PARCOURS : DISCOVERY

Module : Naviguer en toute sécurité

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

Table des matières

Liste des figures

1- Introduction à la sécurité sur Internet

1/ Trois sites consultés

● Article 1 = Cyber malveillance.gouv - comment se protéger sur internet
● Article 2 = CNIL-Sécurité : Sécuriser les sites web
● Article 3 = Kaspersky-Sécurité Internet : Qu'est-ce que c'est et comment vous protéger en ligne ?

2- Créer votre mot de passe fort

1/ Gestionnaire de mot de passe

☒Accède au site de LastPass avec ce lien

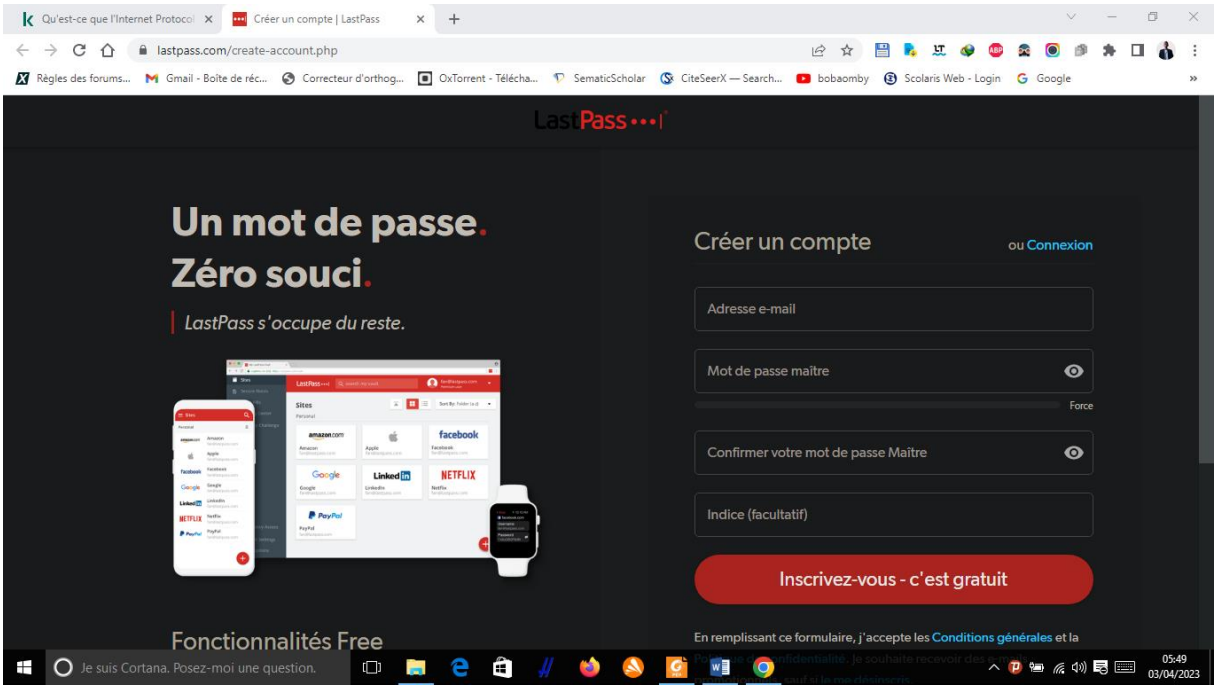

Figure 1: Création d'un compte sur Lastpass

☒Crée un compte en remplissant le formulaire.

☒Exemple de mot de passe maître : c3c!3s!l3M0!2P@SS3 (Ceci est le mot de passe, en remplaçant le "e" par "3" le "i", "t" par "!", "a" par "@" et les premières lettres en minuscules puis majuscules à partir de "mot")

☒Tu peux également générer un mot de passe maître, mais pense à l'écrire dans un endroit sûr pour pouvoir l'utiliser lorsque tu en as besoin

☒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.

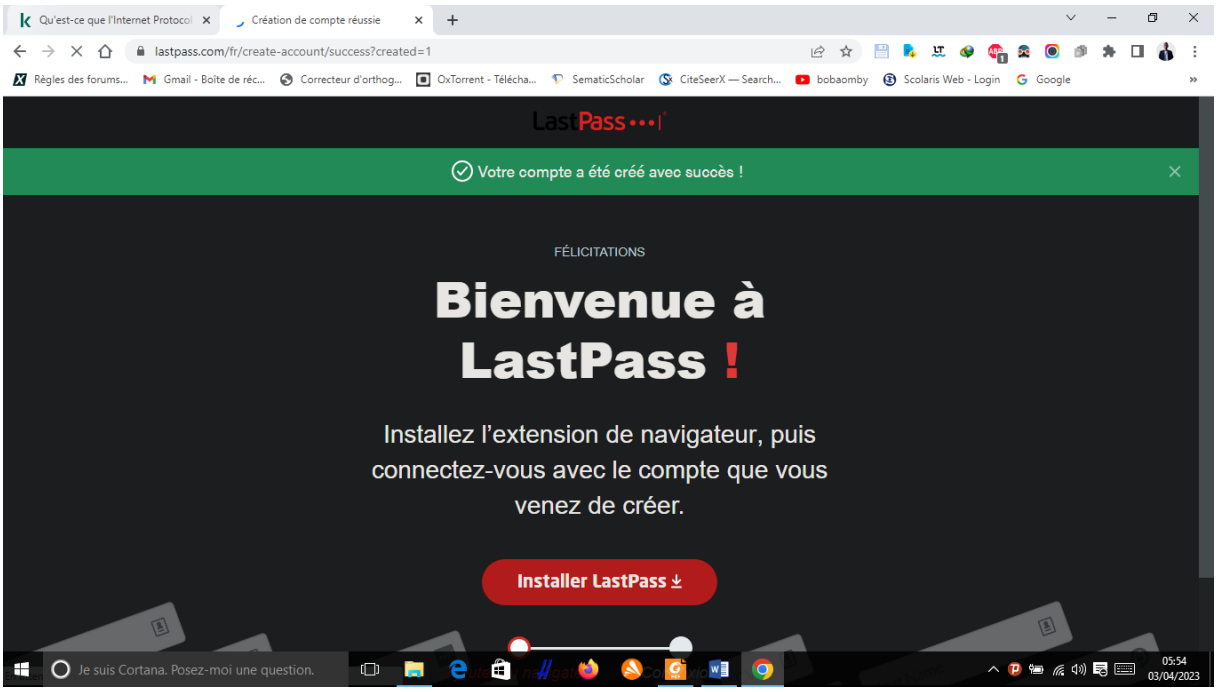

Figure 2:Compte LastPass créé

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

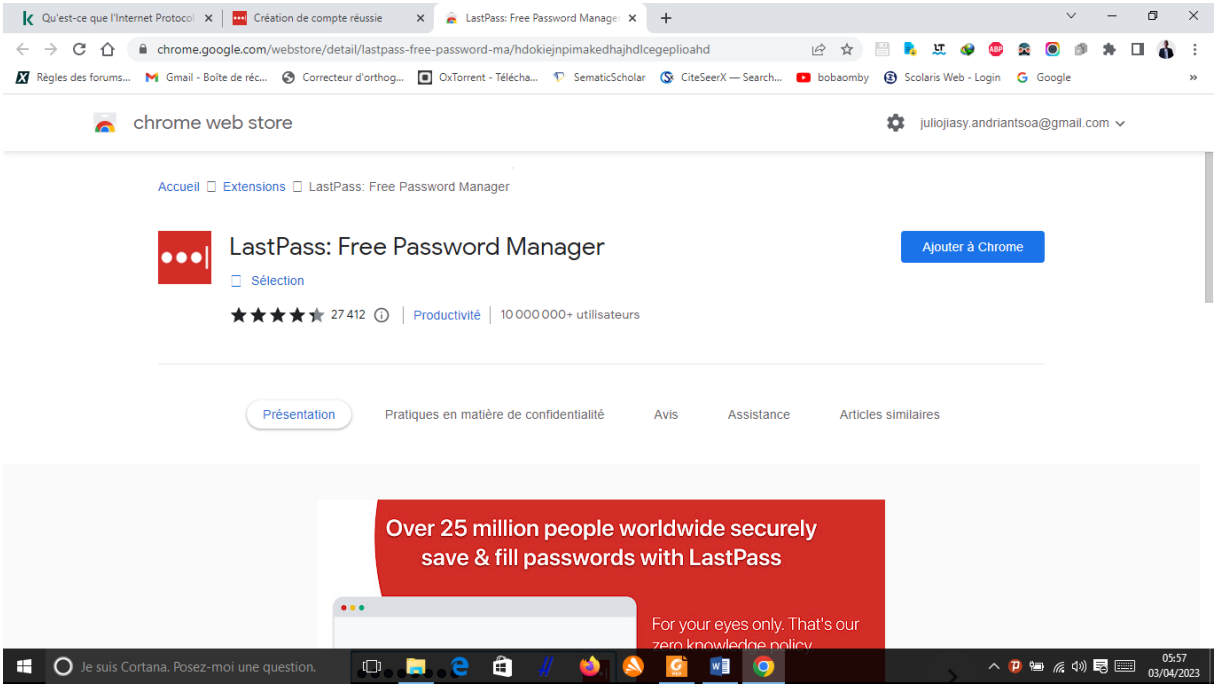

Figure 3:Installation de l'extension LastPass

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

☒(1) En haut à droite du navigateur, clic sur le logo "Extensions"
☒(2) Épingle l'extension de LastPass avec l'icône

