



Parcours : DISCOVERY

Module : Naviguer en toute Sécurité

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

Faite par ZAFINDRAMBOHO Eddy Sergio

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. Pense à vérifier la source des informations et essaie de consulter des articles récents pour que les informations soient à jour. Saisis le nom du site et de l'article.

- Article 1 = nom du site - nom de l'article
- Article 2 = nom du site - nom de l'article
- Article 3 = nom du site - nom de l'article

Réponse :

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

- Article 1 = Kaspersky- 6 conseils pour renforcer votre sécurité en ligne en 2023
- Article 2 = cybermalveillance.gouv- Comment se protéger sur Internet?
- Article 3 = lejde.be- Safer Internet Day: 5 conseils pour surfer en toute sécurité
- Article bonus = codeur - 6 étapes pour sécuriser son site en 2023

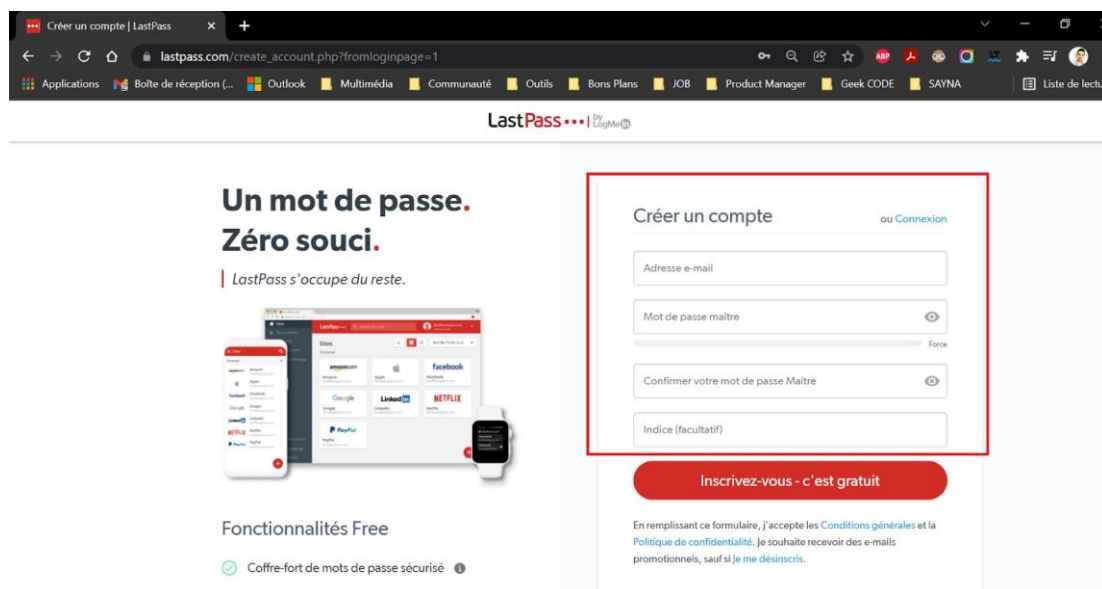
Ravie de vous partager ces articles.

2 - Créer des mots de passe forts :

Objectif : *utiliser un gestionnaire de mot de passe LastPass*

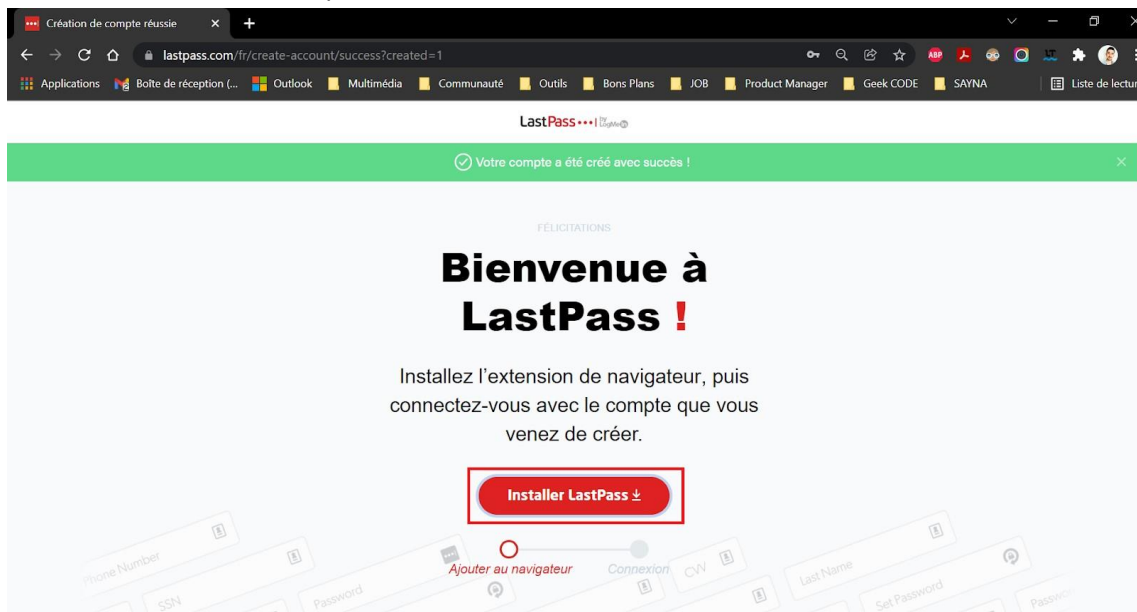
1/ Dans cet exercice, nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Ce gestionnaire prend la forme d'une application web, accessible sur tous supports (PC, Mac, mobile). Il est simple à prendre en main et propose un niveau de sécurité optimal. Suis les étapes suivantes. (Case à cocher)

- ✓ Accède au site de Listas avec ce lien

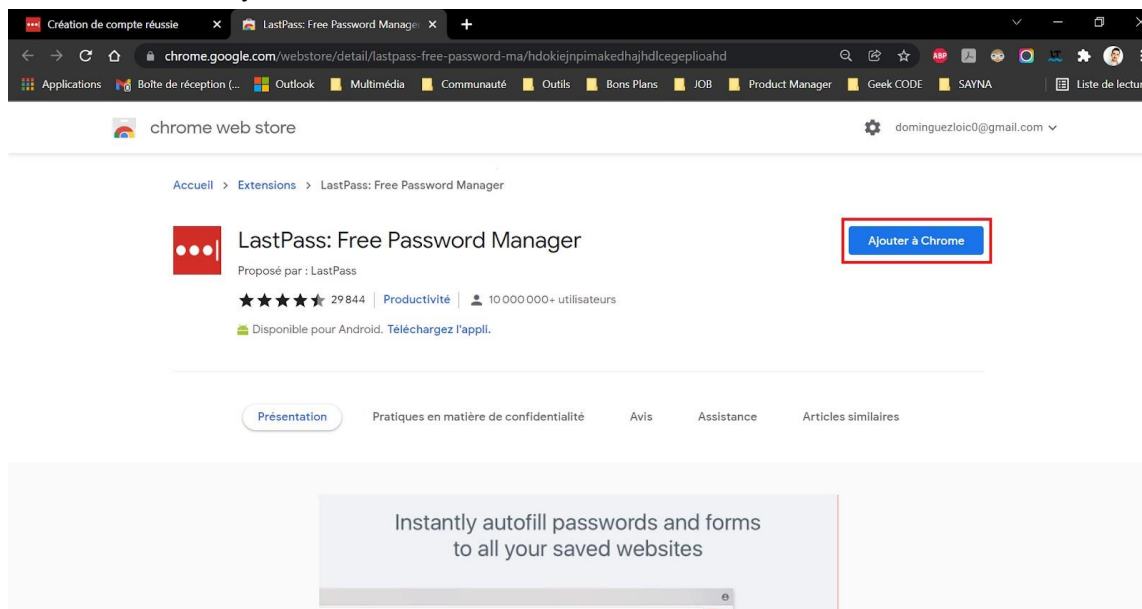
The image is a screenshot of a web browser displaying the LastPass website. The browser's address bar shows the URL 'lastpass.com/create_account.php?fromloginpage=1'. The website has a dark header with the LastPass logo and navigation links. The main content area is divided into two sections. On the left, there's a promotional graphic with the text 'Un mot de passe. Zéro souci.' and 'LastPass s'occupe du reste.' Below this, it lists 'Fonctionnalités Free' including 'Coffre-fort de mots de passe sécurisé'. On the right, there's a 'Créer un compte' (or 'Connexion') form. The form includes fields for 'Adresse e-mail', 'Mot de passe maître' (with a strength indicator), 'Confirmer votre mot de passe Maître', and an optional 'Indice (facultatif)'. A red rectangular box highlights the 'Mot de passe maître' and 'Confirmer votre mot de passe Maître' fields. Below the form is a red button that says 'Inscrivez-vous - c'est gratuit'. At the bottom, there's a small disclaimer about accepting terms and conditions.


