Parcours : DISCOVERY

Module : Naviguer en toute sécurité

Projet 2 – Un peu plus de sécurité, on n'en a jamais assez !

KOUAKOU Yao Souleymane

Sommaire

1 – Introduction à la sécurité

Objectif : á la découverte de la sécurité sur internet

Réponse

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

1 Article = ZDNet - Cybersécurité, news et éclairages sur la sécurité informatique

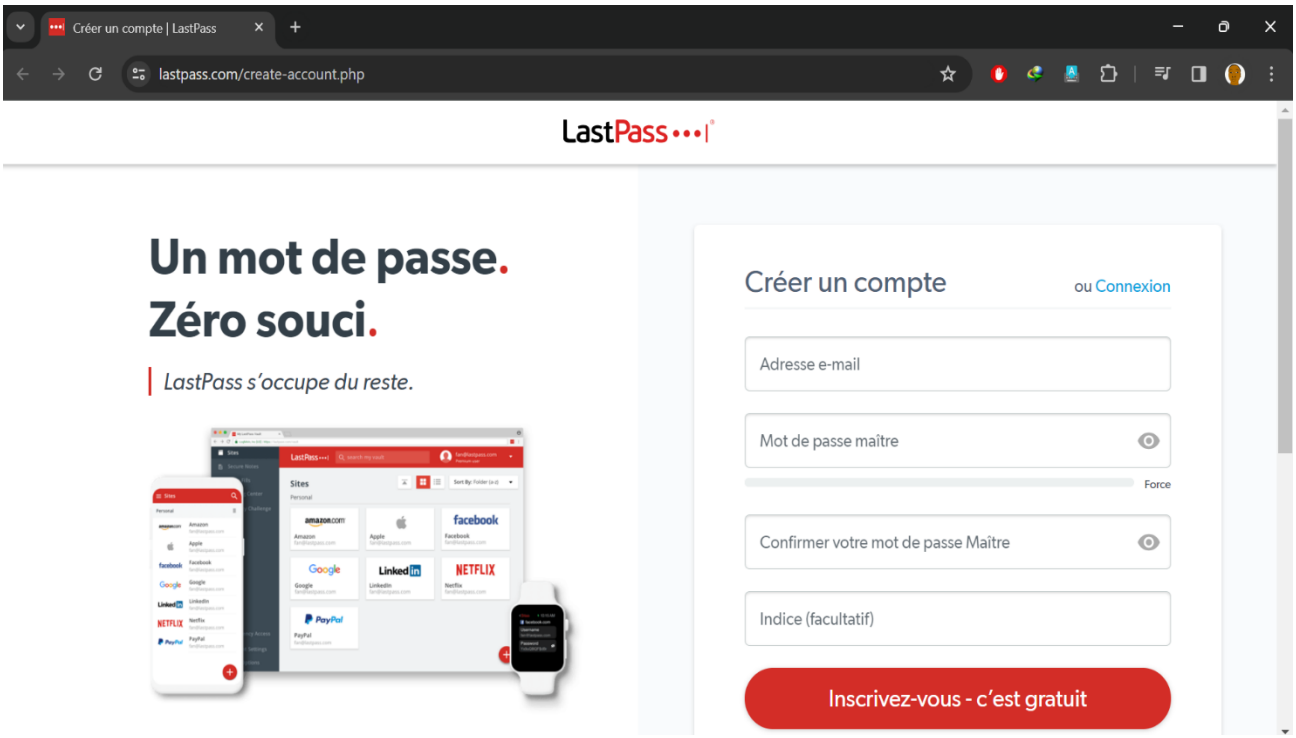
2 Article = Numerama - Sécurité, référencement, prix : quels sont les avantages d'un nom de domaine en .fr