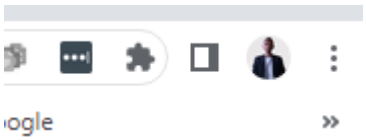

Figure 4: Extension épingler

☒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.

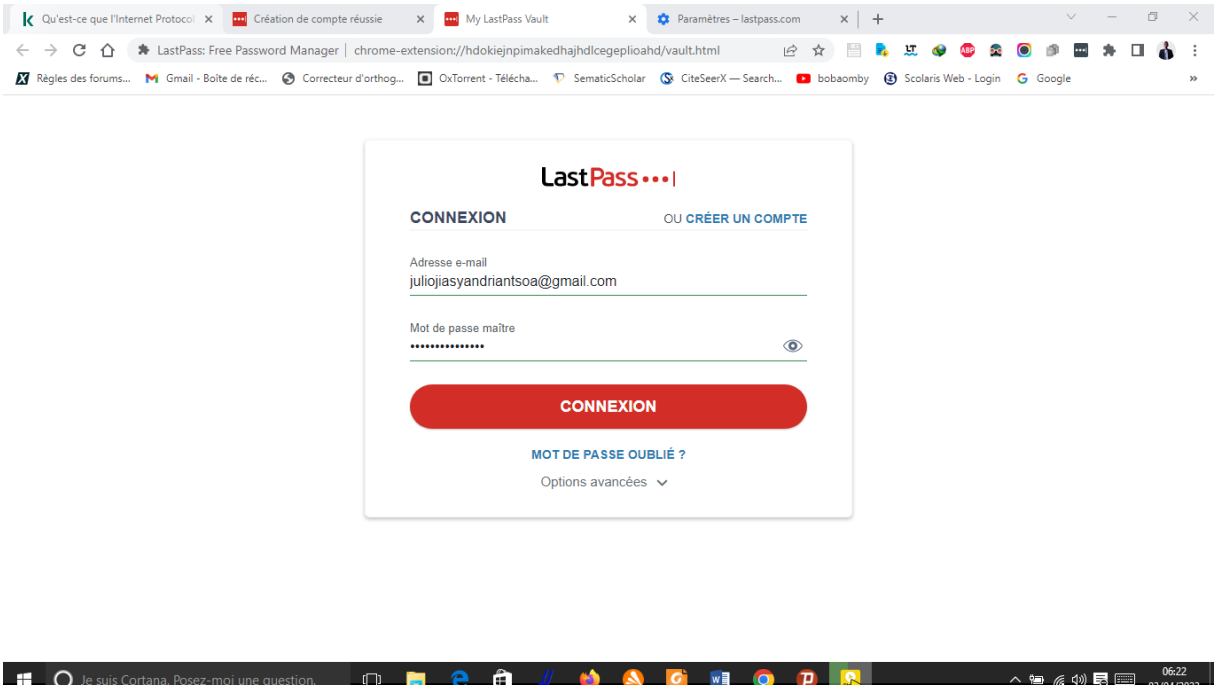

Figure 5: Connexion sur LastPass

2/ Tester LastPass

Pour tester, je me rends dans mon compte Fun Mooc et enregistrer mon mot de passe. Comme j'ai déjà de mot de passe assez fort avant cette formation, je n'ai pour le moment besoins de générer un mot de passe automatique de LastPast. Par contre, ce dernier me serait utile dans l'enregistrement de celui-ci pour une utilisation ultérieure. Voir les figures suivantes :

