

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

- 1 - Introduction à la sécurité sur Internet
- 2 - Créer des mots de passe forts
- 3 - Fonctionnalité de sécurité de votre navigateur
- 4 - Éviter le spam et le phishing
- 5 - Comment éviter les logiciels malveillants
- 6 - Achats en ligne sécurisés
- 7 - Comprendre le suivi du navigateur
- 8 - Principes de base de la confidentialité des médias sociaux
- 9 - 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/ En naviguant sur le web, consultez trois articles qui parlent de sécurité sur internet. Pensez à vérifier la source des informations et essayez de consulter des articles récents pour que les informations soient à jour. Saisissez 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 1

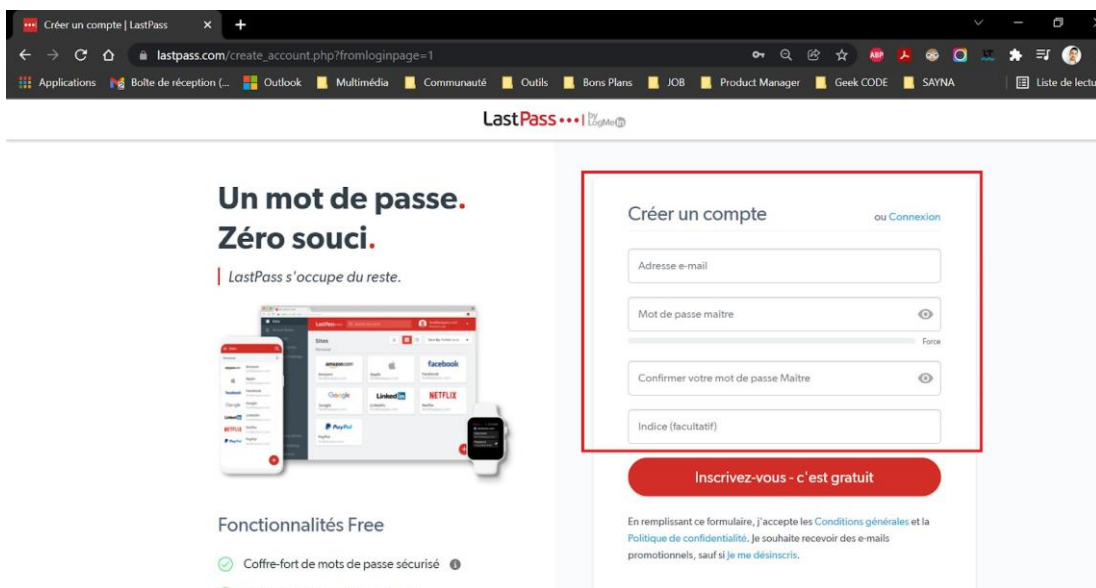
- Article 1 = ISAGRI – 11 règles pour naviguer sur internet en sécurité
- Article 2 = franceinfo -Cybersécurité : pourquoi la fameuse "double authentification" sur Internet n'est plus si sûre que ça ?
- Article 3 = appevise -Cyber Threat Intelligence : apprenez à connaître les menaces informatiques pour mieux les contrer

2 - Créer des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass

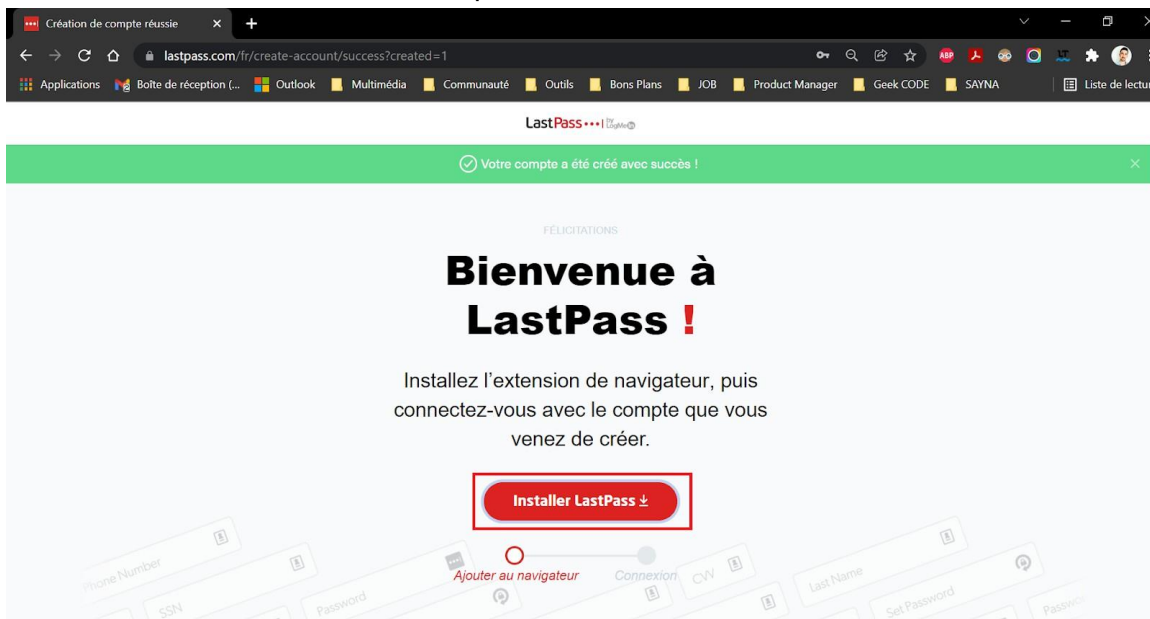
1/ Dans cet exercice, nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Ce gestionnaire prend la forme d'une application web, accessible sur tous supports (PC, Mac, mobile). Il est simple à prendre en main et propose un niveau de sécurité optimal.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