3 Article = UnderNews.fr - Actualité sécurité informatique & cybercrime

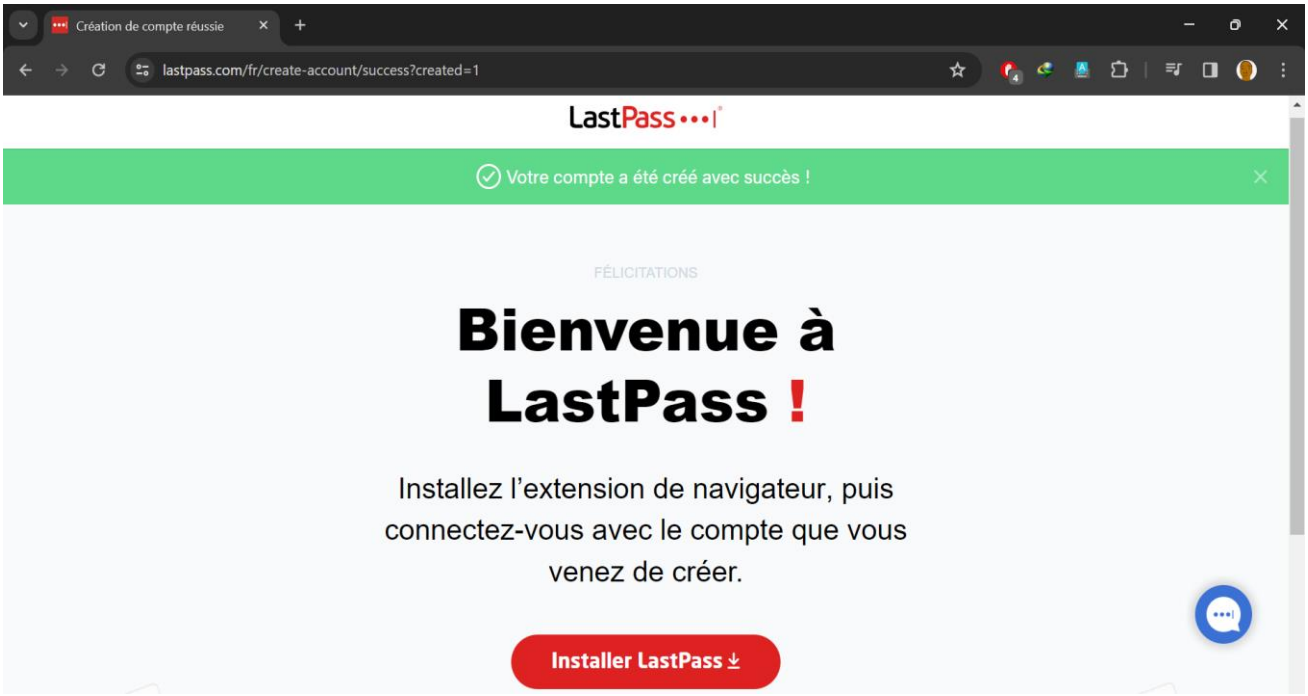
2 – Créer des mots de passe forts

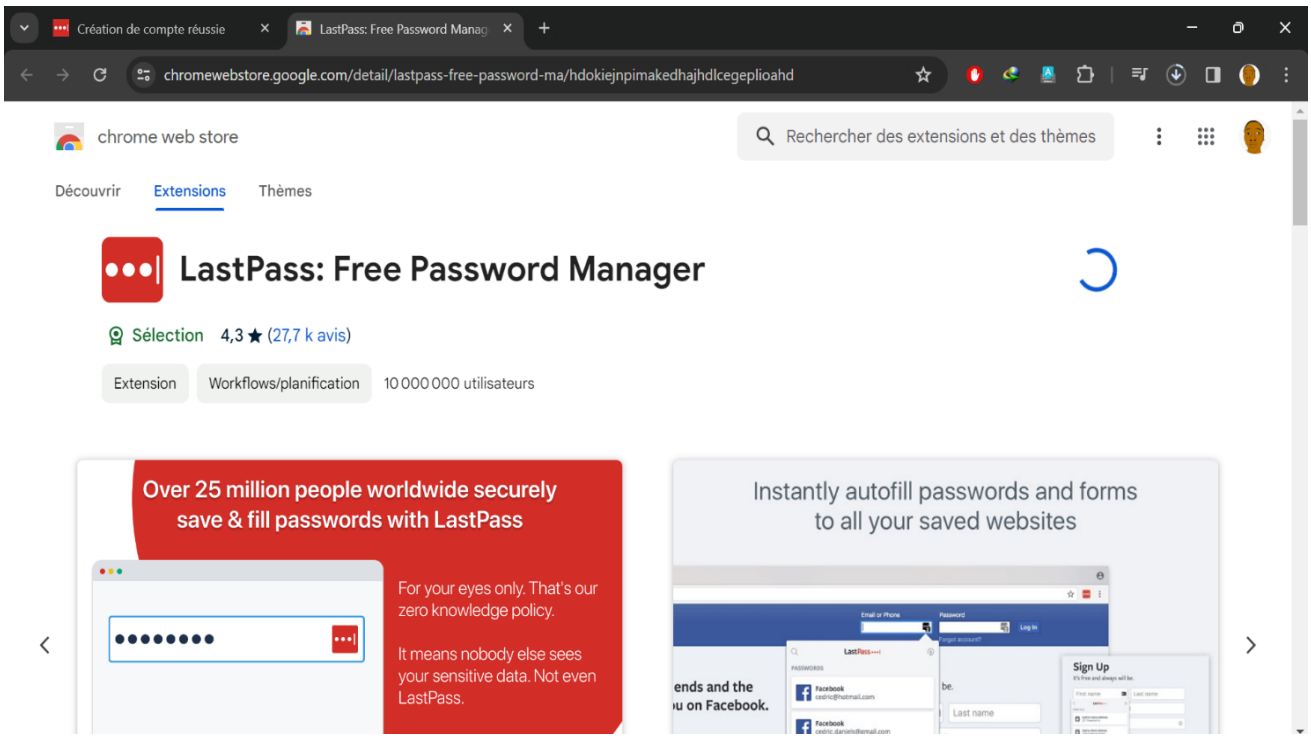
Objectif : Utiliser un gestionnaire de mot de passe LastPass