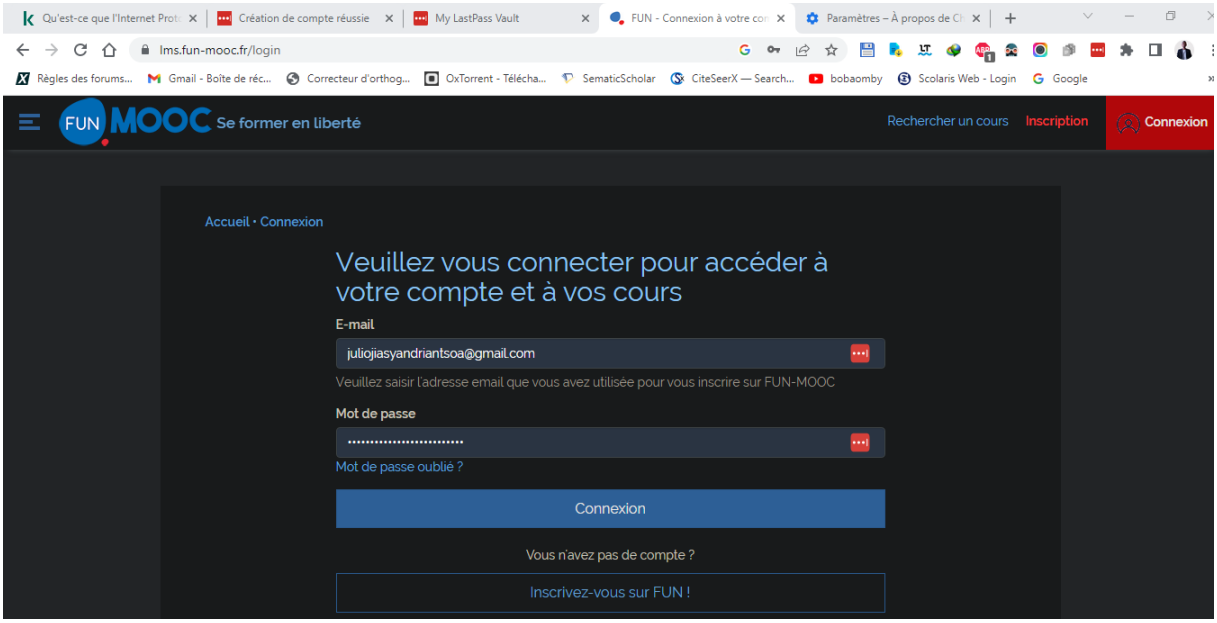

Figure 6: Générer mot de passe fort avec LastPass

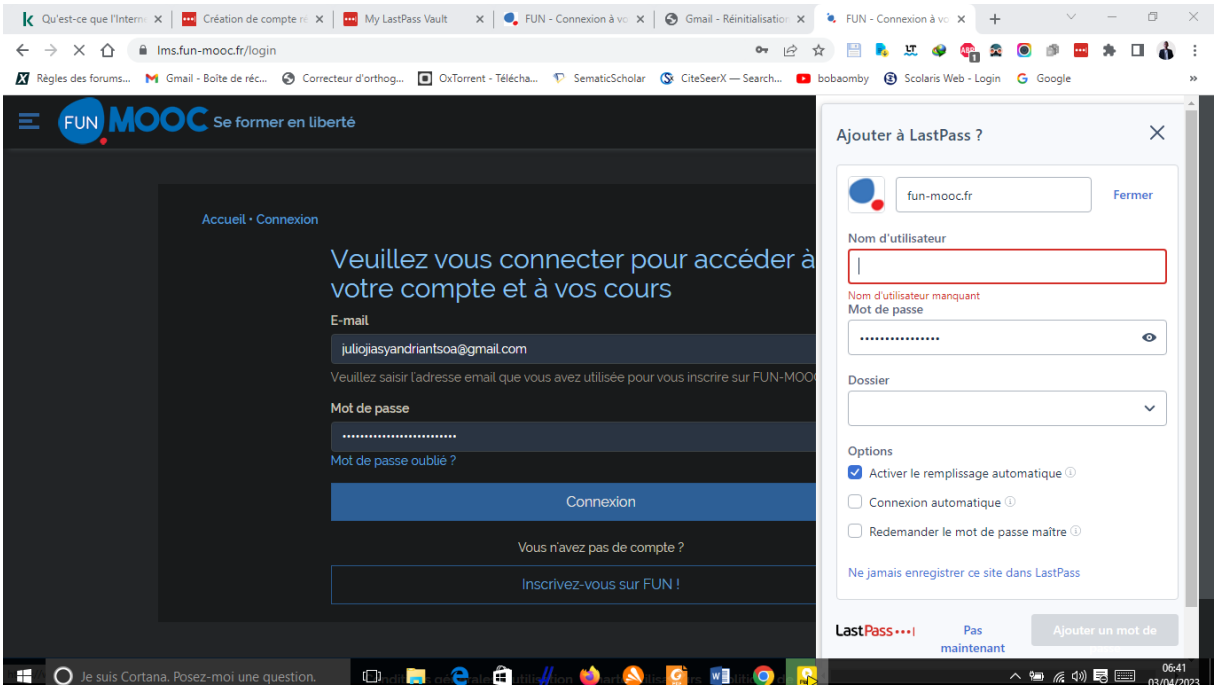

Figure 7: Enregistrement du compte dans LastPass

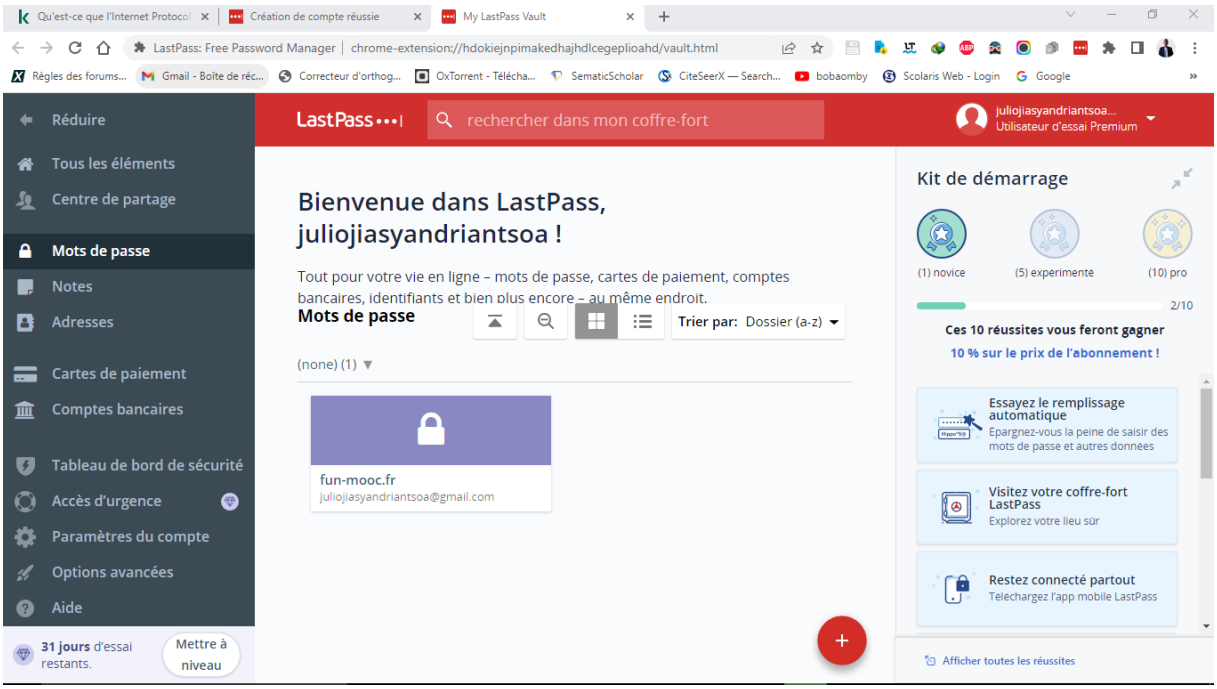

Figure 8: Compte Fun mooc ajouté

3- Fonctionnalité de sécurité de votre navigateur

1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants. (Case à cocher)

☒● www.morvel.com : car ce site n'existe pas réellement et me rédige vers le lien de « Buy Domain ».De plus, si cela existe en temps réel, c'est une version de site de Marvel destiné à arnaquer les gens fans de produits de Marvel ou bien il est destiné à publier gratuitement les produits de Marvel sans l'autorisation de celui-ci.

☐● www.dccomics.com

☐● www.ironman.com

☒● www.fessebook.com : car la personne qui l'a conçu n'a pas respecter les règlements de droit d'auteur attendu que Fessebook est l'homophone de Facebook en quelque sorte. Même mon logiciel de traitement de texte[1] le corrige en Facebook et non en Fessebook.

☐● 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)

☒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

[1] Microsoft Word

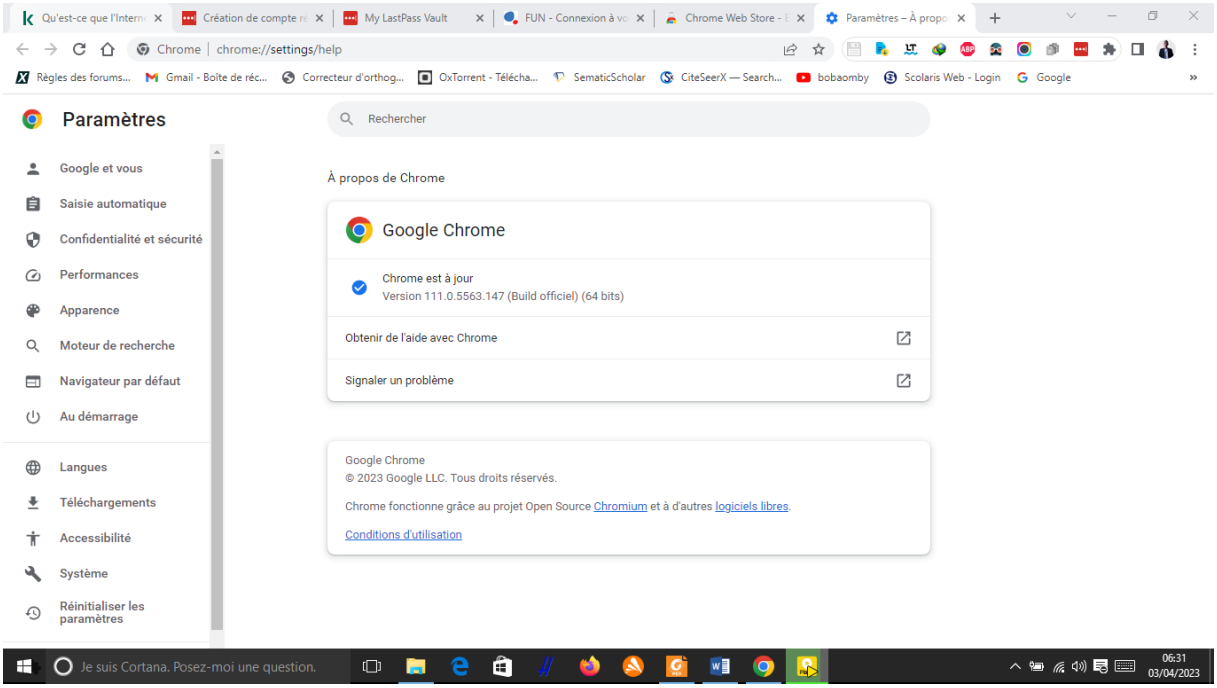

Figure 9: Vérification de mise à jour de Google Chrome

Mon navigateur Google Chrome est à jour.