- ✓ Crée un compte en remplissant le formulaire. Un conseil, on te demande de choisir un mot de passe maître. Pour rappel, ce mot de passe sera unique et te permettra d'accéder à tous tes comptes. Choisis donc un mot de passe avec un niveau de sécurité élevé et assure-toi de pouvoir le retrouver

- 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

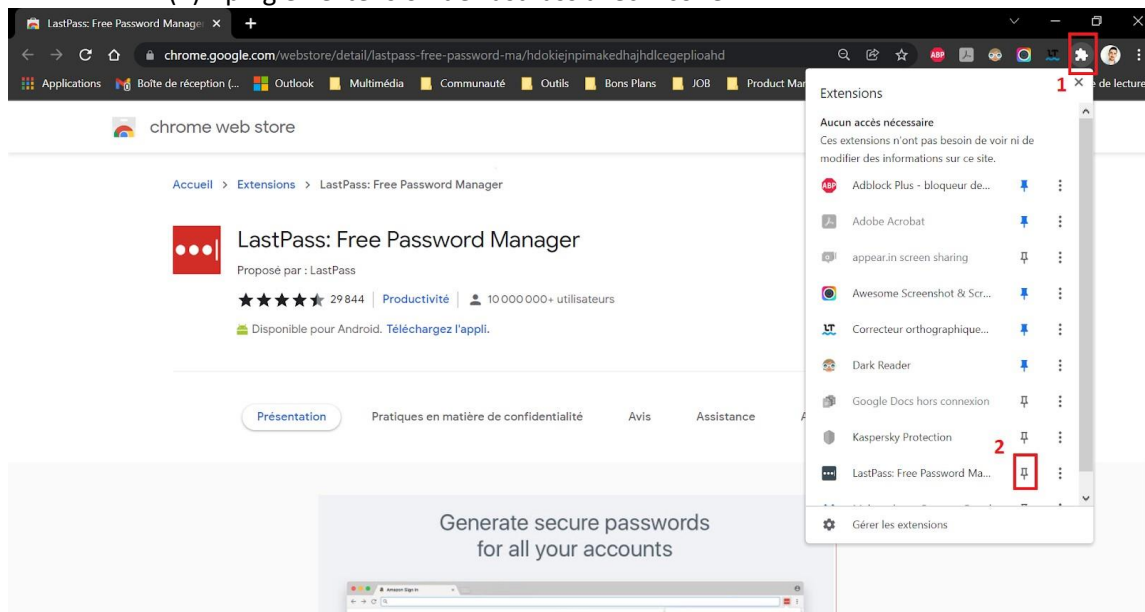


- ✓ Il te suffit de valider l’opération sur le Chrome Web Store en effectuant un clic sur le bouton “Ajouter à Chrome”

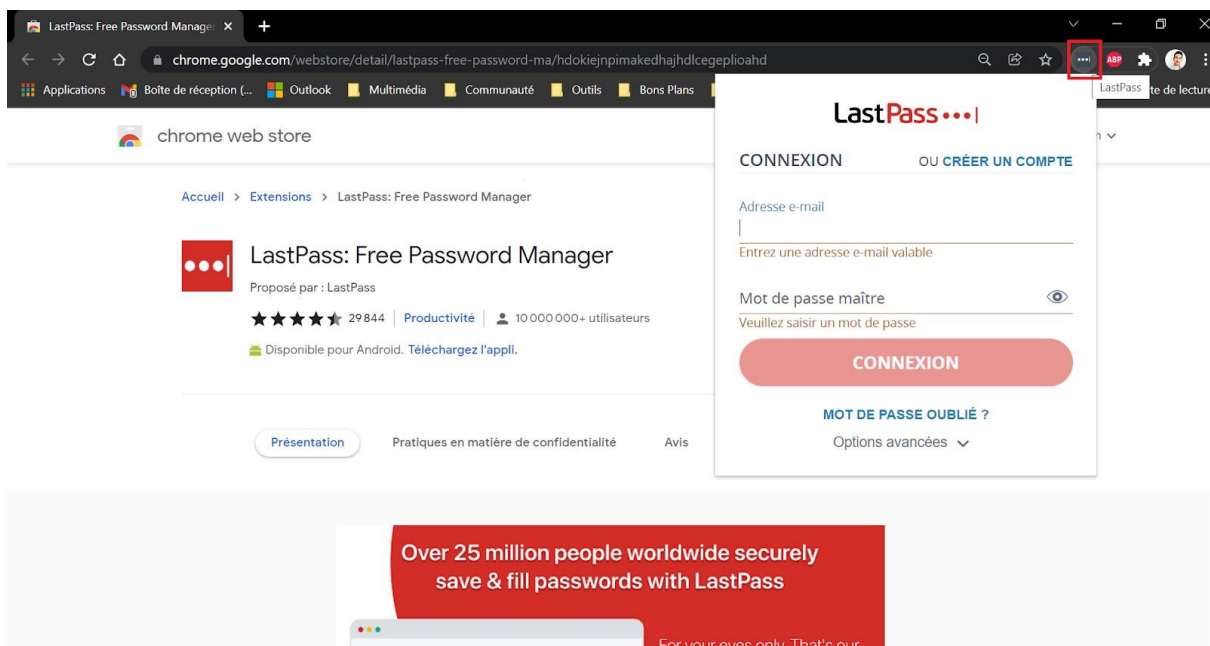


- ✓ Une fois installé, il te suffit d’accéder à cette extension et de t’y connecter
 - (1) En haut à droite du navigateur, clic sur le logo “Extensions” 

o (2) Épingler l'extension de LastPass avec l'icône

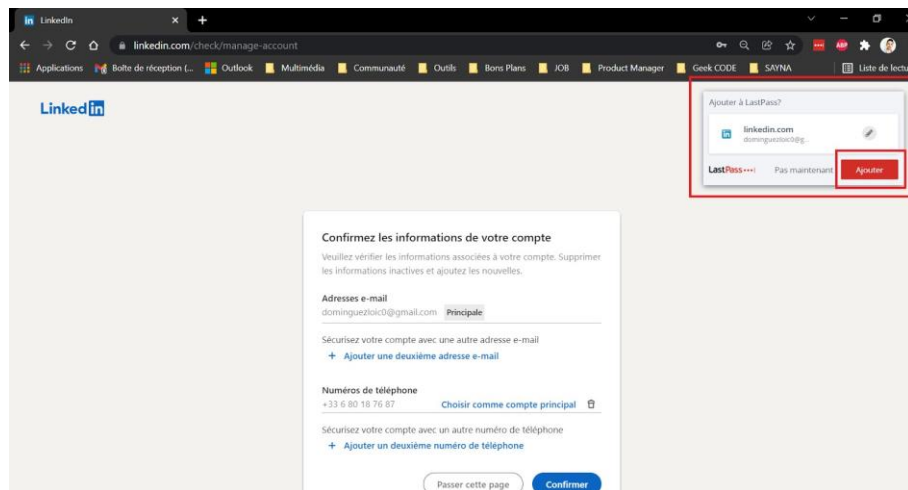


o Il ne te reste plus qu'à te connecter en effectuant un clic sur l'icône de l'extension et en saisissant ton identifiant et mot de passe

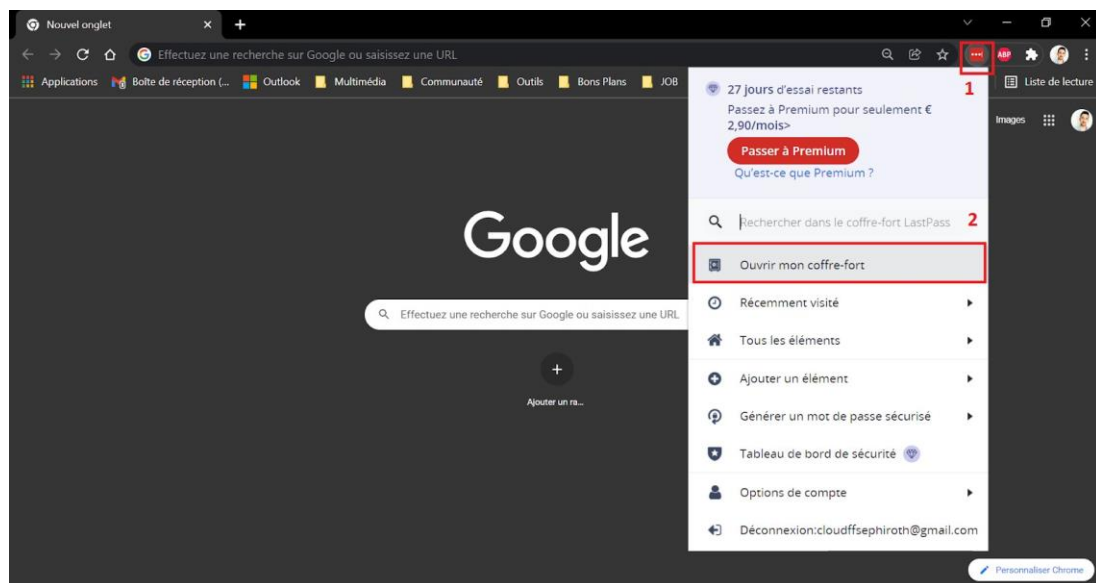


Réponse :

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

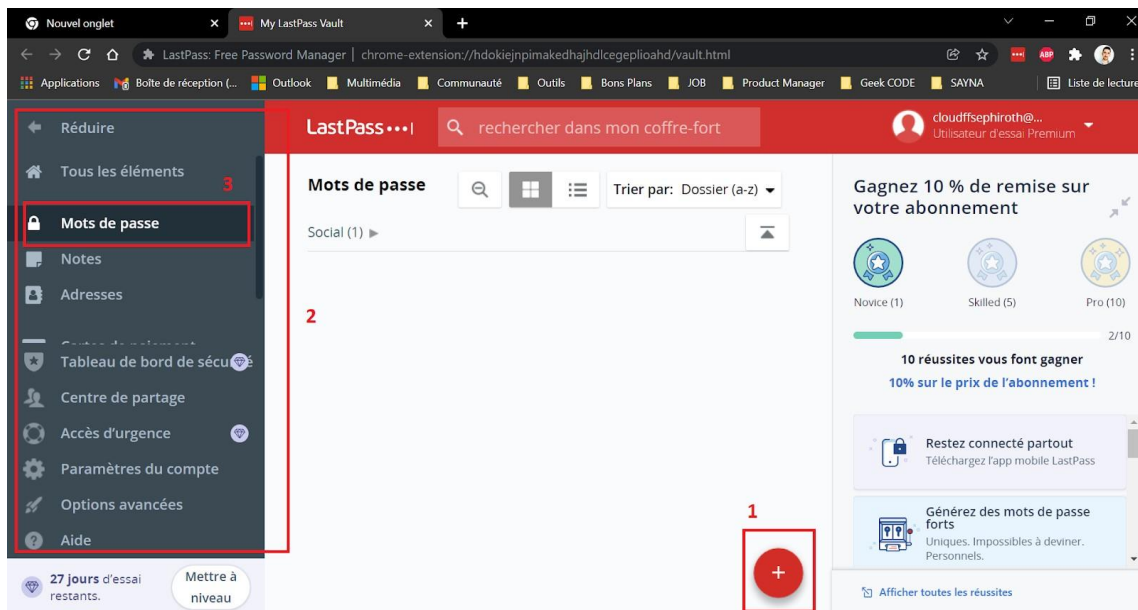


Tu peux également ajouter des comptes manuellement en accédant au coffre-fort, espace de stockage de tous tes mots de passe. Pour y accéder, clic sur l'icône de l'extension puis sur "Ouvrir mon coffre-fort".

