christianrazafiarivelo@gmail.com

Parcours : DISCOVERY

Module : Naviguer en toute sécurité

Projet 1 – Un peu plus de sécurité, on 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, je consulte trois articles qui parlent de sécurité sur internet.

Voici les articles que j'ai consulté (avec les mots-clés "sécurité sur internet"et "comment être en sécurité sur internet" :

Article 1 = wikiHow - Comment surfez en sécurité sur internet

Article 2 = Economie.gouv - Comment assurer votre sécurité numérique

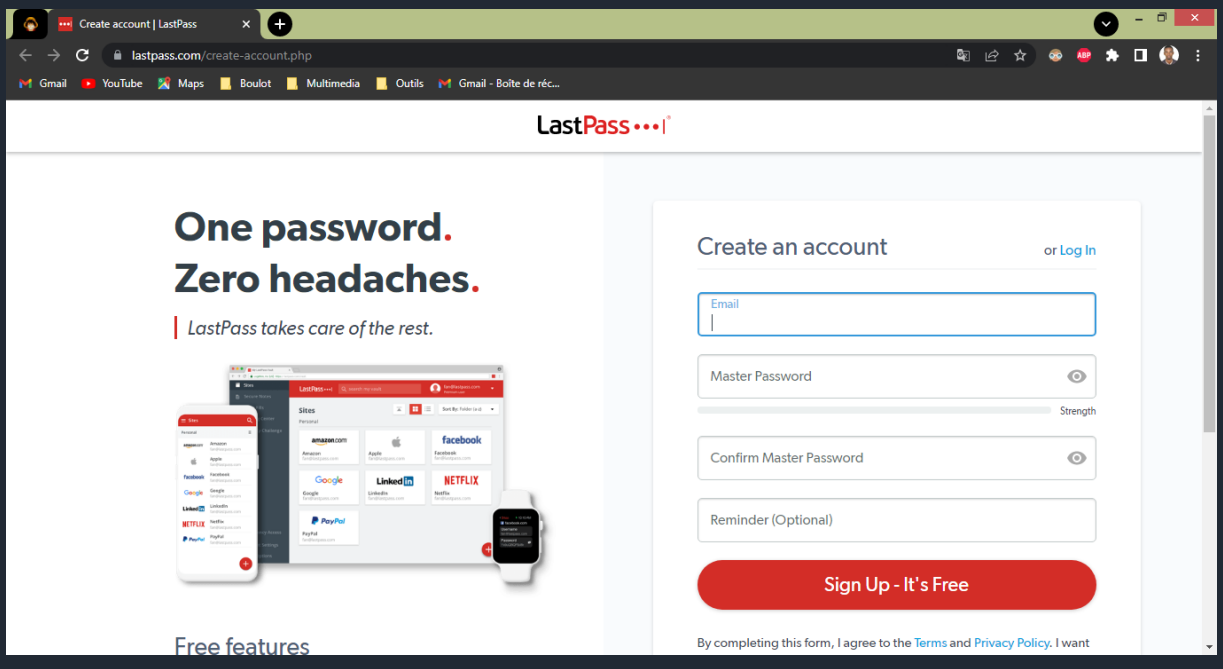
Article 3 = Site W - Naviguez en toute sécurité sur Internet

2 - Créer des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass

1/ Utiliser gestionnaire de mot de passe nommé LastPass.

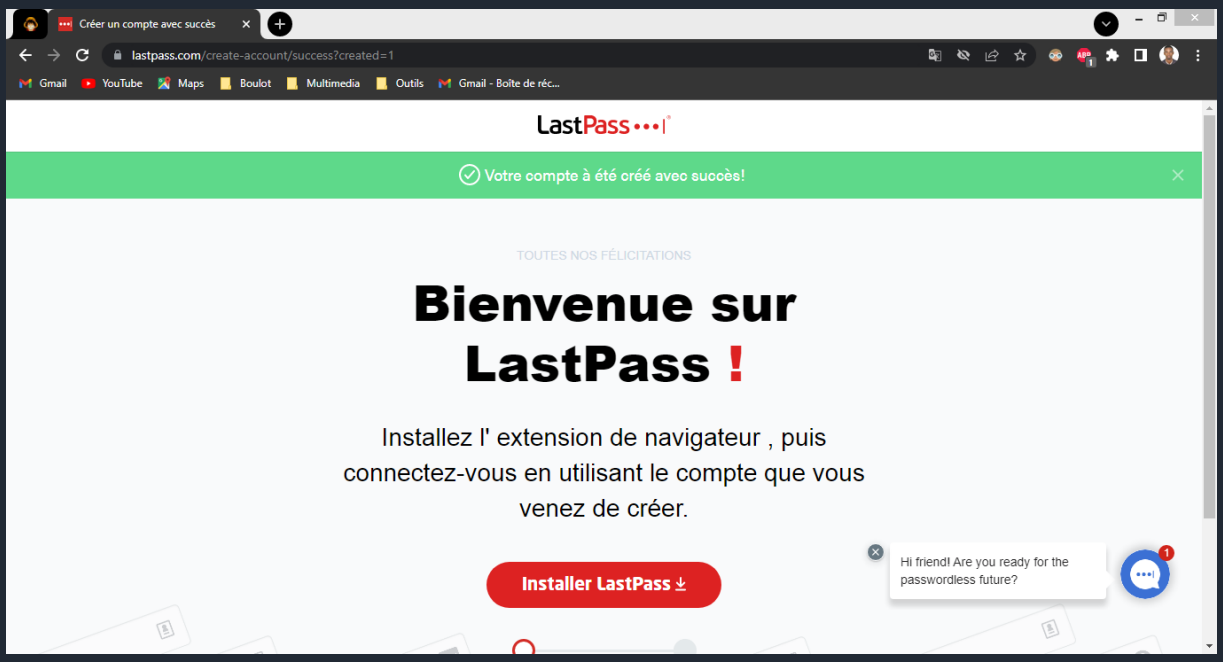
- Naviguer sur le site de LastPass

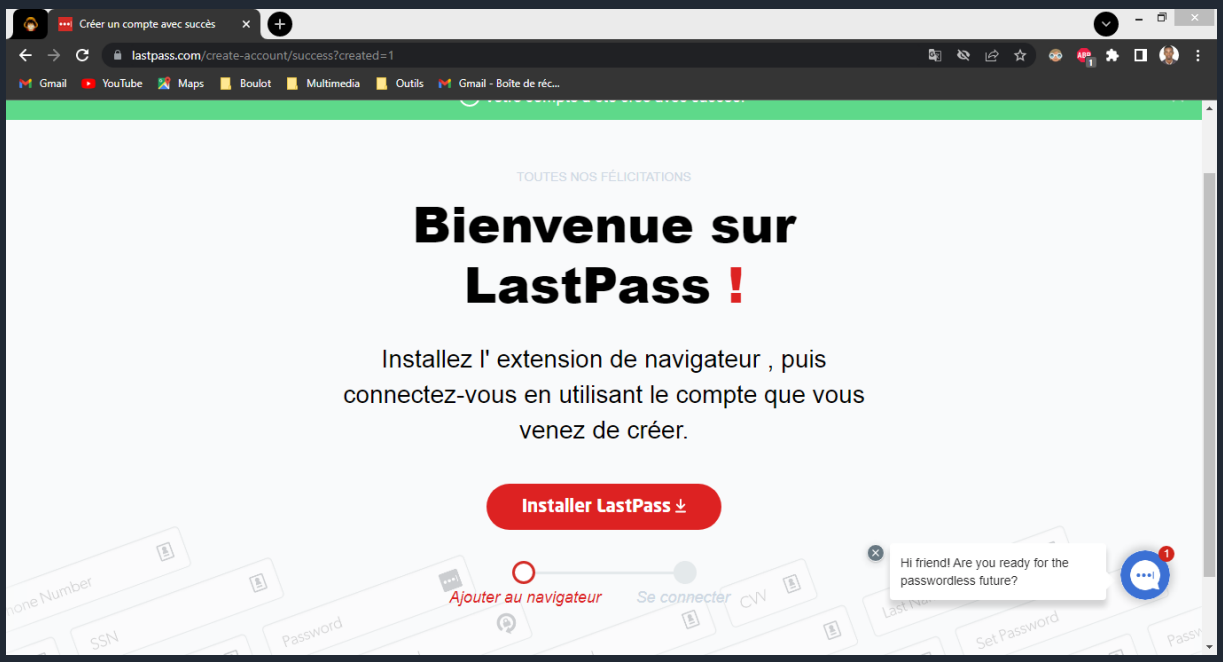


christianrazafiarivelo@gmail.com

- Création de compte :

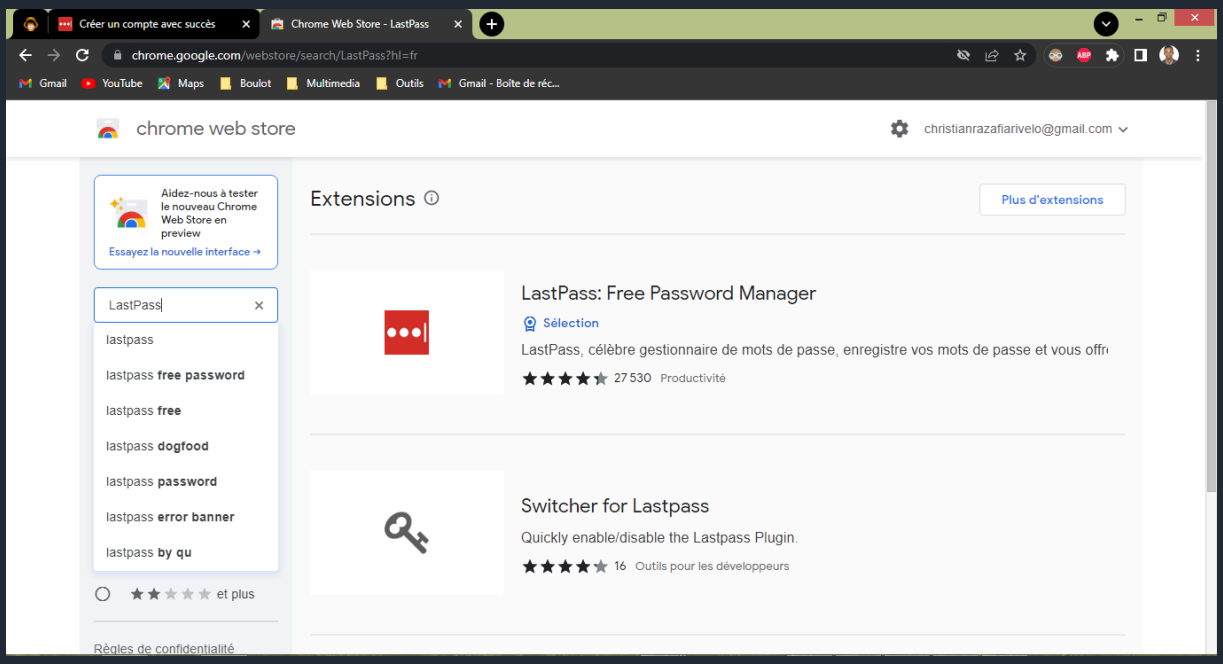
Compte crée avec succès ☺

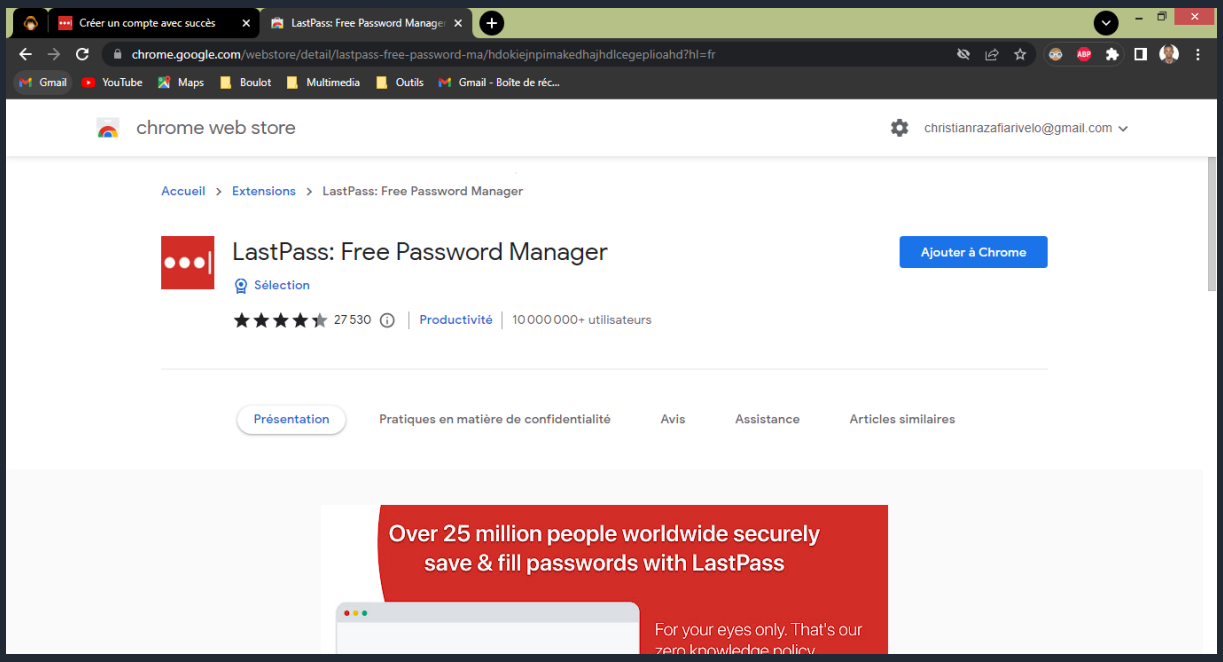




Valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome" :