☒Pour Firefox

☒○ Ouvre le menu du navigateur et accède aux “Paramètres”

☒○ Dans la rubrique “Général”, fais défiler jusqu’à voir la section “Mise à jour de Firefox (astuce : tu peux également saisir dans la barre de recherche (2) “mises à jour” pour tomber directement dessus)

☒○ Vérifie que les paramètres sélectionnés sont identiques que sur la photo

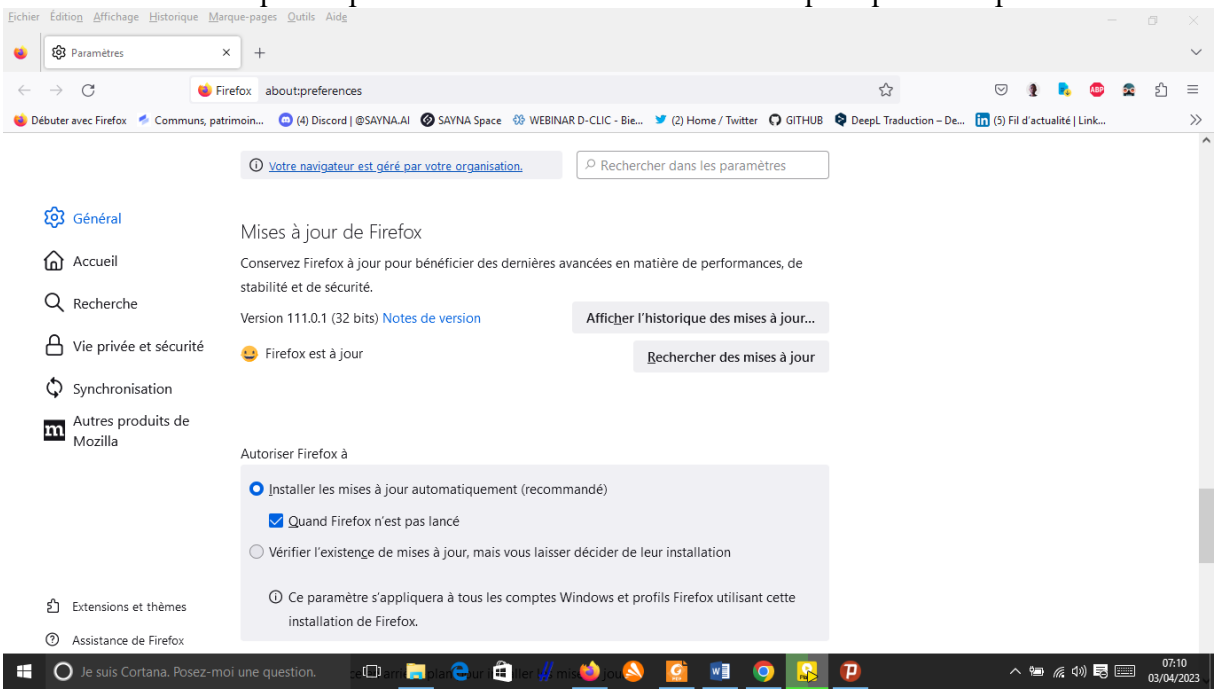

Figure 10:Vérification de mise à jour de Firefox

Firefox est également à jour.

4- Éviter le spam et le phishing

1/ 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]

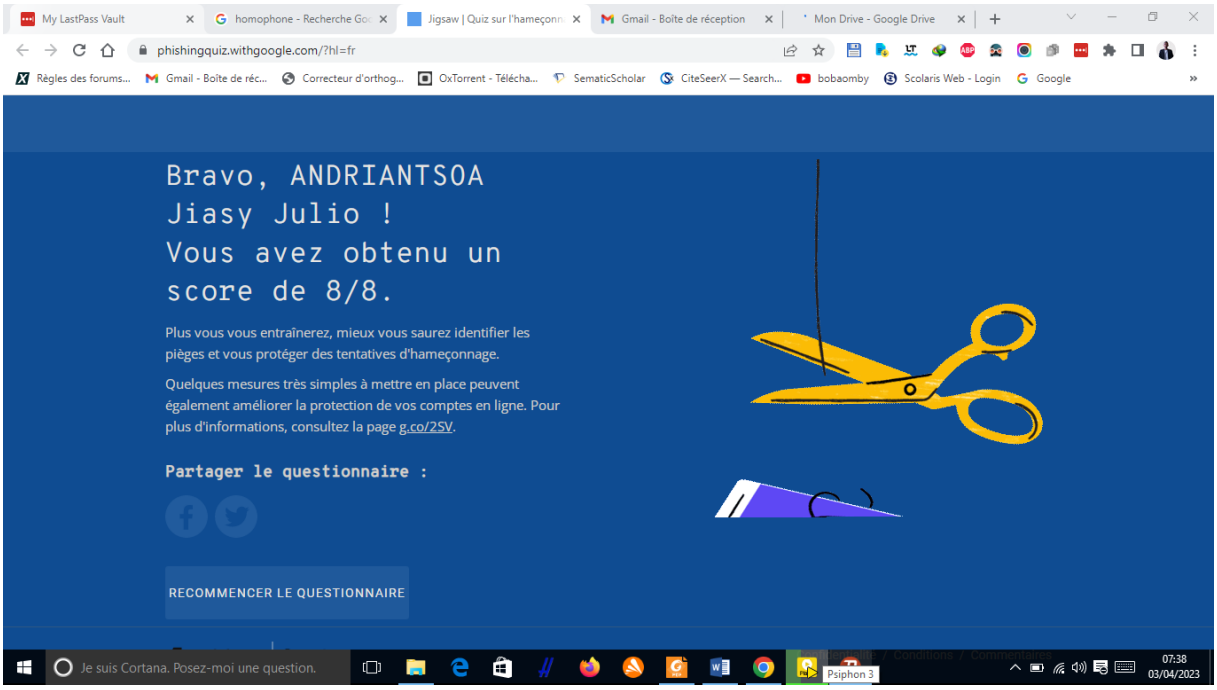

Figure 11: Résultats du questionnaire

5- Comment éviter les logiciels malveillants

1/ Vérification de la Sécurité des sites internet avec Google Transparence des informations

☒● Site n°1

- ☒○ Indicateur de sécurité
  - ☒■ HTTPS
  - ☐■ HTTPS Not secure
  - ☐■ Not secure
- ☒○ Analyse Google
  - ☒■ Aucun contenu suspect
  - ☐■ Vérifier un URL en particulier

