur de sécurité

■ HTTPS 

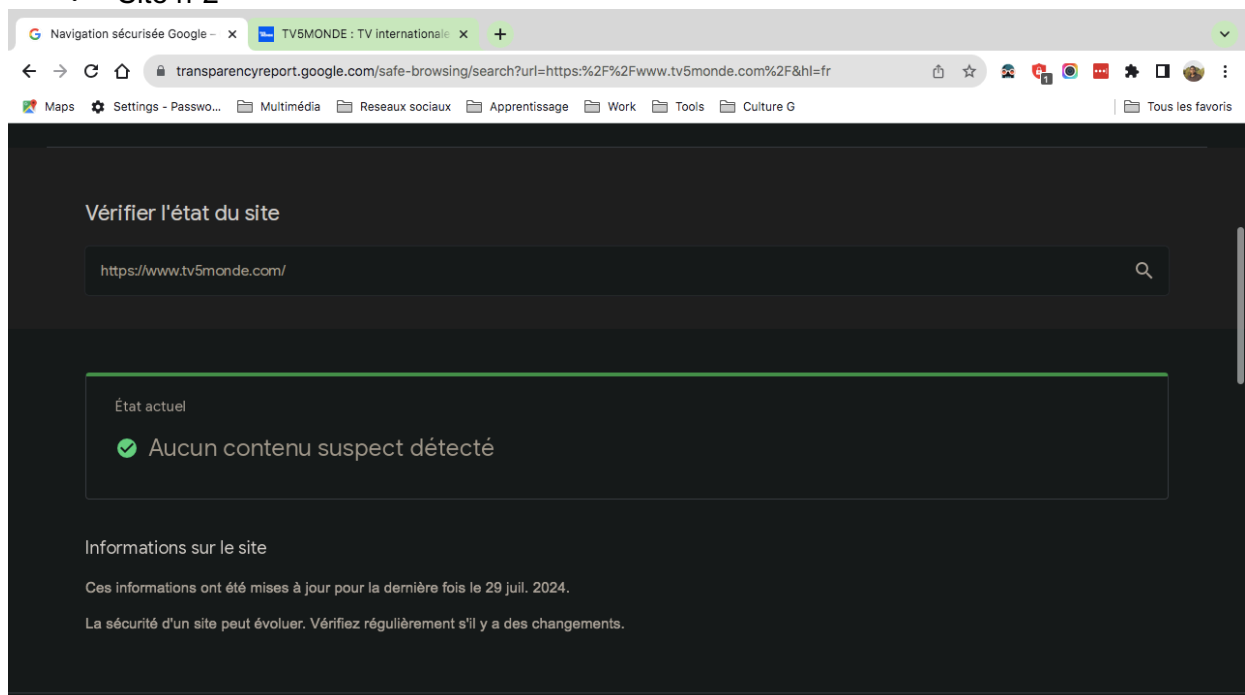
Analyse Google

■ Aucun contenu suspect



The screenshot shows a Google Chrome browser window with two tabs: 'vostfree.tv' and 'Navigation sécurisée Google'. The address bar shows the URL 'transparencypreport.google.com/safe-browsing/search?url=https:%2F%2Fvostfree.tv%2F&hl=fr'. Below the browser window, a dark-themed report titled 'Vérifier l'état du site' is displayed. It contains a search bar with the URL 'https://vostfree.tv/'. Below the search bar, a green box with a checkmark icon and the text 'Aucun contenu suspect détecté' indicates the site is safe. Further down, under 'Informations sur le site', it states that the information was last updated on July 13, 2024, and advises regular checks for updates.

- Site n°2



The screenshot shows a Google Chrome browser window with two tabs: 'Navigation sécurisée Google' and 'TV5MONDE : TV Internationale'. The address bar shows the URL 'transparencypreport.google.com/safe-browsing/search?url=https:%2F%2Fwww.tv5monde.com%2F&hl=fr'. Below the browser window, a dark-themed report titled 'Vérifier l'état du site' is displayed. It contains a search bar with the URL 'https://www.tv5monde.com/'. Below the search bar, a green box with a checkmark icon and the text 'Aucun contenu suspect détecté' indicates the site is safe. Further down, under 'Informations sur le site', it states that the information was last updated on July 29, 2024, and advises regular checks for updates.