- Accédez au site de LastPass avec ce lien

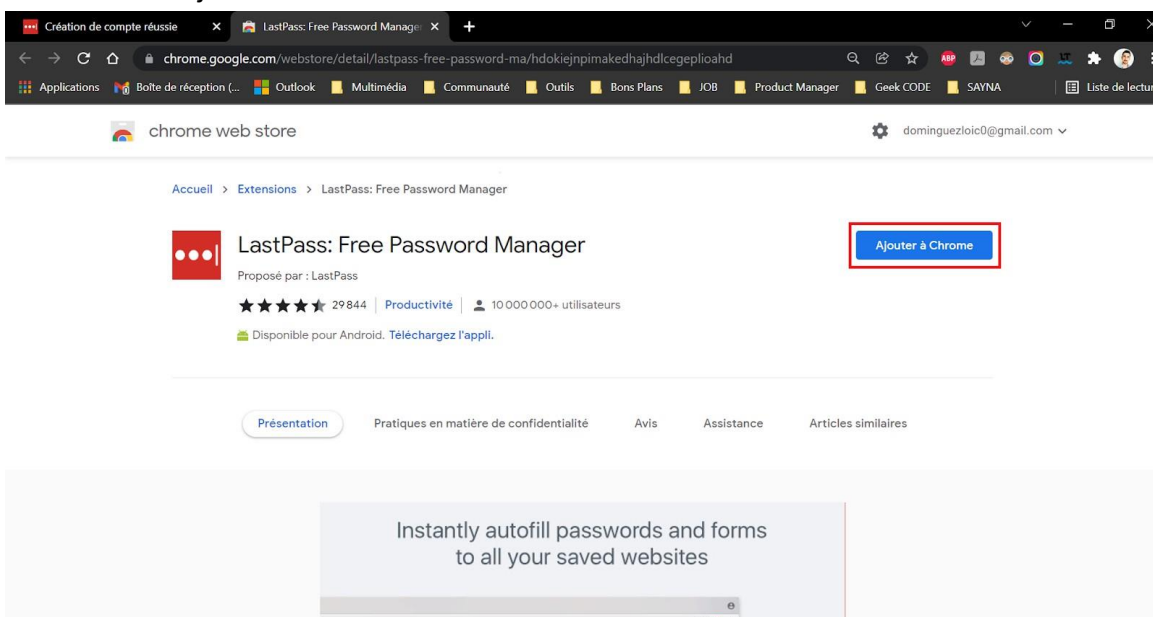


The screenshot shows the LastPass website's account creation page. The browser's address bar displays 'lastpass.com/create_account.php?fromloginpage=1'. The page features the LastPass logo and a navigation bar with links like 'Créer un compte' and 'Connexion'. The main content area is titled 'Un mot de passe. Zéro souci.' and includes a sub-header 'LastPass s'occupe du reste.' Below this, there's a visual representation of the LastPass app on a smartphone and a tablet. To the right, a red-bordered box highlights the 'Créer un compte' form, which contains fields for 'Adresse e-mail', 'Mot de passe maître' (with a strength indicator), 'Confirmer votre mot de passe Maître', and 'Indice (facultatif)'. A red button labeled 'Inscrivez-vous - c'est gratuit' is positioned below the form. At the bottom, a disclaimer states: 'En remplissant ce formulaire, j'accepte les Conditions générales et la Politique de confidentialité. Je souhaite recevoir des e-mails promotionnels, sauf si je me désinscris.'



- 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

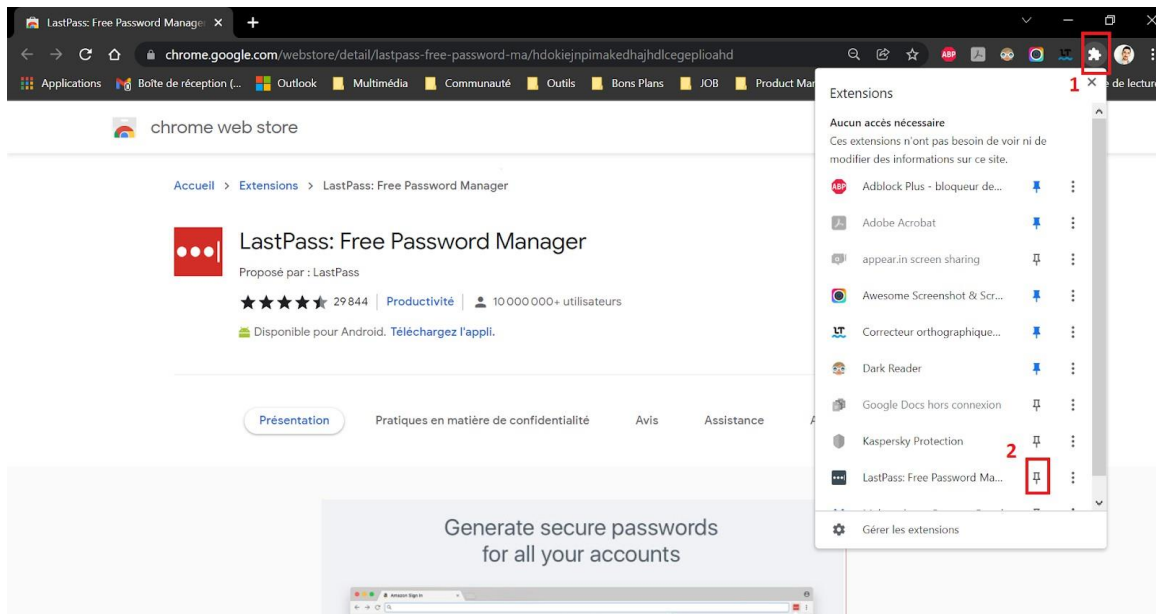


- Il te suffit de valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome"

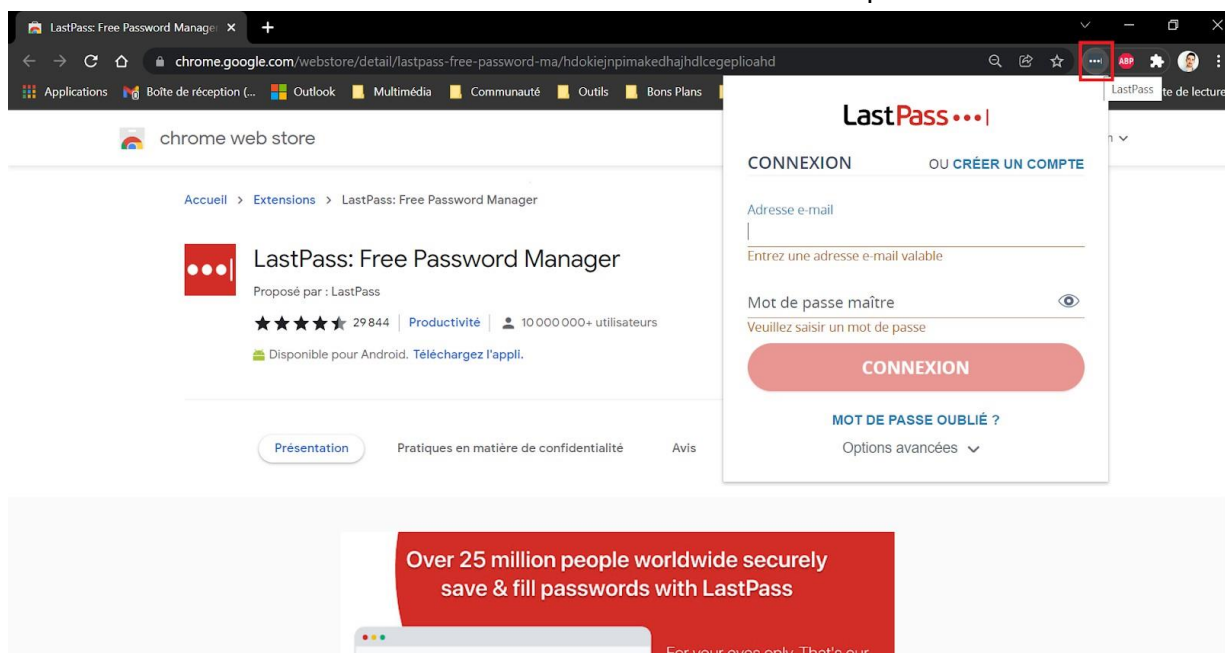


- Une fois installé, il te suffit d'accéder à cette extension et de t'y connecter