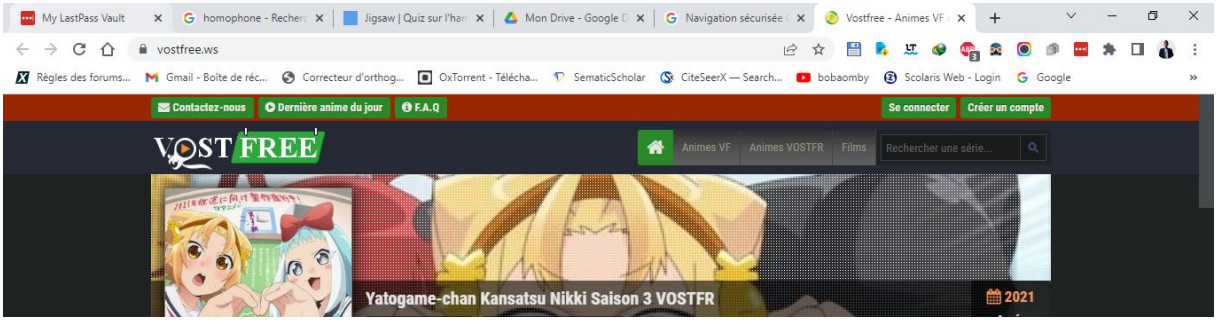

Figure 12: Page d'accueil du site1

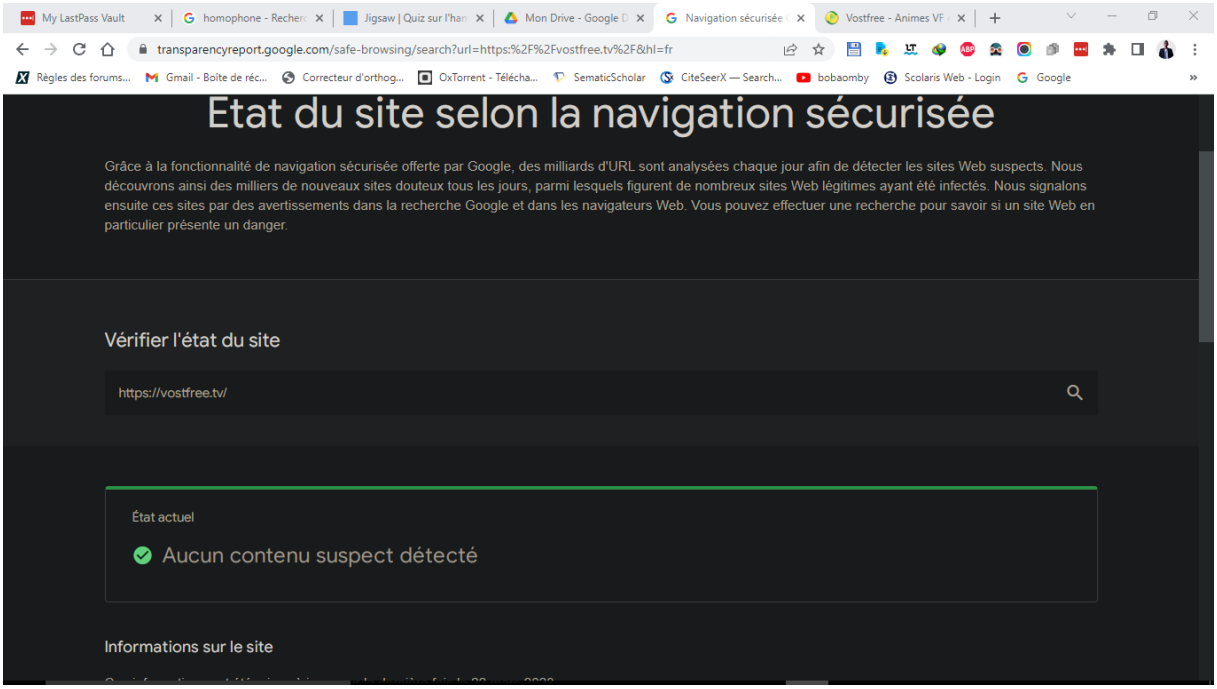

Figure 13:Sécurité du site1

☒● Site n°2

- ☒○ Indicateur de sécurité
  - ☒■ HTTPS
  - ☐■ HTTPS Not secure
  - ☐■ Not secure
- ☒Analyse Google
  - ☒■ Aucun contenu suspect
  - ☐■ Vérifier un URL en particulier

REMARQUE : Avec l'outil de Google, on peut savoir déjà le protocole du site en faisant le collage sur la barre de recherche d'état de site. En outre, les sites avec le protocole http, et non https, ne sont pas forcément des sites non sécurisés.

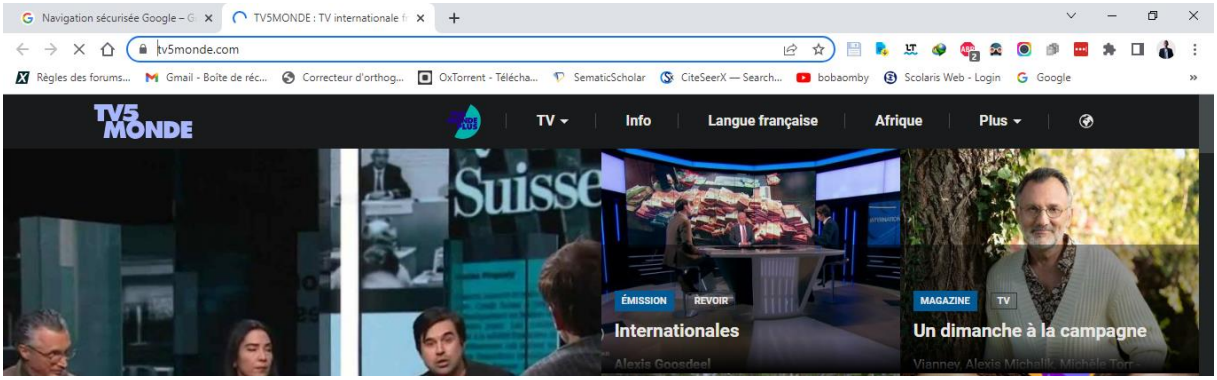

Figure 14: Page d'accueil de TV5 Monde

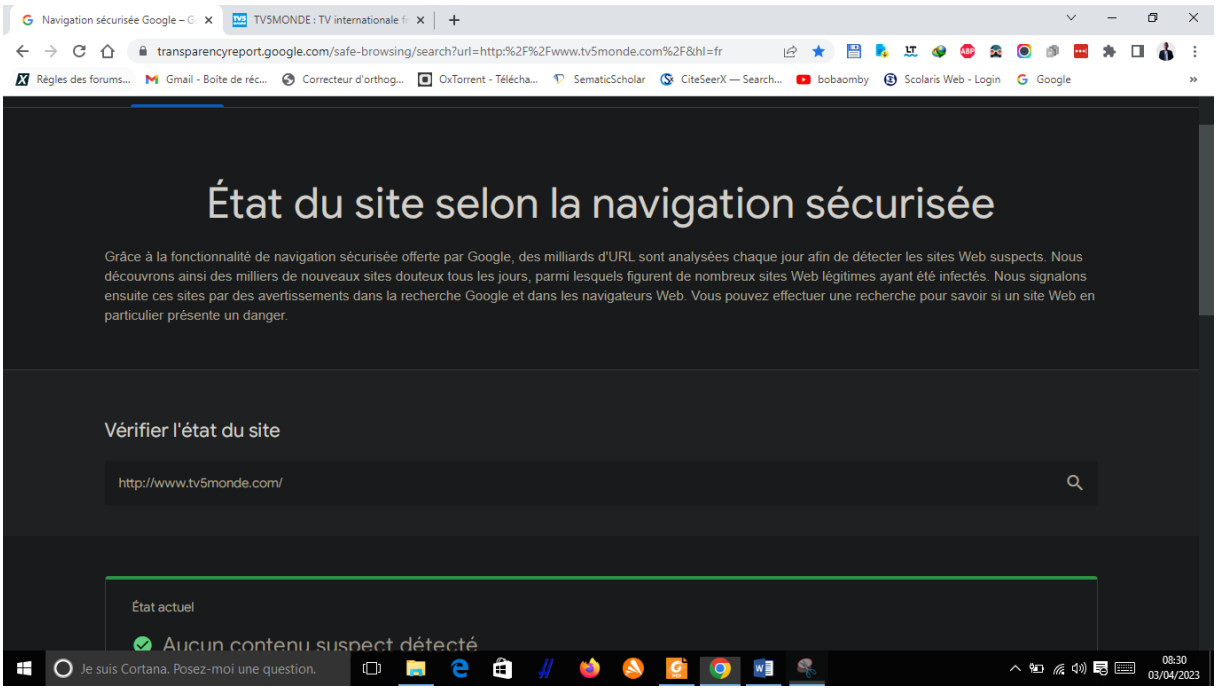

Figure 15: Vérification de la sécurité du site

☒● Site n°3

- ☒○ Indicateur de sécurité
  - ☐■ HTTPS
  - ☐■ HTTPS Not secure
  - ☒■ Not secure
- ☒○ Analyse Google
  - ☐■ Aucun contenu suspect
  - ☒■ Vérifier un URL en particulier