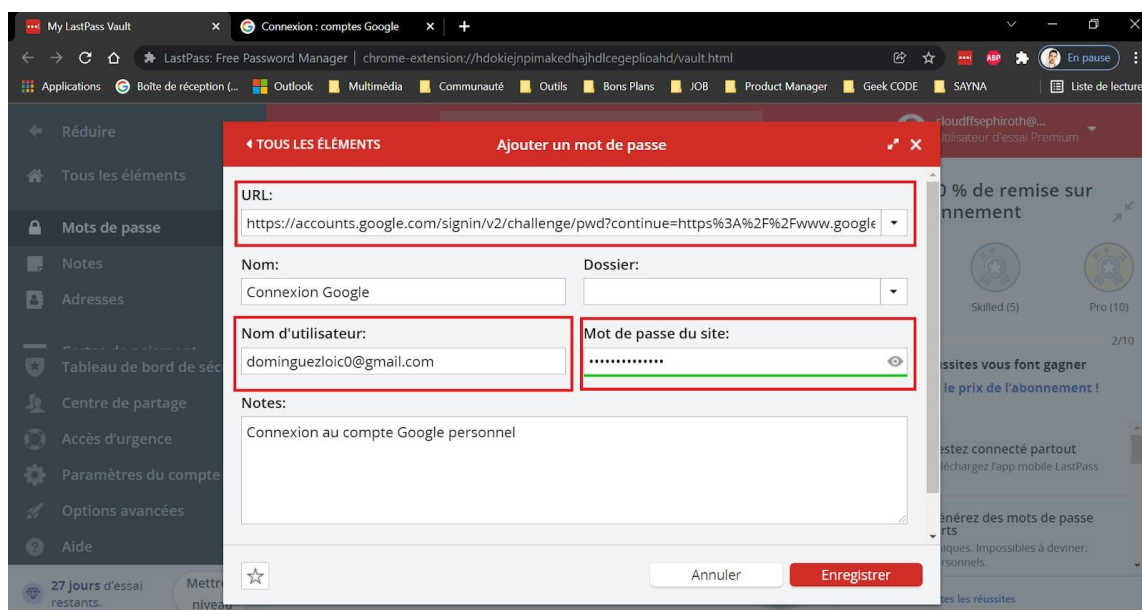


Tu arrives alors sur une page de gestion de ton compte Listas. Pour ajouter un site et une connexion associée (identifiant + mot de passe), accède à la rubrique "Mot de passe"

(2) et (3) puis clic sur "Ajouter un élément" (1).



Une fenêtre s'ouvre pour y insérer toutes les informations à retenir pour automatiser la prochaine connexion. LastPass demande l'URL du site en question ; on conseille de mettre l'URL de la **page de connexion du site**. Ensuite préciser l'id et le mot de passe. On peut personnaliser le nom, un commentaire associé ou encore un dossier si besoin.



Tu connais maintenant les grandes lignes de l'utilisation du gestionnaire de mot de passe Listas.

Pour aller plus loin :

L'abonnement gratuit (fermium) te permet de faire les tâches principales. Si tu trouves cet outil incontournable, tu peux passer au compte premium. Il te permettra notamment de synchroniser ton compte Listas sur tous les supports utilisés.

- Comparatif des gestionnaires de mot de passe :

<https://www.clubic.com/application-web/article-854952-1-gestionnaires-mots-meilleur-logiciel-gratuit-windows.html>

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. (Case à cocher)

- www.morvel.com
- www.dccomics.com
- www.ironman.com
- www.fessebook.com
- www.instagram.com

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

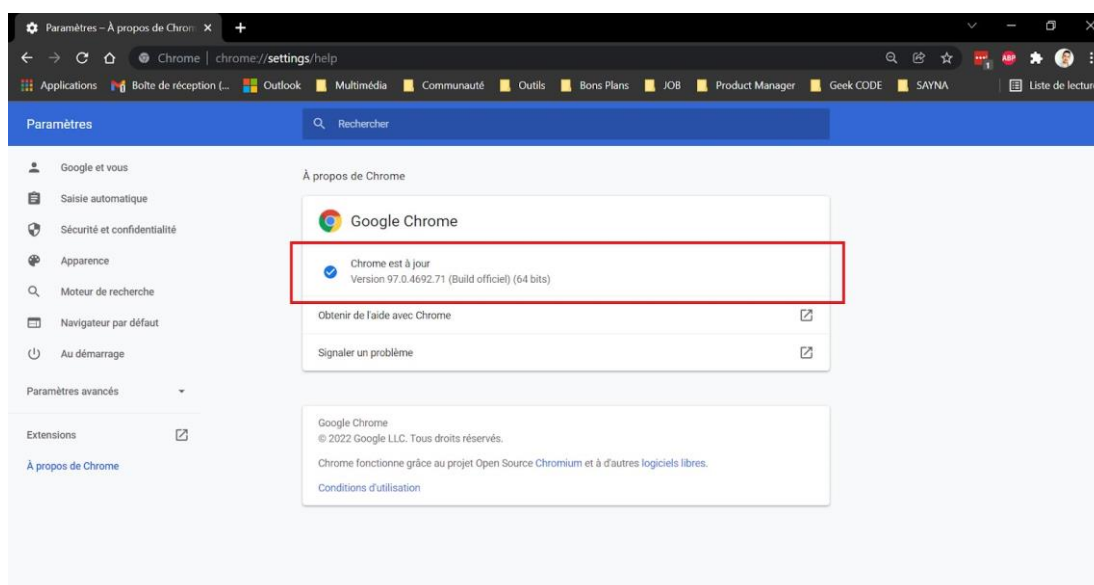
Les seuls sites qui semblaient être cohérents sont donc :

- 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 les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes. (Case à cocher)

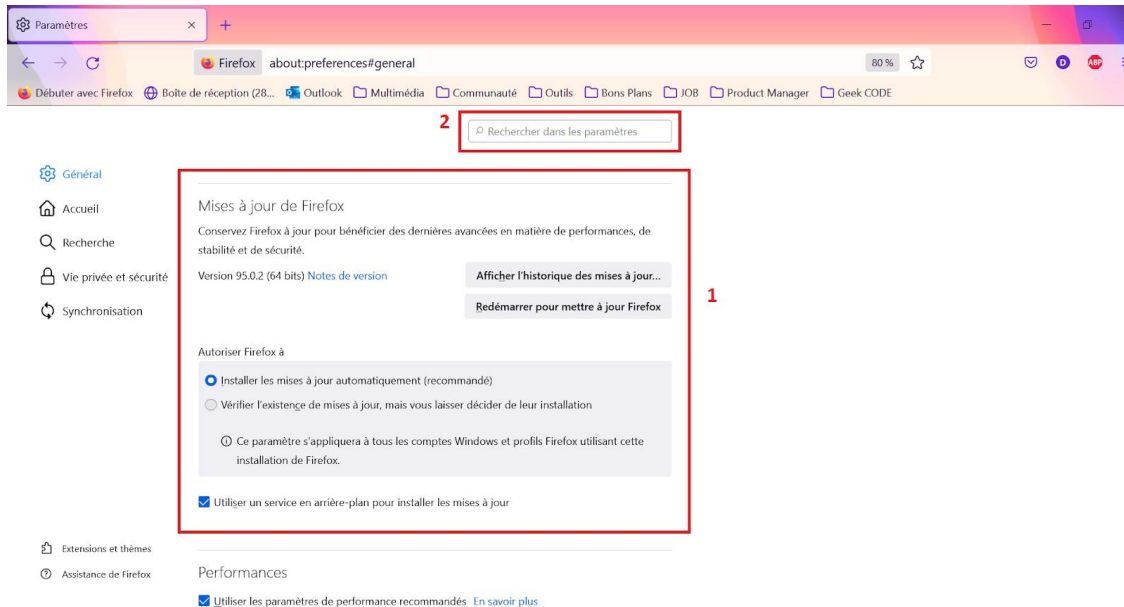
✓ Pour Chrome

- Ouvre le menu du navigateur  et accède aux "Paramètres"
- Clic sur la rubrique "À propos de Chrome"
- Si tu constates le message "Chrome est à jour", c'est Ok



✓ 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

Réponse :

Comme tu as pu le constater, les paramètres par défaut de ces deux navigateurs sont réglés pour réaliser les mises à jour automatiquement. Comme d’habitude, Firefox affiche une personnalisation des paramètres un peu plus poussée.

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.

Réponse :

Tu veux réessayer pour continuer à t’exercer, c’est possible ! Tu peux également consulter des ressources annexes pour t’exercer.

Pour aller plus loin :







- Site du gouvernement [cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr)
<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage>

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 Transparency des Informations (en français). Afin d'améliorer ta lecture de la sécurité sur internet, tu vas devoir analyser les informations de plusieurs sites. Pour chaque site tu devras préciser l'indicateur de sécurité et le rapport d'analyse de l'outil Google. Il te suffit d'accéder aux liens proposés ci-dessous pour observer l'indicateur de sécurité et de copier-coller l'URL du site dans l'outil Google. (Choix multiples)

- Site n°1
 - **Indicateur de sécurité**
 - HTTPS 
 - HTTPS Not sécurée 
 - Not sécurée
 - **Analyse Google**
 - Aucun contenu suspect
 - Vérifier un URL en particulier
- Site n°2
 - **Indicateur de sécurité**
 - HTTPS 
 - HTTPS Not sécurée 
 - Not sécurée
 - **Analyse Google**
 - Aucun contenu suspect
 - Vérifier un URL en particulier
- Site n°3
 - **Indicateur de sécurité**
 - HTTPS 
 - HTTPS Not sécurée 
 - Not sécurée ○
 - **Analyse Google**
 - Aucun contenu suspect

■ Vérifier un URL en particulier

- Site n°4 (site non sécurisé)

Réponse :

- Site n°1 : <https://www.baidu.com/>
 - **Indicateur de sécurité**
 - HTTPS 
 - **Analyse Google**
 - Vérifier un URL en particulier
- Site n°2 : <http://xinhuanet.com/>
 - **Indicateur de sécurité**
 - Not secure
 - **Analyse Google**
 - Aucun contenu suspect
- Site n°3 : <http://myshopify.com/>
 - **Indicateur de sécurité**
 - Not secure
 - **Analyse Google**
 - Vérifier un URL en particulier (analyse trop générale)

J'ai testé les sites de ce lien. Ce site référence et explique les défauts de sécurité des sites dans le monde.