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

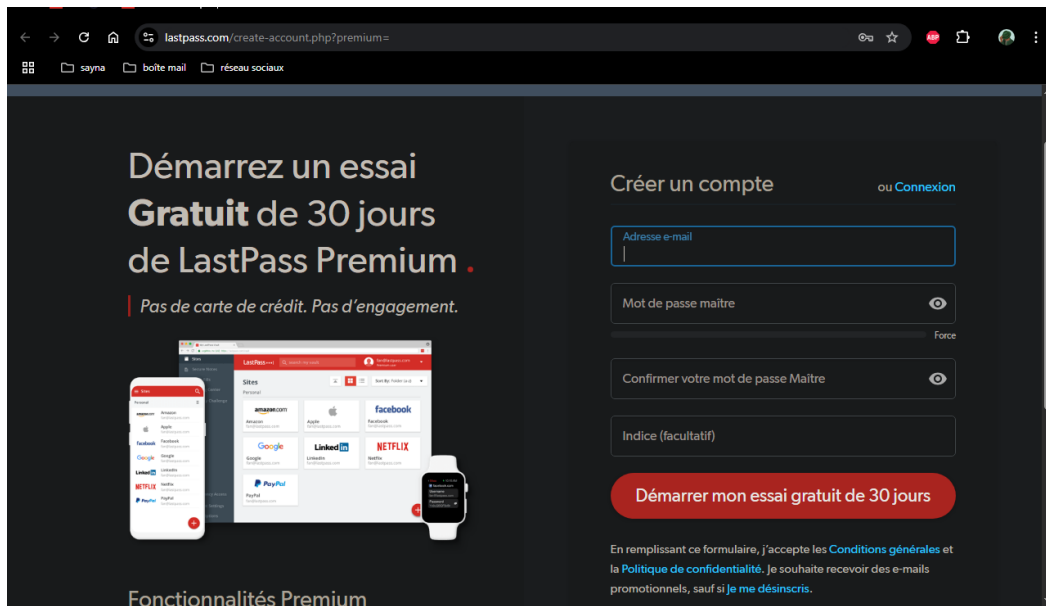


- Il ne te reste plus qu'à te connecter en effectuant un clic sur l'icône de l'extension et en saisissant ton identifiant et mot de passe

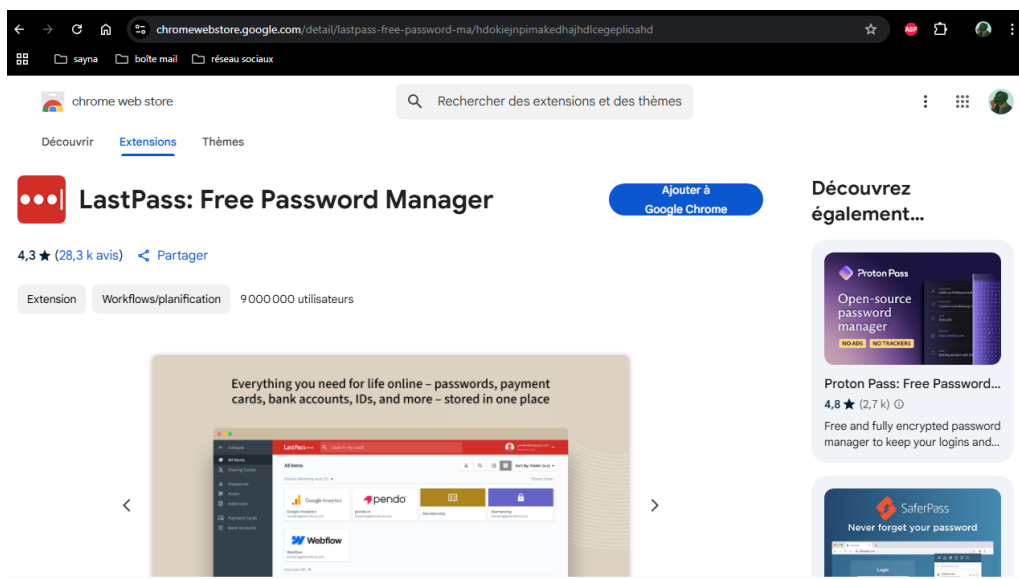


Réponse 1

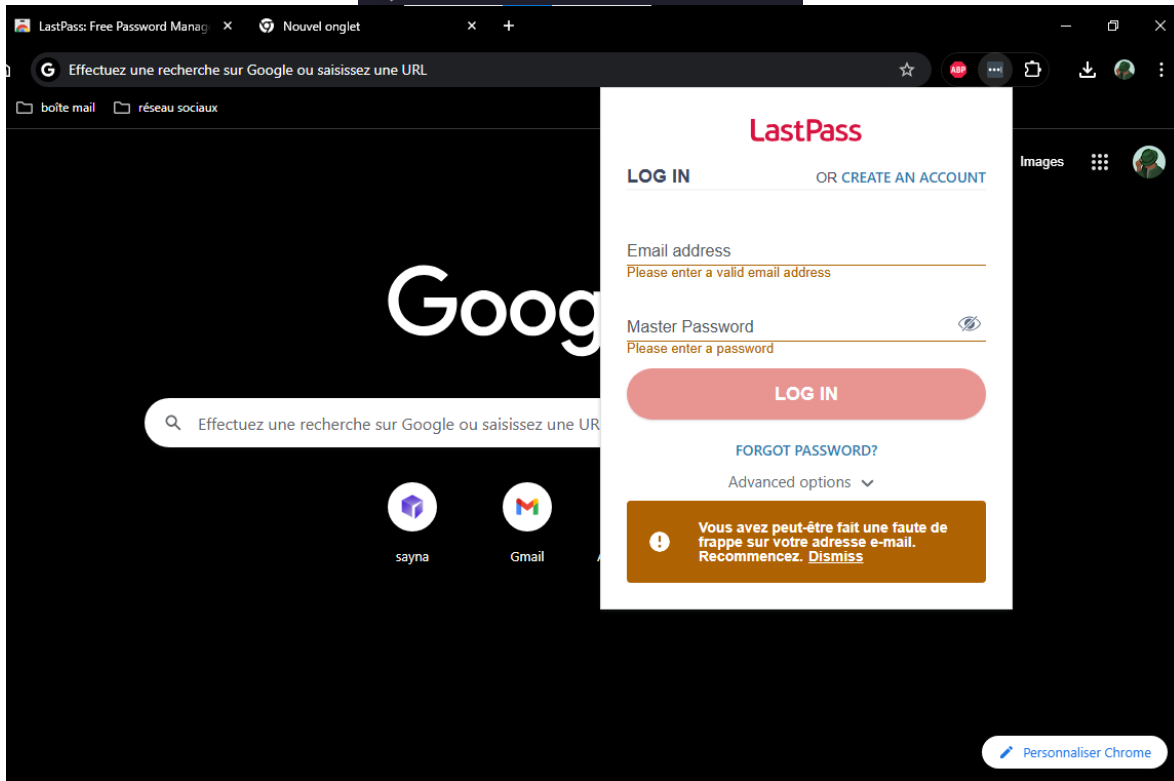
- Après avoir suivi les instructions et les liens précédents, je suis maintenant à l'étape d'inscription