Figure 16: Page d'accueil du site baidu

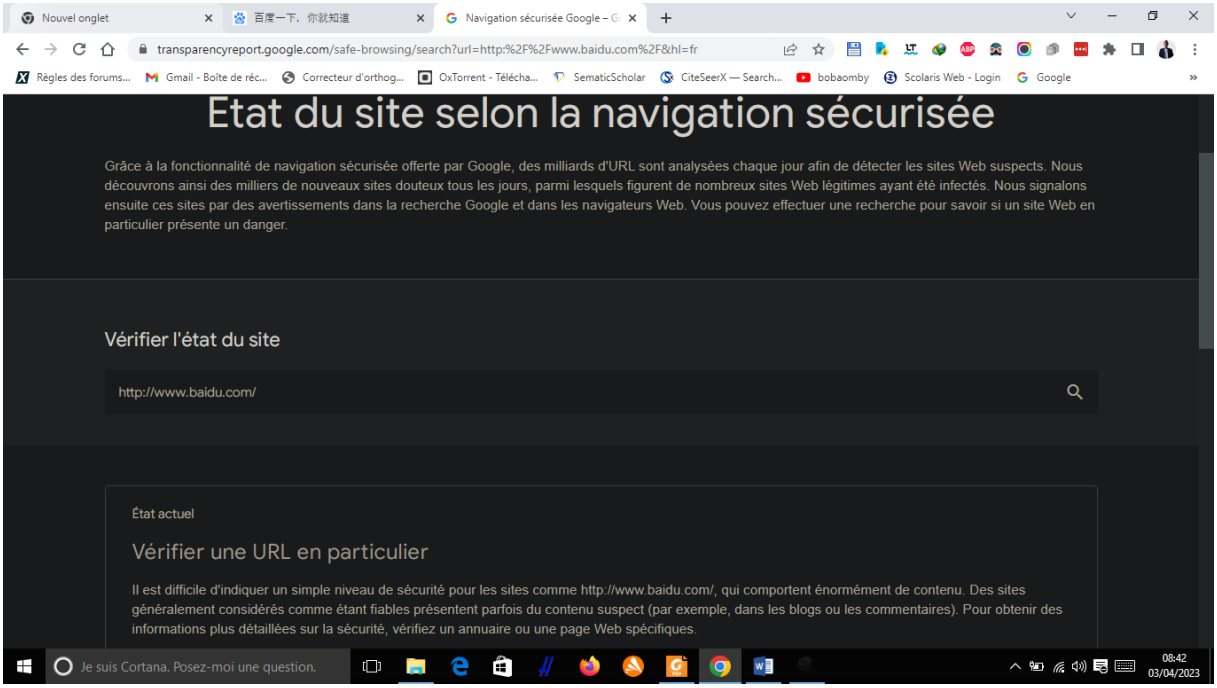

Figure 17:Vérification du site

6- Achats en ligne sécurisés

1/ Registre des achats

1. Sur ta messagerie électronique

☒Pour commencer, accède à ta messagerie électronique. Pour rappel, tu peux y accéder rapidement en ouvrant un nouvel onglet (dans la barre des favoris ou via le raccourci)

☒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)

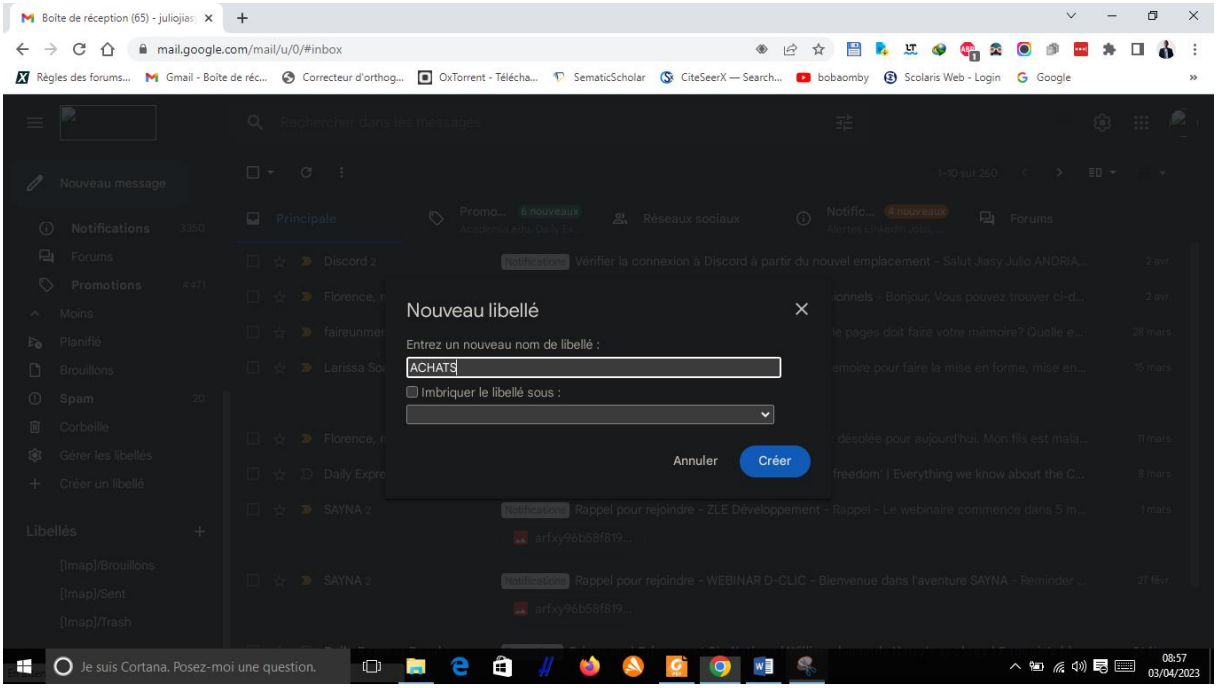

Figure 18:Création de libellé Achats

☒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).

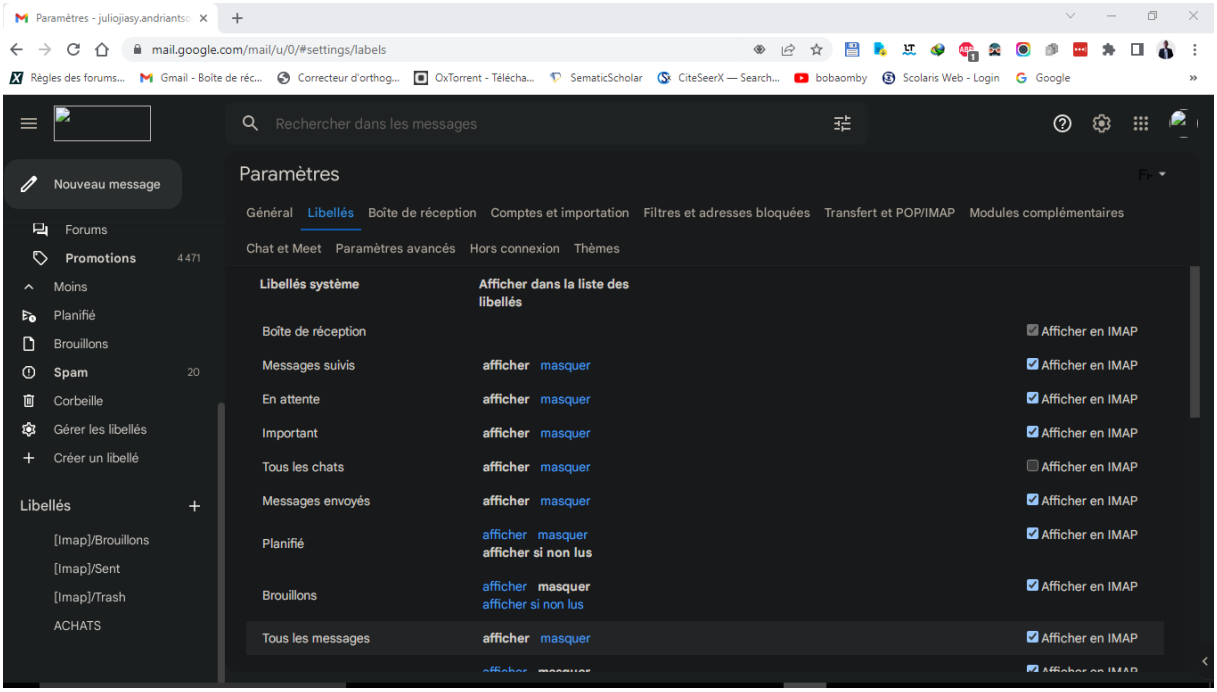

Figure 19:Paramêtre de libellé

☒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

Déjà fait.