6 - Achats en ligne sécurisés :

Objectif : *créer un registre des achats effectués sur internet*

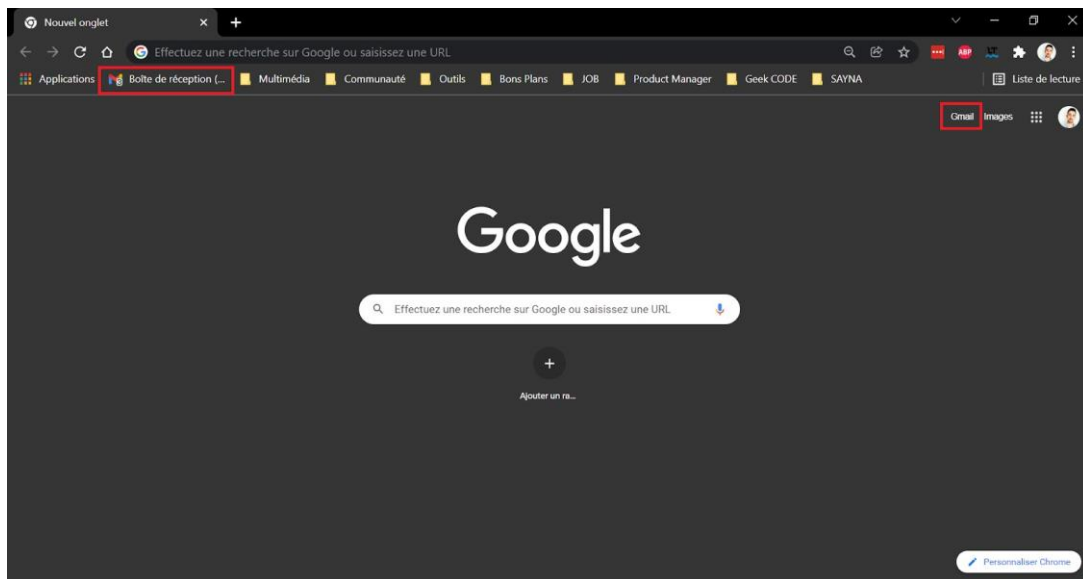
1 / Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le bilan de tes dépenses du mois.

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

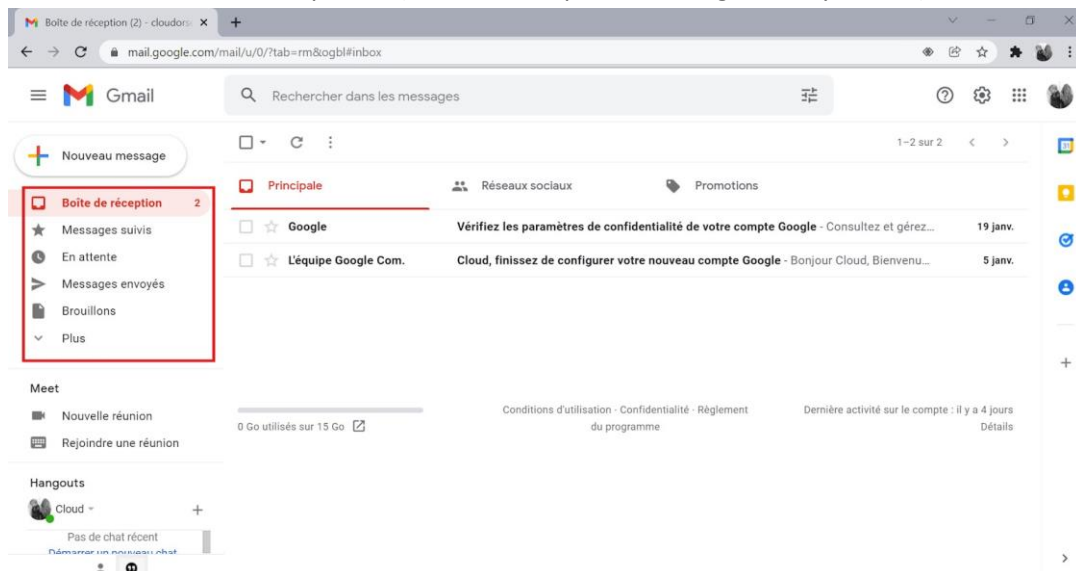
1. **Créer un dossier sur ta messagerie électronique**
2. **Créer un dossier sur ton espace de stockage personnel (en local ou sur le cloud)**

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)

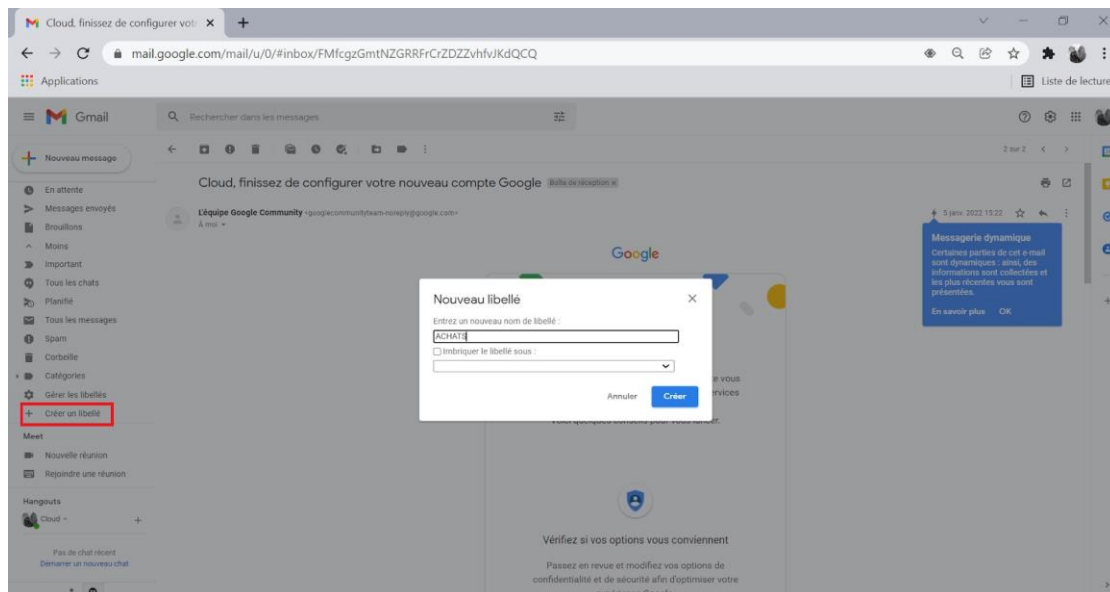
- Pour commencer, accède à ta messagerie électronique. Pour rappel, tu peux y accéder rapidement en ouvrant un nouvel onglet (dans la barre des favoris ou via le raccourci)



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

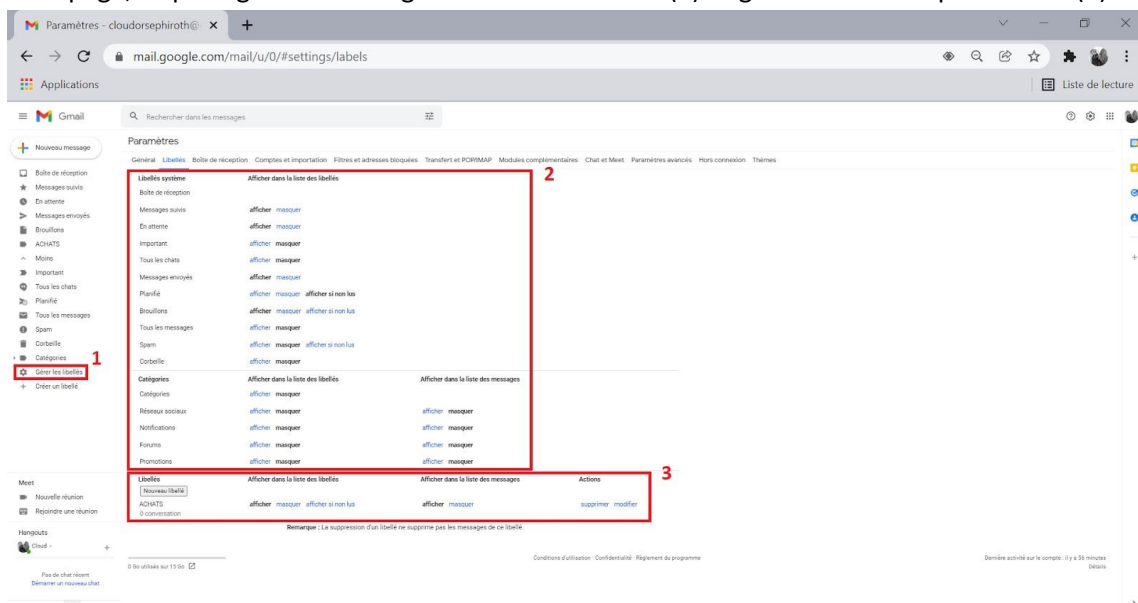


- C'est dans cette partie que tu vas créer ta rubrique des achats. Pour ce faire, clic sur "Plus" et va tout en bas des libellés. Pour créer un libellé rapidement il te suffit d'effectuer un clic sur "Créer un libellé" et de le nommer "ACHATS" (pour notre exercice)



- 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

Réponse :

Voici un exemple d’organisation de libellé pour gérer sa messagerie électronique :