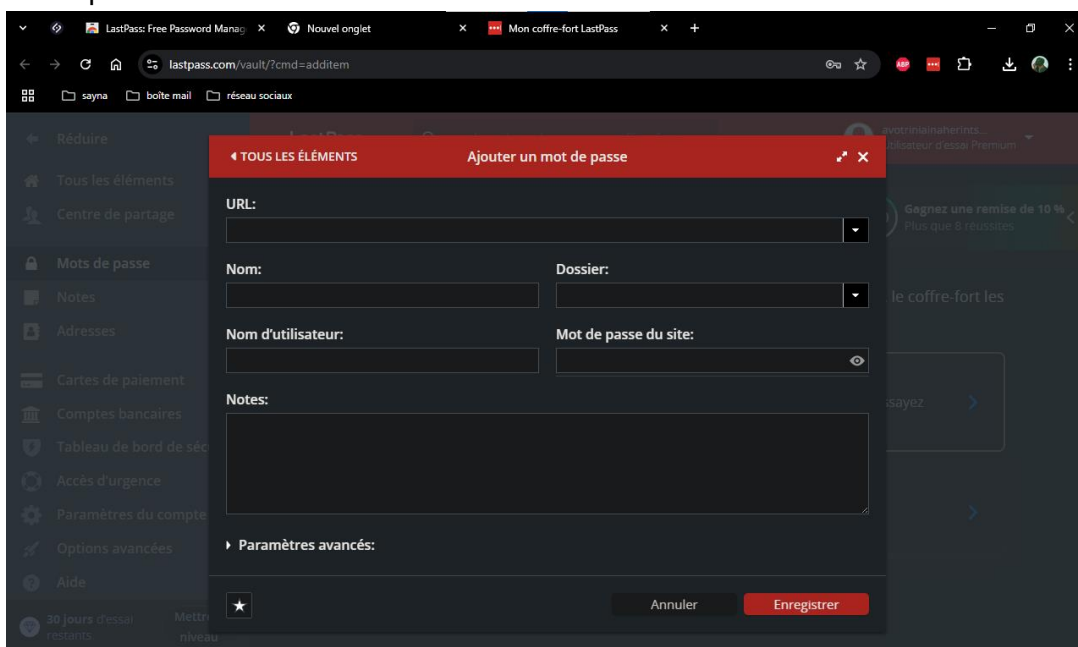
- Après avoir terminé l'inscription et installé l'application, je suis arrivé à l'étape d'ajout de l'extension à mon navigateur Chrome



- J'ai terminé toutes les étapes précédentes. Lorsque j'ai commencé à accéder à l'extension LastPass, il m'a demandé de saisir mon adresse e-mail et mon mot de passe.



- Après avoir suivi toutes les étapes que j'ai indiquées précédemment, je suis arrivé à l'interface où il est possible de gérer un gestionnaire de mots de passe. Ce que je souhaite faire ici, c'est gérer les mots de passe que je veux conserver et organiser de manière sécurisée, afin qu'ils ne soient pas facilement accessibles aux pirates ou aux personnes malintentionnées.



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

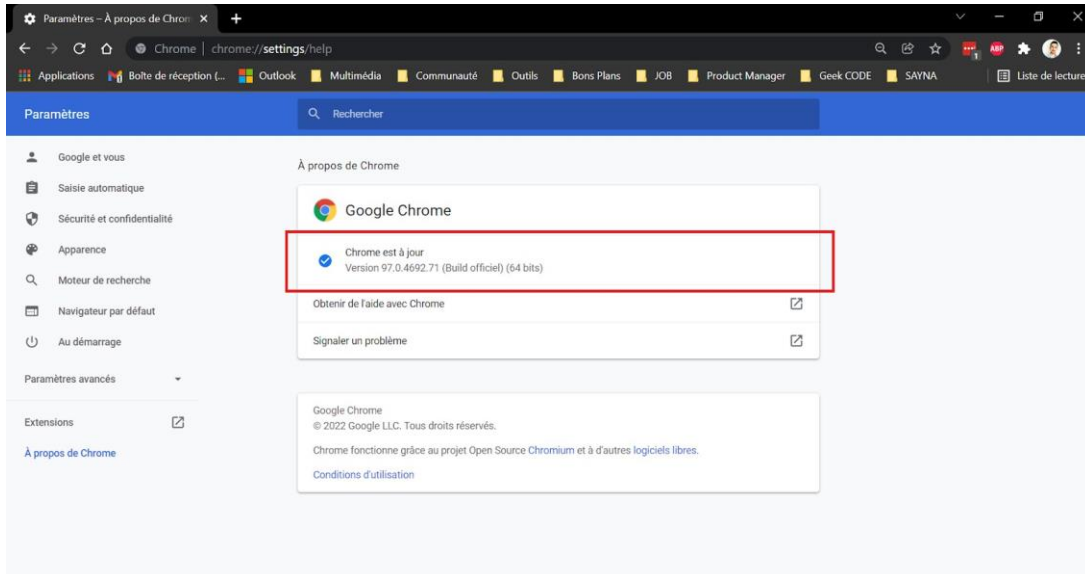
Réponse 1 :

Pour naviguer sur Internet en toute sécurité, il est important d'être vigilant et de repérer les sites web suspects qui pourraient potentiellement être malveillants. Voici l'analyse des sites listés dans le sujet :

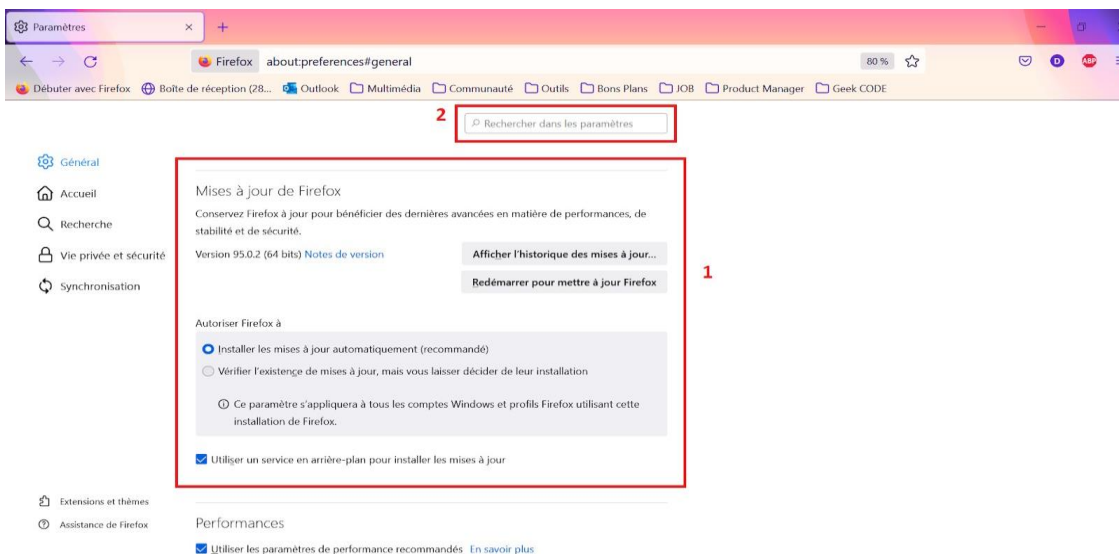
1. www.morvel.com
Ce site semble suspect. Le nom "morvel" est probablement une tentative de phishing en remplaçant le "a" de "Marvel" par un "o". Ce type de manipulation de l'URL vise à tromper les utilisateurs pour les faire croire qu'ils sont sur un site officiel, alors qu'il s'agit d'un site malveillant.
2. www.dccomics.com
Ce site est fiable. Il s'agit du domaine officiel de DC Comics, l'un des plus grands éditeurs de comics. Aucune modification suspecte dans l'URL, et le site est donc sécuritaire.
3. www.ironman.com
Bien que l'URL puisse prêter à confusion en raison de l'association avec le super-héros Marvel, www.ironman.com est en réalité le site officiel de l'événement international de triathlon appelé "Ironman". Il ne s'agit donc pas d'un site malveillant. Cependant, l'URL pourrait induire en erreur et c'est pourquoi il est important de vérifier les détails avant d'entrer.
4. www.fessebook.com
Ce site est clairement suspect. Le nom est une variation de facebook.com, avec une faute de frappe intentionnelle, ce qui est typiquement une méthode de phishing. Les sites avec des erreurs de frappe dans les noms de domaines sont souvent utilisés pour voler des informations personnelles.
5. www.instagram.com
Ce site présente également un risque. "Instagam" au lieu de "Instagram" est une faute de frappe évidente. Ce type de manipulation de l'URL est souvent utilisé pour créer des copies de sites populaires dans le but de collecter des informations personnelles des utilisateurs, et il est donc conseillé de ne pas y accéder.