christianrazafiarivelo@gmail.com

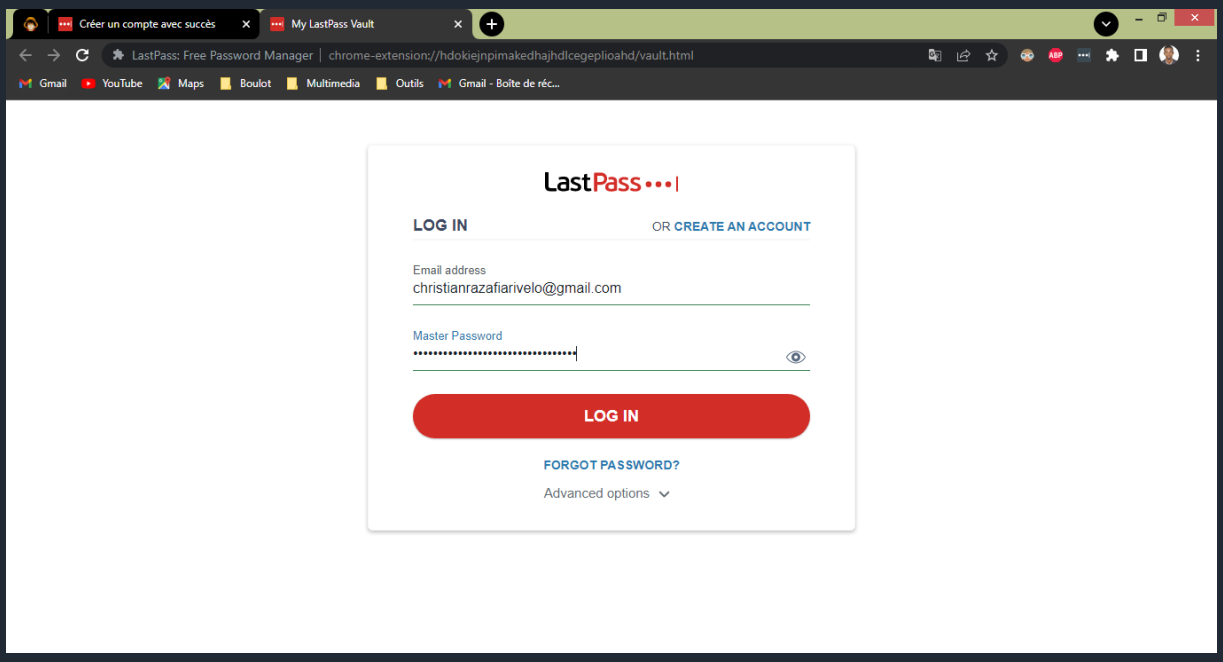


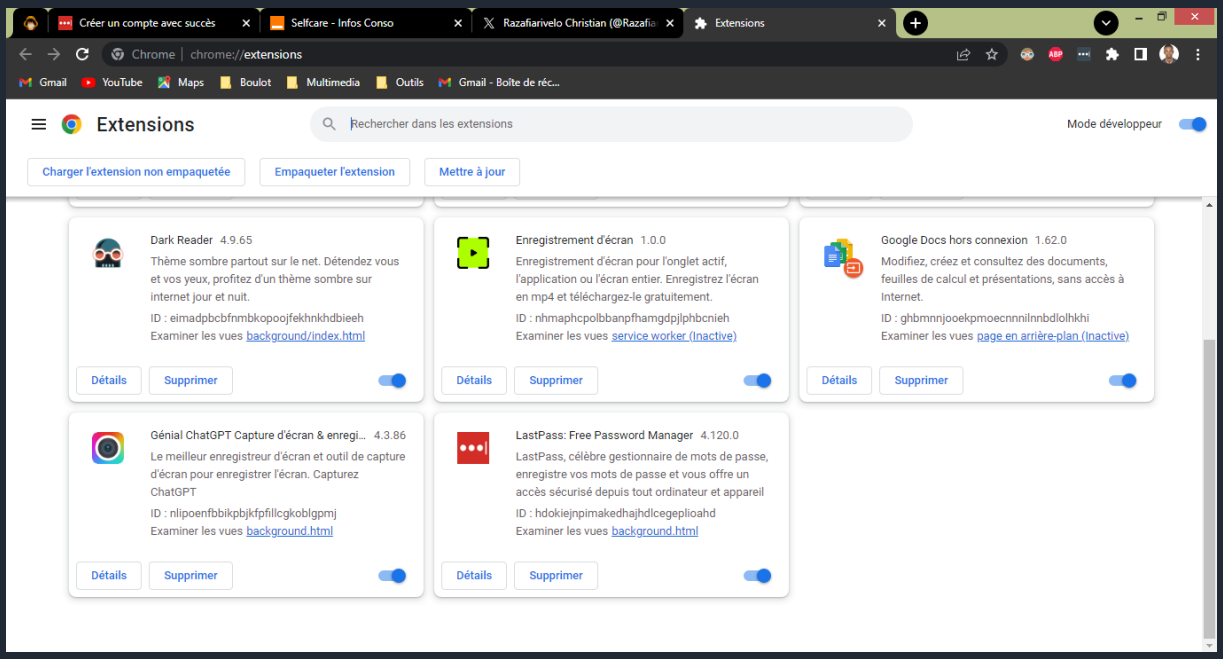


Désormais, lorsque tu te connectes à tes comptes, tu peux enregistrer le mot de passe grâce à LastPass.

L’extension est installer, je vais maintenant connecter à LastPass pour pouvoir beneficier du service.

christianrazafiarivelo@gmail.com





Je suis maintenant connecté, je peux alors bénéficier du service :

Désormais, lorsque je me connecte à mes comptes, je peux enregistrer le mot de passe grâce à LastPass.

3 - Fonctionnalité de sécurité de votre navigateur

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

1/ Les adresses internet qui me semblent provenir de sites web 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

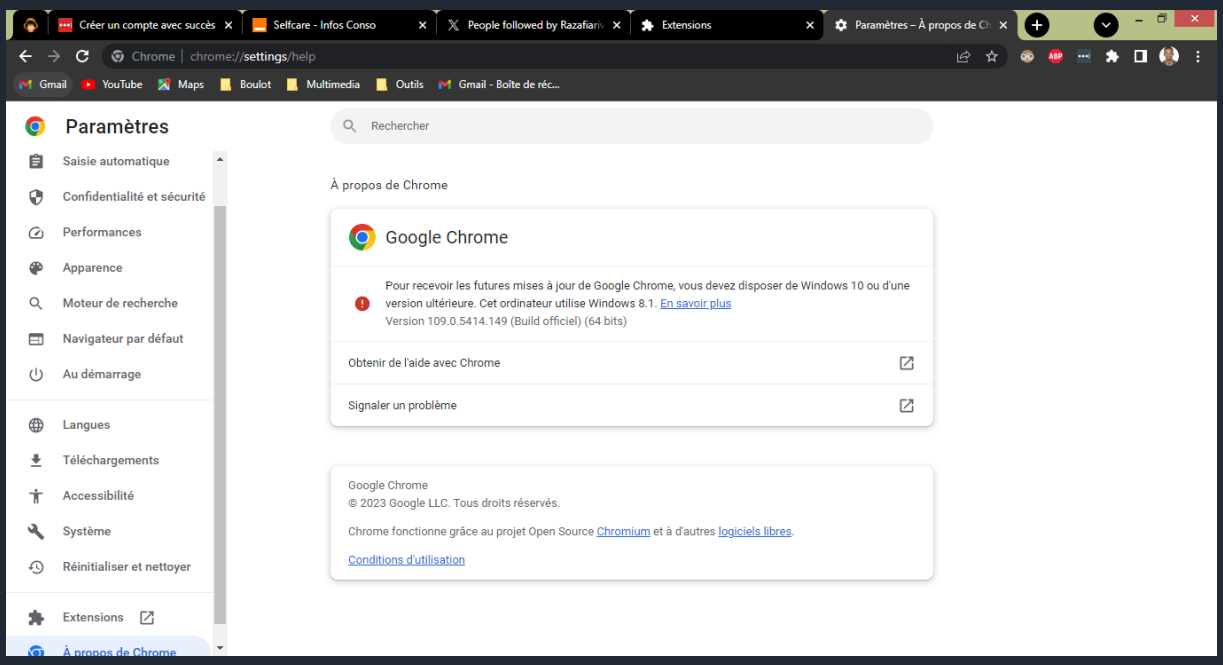
Les seuls sites qui semblaient être cohérents sont donc :

- 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/ Vérifier si les navigateurs utilisés, Chrome et Firefox, sont à jour :

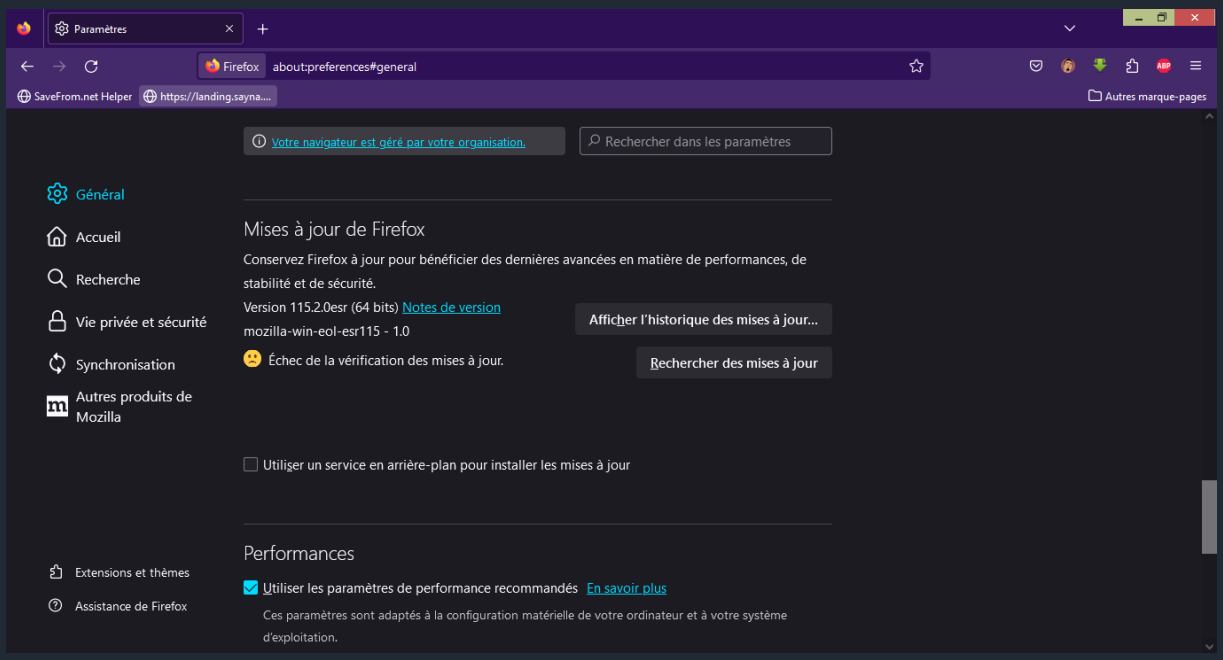
Pour Chrome :

Mon ordinateur utilise le système windows 8.1, donc ne peut pas recevoir les mises à jours de chrome. Voir figures ci-après :



Pour Firefox :

christianrazafiarivelo@gmail.com



D'après la figure ci-dessus, mon navigateur Firefox est maintenant sur la version 115.2.0esr (64 bit) qui est la version du 30 Août 2023. Vous voyez aussi qu'il y a eu Echec de la vérification des mises à jours, cela est à cause de ma connexion actuel qui très faible (J'ai déjà donnée ma vitesse de connexion dans le projet comment internet fonctionne).

4 - Éviter le spam et le phishing

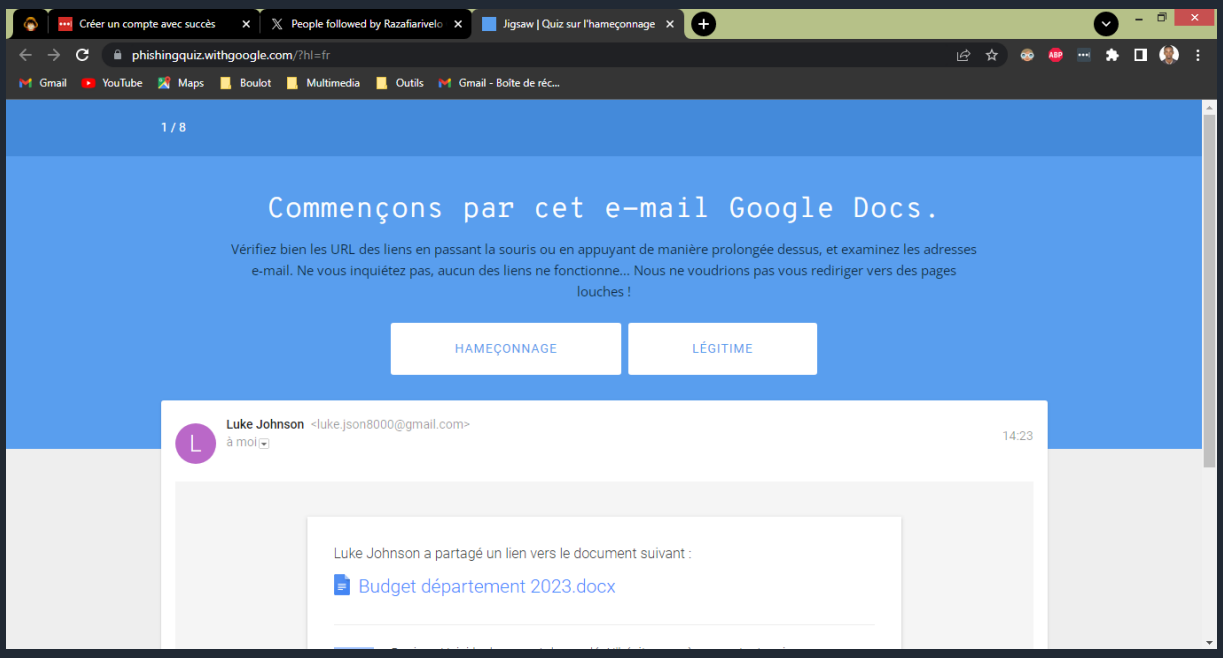
Objectif : Reconnaître plus facilement les messages frauduleux

1/ Déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.

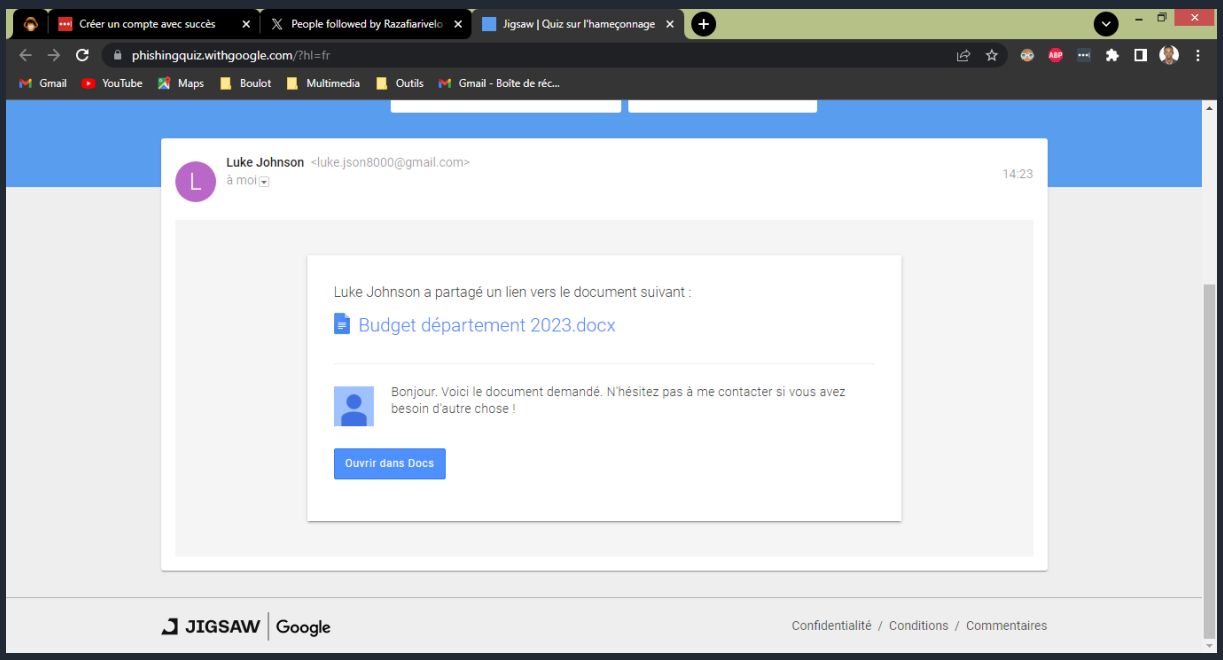
Je vais suivre les étapes dans ce site pour déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.