8- Principes de base de la confidentialité des médias sociaux

1/ Réglage des paramètres de confidentialité pour Facebook

☒● 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

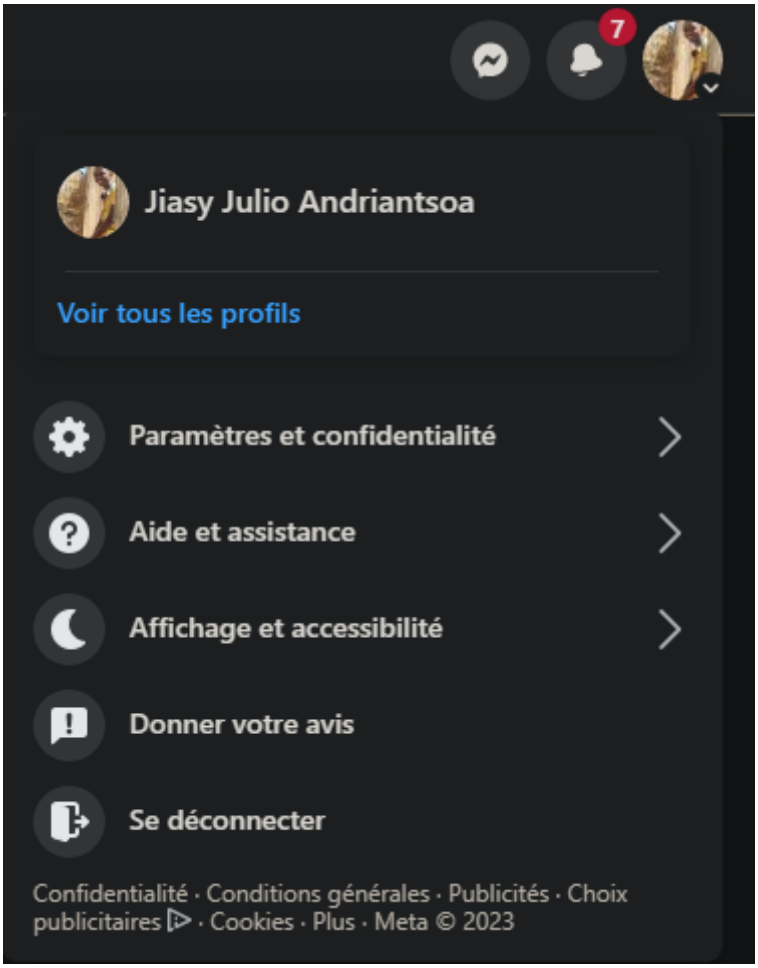

Figure 20:Paramêtres et confidentialité sur Facebook

☒● Ce sont les onglets "Confidentialité" et "Publications publiques" qui nous intéressent. Accède à "Confidentialité" pour commencer et clic sur la première rubrique

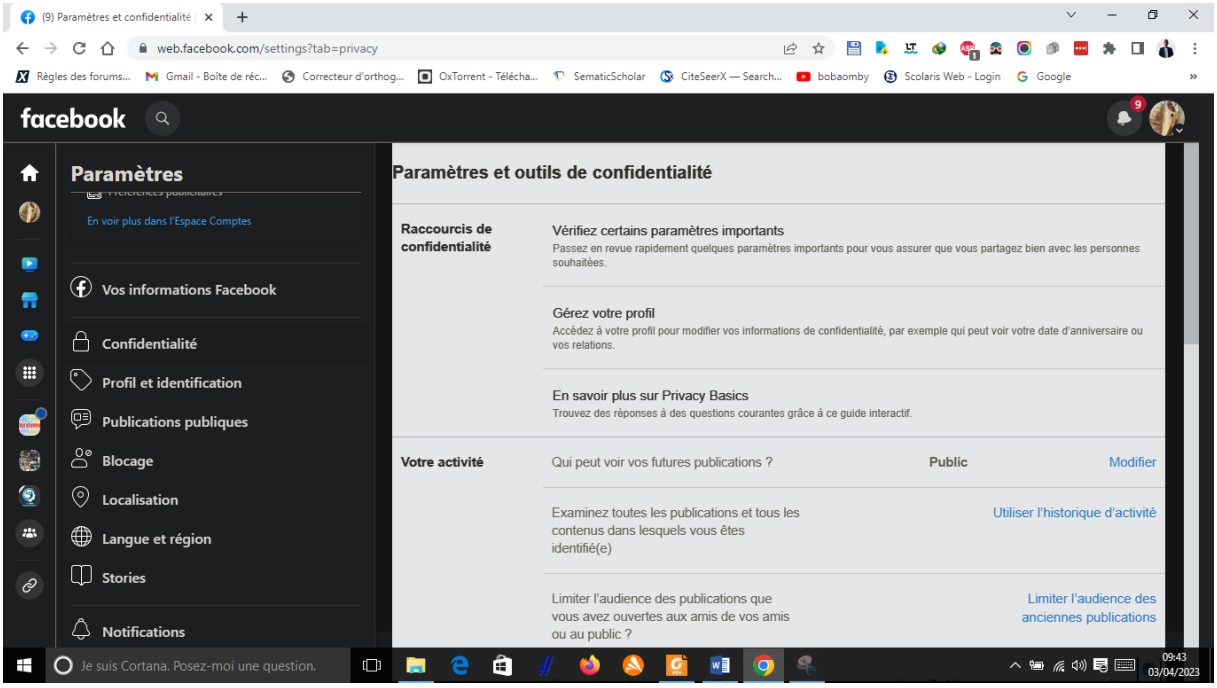

Figure 21:Paramètres et outils de confidentialité

☒● 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

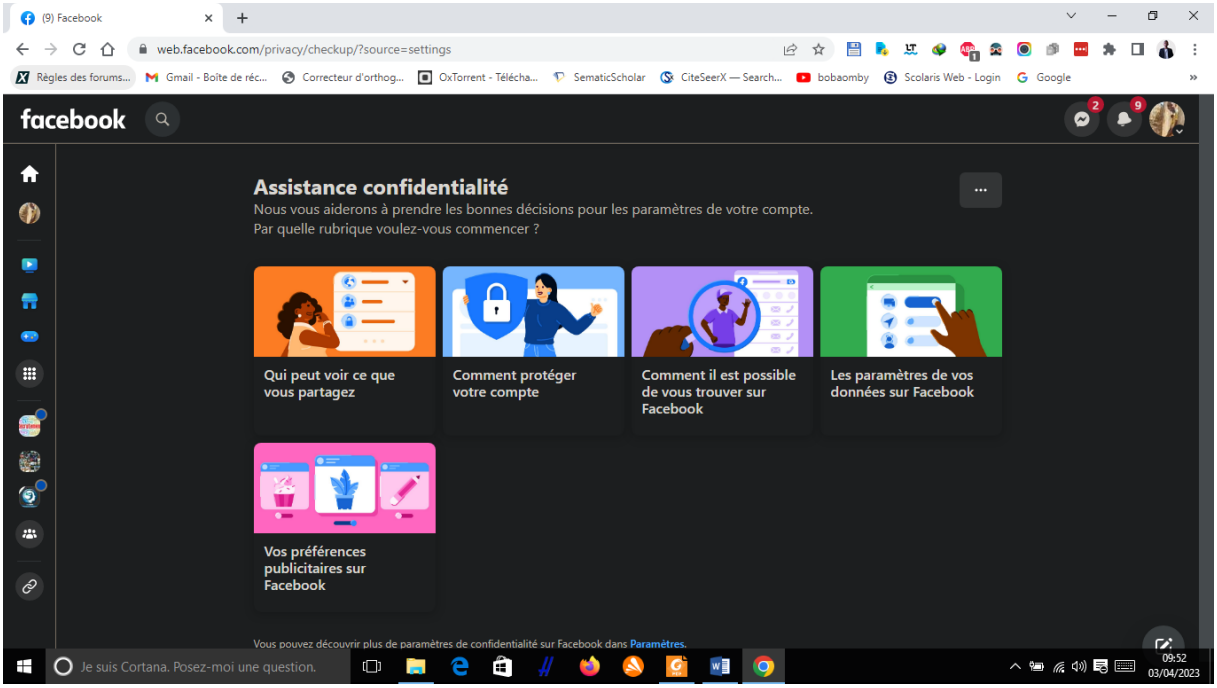

Figure 22:Assistance de confidentialité

☒● 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 ????????

Dans le cas où vous ne savez pas si votre appareil comme ordinateur n'est pas en sécurité ou le contraire, il importe de vous dire que des solutions sont là et elles sont quasiment gratuites. Nombreux d'entre nous se pose la question si un ordinateur dispose déjà un antivirus intégré dans le système d'exploitation ou encore existe-t-il un moyen comme pare-feu de bloquer toute intrusion. La réponse est oui. Mais le problème ce que nous ne savons pas comment l'utiliser

et à quel moment en prendre soin. Nous faisons trop confiance aux antivirus au risque d'oublier l'élément principal : la méfiance. Que ce soit avec Windows 7 ou 8 ou 10, le procédé est le même. Alors comment faire pour être en sécurité que ce soit en ligne ou hors ligne ?
En ligne, il faut s'exercer à :

- Eviter les sites internet ou « lien redirigé » qui pourraient vous amener à télécharger des virus.
- Paramétrer votre navigateur en ce qui concerne les webcams, car ça pourrait donner aux curieux de savoir votre vie privée (Même si le réseau est domestique) : le désactiver si possible. Sinon, scotcher le devant de la caméra.
- Bloquer les popup, car dès fois les sites vous demandent une autorisation pour accéder à vos micros, caméra, ou même avec votre compte mail.