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 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 2

J'ai réussi à effectuer la mise à jour des navigateurs Chrome et Firefox après avoir suivi les étapes que l'on m'a indiqué précédemment.

- Firefox

-  Général
-  Accueil
-  Recherche
-  Vie privée et sécurité
-  Synchronisation
-  Firefox Labs
-  Autres produits de Mozilla

Mises à jour de Firefox

Conservez Firefox à jour pour bénéficier des dernières avancées en matière de performances, de stabilité et de sécurité.


Version 137.0 (64 bits) [Notes de version](#)

[Afficher l'historique des mises à jour...](#)

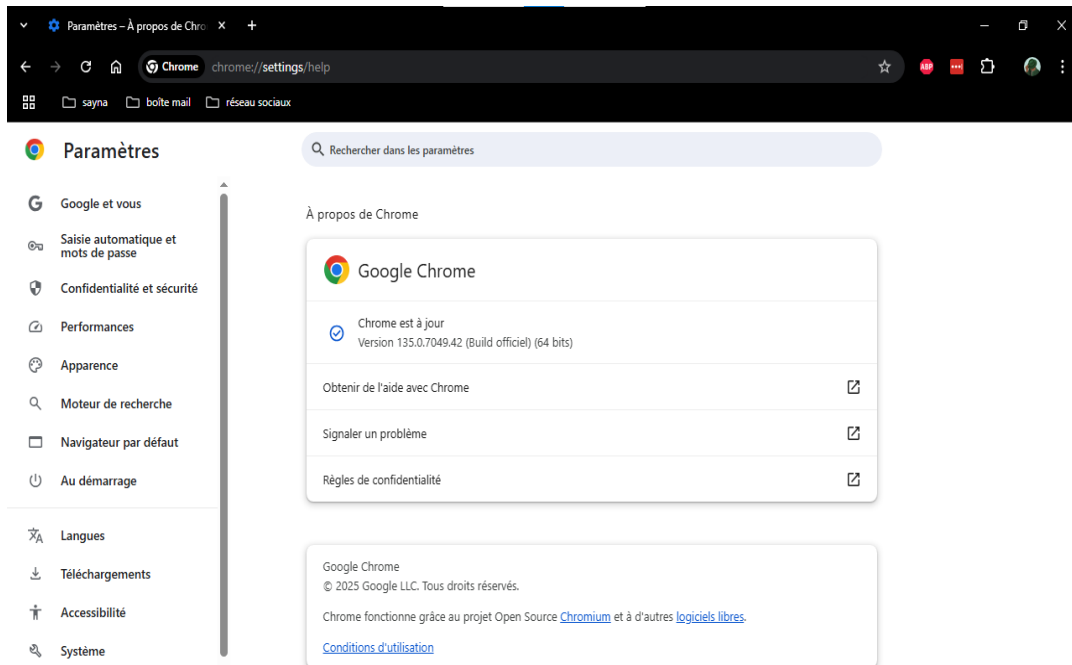
 Firefox est à jour

[Rechercher des mises à jour](#)

Autoriser Firefox à

- ☒ Installer les mises à jour automatiquement (recommandé)
 - ☒ Quand Firefox n'est pas lancé
 - ☐ Vérifier l'existence de mises à jour, mais vous laisser décider de leur installation
-  Ce paramètre s'appliquera à tous les comptes Windows et profils Firefox utilisant cette installation de Firefox.

• Chrome



The screenshot shows the Google Chrome settings page in French. The left sidebar contains a list of settings categories: Paramètres, Google et vous, Saisie automatique et mots de passe, Confidentialité et sécurité, Performances, Apparence, Moteur de recherche, Navigateur par défaut, Au démarrage, Langues, Téléchargements, Accessibilité, and Système. The main content area is titled 'À propos de Chrome' (About Chrome) and displays the Google Chrome logo, version information (Version 135.0.7049.42 (Build officiel) (64 bits)), and a status 'Chrome est à jour' (Chrome is up to date). Below this, there are links for 'Obtenir de l'aide avec Chrome', 'Signaler un problème', and 'Règles de confidentialité'. At the bottom, there is a section for 'Google Chrome' with copyright information (© 2025 Google LLC) and a link to the 'Conditions d'utilisation' (Terms of Use).

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 1

1. Comprendre le phishing et le spam :

- Comprendre le Phishing et le Spam :
Le phishing est une méthode de fraude utilisant des messages (souvent par e-mail) pour tromper l'utilisateur et lui voler des informations sensibles.
- Le spam, quant à lui, concerne les messages non sollicités, généralement des publicités envoyées en masse.

2. Comment Identifier un Message de Phishing

- Adresse e-mail : Vérifiez l'adresse de l'expéditeur, surtout s'il y a des modifications subtiles dans le nom de l'entreprise.
- Contenu du message : Les erreurs de grammaire ou d'orthographe sont souvent des signes de phishing.
- Liens et pièces jointes : Ne cliquez jamais sur un lien ou n'ouvrez pas une pièce jointe provenant d'un expéditeur inconnu.
- Demande d'informations personnelles : Les entreprises légitimes ne demandent jamais d'informations sensibles par e-mail.
- Urgence excessive : Méfiez-vous des messages qui créent un sentiment d'urgence pour vous pousser à agir rapidement.

3. Outils et Ressources pour la Prévention

Consultez des ressources fiables, comme le site cybermalveillance.gouv.fr, pour en savoir plus sur la détection des tentatives de phishing.