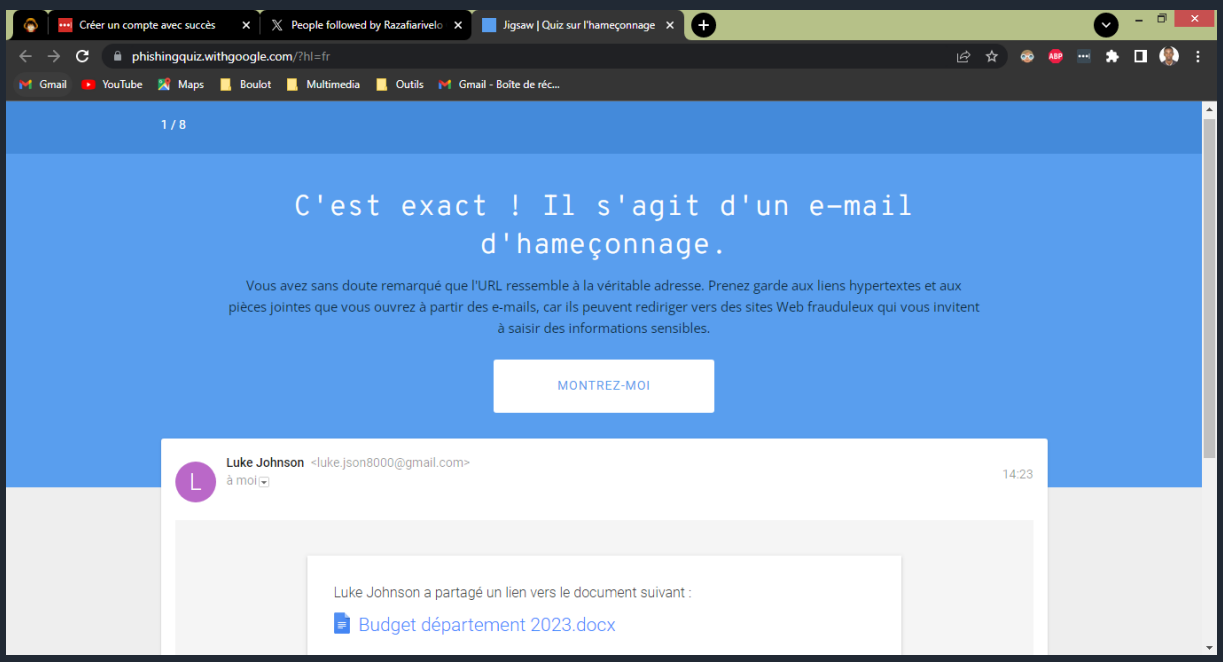
Etape 1 :

christianrazafiarivelo@gmail.com



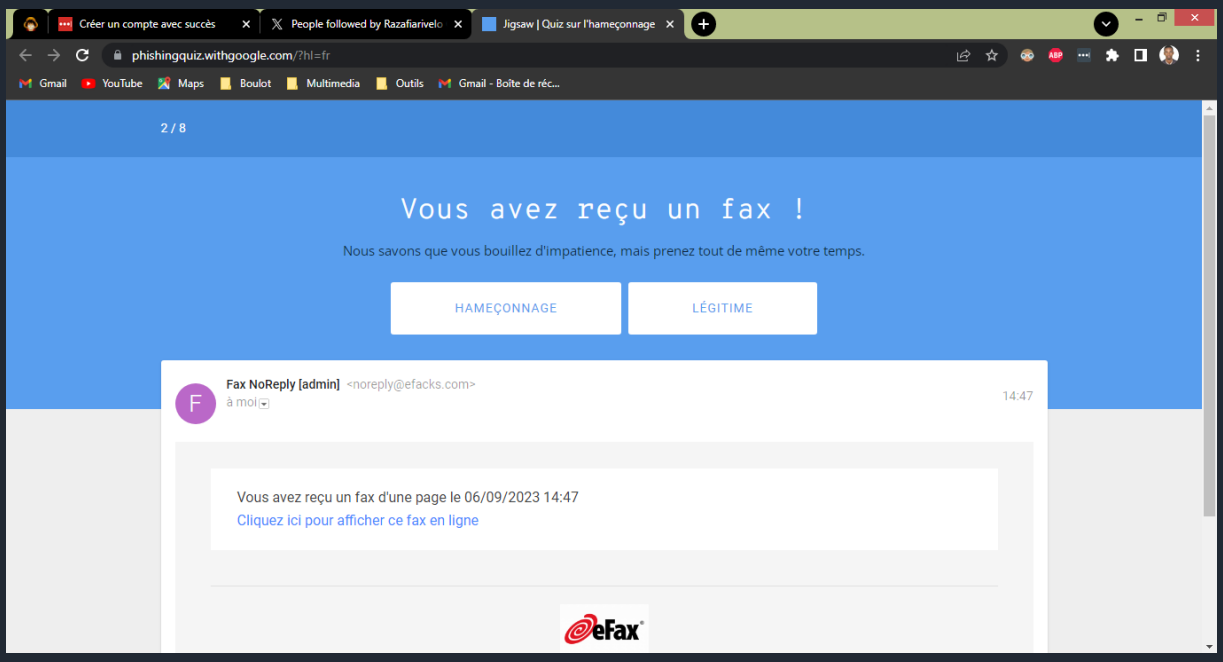
christianrazafiarivelo@gmail.com

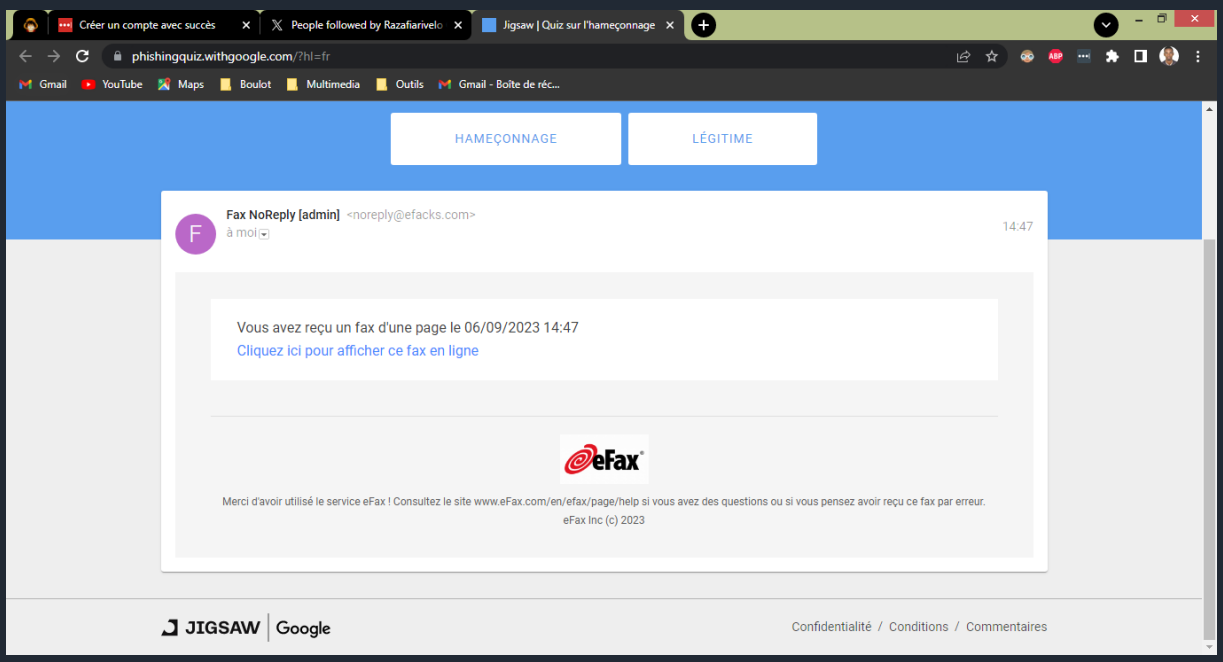




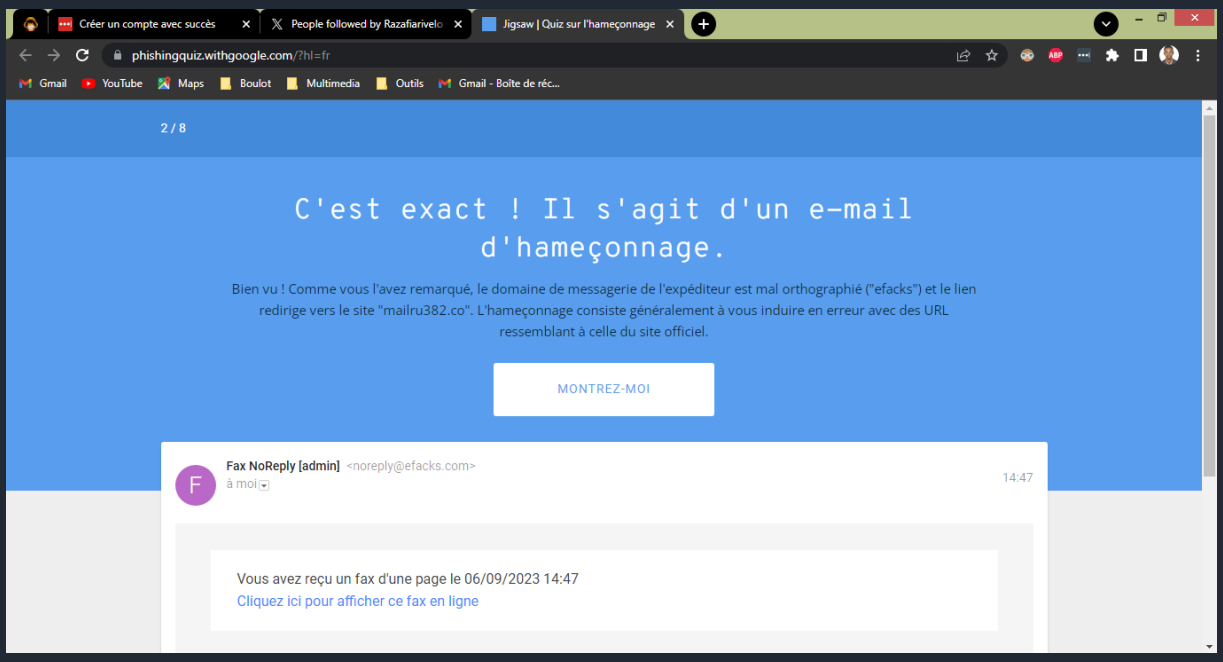
Etape 2 :

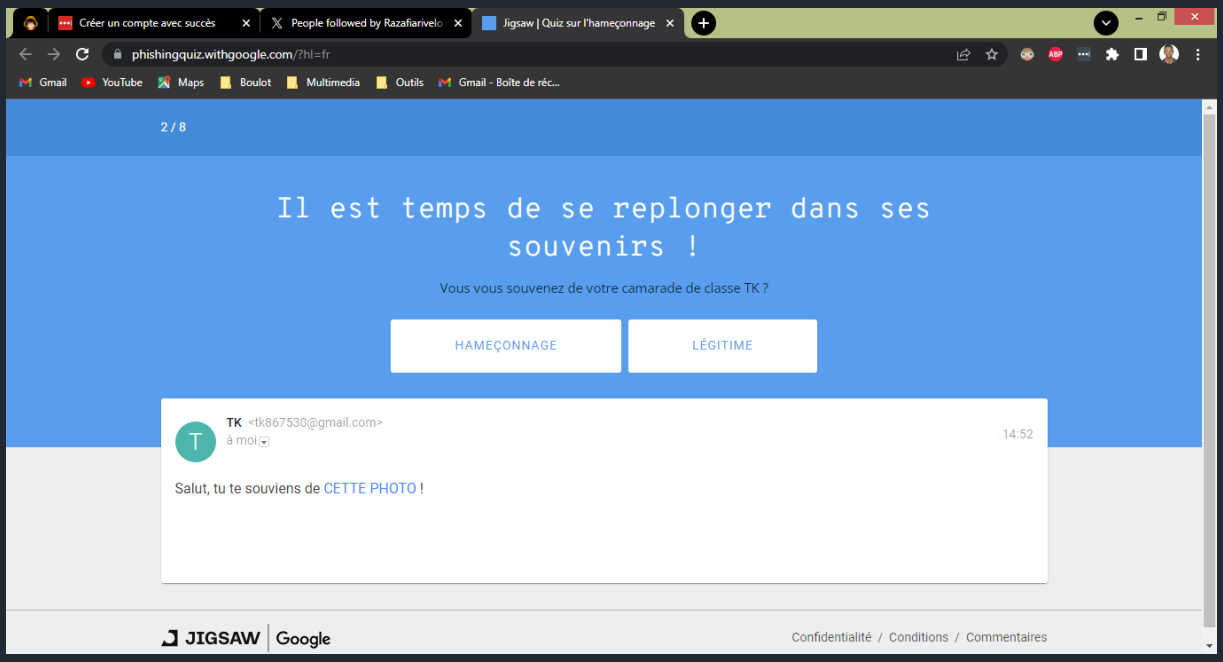
christianrazafiarivelo@gmail.com





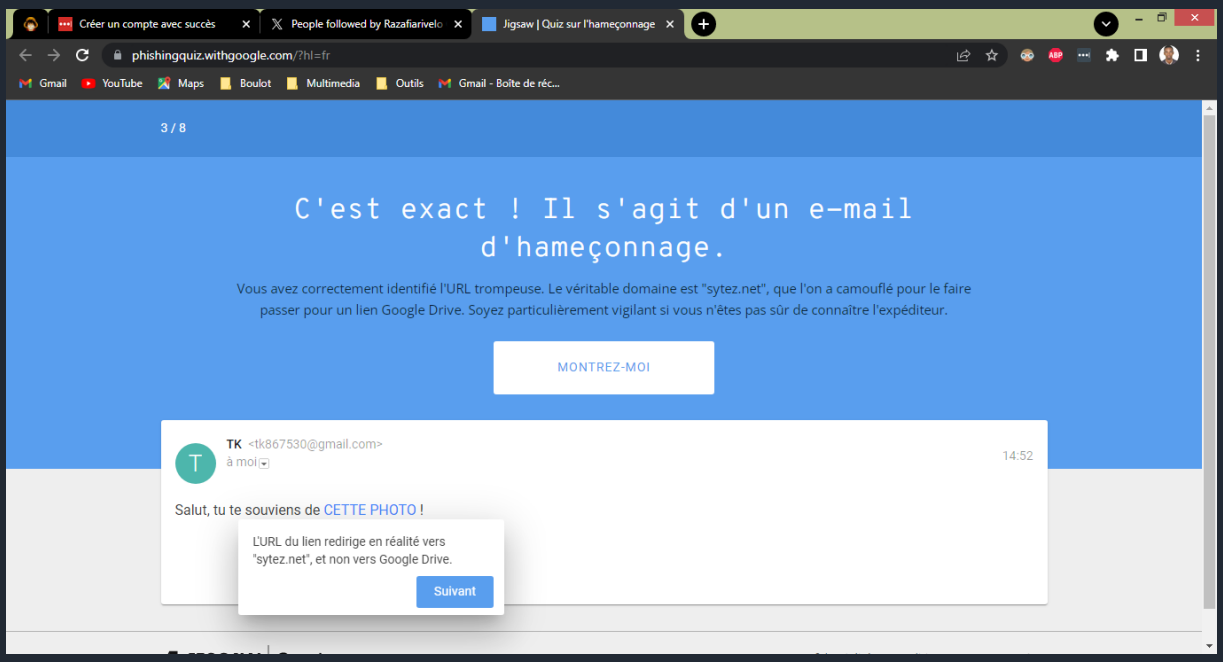
christianrazafiarivelo@gmail.com



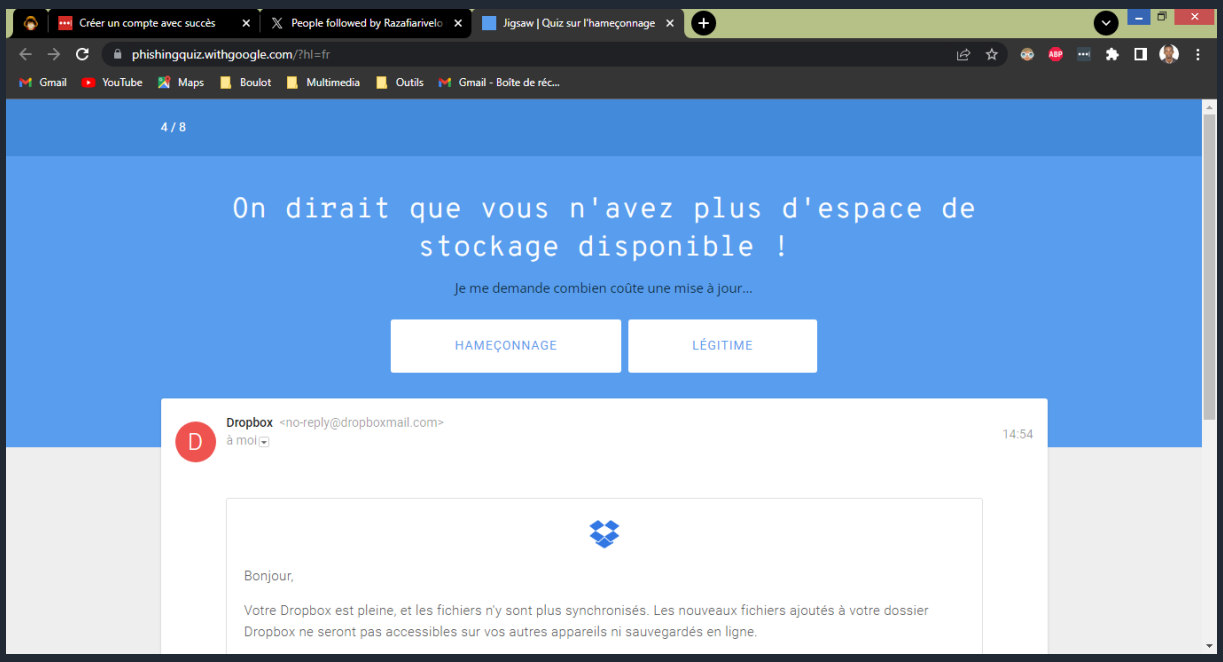


Etape 3 :