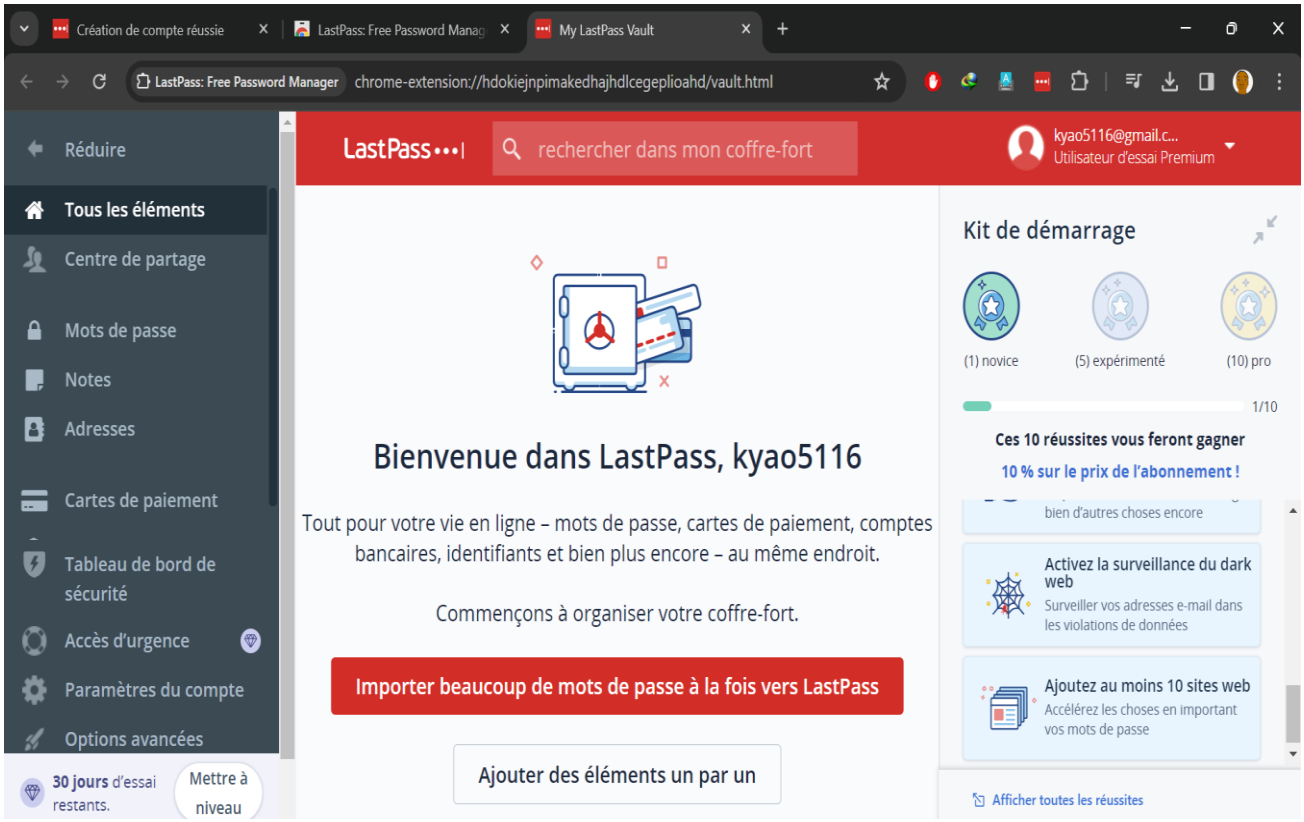
- Accède au site de LastPas avec un lien



- Création d’un compte en remplissant le formulaire.
- Installation de l’extension


Création de compte réussie
lastpass.com/fr/create-account/success?created=1
LastPass
Votre compte a été créé avec succès !
FÉLICITATIONS
Bienvenue à LastPass !
Installez l'extension de navigateur, puis connectez-vous avec le compte que vous venez de créer.
Installer LastPass


Création de compte réussie
LastPass: Free Password Manag
chromewebstore.google.com/detail/lastpass-free-password-ma/hdokiejnpimakedhajhdlcegeplioahd
chrome web store
Rechercher des extensions et des thèmes
Découvrir
Extensions
Thèmes
LastPass: Free Password Manager
Sélection
4,3 ★ (27,7 k avis)
Extension
Workflows/planification
10 000 000 utilisateurs
Over 25 million people worldwide securely save & fill passwords with LastPass
For your eyes only. That's our zero knowledge policy.
It means nobody else sees your sensitive data. Not even LastPass.
Instantly autofill passwords and forms to all your saved websites
Sign Up



Réponse

Désormais, lorsque je veux me connecter à l'un de 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/ Identifie les adresses internet qui te semblent provenir de sites web malveillants.