Achats : historique, facture, conversations liés aux achats

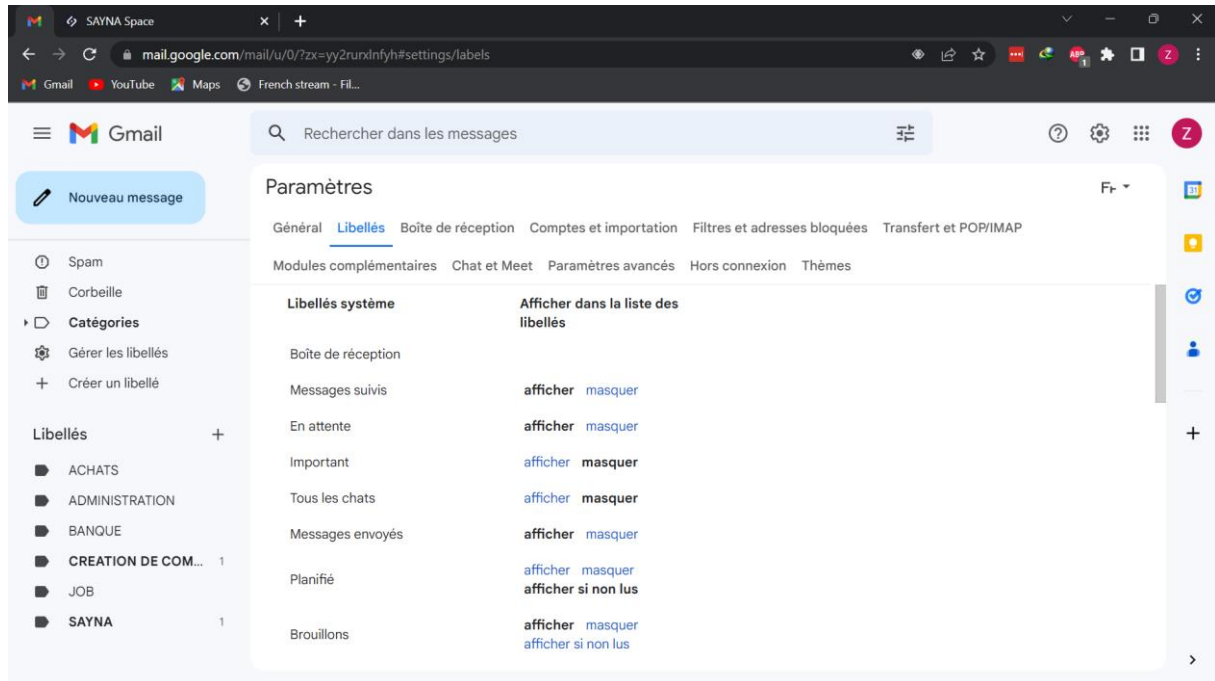
Administratif : toutes les démarches administratives

Banque : tous les documents et les conversations liés à la banque personnelle

Création de compte : tous les messages liés à la création d’un compte (message de bienvenue, résumé du profil, etc.)

Job : tous les messages liés à mon projet professionnel

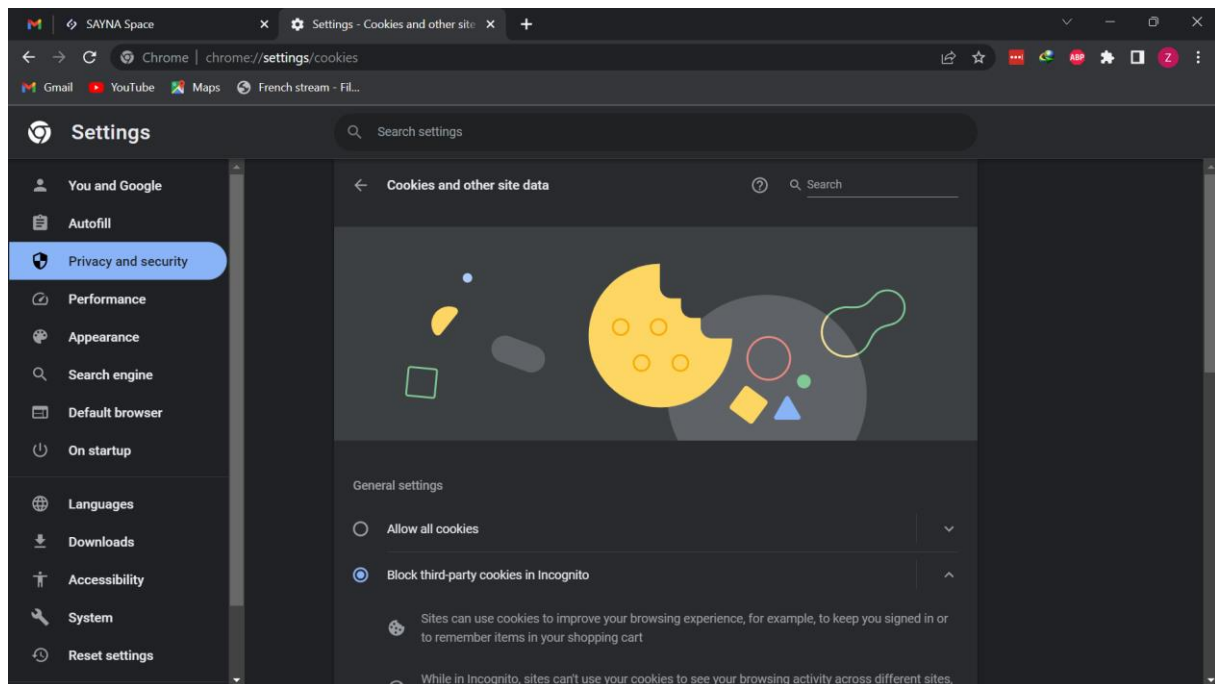
SAYNA : tous les messages liés mon activité avec SAYNA



7 - Comprendre le suivi du navigateur :

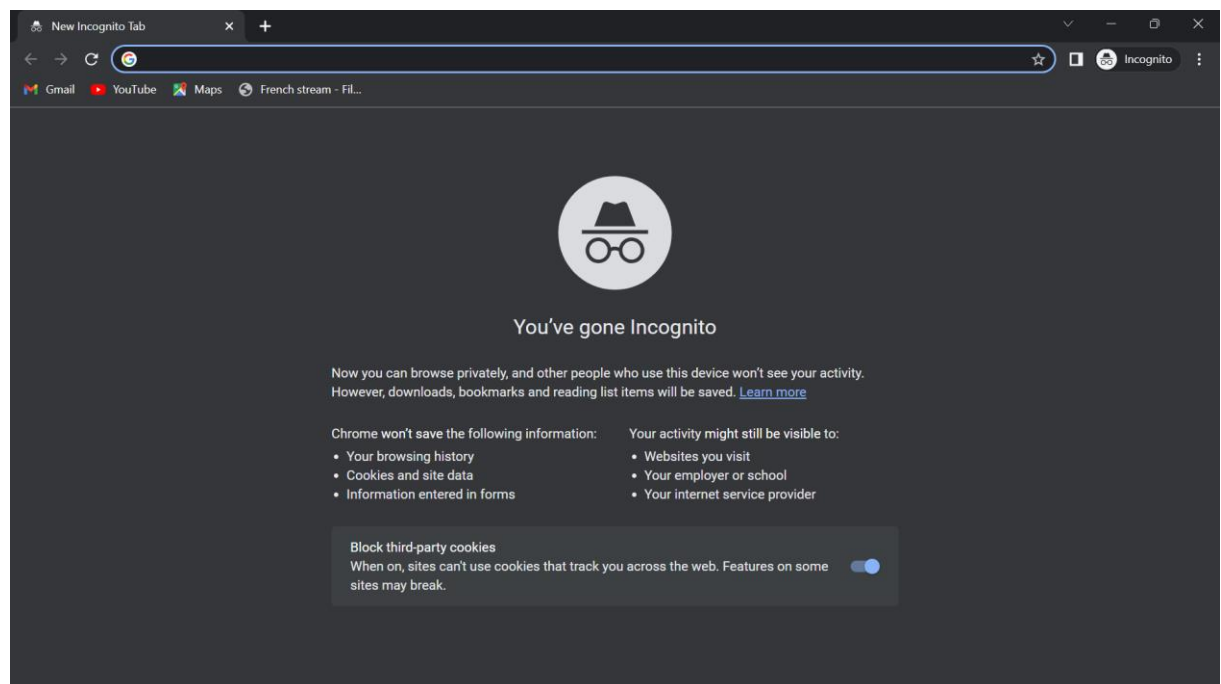
Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée

- La gestion de cookies : limite ou de contrôler les informations que les sites veulent enregistrer pour une meilleure interaction entre le site et l'utilisateur. Ces informations peuvent être votre identifiant client auprès d'un site marchand, le contenu courant de votre panier d'achat, la langue d'affichage de la page web, un identifiant permettant de tracer votre navigation à des fins statistiques ou publicitaires, etc.



C'est là que se trouve les paramètres de cookies pour mieux les gérer sur Chrome.

- La navigation privée : Le navigateur que vous utilisez n'enregistre pas votre historique de navigation ni vos cookies, vos données de sites ou les informations saisies dans les formulaires. Les fichiers que vous téléchargez et les favoris que vous créez sont conservés.




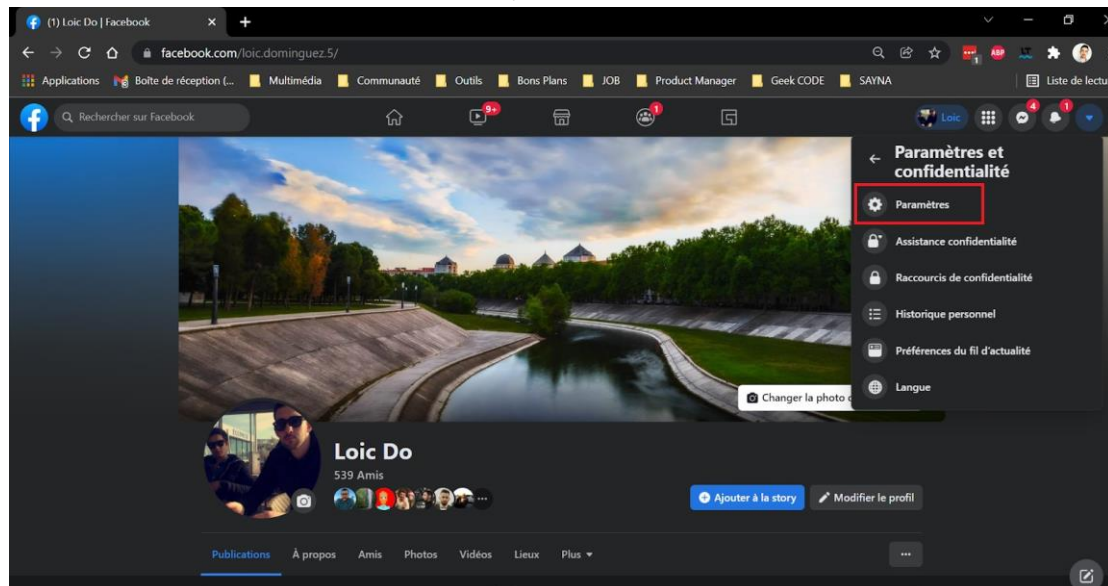
La navigation privée ressemble à ça sur chrome. On peut remarquer la petite image de chapeau avec une lunette en haut à droite de l'écran pour désigner que vous êtes en mode navigation privée.