Indicateur de sécurité

- HTTPS

Analyse Google

- Aucun contenu suspect

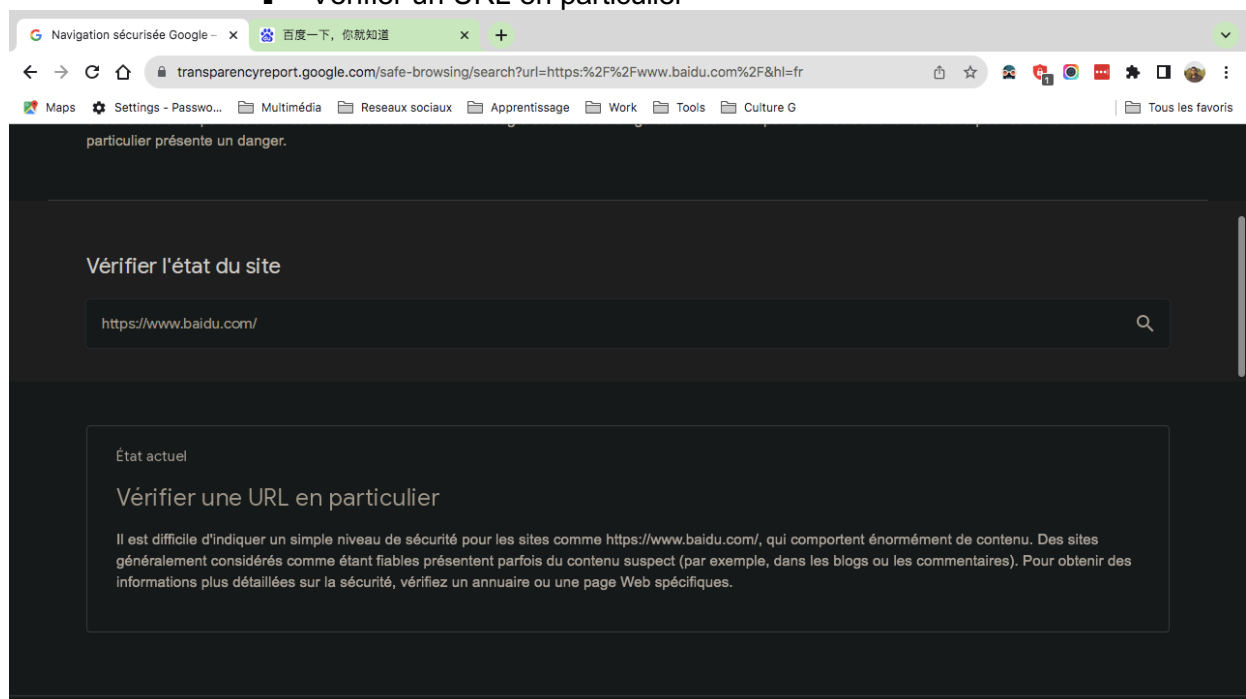
- Site n°3

- Indicateur de sécurité

- Not secure

- Analyse Google

- Vérifier un URL en particulier



- Site n°4 (site non sécurisé)

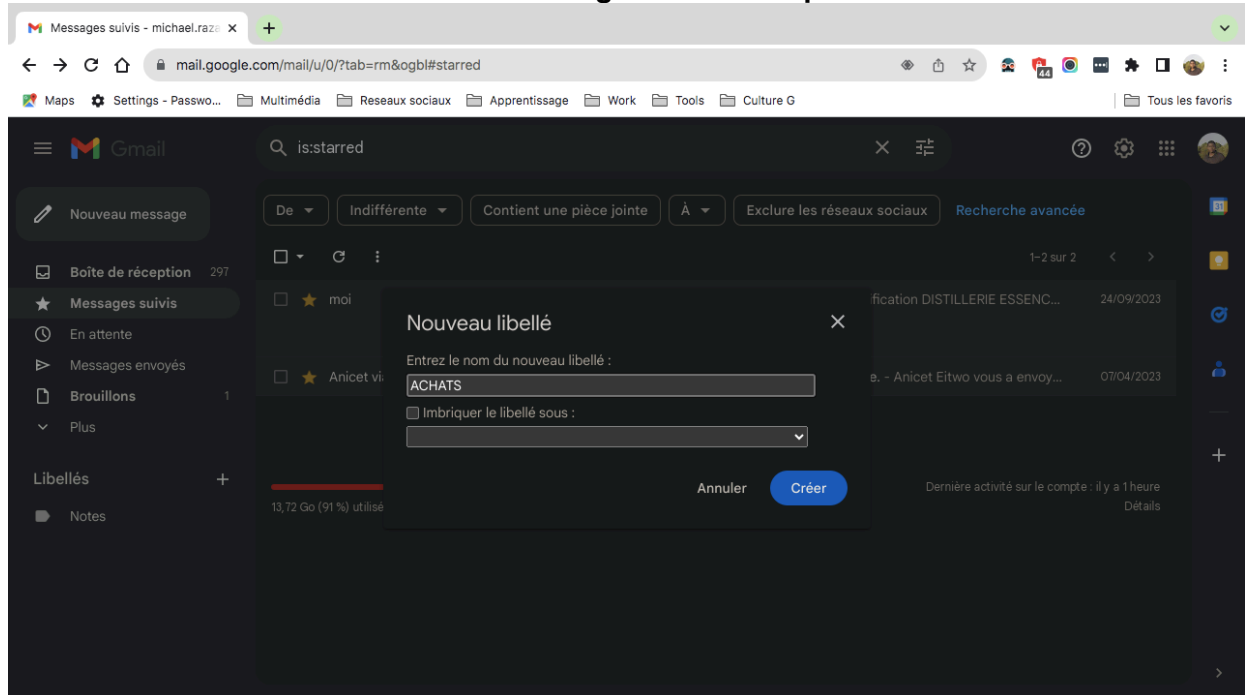
6 - Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