Réponse

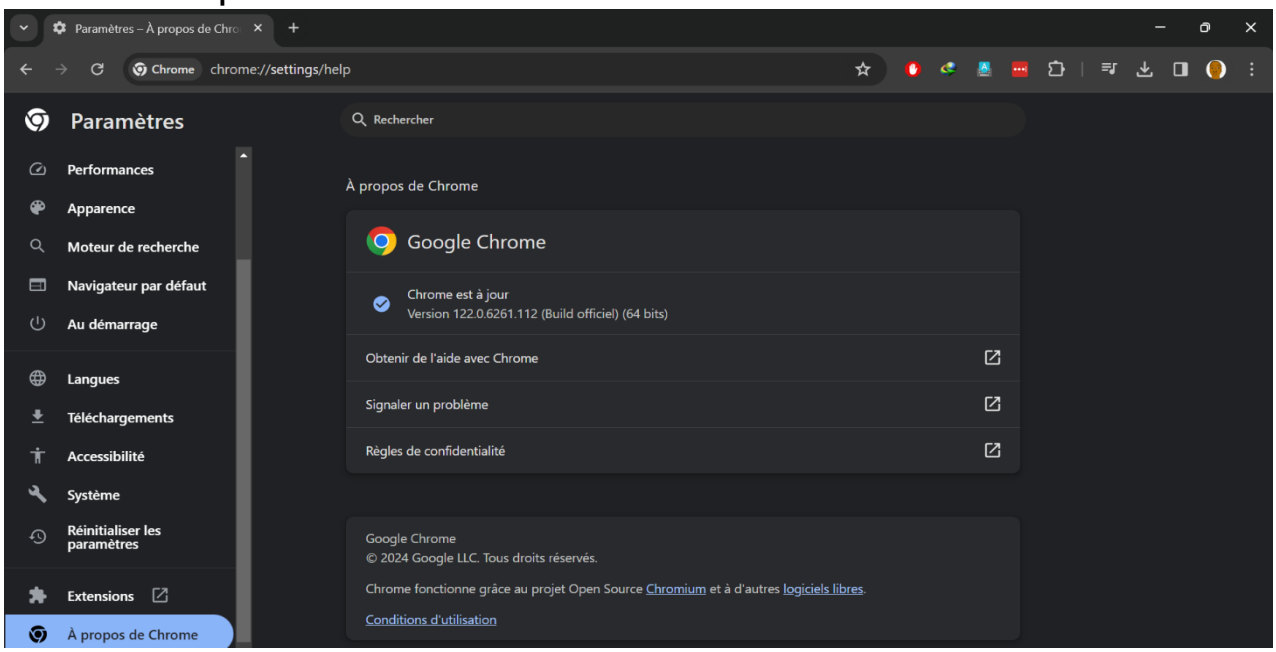
Les sites web qui semblent être malveillants sont :

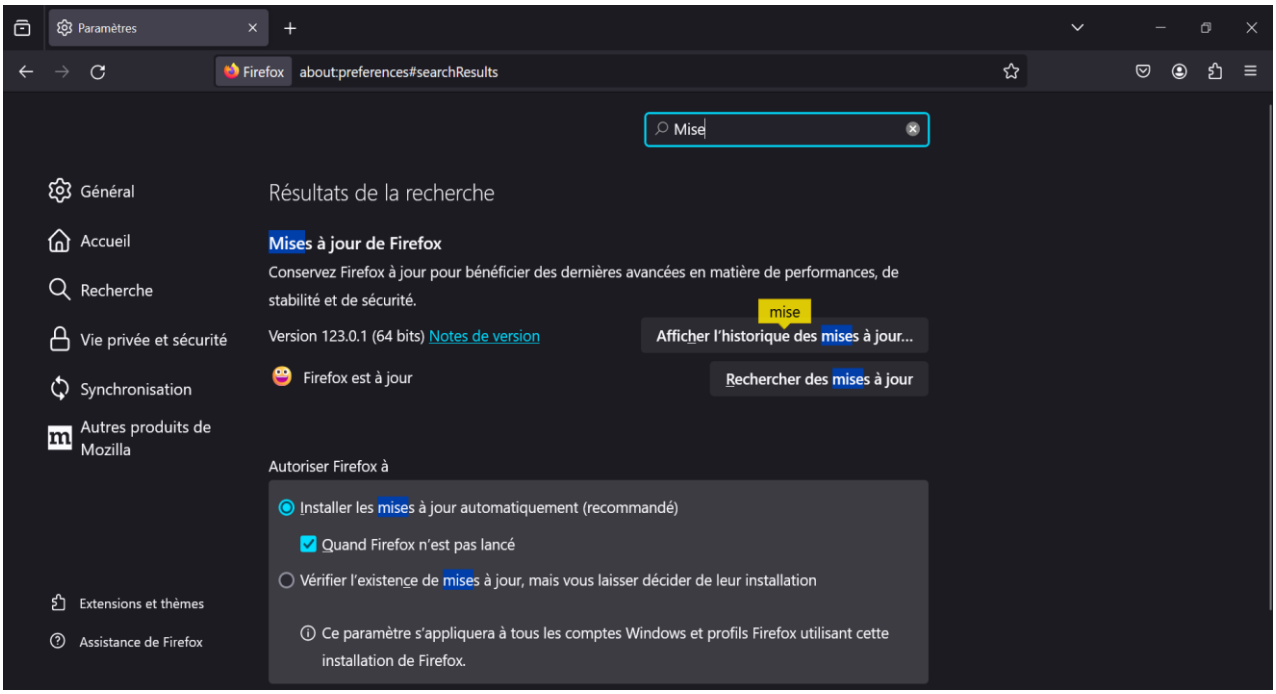
- ✓ www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel.
- ✓ www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde.