8 - Principes de base de la confidentialité des médias sociaux :

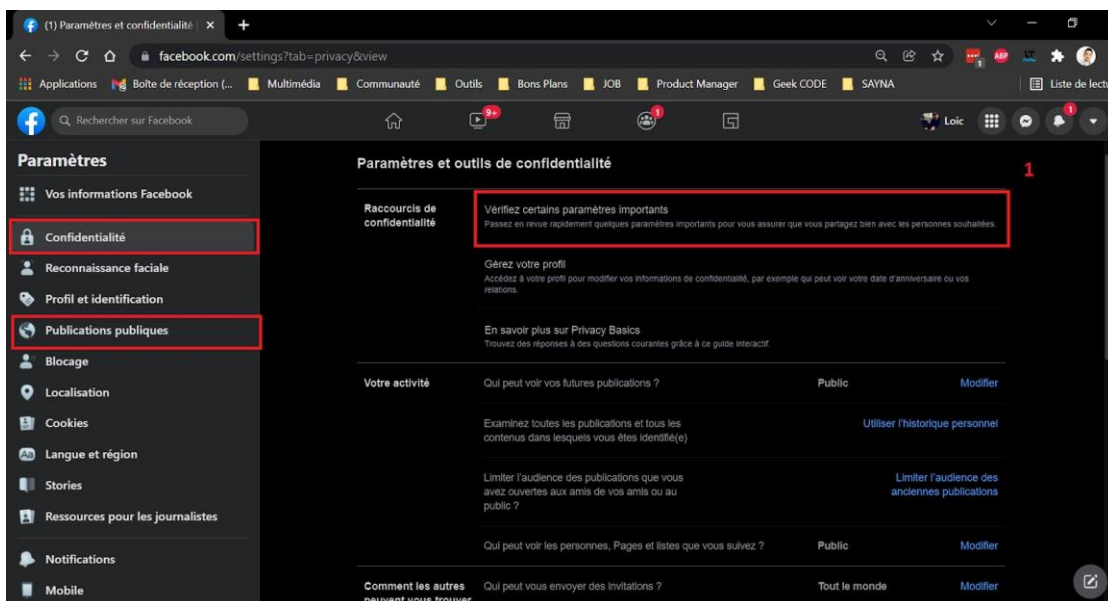
Objectif : *Régler les paramètres de confidentialité de Facebook*

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. (Case à cocher)

- 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"



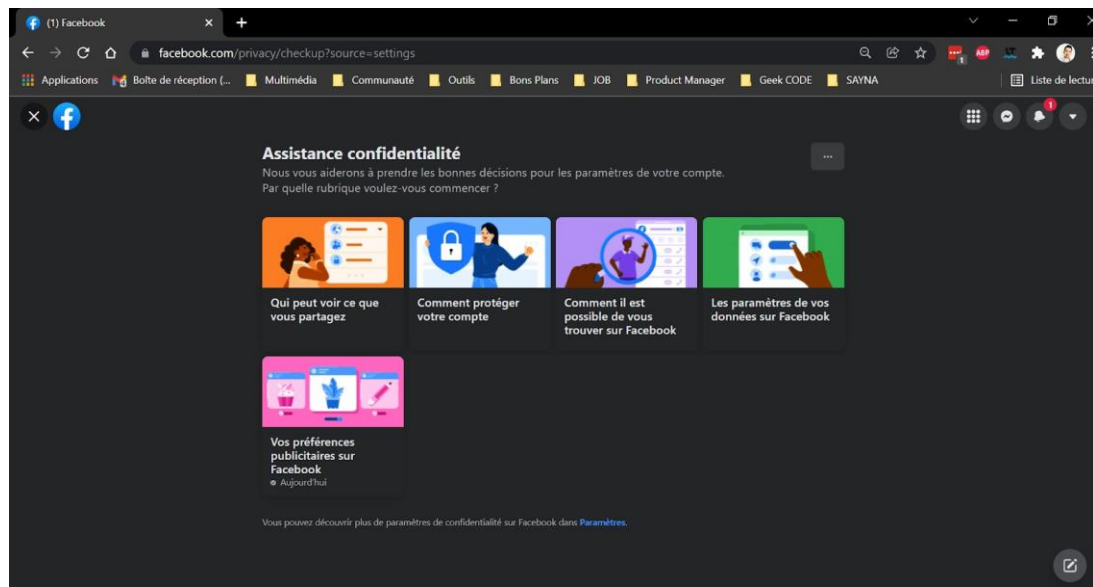
✓ Ce sont les onglets "Confidentialité" et "Publications publiques" qui nous intéressent. Accède à "Confidentialité" pour commencer et clic sur la première rubrique



✓ Cette rubrique résume les grandes lignes de la confidentialité sur Facebook

- o 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

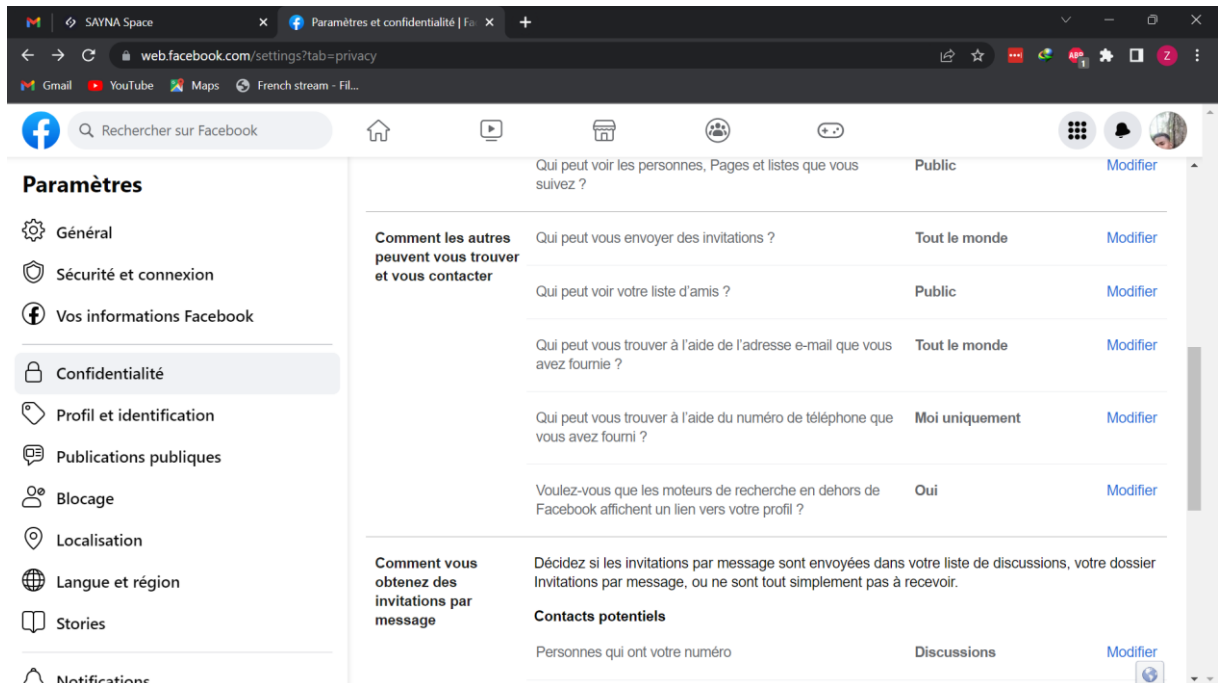


- ✓ Retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à gauche. Tu peux continuer à explorer les rubriques pour personnaliser tes paramètres. On ne peut pas te dire ce que tu dois faire. C'est à toi de choisir les informations que tu souhaites partager et celles que tu veux garder privées. Voici tout de même quelques conseils :
 - Si tu utilises ton compte Facebook uniquement pour communiquer avec tes amis, règle 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 hâter 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.

Réponse :

Voici mes paramétrages de compte Facebook pour une utilisation plus personnalisée :

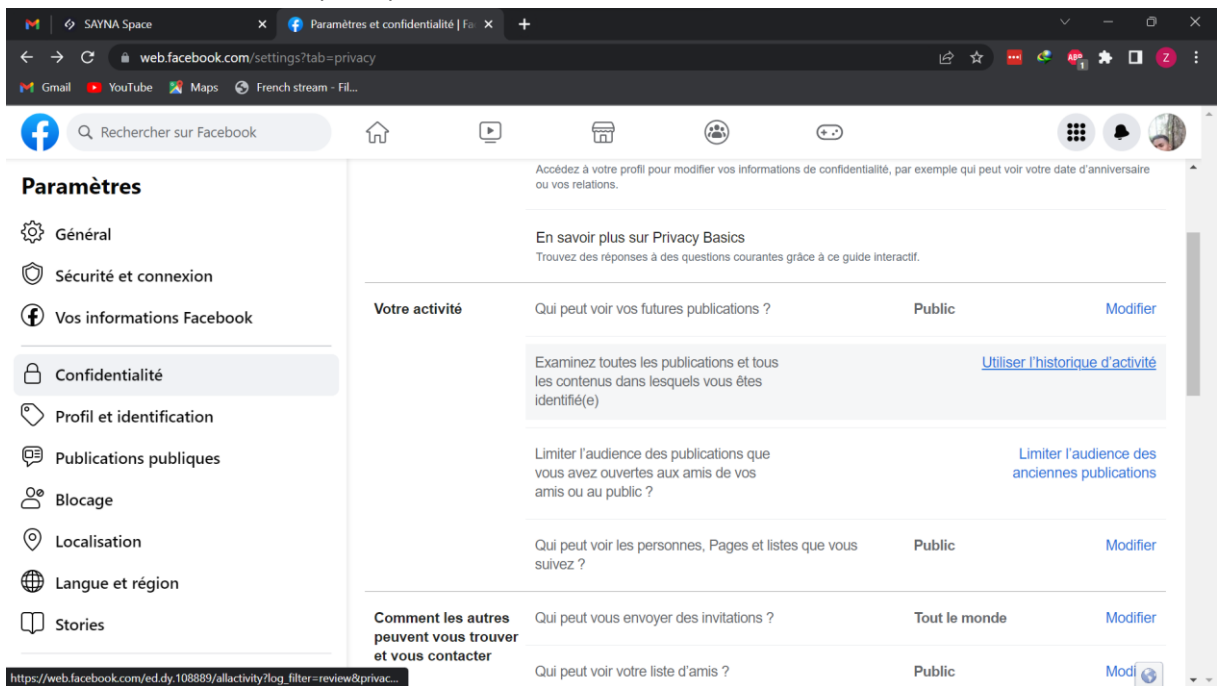
○ Confidentialité



The screenshot shows the Facebook 'Paramètres et confidentialité' (Settings and Privacy) page. The left sidebar lists various settings categories, with 'Confidentialité' (Privacy) selected. The main content area is titled 'Qui peut voir les personnes, Pages et listes que vous suivez ?' (Who can see the people, pages and lists you follow?) and is set to 'Public'. Below this, there are several sections for controlling who can interact with the user's profile:

- Comment les autres peuvent vous trouver et vous contacter** (How others can find and contact you):
 - Qui peut vous envoyer des invitations ? (Who can send you invitations?): Tout le monde (Everyone)
 - Qui peut voir votre liste d'amis ? (Who can see your friends list?): Public
 - Qui peut vous trouver à l'aide de l'adresse e-mail que vous avez fournie ? (Who can find you using the email you provided?): Tout le monde
 - Qui peut vous trouver à l'aide du numéro de téléphone que vous avez fourni ? (Who can find you using the phone number you provided?): Moi uniquement (Only me)
 - Voulez-vous que les moteurs de recherche en dehors de Facebook affichent un lien vers votre profil ? (Do you want search engines outside Facebook to show a link to your profile?): Oui (Yes)
- Comment vous obtenez des invitations par message** (How you get messages):
 - Décidez si les invitations par message sont envoyées dans votre liste de discussions, votre dossier Invitations par message, ou ne sont tout simplement pas à recevoir.
- Contacts potentiels** (Potential contacts):
 - Personnes qui ont votre numéro (People who have your number): Discussions (Discussions)

○ Publications publiques



The screenshot shows the Facebook 'Paramètres et confidentialité' (Settings and Privacy) page, specifically the 'Publications publiques' (Public Posts) section. The left sidebar shows 'Publications publiques' selected. The main content area provides information about public posts and offers options to manage them:

- Accédez à votre profil pour modifier vos informations de confidentialité, par exemple qui peut voir votre date d'anniversaire ou vos relations.** (Access your profile to change your privacy settings, for example who can see your birthday or relationships.)
- En savoir plus sur Privacy Basics** (Learn more about Privacy Basics): Trouvez des réponses à des questions courantes grâce à ce guide interactif.
- Votre activité** (Your activity):
 - Qui peut voir vos futures publications ? (Who can see your future posts?): Public
 - Examinez toutes les publications et tous les contenus dans lesquels vous êtes identifié(e) (Review all posts and content you're tagged in): [Utiliser l'historique d'activité](#)
 - Limiter l'audience des publications que vous avez ouvertes aux amis de vos amis ou au public ? (Limit the audience of posts you've shared with friends of friends or the public?): [Limiter l'audience des anciennes publications](#)
 - Qui peut voir les personnes, Pages et listes que vous suivez ? (Who can see the people, pages and lists you follow?): Public
- Comment les autres peuvent vous trouver et vous contacter** (How others can find and contact you):
 - Qui peut vous envoyer des invitations ? (Who can send you invitations?): Tout le monde
 - Qui peut voir votre liste d'amis ? (Who can see your friends list?): Public

Pour aller plus loin :

Les conseils pour utiliser en toute sécurité les médias sociaux

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

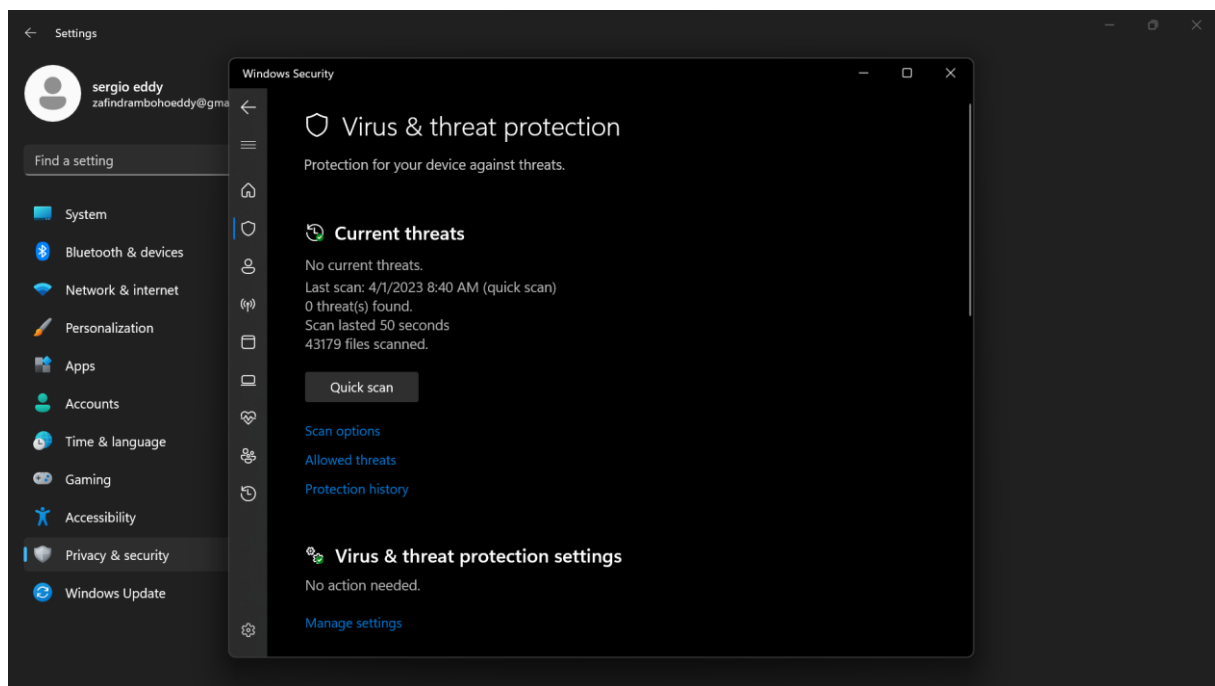
Objectif :

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

- Si vous utilisez Windows 7 ou plus : vous pouvez installer faire un scan de votre ordinateur à partir de Windows Defender.
 - Sélectionner Démarrer > Paramètres > Mise à jour et sécurité > Sécurité Windows, puis Protection contre les virus et menaces.



- Après ça vous entrer dans Ouvrir sécurité Windows pour accéder Windows Defender ou entrer directement dans protection contre les virus et Threats.



- Vous n'aurez qu'à cliquer sur scanne rapide (cela peut prendre quelques minutes) pour vérifier si votre système a des logiciels malveillants intégrés là-dedans ou pas.

Remarque : Si Windows Defender trouve des logiciels malveillants, il va l'effacer et le mettre en quarantaine selon le niveau de gravité de l'impact du logiciel malveillant sur votre système.

- Le plus souvent, et utilisable sur tout type d'appareil, télécharger un logiciel antivirus (il y en a beaucoup qui sont gratuits) et utiliser le pour faire le scan de votre appareil pour trouver les virus qui sont dedans.
 - Pour les ordinateurs (que ça soit Windows ou Mac), vous pouvez utiliser Avast, un logiciel antivirus populaire, gratuit et qui avait fait preuve.

Lien du site officiel de Avast : www.avast.com

Lien pour aller plus loin : <https://www.01net.com/antivirus/antivirus-gratuit/>

- Pour les smartphones et les tablettes (Disponible sur Android et iOS), vous pouvez Bitdefender Mobile Security, un excellent antivirus qui dispose d'une version gratuite.

Lien du site officiel : www.bitdefender.com

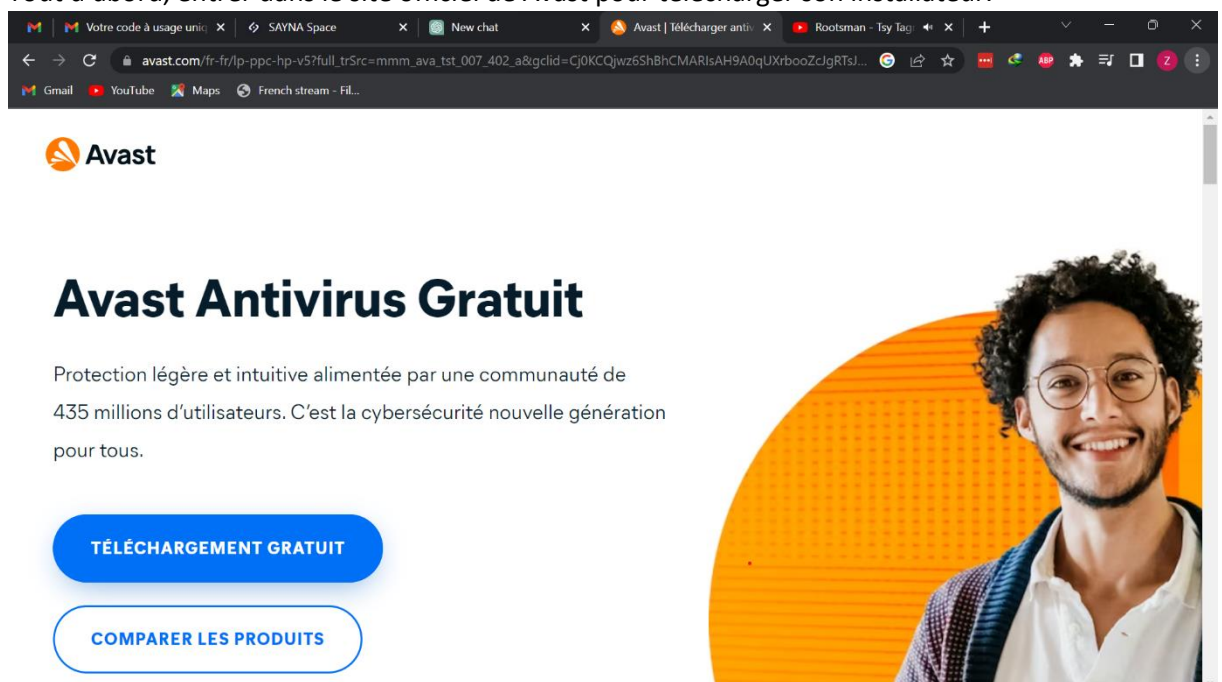
Lien pour aller plus loin :