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 Transparence 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 Not secure 
 - Not secure
 - **Analyse Google**
 - Aucun contenu suspect
 - Vérifier un URL en particulier
- Site n°2
 - **Indicateur de sécurité**
 - HTTPS 
 - HTTPS Not secure 
 - Not secure
 - **Analyse Google**

- Aucun contenu suspect
 - Vérifier un URL en particulier
- Site n°3
 - **Indicateur de sécurité**
 - HTTPS 
 - HTTPS Not secure 
 - Not secure
 - **Analyse Google**
 - Aucun contenu suspect
 - Vérifier un URL en particulier
- Site n°4 (site non sécurisé)

Réponse 1 :

Site n°1 :

- **Indicateur de sécurité :**
 - *HTTPS* (sécurisé)
 - *Not secure* (non sécurisé)
 - *HTTPS Not secure* (sécurisé mais certains éléments du site ne le sont pas)
- **Analyse Google :**
 - *Aucun contenu suspect*
 - *Vérifier un URL en particulier*

Site n°2 :

- **Indicateur de sécurité :**
 - *HTTPS*
 - *Not secure*
 - *HTTPS Not secure*
- **Analyse Google :**
 - *Aucun contenu suspect*
 - *Vérifier un URL en particulier*

Site n°3 :

- **Indicateur de sécurité :**
 - *HTTPS*
 - *Not secure*
 - *HTTPS Not secure*
- **Analyse Google :**
 - *Aucun contenu suspect*
 - *Vérifier un URL en particulier*

Site n°4 (site non sécurisé) :

- **Indicateur de sécurité :**
 - *Not secure* (non sécurisé)



- **Analyse Google :**
 - *Vérifier un URL en particulier* (cela indique que le site présente un risque ou n'est pas recommandé)

6 - Achats en ligne sécurisés

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

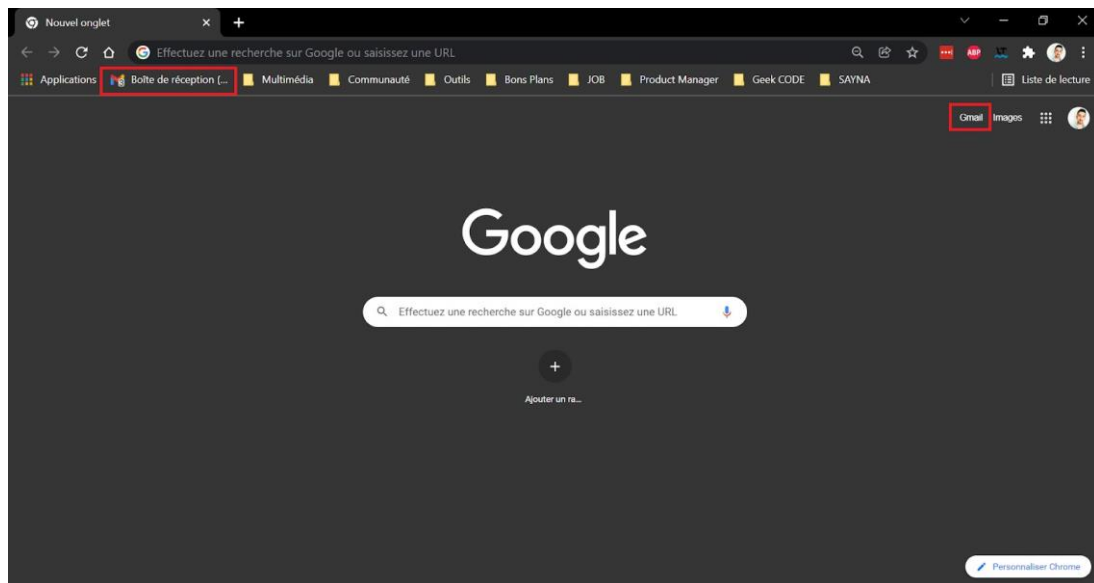
1/ Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le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

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

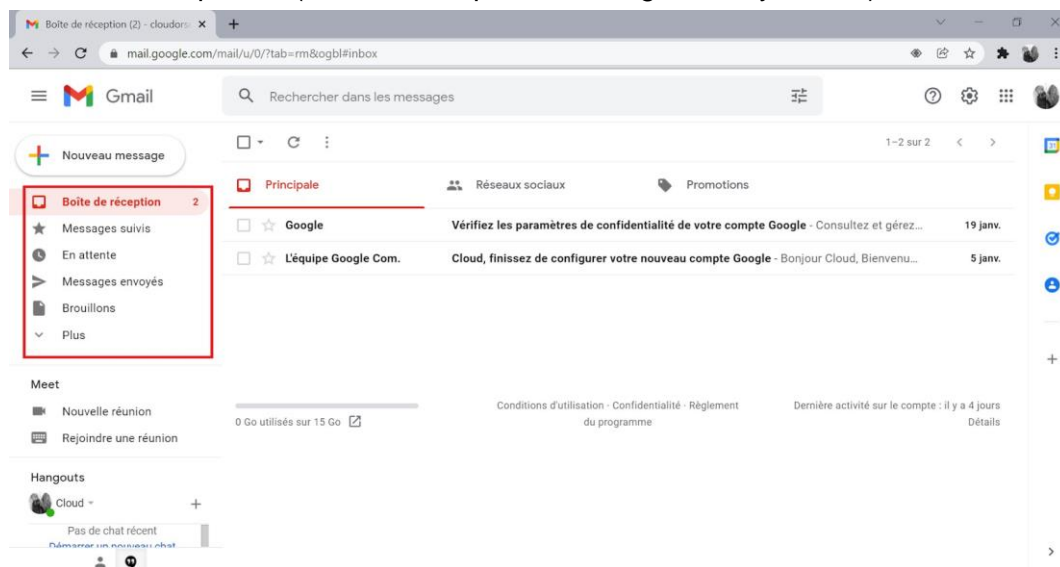
- 1. Créer un dossier sur ta messagerie électronique**
- 2. Créer un dossier sur ton espace de stockage personnel (en local ou sur le cloud)**

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)

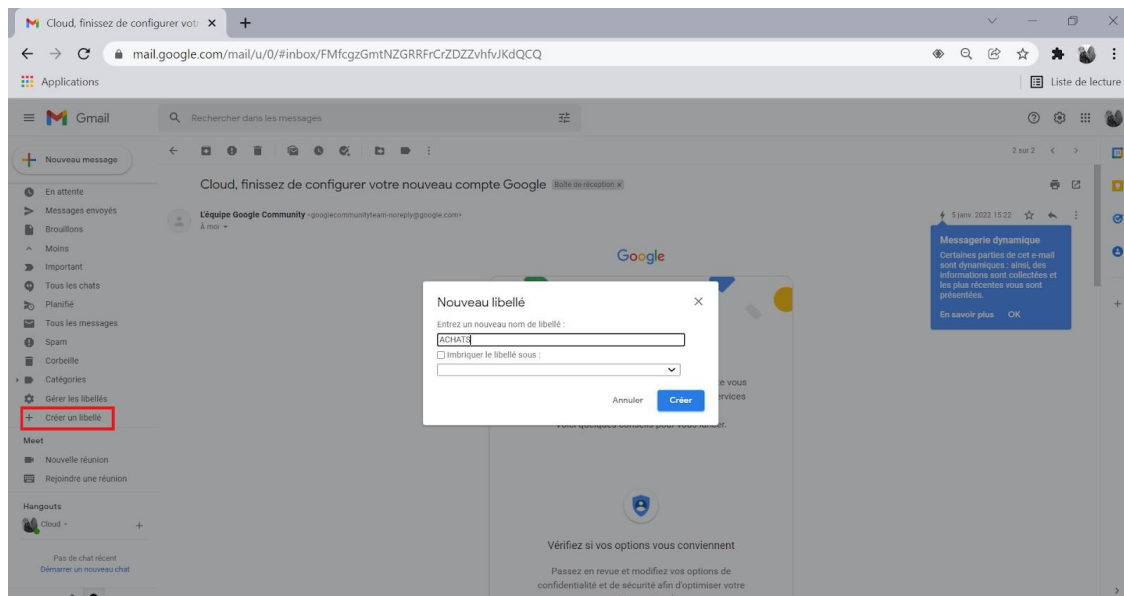
- Pour commencer, accède à ta messagerie électronique. Pour rappel, tu peux y accéder rapidement en ouvrant un nouvel onglet (dans la barre des favoris ou via le raccourci)