- ✓ 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.

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.





Réponse

Après vérification, Chrome et Firefox sont à jour.

4 – Éviter le spam et le phishing

Objectif : Reconnaitre 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

Réponse

Bravo, KOUAKOU !
Vous avez obtenu un score de 8/8.

5 – Comment éviter les logiciels malveillants

Objectif : Sécuriser votre ordinateur et identifier les liens suspects

Réponse

https://vostfree.tv/
- Indicateur de sécurité
  - HTTPS
- Analyse Google
  - Aucun contenu suspect

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

https://www.baidu.com/
- Indicateur de sécurité

        - HTTPS
    - Analyse Google
        - Aucun contenu suspect

http://w3.uqo.ca/iglewski/ens/inf1493/src/html2/html2_http.php

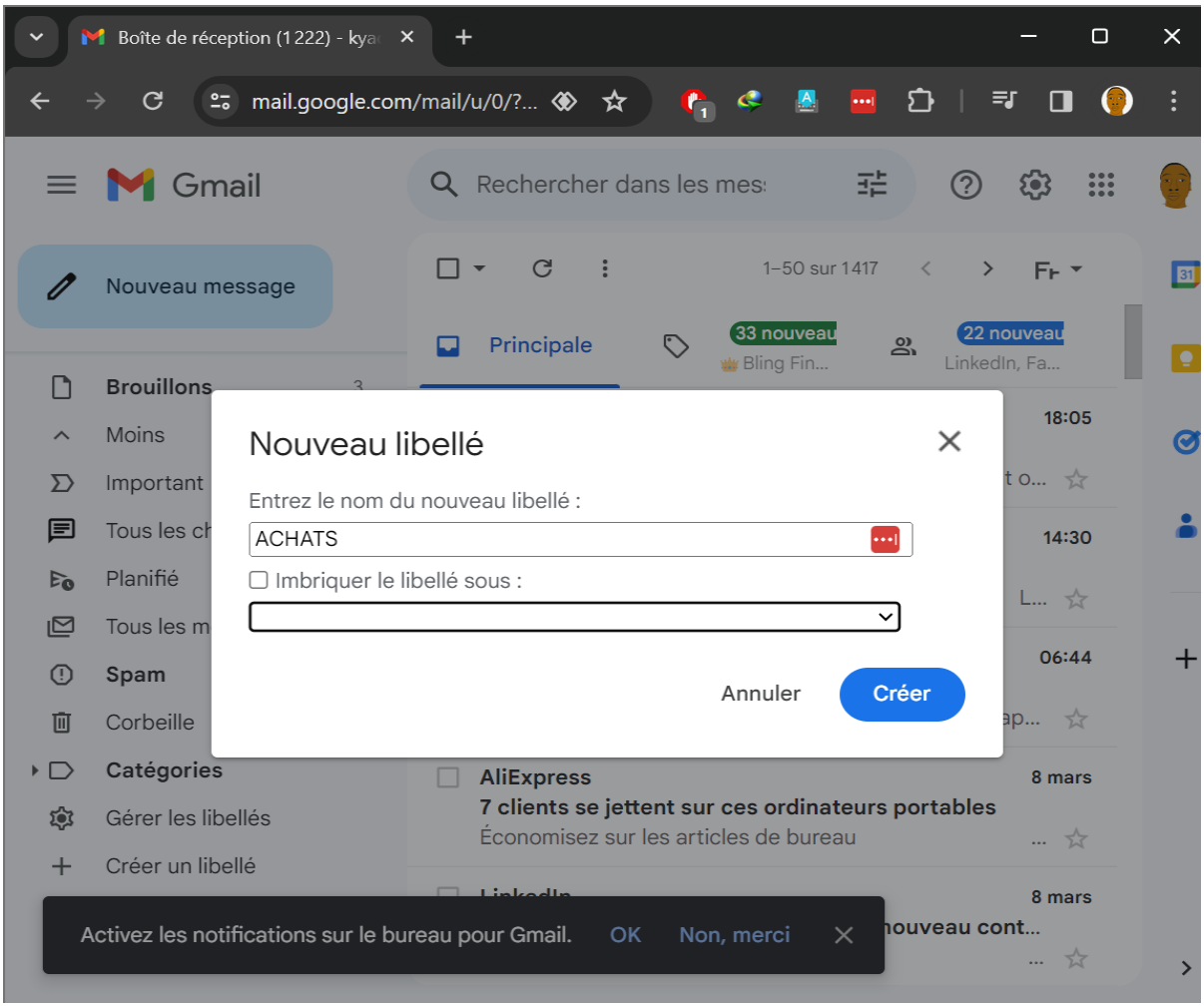
- Indicateur de sécurité
    - Not secure
- Analyse Google
    - Aucun contenu suspect