<https://www.journaldugeek.com/antivirus/android/#:~:text=Le%20meilleur%20antivirus%20Android%20est,option%20pour%20optimiser%20les%20performances.>

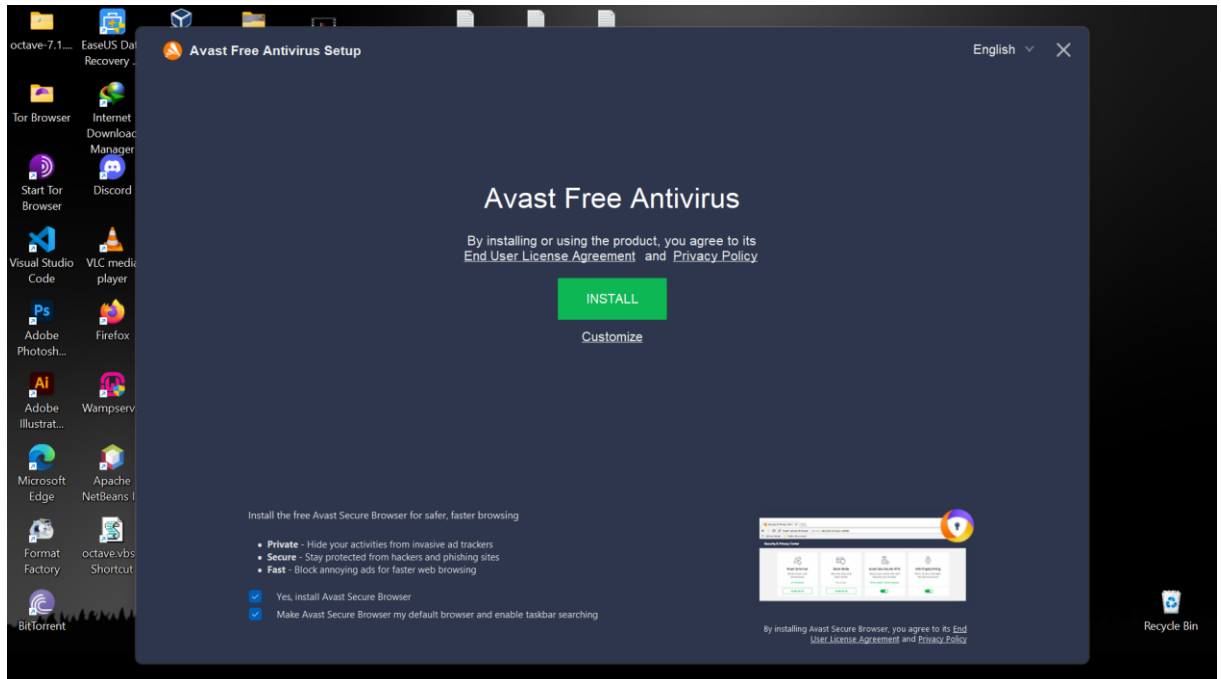
2/ Proposer un exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé.

Je vous propose donc d'installer Avast, un logiciel qui est à la fois un antivirus et un antimalware, disponible sur tout type d'appareil (Windows, Mac, Android, iOS). Aujourd'hui, On va l'installer sur Windows 11.

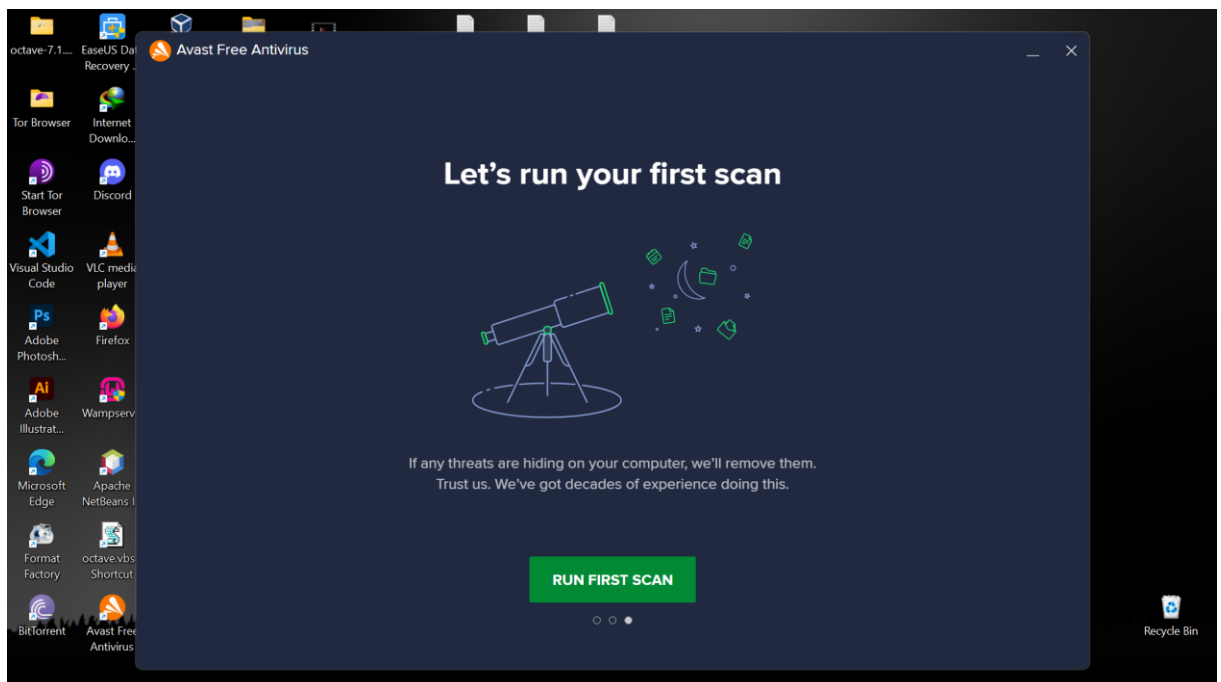
- Tout d'abord, entrer dans le site officiel de Avast pour télécharger son installateur.



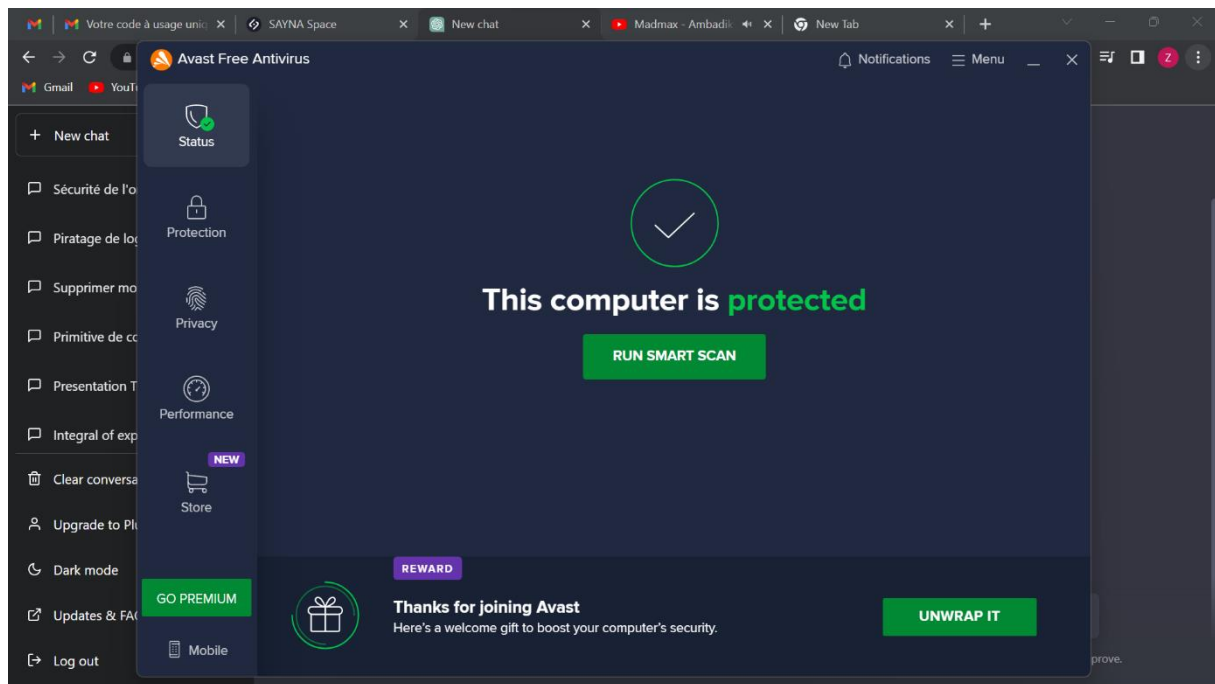
- Appuyer sur téléchargement gratuit pour télécharger l'installateur de Avast. Après ça, exécuter l'installateur un fichier .exe pour installer Avast. L'installation nécessite une connexion internet pour se faire.



- Appuyer sur « install » pour que l'installation commence. Suivez les indications lors de l'installation.



- Lors de la finition il proposera un scan de votre appareil pour trouver les virus, malware et les brèche ou faille dans votre système que les personnes malveillantes peuvent utiliser pour vous nuire.



Et voila l'installation de Avast est terminer et votre appareil est maintenant protégé.

Son utilisation est facile vue que les outils importants comme les scannes et autre sont facile à trouver, il suffit juste de lire.