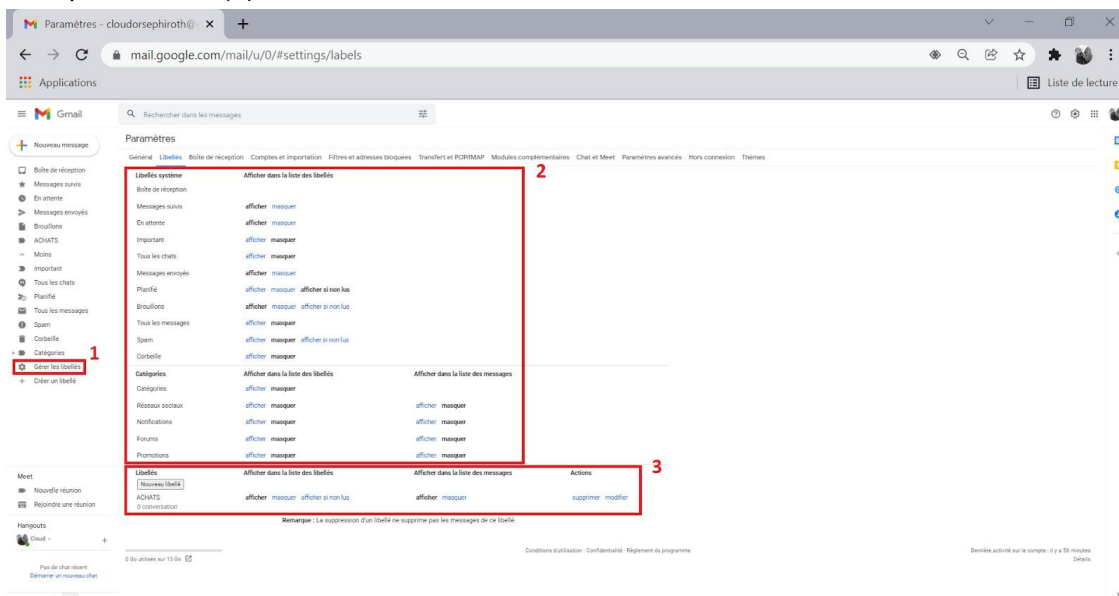
- Sur la page d'accueil de ta messagerie, tu trouveras sur la gauche les libellés initialement prévus (boîte de réception, messages envoyés, etc.)



- 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)



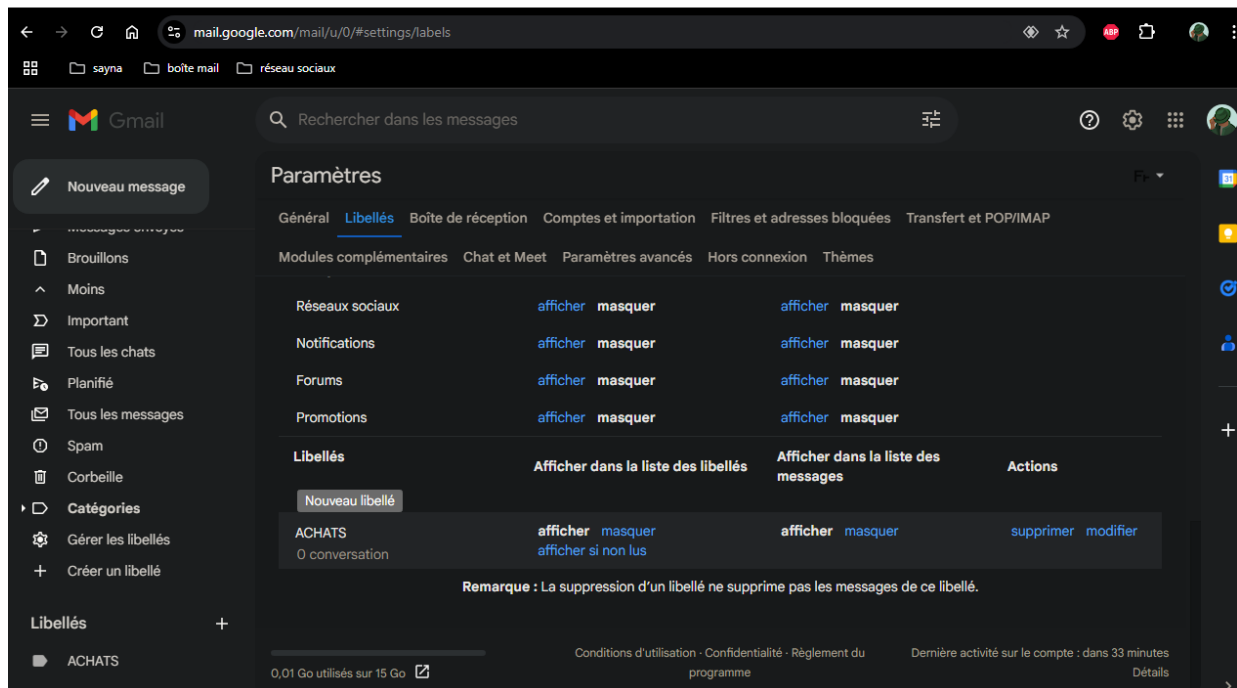
- Effectuer un clic sur le bouton “Créer” pour valider l’opération
- Tu peux également gérer les libellés en effectuant un clic sur “Gérer les libellés”(1). Sur cette page, tu peux gérer l’affichage des libellés initiaux (2) et gérer les libellés personnels (3)



- 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 1

Après avoir suivi toutes les étapes précédentes, je suis arrivé à la création du libellé ACHATS dans ma messagerie électronique. C'est maintenant terminé.



7 - Comprendre le suivi du navigateur

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

Réponse :

Fonctionnement des cookies :

1. Les cookies peuvent être de deux types principaux :

- ❖ Cookies de session : Ils conservent des informations temporaires pendant que l'utilisateur est sur un site (par exemple, pour maintenir une session active ou un panier d'achat).
- ❖ Cookies de suivi : Ces cookies suivent l'utilisateur d'un site à l'autre et peuvent être utilisés pour des fins commerciales, comme la personnalisation des publicités.

2. Impact sur la vie privée :

Les cookies peuvent poser des risques pour la vie privée car ils permettent de collecter des données sensibles, comme les sites visités, les habitudes de navigation et même les informations personnelles. De ce fait, leur utilisation soulève des préoccupations concernant le respect de la confidentialité des utilisateurs.