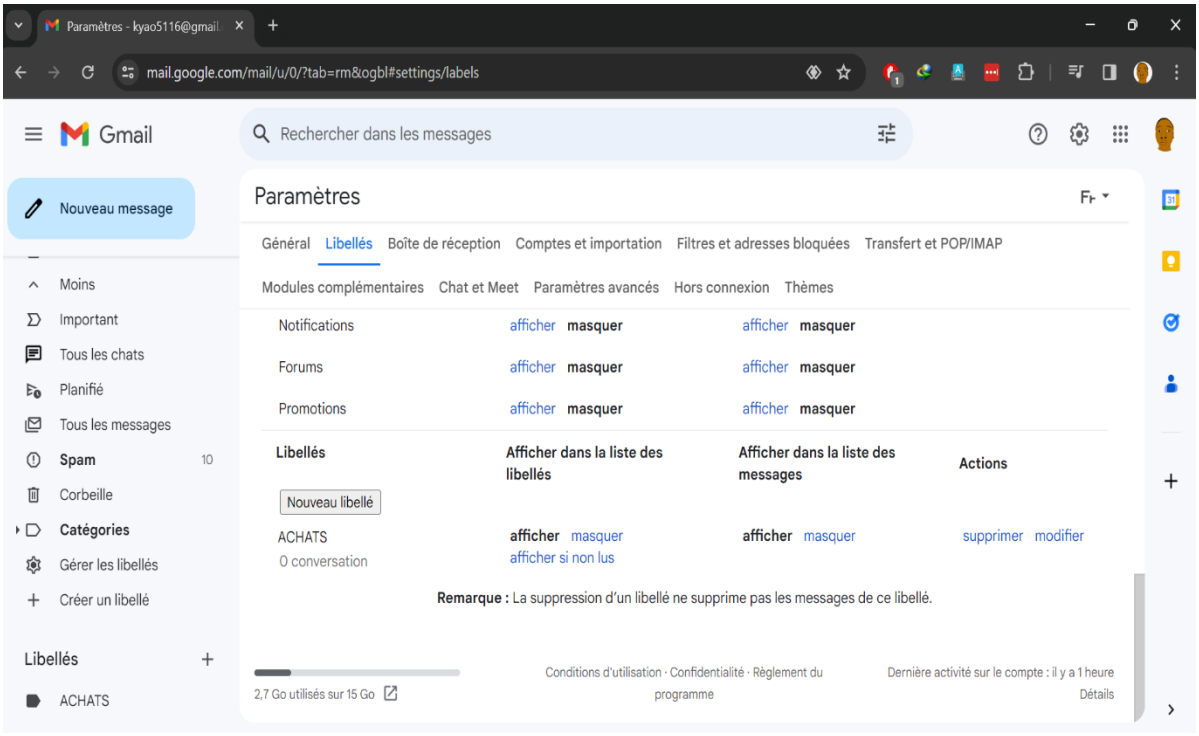
6 – Achats en ligne sécurisés

Objectif : Créer un registre des achats effectués sur internet

Réponse

J'ai créé un libellé pour stocker tous mes e-mails relatifs aux achats effectués sur internet.