Hors ligne, il faut :

- Toujours activer son antivirus. Un seul antivirus suffit, mais il faut bien le choisir.
- Eviter les périphériques qui ne sont pas sécurisés : Usb, CartSD,…
- Toujours mettre un mot de passe dans son ordinateur et masquer les éléments qui vous sont sensibles.

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

Pour installer un antivirus et antimalware, il faut procéder comme suit :

- D'abord, il faut savoir de quel antivirus vous voulez installer et vous inspire de confiance. Pour ma part j'utilise Avast offline. Pour télécharger cet antivirus et malware, veuillez-vous rendre sur ce lien.
- Une fois téléchargé, il faut l'installer :
    - Si vous avez la version offline (600Mo environ), il suffit juste exécuter le fichier et l'installer directement.
    - Si vous avez la version online, vous devriez être en ligne pour télécharger les packages de l'antivirus.
- Pendant l'installation, vous pouvez remarquer que Windows defender envoie des nouvelles notifications pour vous informer la présence d'un nouvel antivirus.
- Si l'installation est terminée, il vous demande de faire une analyse pour la première. Cette étape est nécessaire pour supprimer les éléments malveillants.
- Dans un cas où il détecte des virus, il ne le supprime pas directement, mais il les met dans la zone de quarantaine pour vous donner la chance de restaurer où récupérer les données qui ne devraient être pas supprimé ou vous accorder de faire les actions possibles.

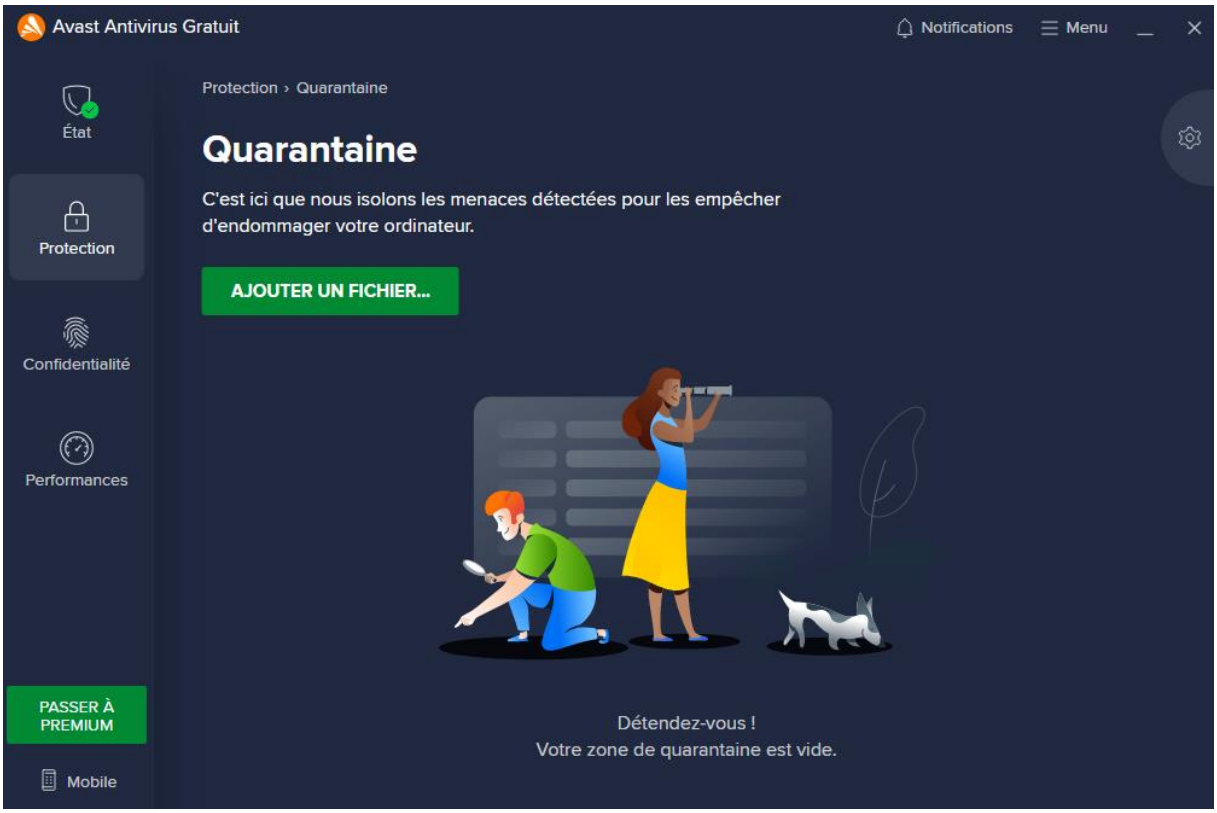

Figure 23: Zone de quarantaine

- Il ne faut pas oublier que dès que Avast est mis en marche, Windows defender sera désactivé pour lui laisser agir à sa place.

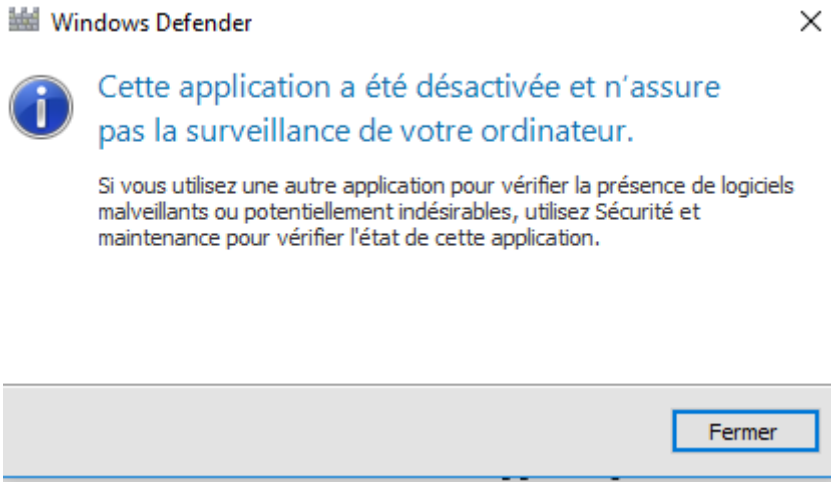

Figure 24: Windows defender Désactivé

- Avast propose également un antimalware par l'intermédiaire de l'anti-ransomware.

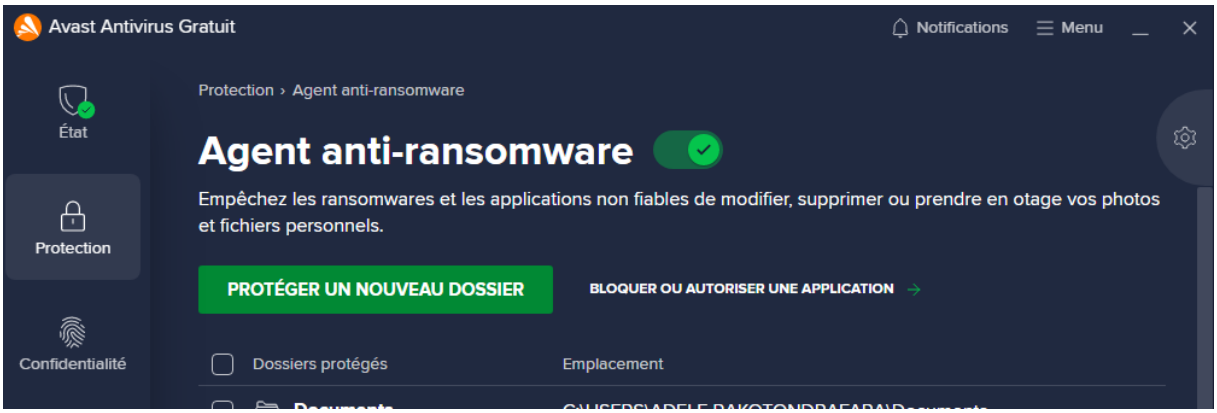

Figure 25:Agent anti-ransomware

- Enfin, comme tout antivirus, il faut toujours mettre à jour les moteurs et bases de données virales si vous voulez que votre ordinateur soit protégé.