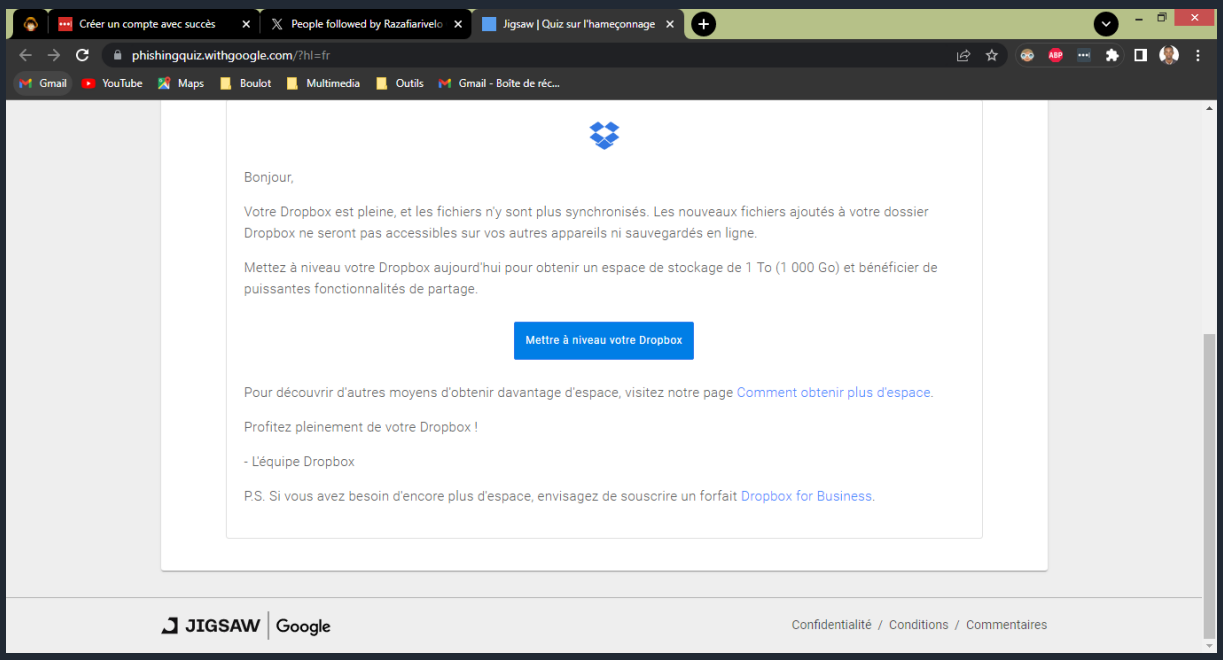
christianrazafiarivelo@gmail.com

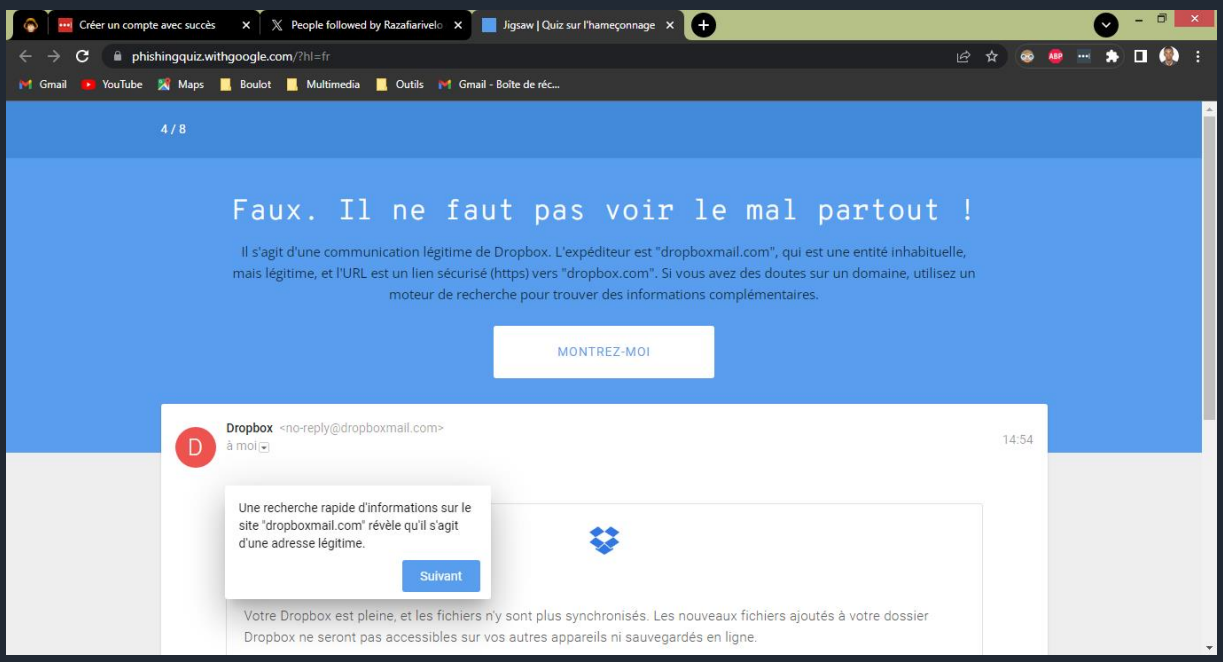


Etape 4 :