7 – Comprendre le suivi du navigateur

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

Réponse

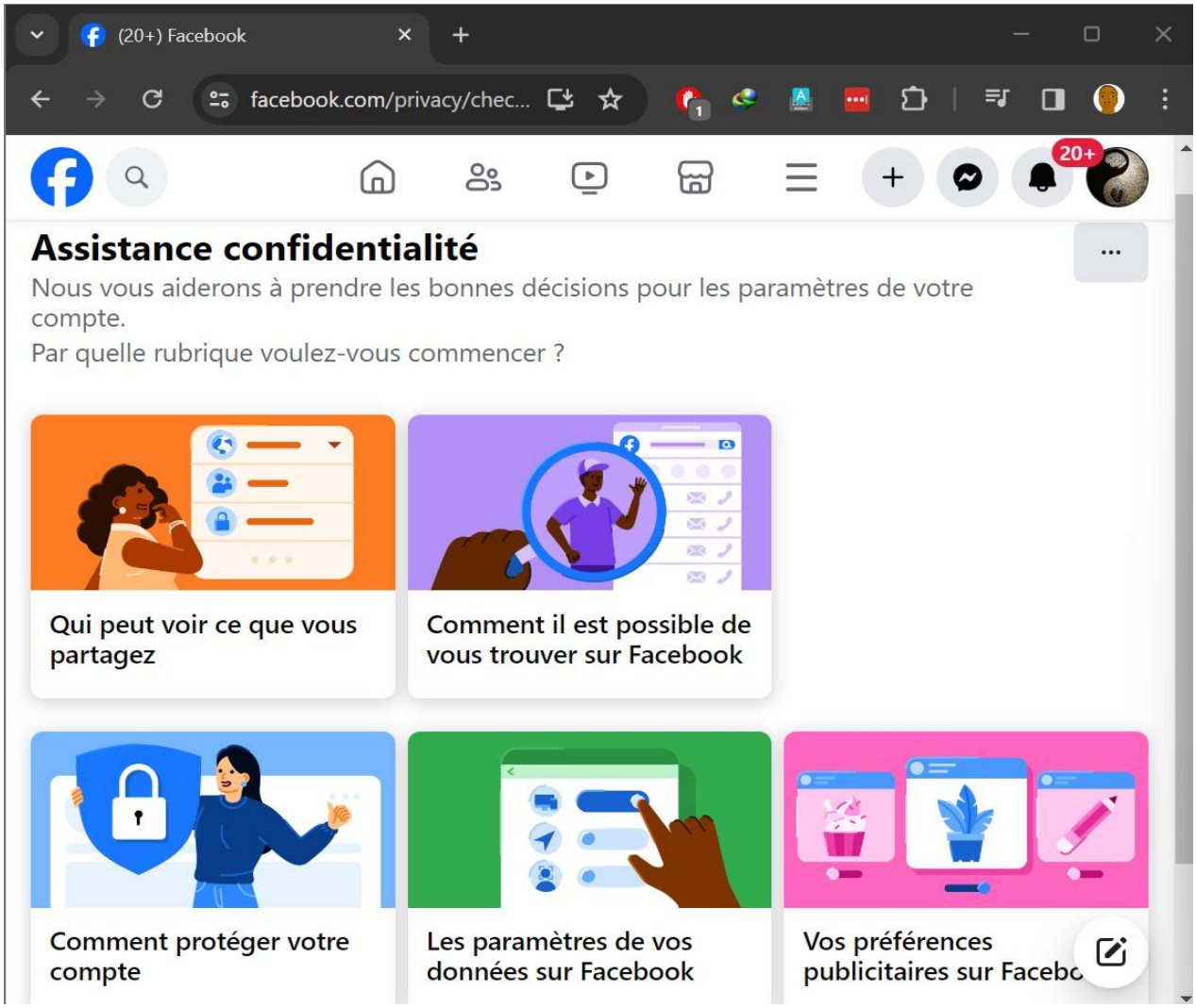
- La gestion des cookies est cruciale pour la protection de la vie privée et la sécurité en ligne. Il est recommandé d'ajuster régulièrement les paramètres de confidentialité du navigateur pour contrôler les cookies. Les cookies essentiels sont indispensables au bon fonctionnement des sites fréquemment visités, tandis que la suppression des cookies superflus est conseillée. Des extensions de confidentialité telles que "Privacy Badger" ou "uBlock Origin" peuvent aider à bloquer les cookies non désirés. Il est également préconisé de désactiver les publicités ciblées, de limiter l'utilisation des cookies tiers, de gérer les cookies par site, et de favoriser les connexions sécurisées (https). Enfin, il est essentiel de comprendre les politiques de confidentialité des sites web pour connaître leur utilisation des cookies.