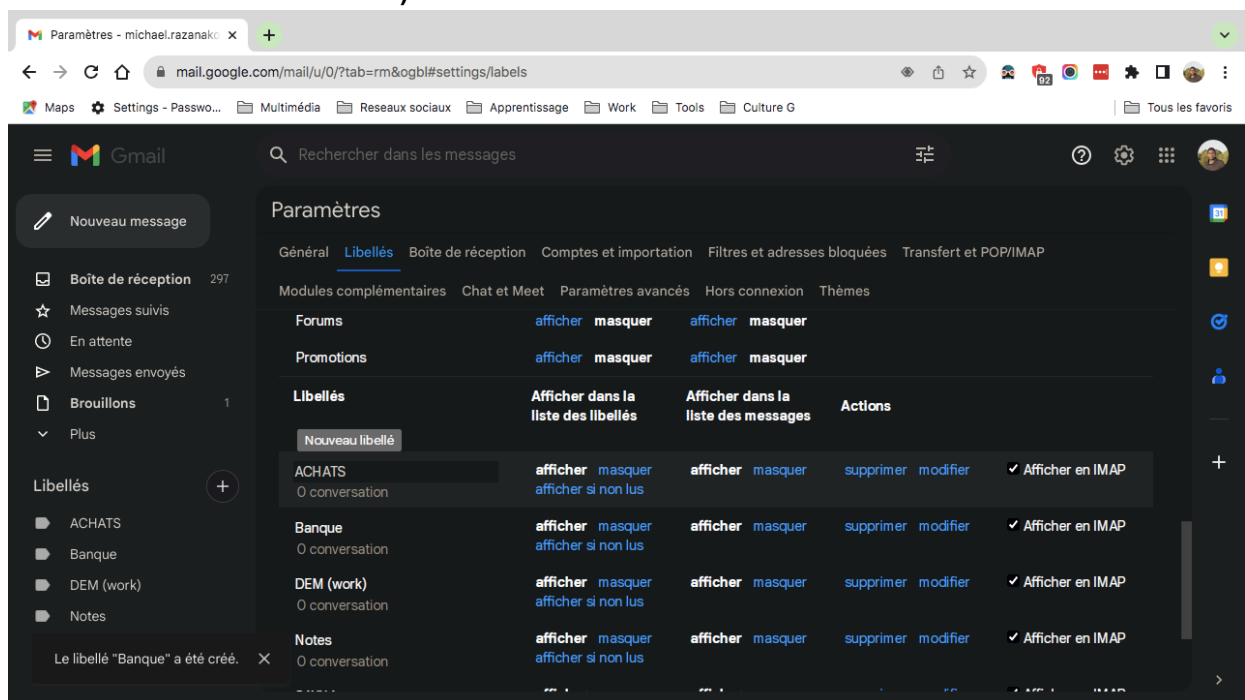
1/ Dans cet exercice, on va t'aider à créer un registre des achats..