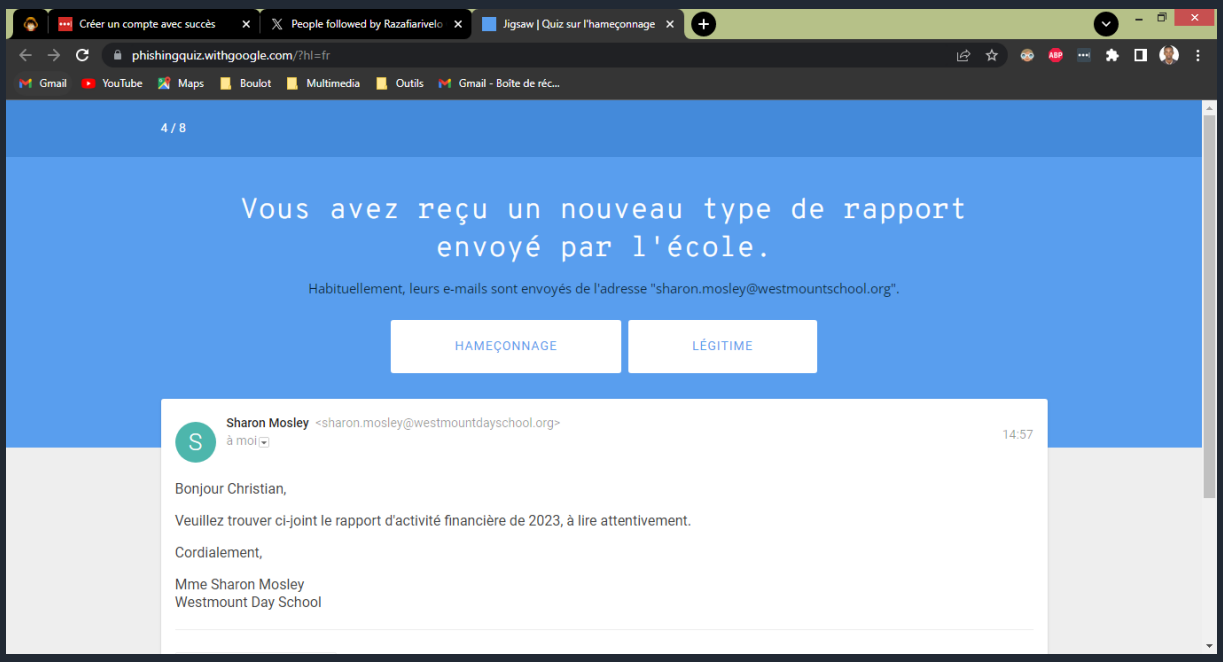


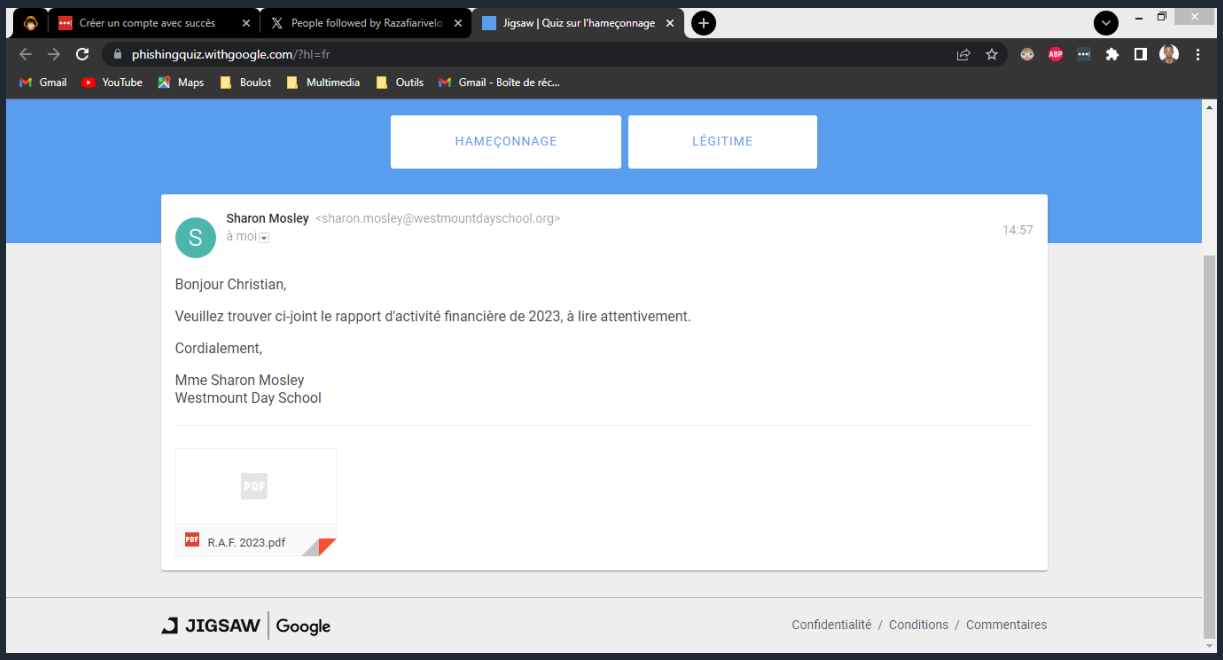
christianrazafiarivelo@gmail.com





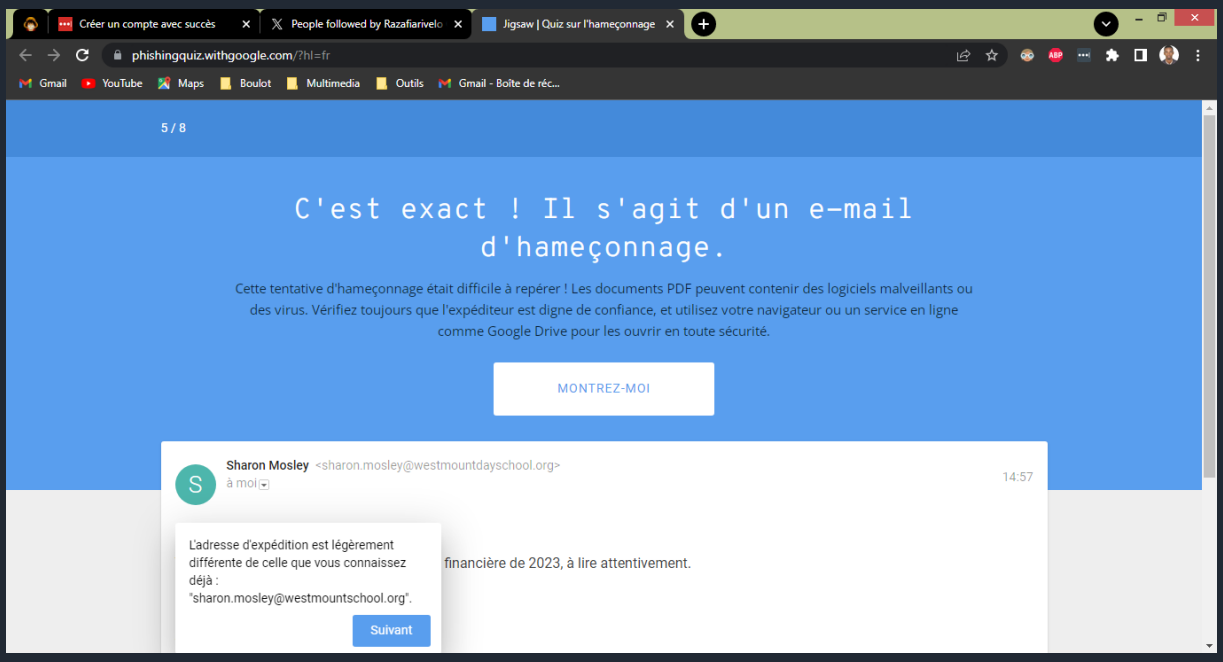
christianrazafiarivelo@gmail.com

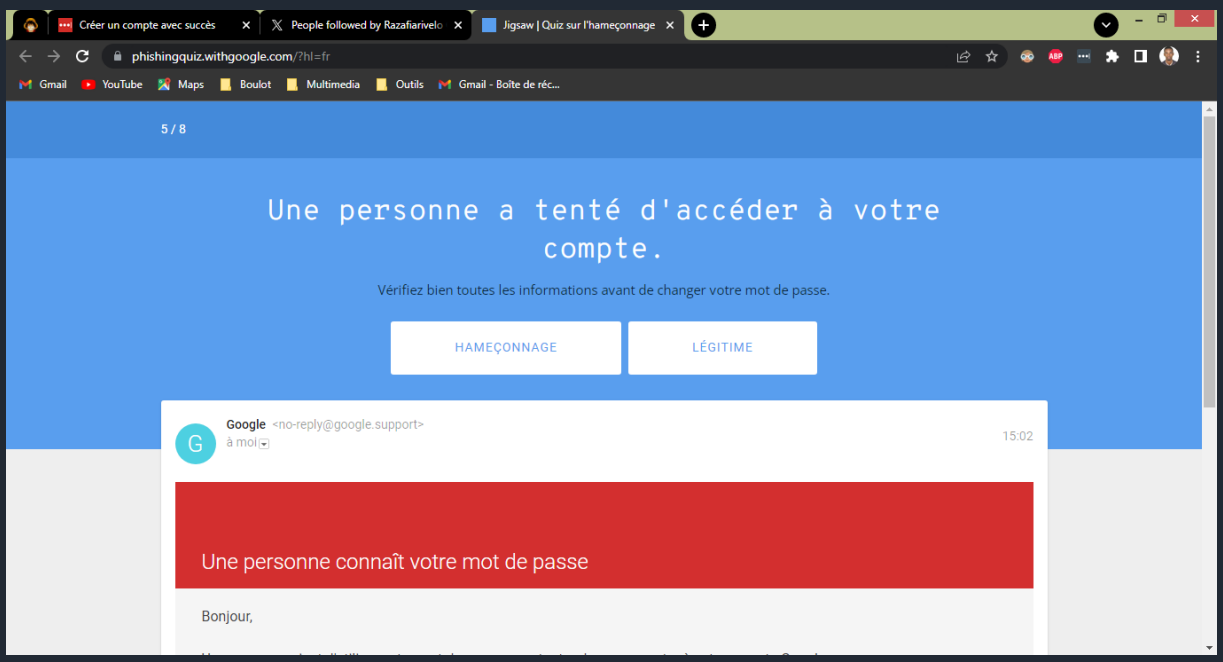




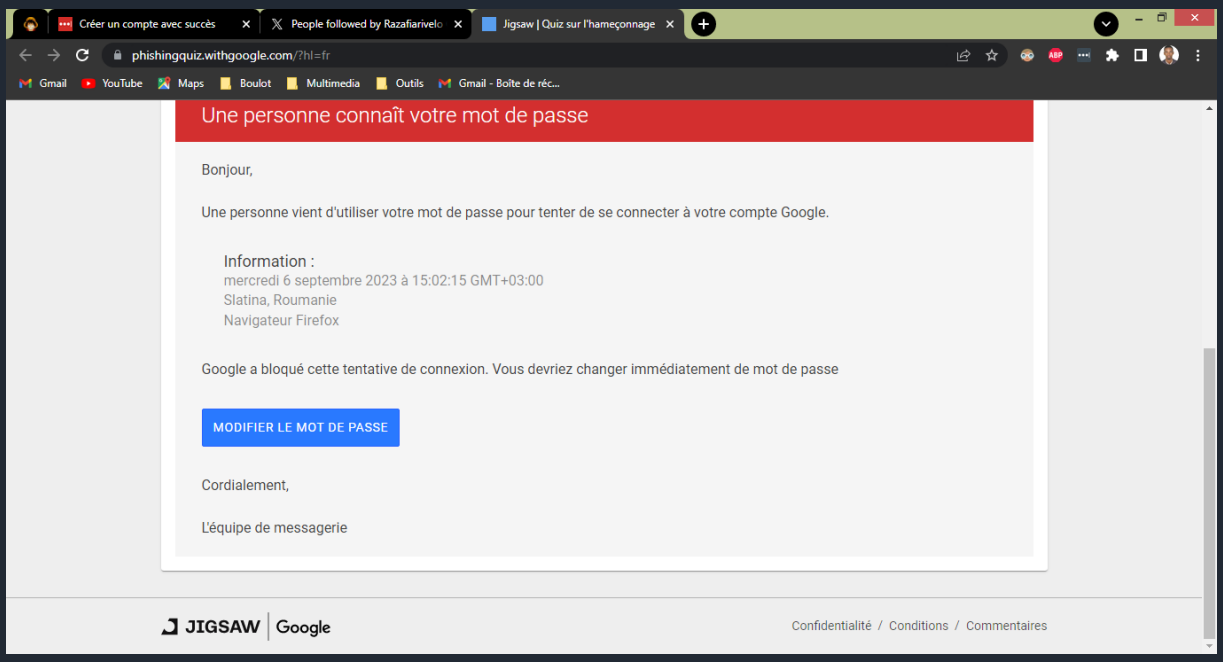
Etape 5 :

christianrazafiarivelo@gmail.com

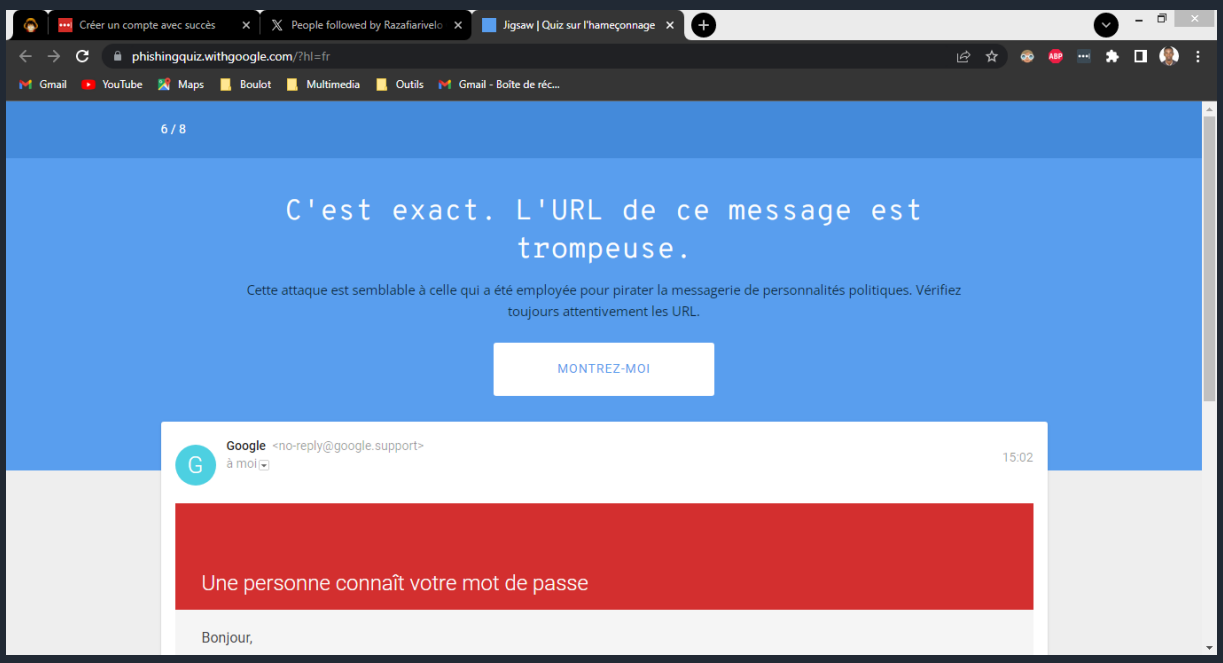




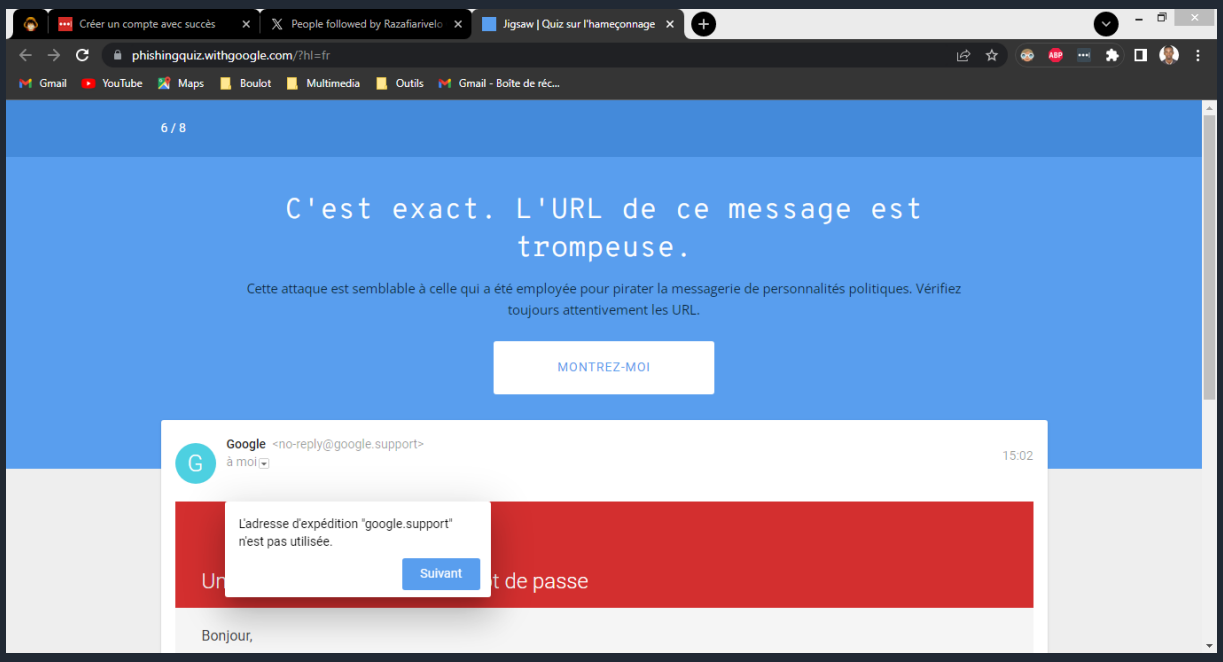
christianrazafiarivelo@gmail.com

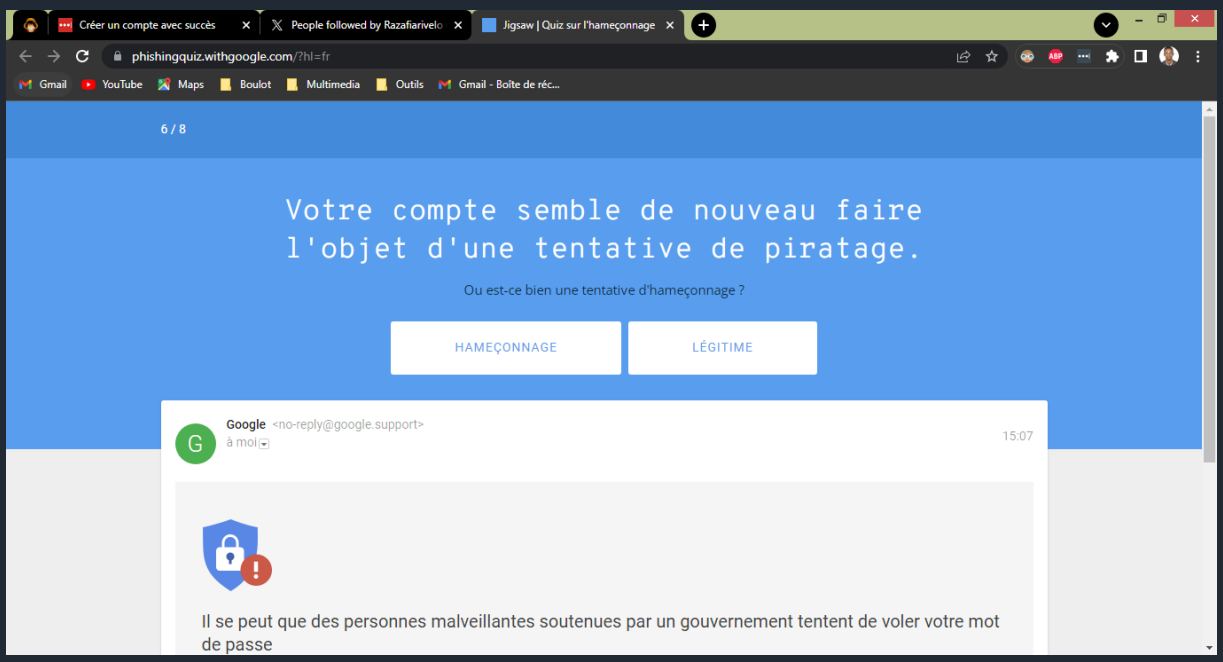


Etape 6 :