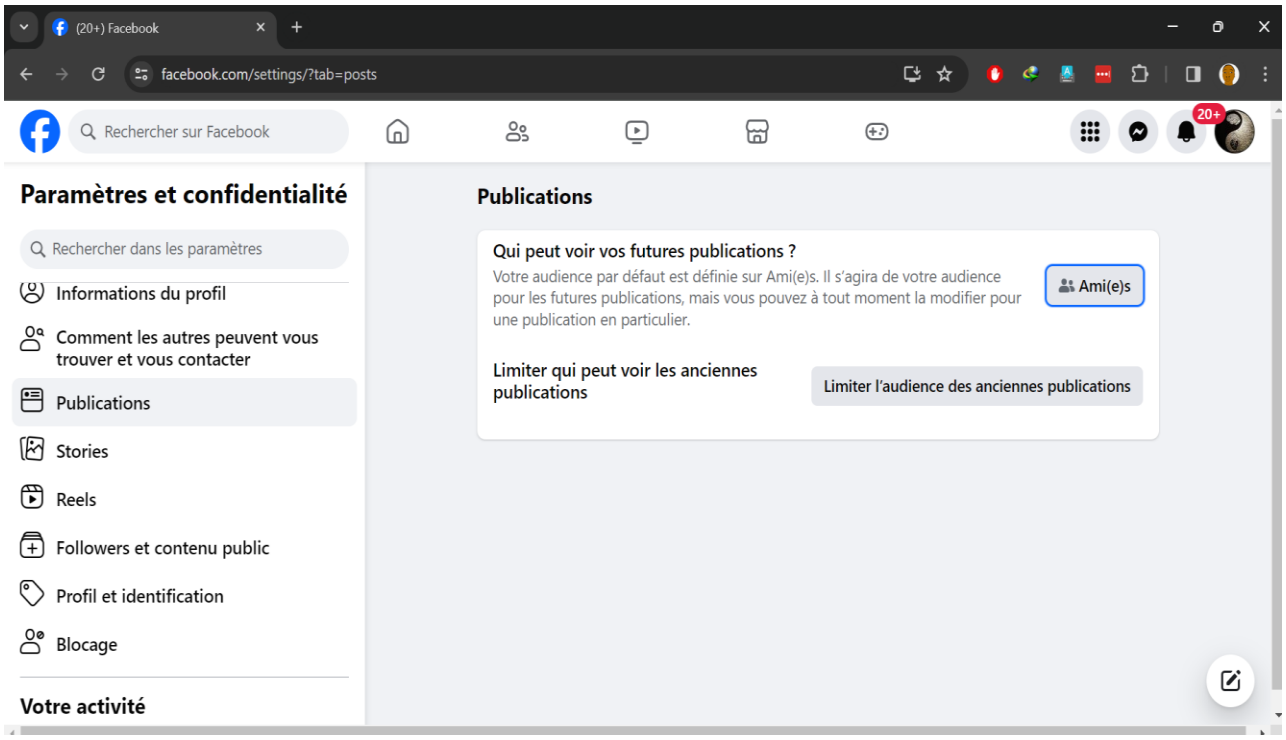
- la navigation privée est utile pour maintenir la confidentialité en ligne, éviter le suivi publicitaire, protéger les informations personnelles et naviguer discrètement sur des appareils partagés.

8 – Principes de base de la confidentialité des médias sociaux

Objectif : Régler les paramètres de confidentialité de Facebook

Réponse





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 ???

Exercice 1 : Simulation de phishing par e-mail

Scénario : Envoyez un e-mail fictif simulant une communication officielle provenant d'une institution financière ou d'un service en ligne. Indiquez une situation urgente nécessitant une action immédiate, telle que la mise à jour d'un mot de passe.

Objectif : Demandez aux participants de reconnaître les signaux d'arnaque dans l'e-mail, tels que des fautes d'orthographe, des liens suspects ou une pression pour agir rapidement. Encouragez-les à vérifier l'adresse e-mail de l'expéditeur et à ne pas cliquer sur les liens, mais plutôt à accéder au site directement via le navigateur.

Débriefing : Discutez des indices qui ont permis de détecter l'arnaque, soulignant l'importance de la prudence lors de la réception d'e-mails inattendus.
Exercice 2 : Reconnaissance des sites non sécurisés

Scénario : Proposez une liste de liens vers des sites web. Certains sont sécurisés (https) et d'autres non (http).

Objectif : Demandez aux participants de distinguer les sites sécurisés des sites non sécurisés en examinant l'URL. Encouragez-les à identifier les signaux de sécurité, tels que le cadenas dans la barre d'adresse.

Débriefing : Discutez des moyens de reconnaître la sécurité d'un site web, soulignant l'importance de ne fournir des informations sensibles que sur des sites sécurisés.

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

Pour un exercice d’installation et d’utilisation d’un antivirus et d’un antimalware, commencez par choisir un logiciel adapté à votre appareil (Windows, Mac, Android, iOS). Téléchargez le logiciel à partir du site officiel ou du magasin d’applications de votre appareil. Suivez les instructions d’installation, qui comprennent généralement l’acceptation des termes et conditions, la sélection du type d’installation (standard ou personnalisée), et la configuration des paramètres de protection. Une fois installé, ouvrez le logiciel et effectuez une analyse initiale de votre appareil pour détecter les menaces potentielles. Ensuite, configurez les paramètres de l’antivirus et de l’antimalware pour des analyses régulières et automatiques. Assurez-vous de garder le logiciel à jour pour une protection optimale.