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

1. Création de dossier sur ma messagerie électronique



2. Création de dossier de dossier sur mon espace de stockage personnel (en local ou sur le cloud)



7 - Comprendre le suivi du navigateur

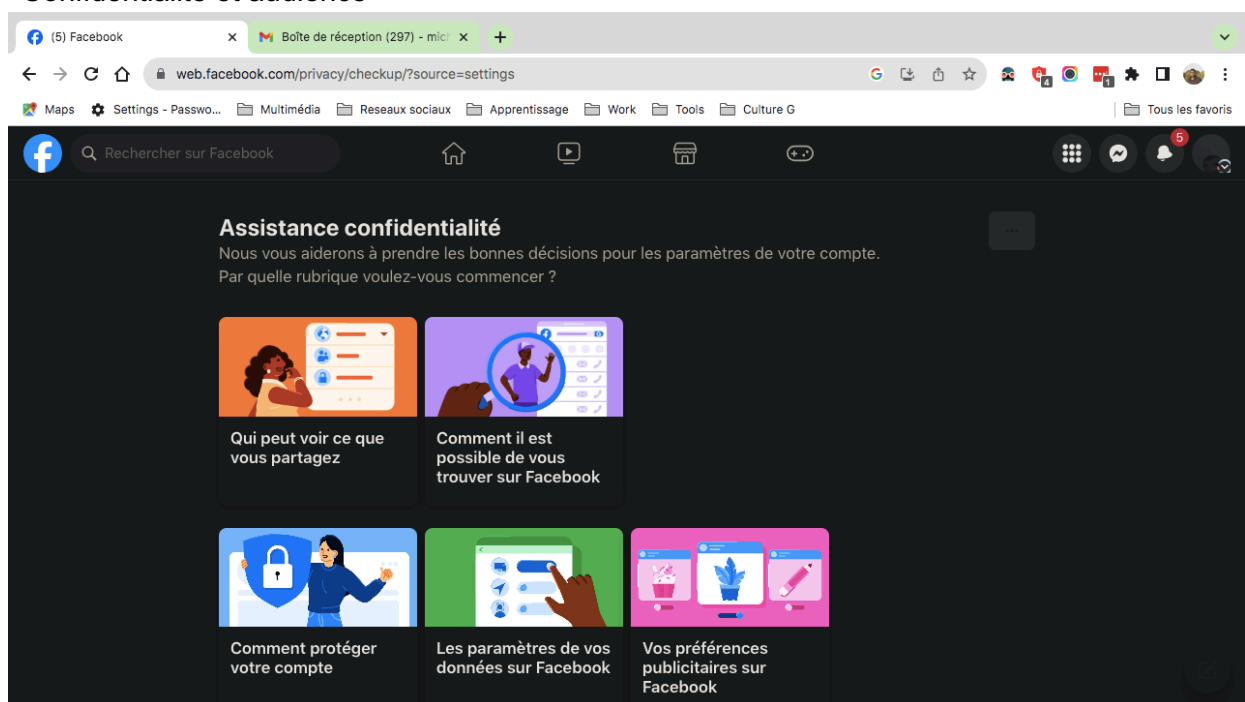
Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée

8 - Principes de base de la confidentialité des médias sociaux

Objectif : *Régler les paramètres de confidentialité de Facebook*

1/ Réglage des paramètres de confidentialité pour Facebook.

Confidentialité et audience



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 ??????? Comment faire ????????

Téléphone :

- ⇒ Ouvrez l'application Paramètres de votre téléphone.
- ⇒ Appuyez sur Sécurité.
- ⇒ L'état de sécurité de votre appareil et de votre compte Google s'affiche en haut de l'écran. Vous verrez apparaître un message d'avertissement si des actions importantes sont nécessaires pour sécuriser votre appareil ou vos comptes.

Ordinateur

- ⇒ Sélectionnez Démarrer



- ⇒ Paramètres
- ⇒ Mise à jour et sécurité
- ⇒ Sécurité Windows
- ⇒ Protection contre les virus et menaces.

Le moyen le plus sûr pour assurer la sécurité de son appareil est d'installer un anti-virus pour qu'il fasse une analyse régulière du système et des fichiers.

- ⇒ Si l'ordinateur est infecté :
 - Ouvrez l'anti-virus et lancez une analyse complète
 - Supprimez ou mettez en quarantaine les virus détectés
 - Redémarrez l'ordinateur
 - Modifiez tous vos mots de passe
 - Mise à jour du système d'exploitation, des logiciels et de votre navigateur.

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

- ⇒ Téléchargez et installez un antivirus avec antimalware fiable
- ⇒ Effectuez une analyse complète
- ⇒ Examinez les menaces découvertes et les actions recommandées
- ⇒ Configurer les paramètres pour que l'anti-virus fasse des analyses de système de façon régulière et qu'il s'exécute en arrière-plan.