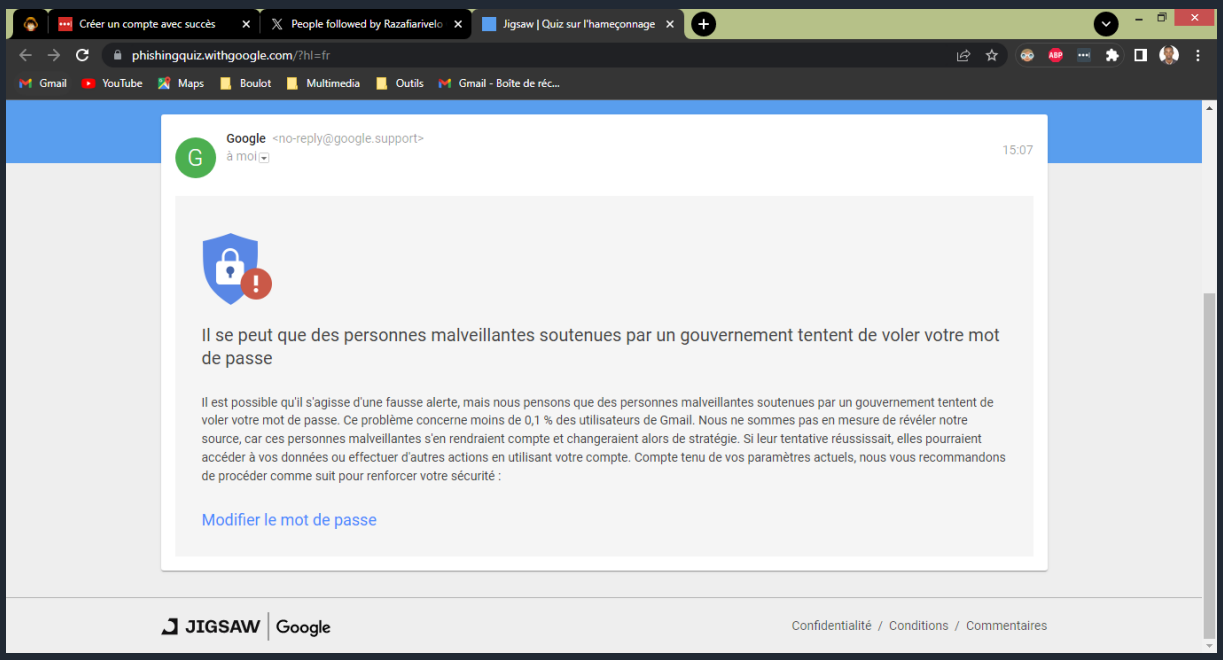


christianrazafiarivelo@gmail.com

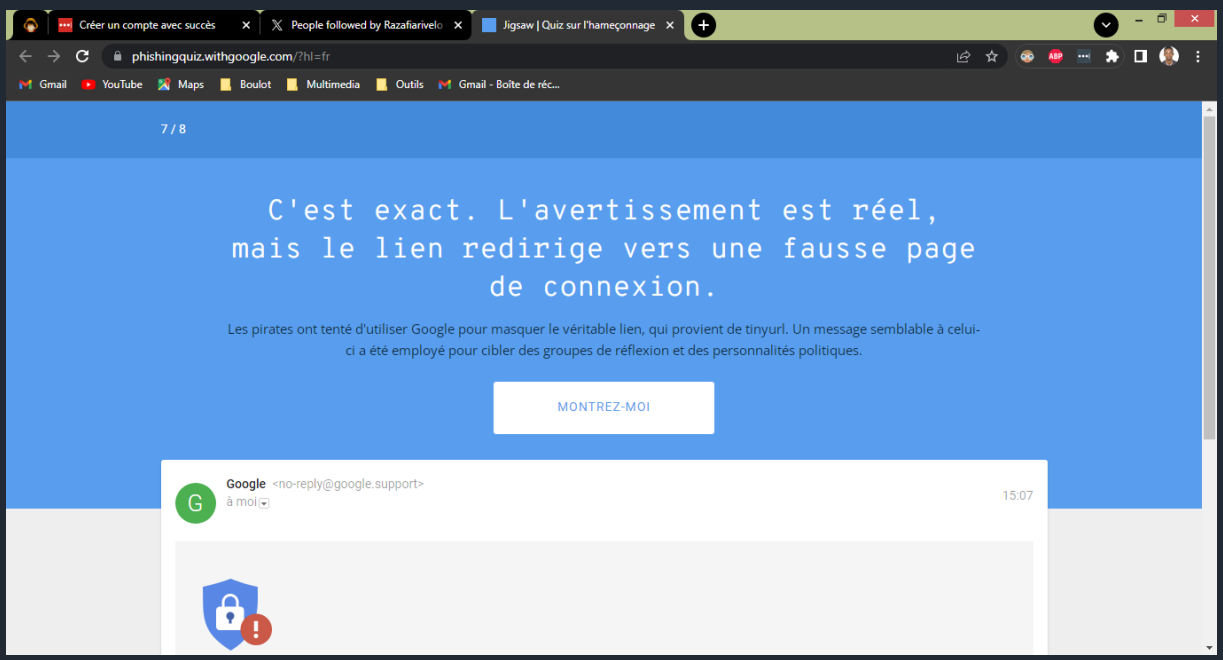




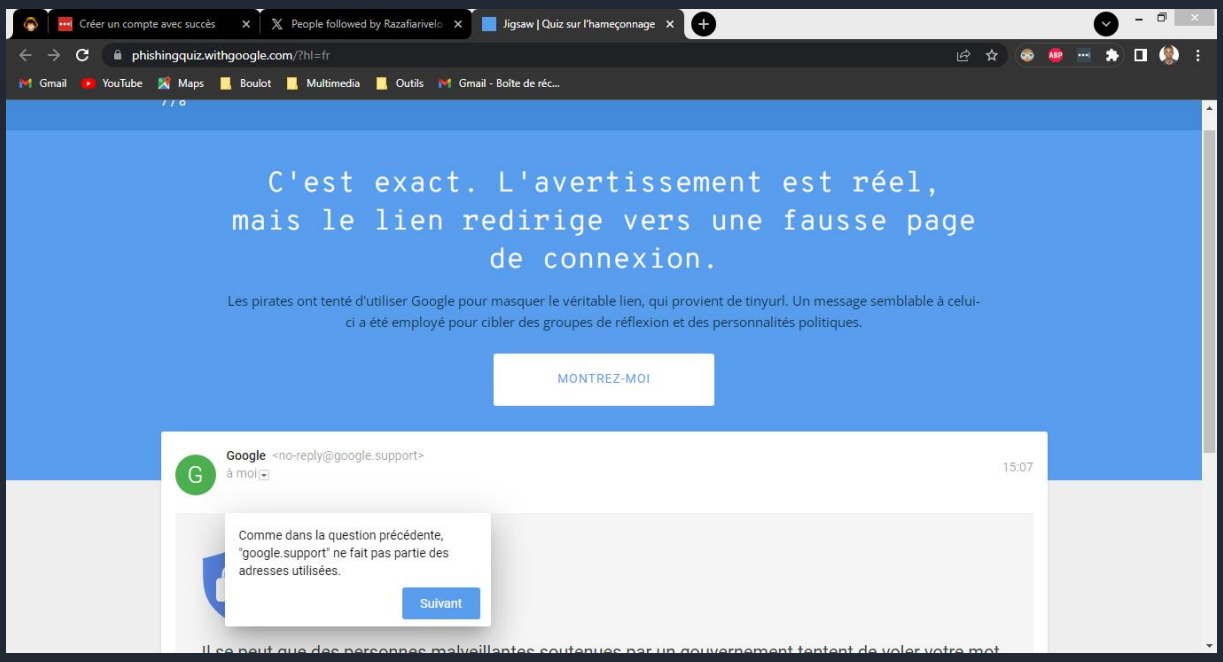
christianrazafiarivelo@gmail.com

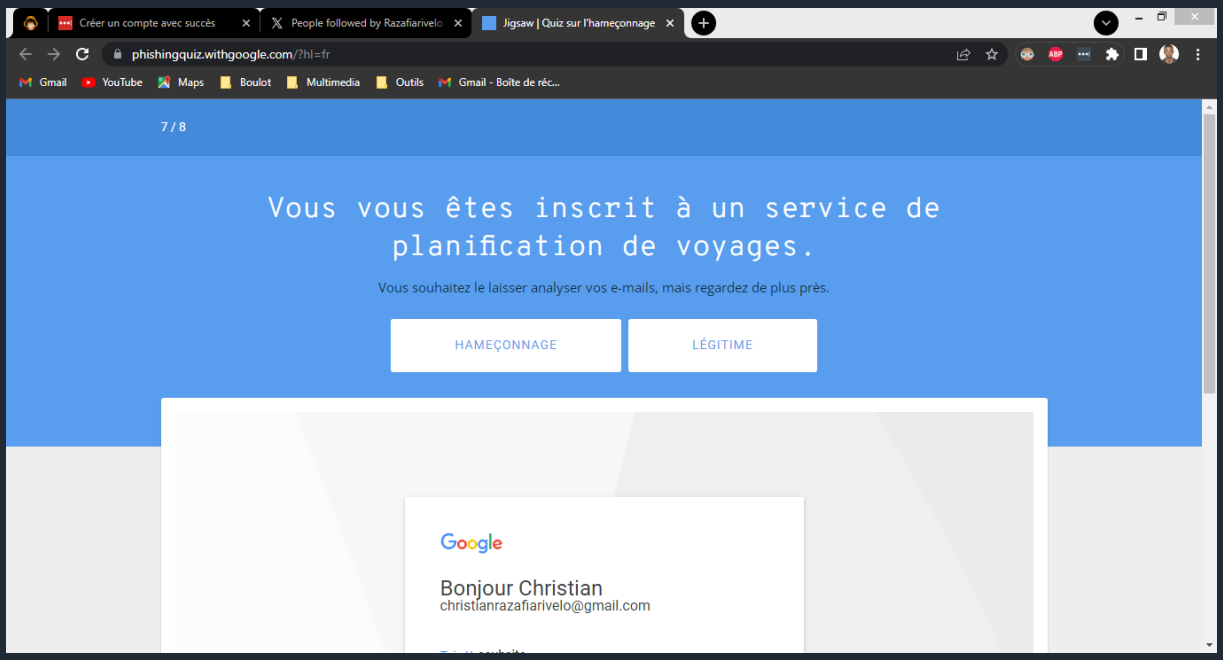


Étape 7 :

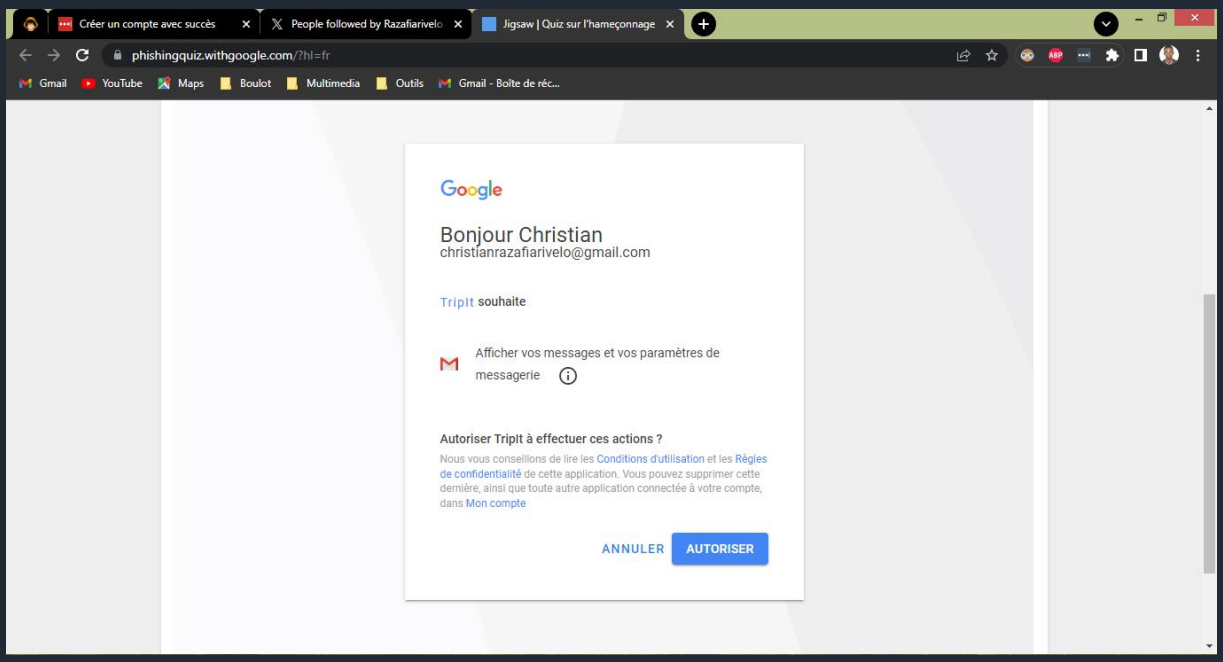


christianrazafiarivelo@gmail.com

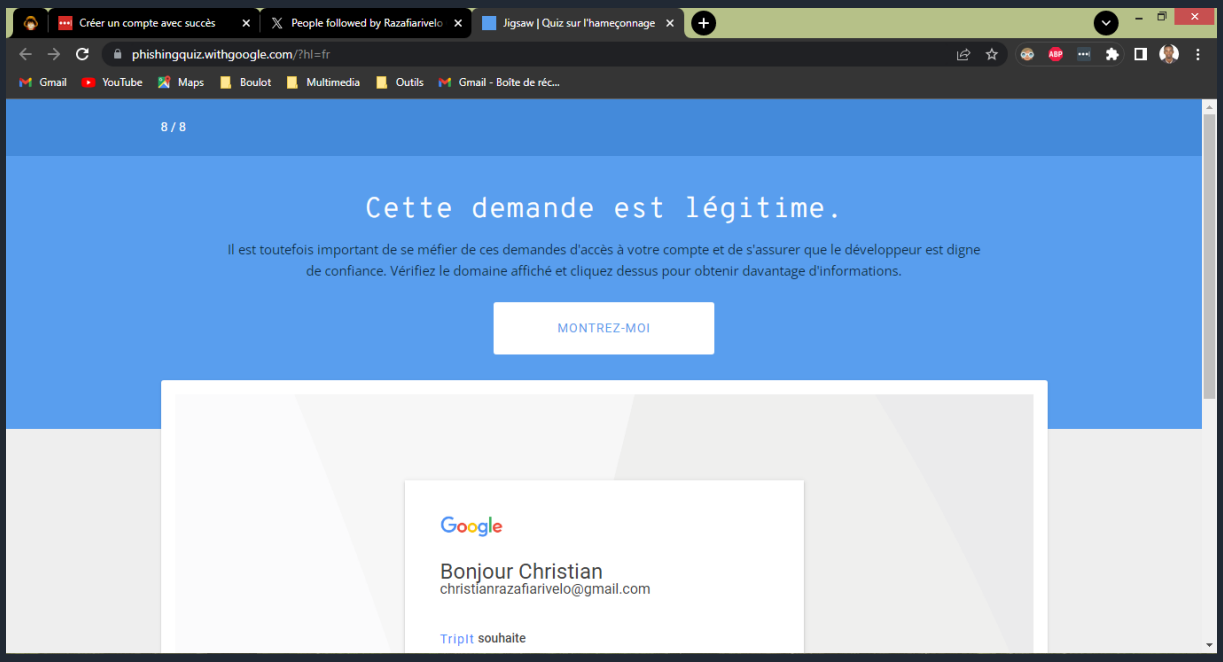




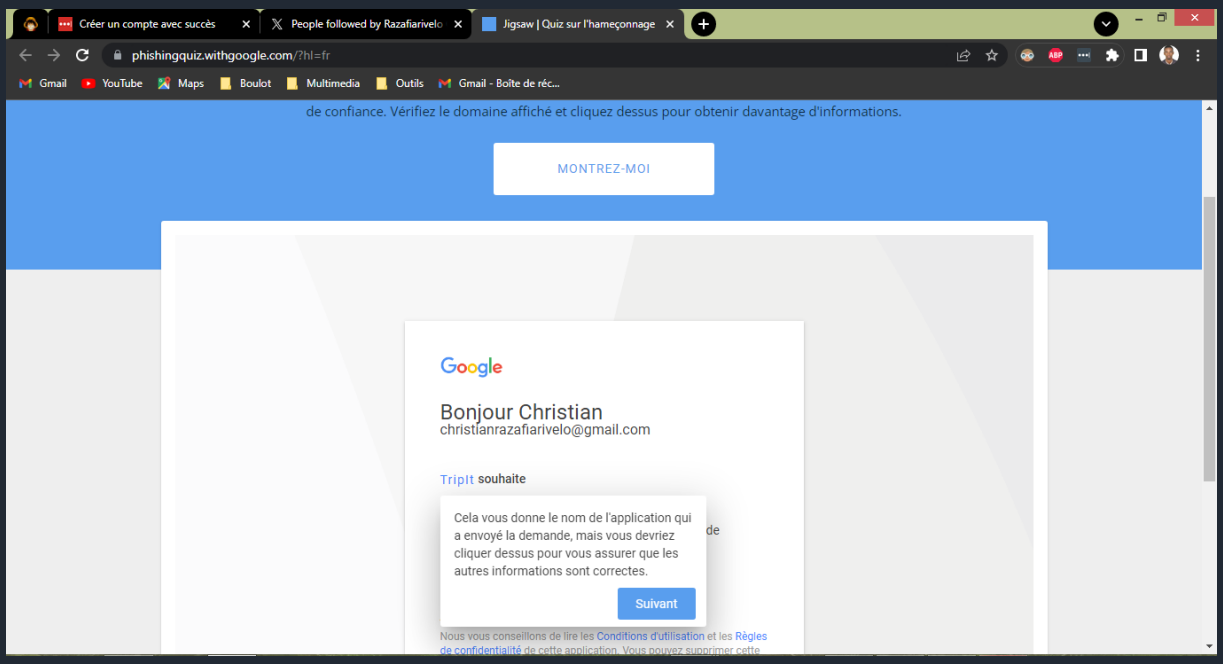
christianrazafiarivelo@gmail.com

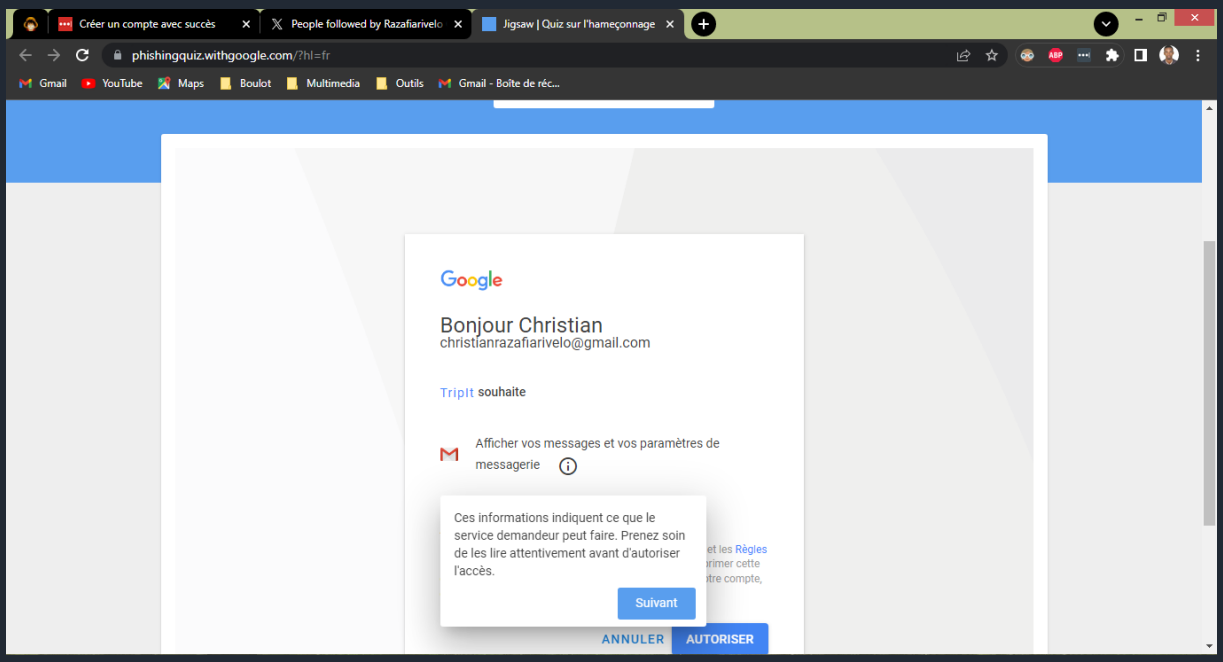


Étape 8 :

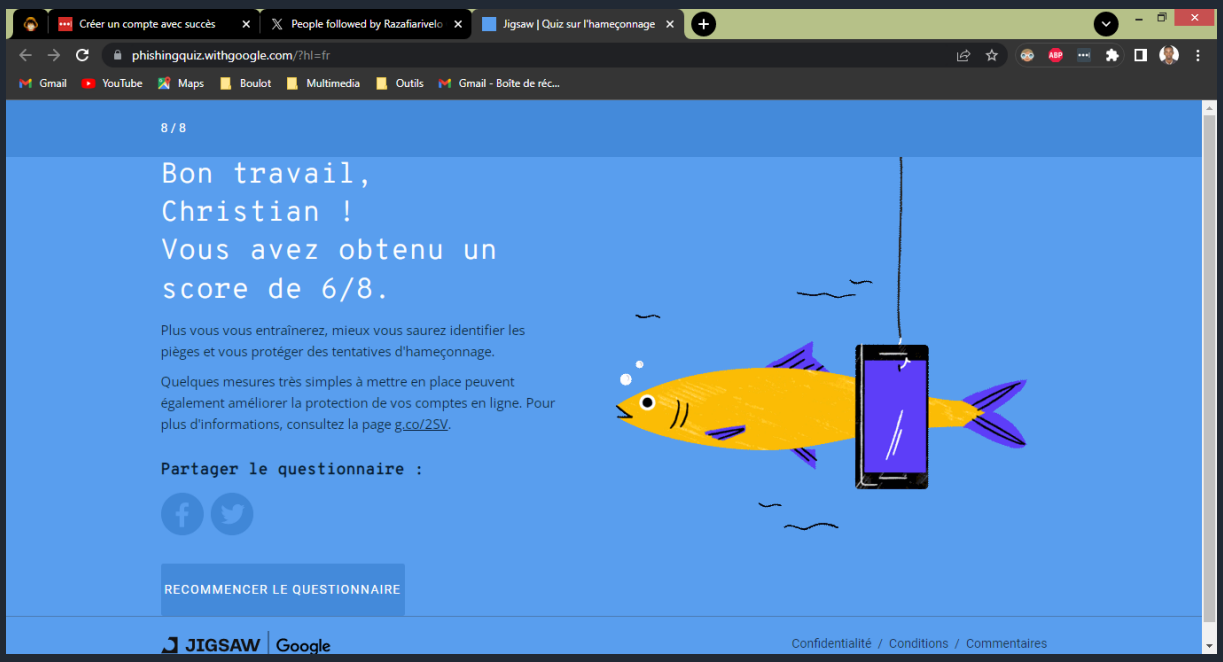


christianrazafiarivelo@gmail.com





christianrazafiarivelo@gmail.com



Voilà, j'ai terminé tous les 8 étapes !!

5 - Comment éviter les logiciels malveillants

Objectif : *sécuriser votre ordinateur et identifier les liens*

3/ Indicateurs de sécurité

- Site n°1
  - **Indicateur de sécurité**
    - ✓ HTTPS
  - **Analyse Google**
    - ✓ Aucun contenu suspect
- Site n°2
  - **Indicateur de sécurité**
    - ✓ Not secure
  - **Analyse Google**
    - ✓ Aucun contenu suspect
- Site n°3
  - **Indicateur de sécurité**
    - ✓ Not secure
  - **Analyse Google**
    - ✓ Vérifier un URL en particulier (analyse trop générale)

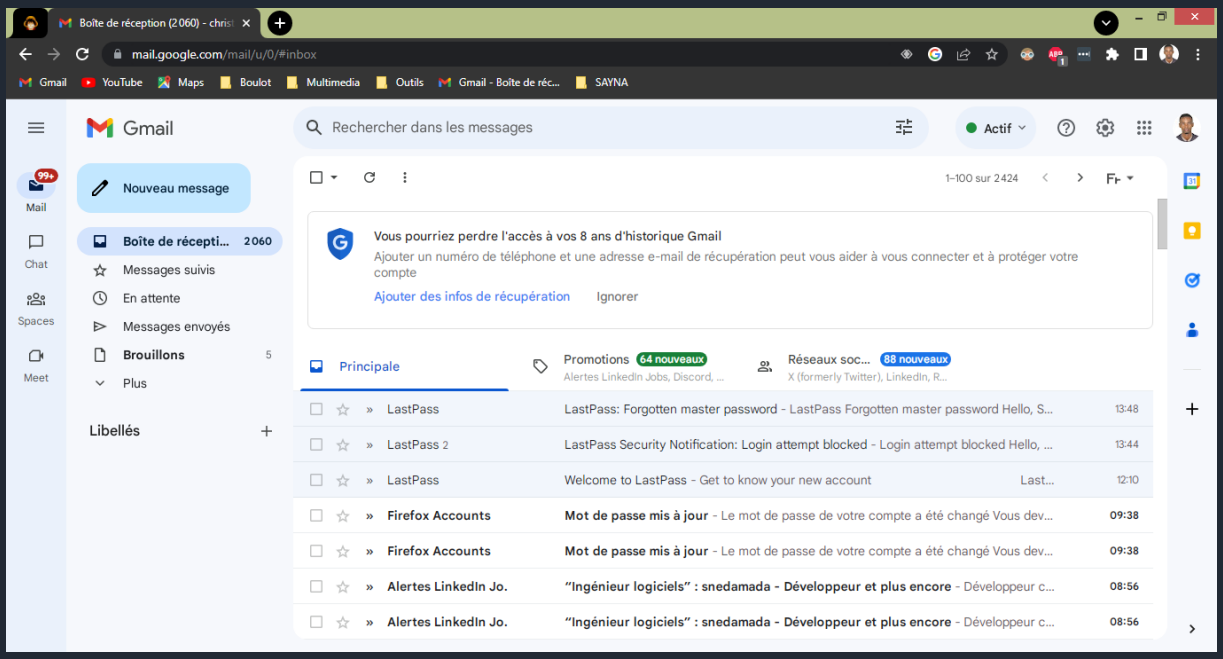
christianrazafiarivelo@gmail.com

6 - Achat en ligne

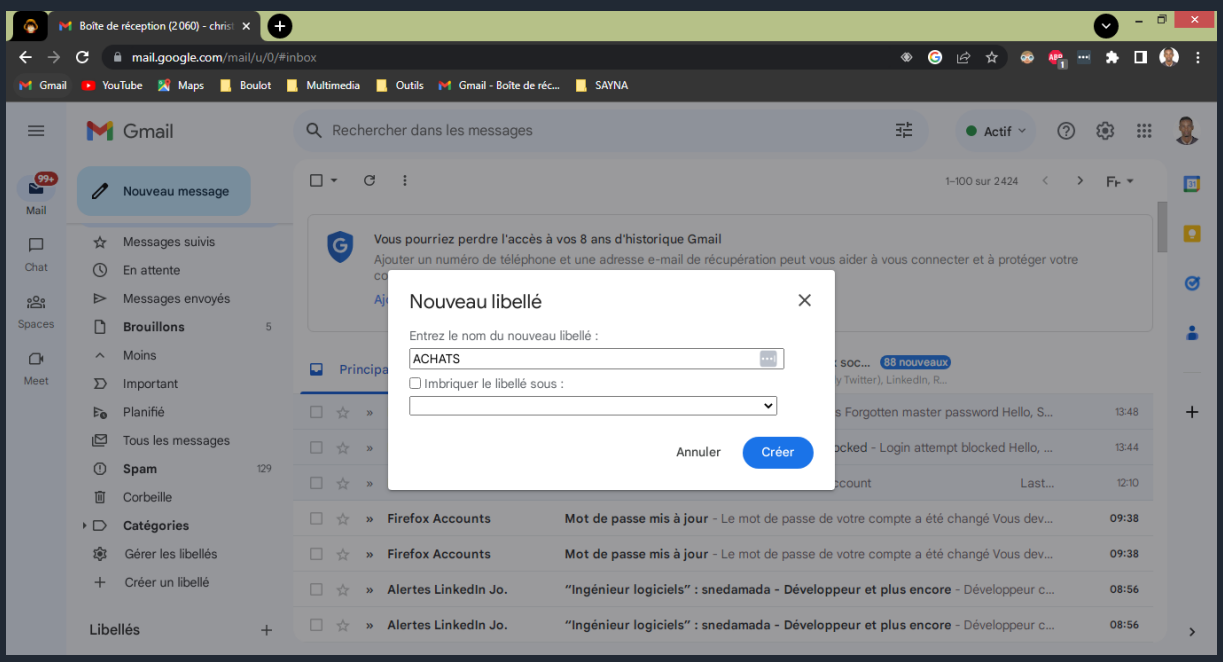
Objectif : créer un registre des achats effectués sur internet

1/ Crée un registre des achats

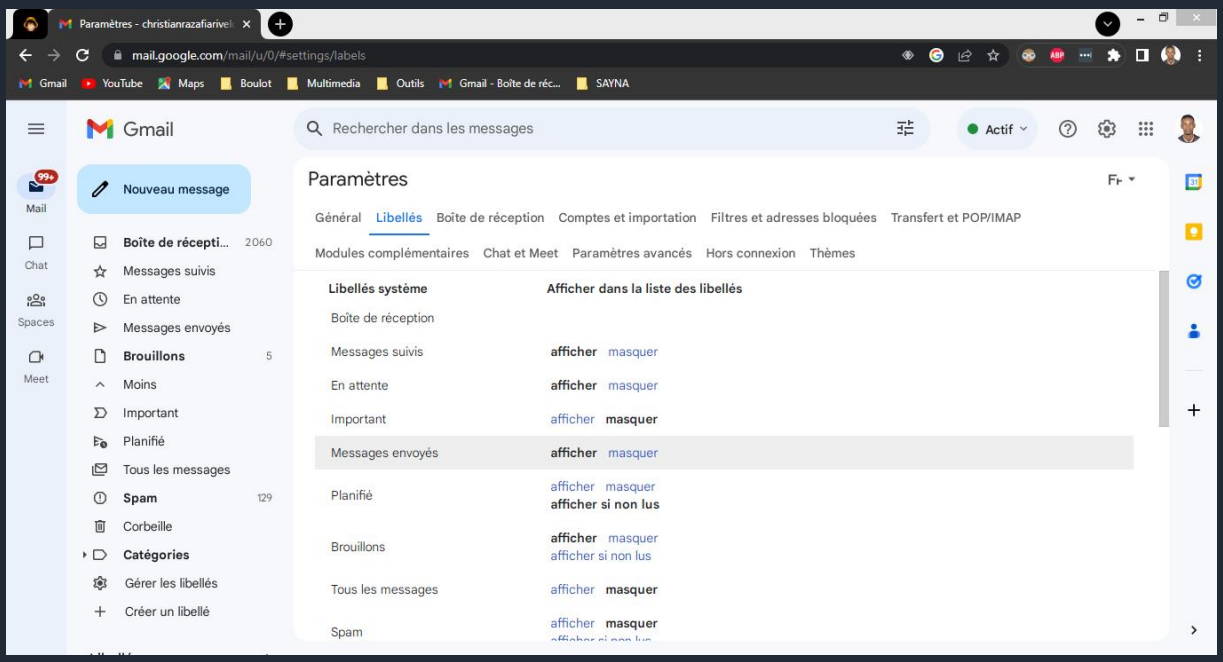
Pour commencer, accède à ma messagerie électronique.

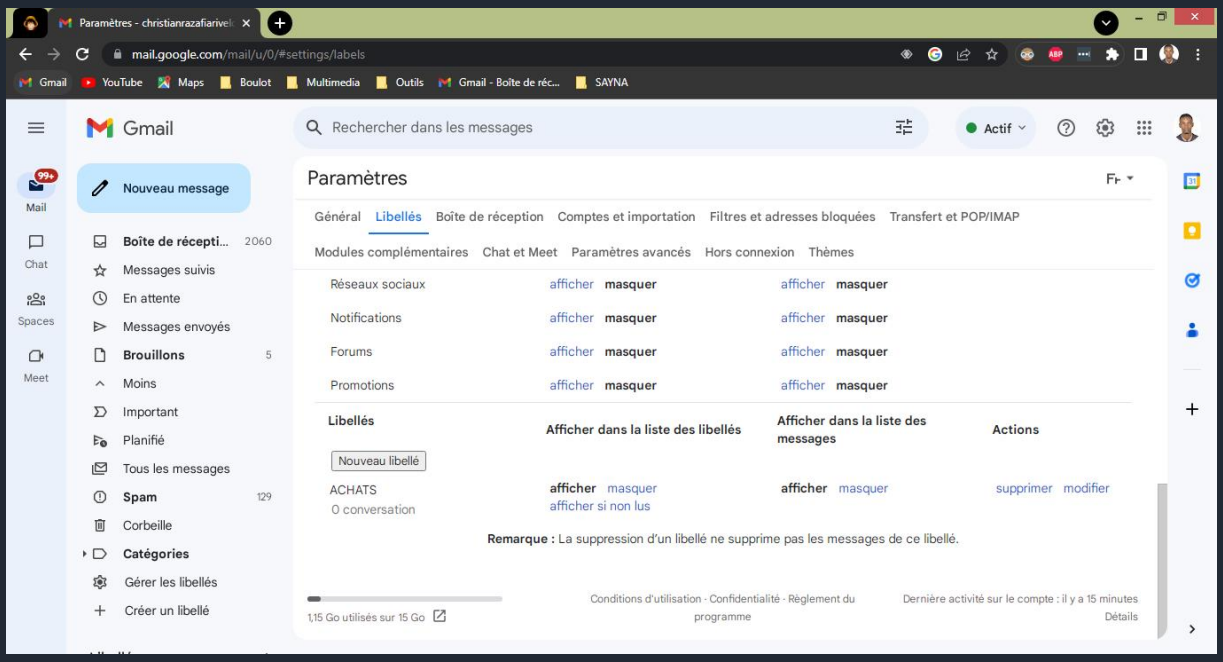


Je vais maintenant créer ma rubrique des achats. Je nomme ma libellé « ACHATS » :



christianrazafiarivelo@gmail.com





J'ai 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.

christianrazafiarivelo@gmail.com

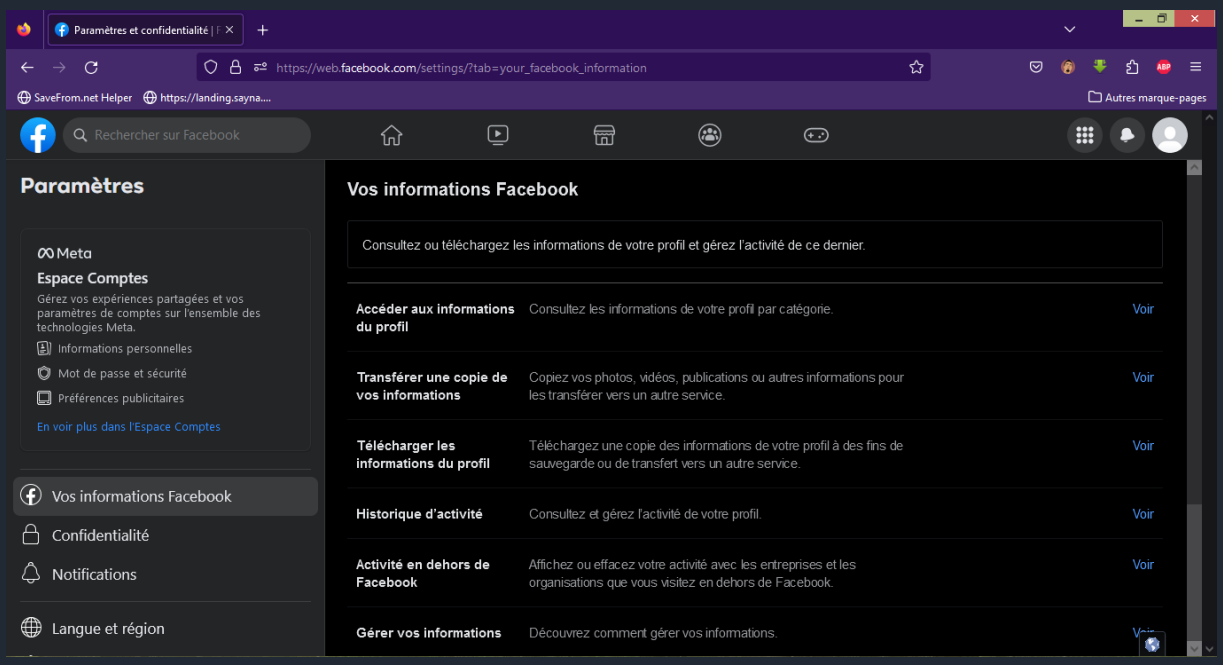
7 - Comprendre le suivi du navigateur

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

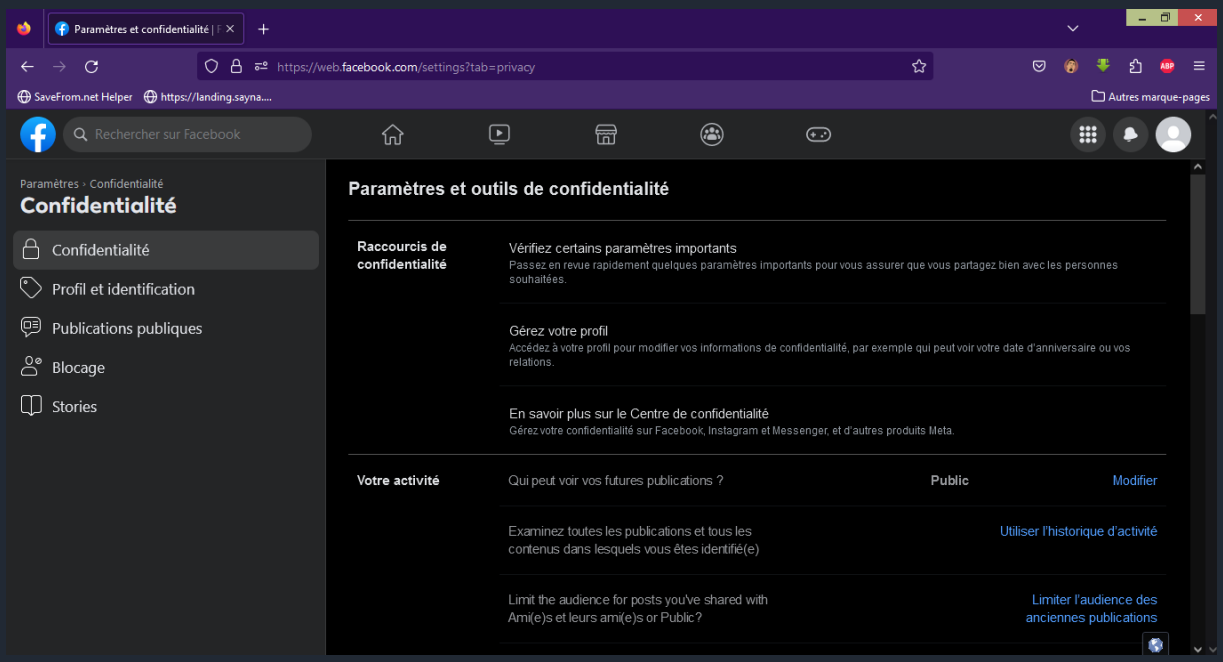
Objectif : Régler les paramètres de confidentialité de Facebook (J'ai déjà fait).

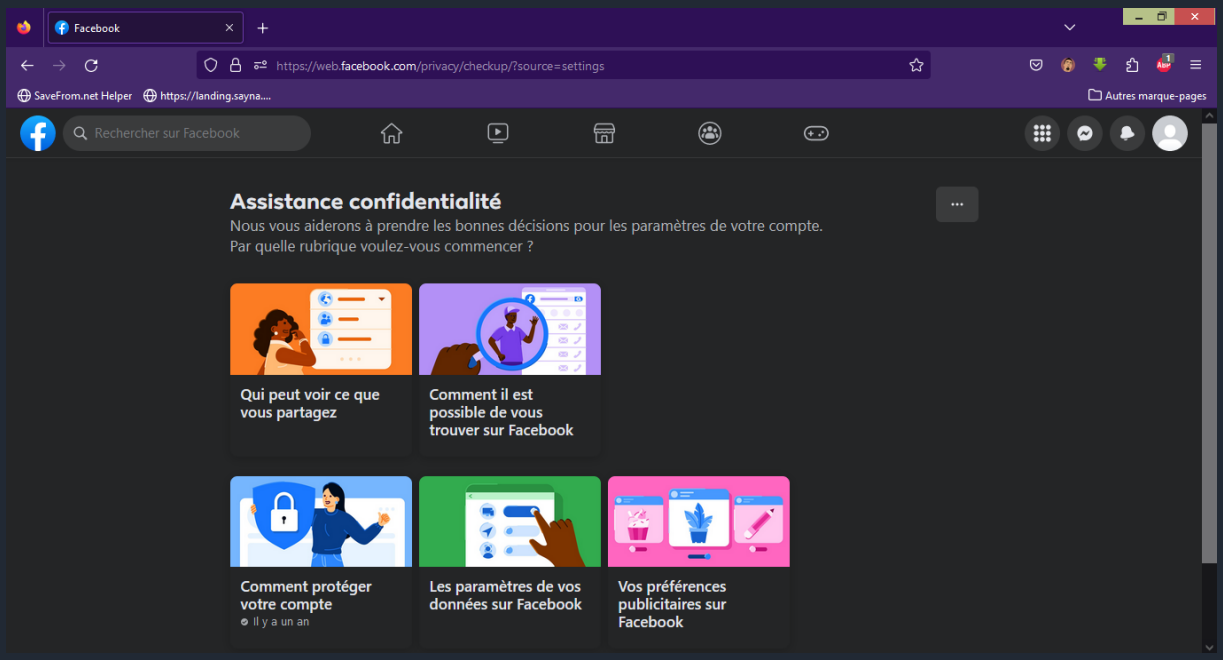
1/ Voici un exemple de paramétrage de compte Facebook pour une utilisation privilégiant les échanges avec les amis, mais autorisant le contact avec des inconnus (limite de leurs actions) :



Confidentialité :

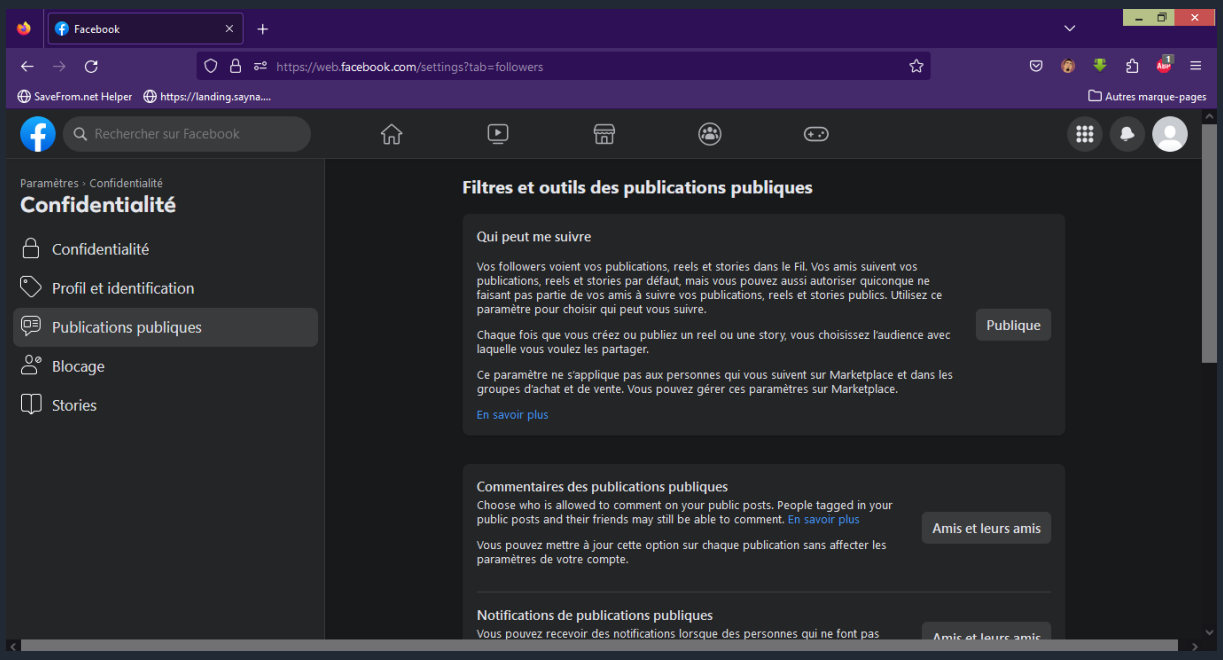
christianrazafiarivelo@gmail.com





Publication publique :

christianrazafiarivelo@gmail.com



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

Objectif :

1/ Pour vérifier la sécurité en fonction de l'appareil utilisé :
Voici quelques exercices spécifiques qu'on peut effectuer pour vérifier la sécurité de différents types d'appareils :

Pour un ordinateur (Windows ou macOS) :

1. Mises à jour système :

- Exercice : Vérifiez si le système d'exploitation est à jour en recherchant les dernières mises à jour.

- Comment faire : Sur Windows, allez dans "Paramètres" > "Mise à jour et sécurité". Sur macOS, allez dans "Préférences Système" > "Mise à jour de logiciels".

2. Analyse antivirus :

- Exercice : Effectuer une analyse antivirus complète pour détecter d'éventuelles menaces.

- Comment faire : Utilise le logiciel antivirus installé pour effectuer une analyse.

3. Pare-feu :

- Exercice : Assurer que le pare-feu de l'ordinateur est activé.

- Comment faire : Sur Windows, allez dans "Paramètres" > "Mise à jour et sécurité" > "Sécurité Windows" > "Pare-feu et protection du réseau". Sur macOS, allez dans "Préférences Système" > "Sécurité et confidentialité" > "Pare-feu".

4. Gestion des comptes :

- Exercice : Vérifier la liste des comptes d'utilisateurs sur l'ordinateur et assurer qu'il n'y a pas de comptes inconnus.

- Comment faire : Sur Windows, allez dans "Paramètres" > "Comptes" > "Famille et autres utilisateurs". Sur macOS, allez dans "Préférences Système" > "Utilisateurs et groupes".

Pour un smartphone (Android ou iOS) :

1. Mises à jour système :

- Exercice : Assurer que le smartphone exécute la dernière version du système d'exploitation.

- Comment faire : Sur Android, allez dans "Paramètres" > "Système" > "Mises à jour du système". Sur iOS, allez dans "Réglages" > "Général" > "Mise à jour logicielle".

2. Autorisations des applications :

- Exercice : Revoyez les autorisations accordées aux applications installées et révoquer celles qui semblent excessives.

- Comment faire : Sur Android, allez dans "Paramètres" > "Applications" > [Nom de l'application] > "Autorisations". Sur iOS, allez dans "Réglages" > "Confidentialité".

3. Verrouillage de l'écran :

- Exercice : Assurez-vous que votre smartphone est verrouillé par un code PIN, un mot de passe, une empreinte digitale ou la reconnaissance faciale.

- Comment faire : Sur Android, allez dans "Paramètres" > "Sécurité" > "Verrouillage de l'écran". Sur iOS, allez dans "Réglages" > "Face ID et code" ou "Touch ID et code".

4. Gestion des appareils connectés :

- Exercice : Vérifiez la liste des appareils connectés à votre smartphone via Bluetooth ou Wi-Fi et déconnectez tout appareil non autorisé.

- Comment faire : Sur Android, allez dans "Paramètres" > "Connexions" > "Bluetooth" ou "Wi-Fi". Sur iOS, allez dans "Réglages" > "Bluetooth" ou "Wi-Fi".

Donc à la fin assurer de suivre ces exercices régulièrement pour maintenir la sécurité d'appareils utiliser. Soyez vigilant face aux menaces en ligne, ne téléchargez pas d'applications suspectes et évitez de cliquer sur des liens non vérifiés ou des pièces jointes douteuses dans les e-mails ou les messages.

2/ Installer et utiliser un antivirus et un antimalware est essentiel pour maintenir la sécurité d'appareil, que ce soit un ordinateur ou un smartphone. Voici un exercice pour installer et utiliser ces logiciels en fonction de l'appareil utilisé :

Exercice : Installer et utiliser un antivirus et un antimalware sur un ordinateur (Windows)

Objectif : Protéger votre ordinateur Windows contre les virus et les logiciels malveillants en installant un antivirus et un antimalware.

Étapes :

1. Recherche de logiciels :

- Ouvrez votre navigateur web et recherchez un antivirus et un antimalware de confiance. Des options populaires incluent Avast, AVG, Norton, McAfee, Malwarebytes, etc.

2. Téléchargement :

- Visitez le site web du logiciel antivirus que vous avez choisi.

- Téléchargez la version gratuite ou d'essai du logiciel depuis le site officiel.

3. Installation :

- Exécutez le fichier d'installation que vous avez téléchargé.

- Suivez les instructions à l'écran pour installer le logiciel.

4. Configuration :

- Une fois l'installation terminée, ouvrez le logiciel antivirus.

- Suivez le processus de configuration initial, qui peut inclure la création d'un compte ou l'activation d'une licence.

5. Mise à jour :

- Assurez-vous que le logiciel antivirus est à jour en recherchant des mises à jour depuis son interface.

6. Analyse complète :

- Lancez une analyse complète de votre ordinateur pour détecter et supprimer les virus et les logiciels malveillants. Cette option est généralement disponible dans l'interface du logiciel.

7. Planification des analyses :

- Configurez le logiciel pour qu'il effectue des analyses régulières automatiquement, par exemple une fois par semaine.

8. Utilisation de l'antimalware :

- Si vous avez également téléchargé un logiciel antimalware (comme Malwarebytes), assurez-vous de le mettre à jour et de lancer des analyses régulières.

9. Surveillance continue :

- Gardez le logiciel antivirus et antimalware actifs en arrière-plan pour une protection continue.

10. Sensibilisation :

- Éduquez-vous sur les signes de menace en ligne, comme les e-mails suspects ou les téléchargements douteux, pour éviter d'infecter votre ordinateur.

POUR SMARTPHONE :

Exercice : Installer et utiliser un antivirus et un antimalware sur un smartphone Android

Objectif : Protéger votre smartphone Android contre les virus et les logiciels malveillants en installant un antivirus et un antimalware.

Étapes :

1. Recherche de logiciels :

- Ouvrez le Google Play Store sur votre smartphone Android.

- Recherchez des applications antivirus et antimalware en utilisant des termes comme "antivirus", "sécurité mobile", "antimalware", etc.

2. Téléchargement et installation :

- Sélectionnez un antivirus de confiance (par exemple, Avast, Norton, Bitdefender, McAfee) et un antimalware (comme Malwarebytes).

- Cliquez sur le bouton d'installation pour télécharger et installer l'application antivirus et l'application antimalware de votre choix.

3. Configuration :

- Ouvrez l'application antivirus après l'installation.

- Suivez les instructions à l'écran pour configurer l'application, y compris la création d'un compte si nécessaire.

4. Mise à jour :

- Assurez-vous que l'application antivirus est à jour en vérifiant les mises à jour depuis le Google Play Store. Mettez à jour si nécessaire.

5. Analyse complète :

- À l'intérieur de l'application antivirus, recherchez l'option pour lancer une analyse complète de votre smartphone.

- Lancez l'analyse pour détecter et supprimer les virus et les logiciels malveillants.

6. Planification des analyses :

- Configurez l'application antivirus pour qu'elle effectue des analyses automatiques régulières (par exemple, une fois par semaine).

7. Utilisation de l'antimalware :

- Ouvrez l'application antimalware que vous avez installée.

- Mettez à jour l'antimalware et effectuez régulièrement des analyses de votre smartphone.

8. Surveillance continue :

- Gardez l'application antivirus et l'application antimalware actives en arrière-plan pour une protection continue.

9. Sensibilisation :

- Éduquez-vous sur les pratiques de sécurité mobile, comme l'installation d'applications à partir de sources fiables et l'évitement de liens et de pièces jointes douteux.

10. Gestion des autorisations :

- Revoyez les autorisations accordées aux applications sur votre smartphone et révoquez celles qui semblent excessives.