3. La navigation privée :

Le mode incognito ou navigation privée permet aux utilisateurs de naviguer sans laisser d'historique, de cookies ou de données de recherche sur l'appareil utilisé. Cependant, il est essentiel de souligner que ce mode ne garantit pas l'anonymat complet. Les sites peuvent toujours voir l'adresse IP de l'utilisateur, et les fournisseurs d'accès à Internet peuvent suivre ses activités.

4. Gestion et contrôle :

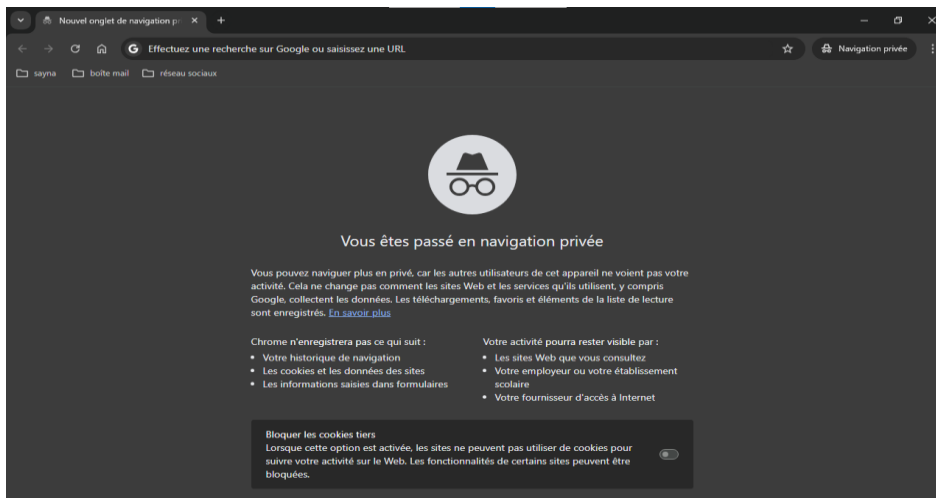
L'utilisateur a la possibilité de gérer et de contrôler l'utilisation des cookies à travers les paramètres de son navigateur. Il peut désactiver les cookies, les supprimer régulièrement, ou utiliser la navigation privée pour minimiser le suivi.

5. Objectifs :

L'objectif principal de la gestion des cookies et de la navigation privée est de protéger la vie




privée de l'utilisateur et de lui offrir un contrôle sur ses données personnelles. Cela permet de limiter le suivi non souhaité, de mieux comprendre la collecte de données et de préserver la confidentialité lors de la navigation en ligne.

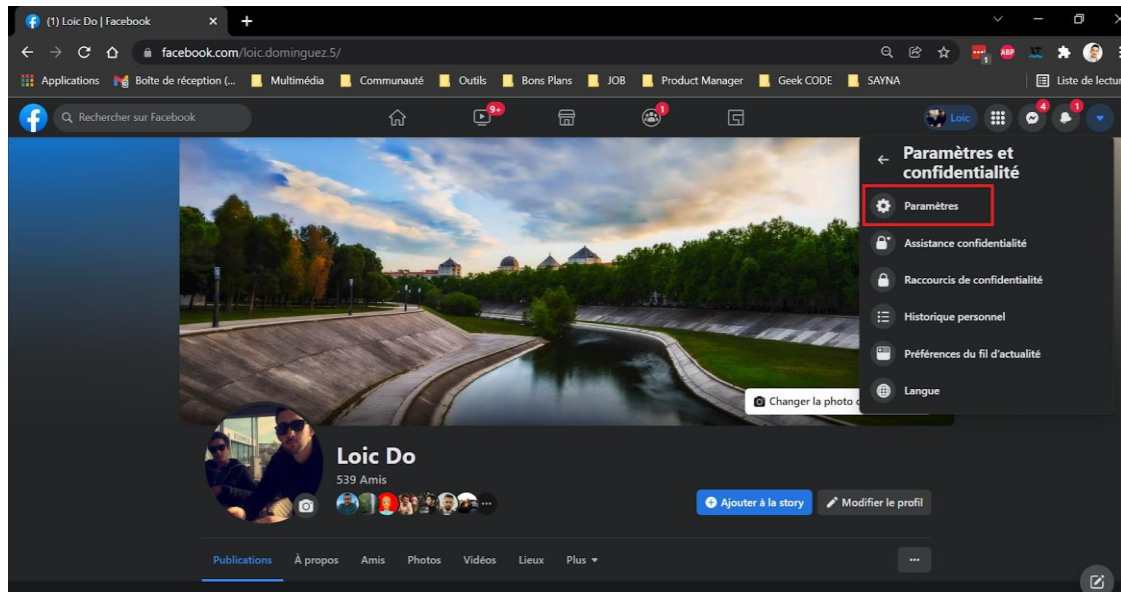


8 - Principes de base de la confidentialité des médias sociaux

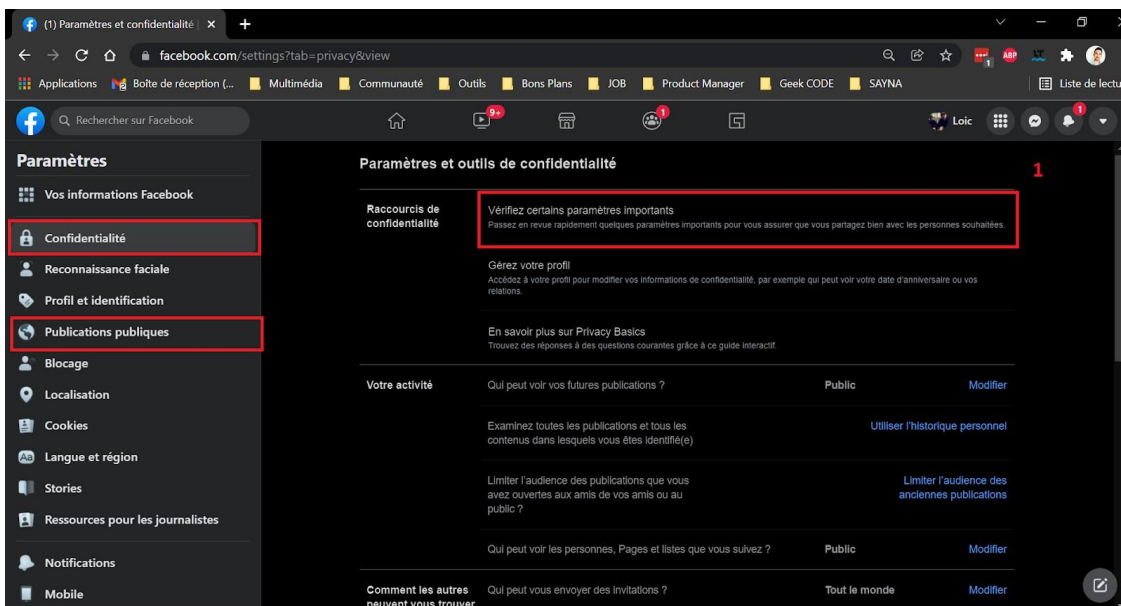
Objectif : *Régler les paramètres de confidentialité de Facebook*

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)

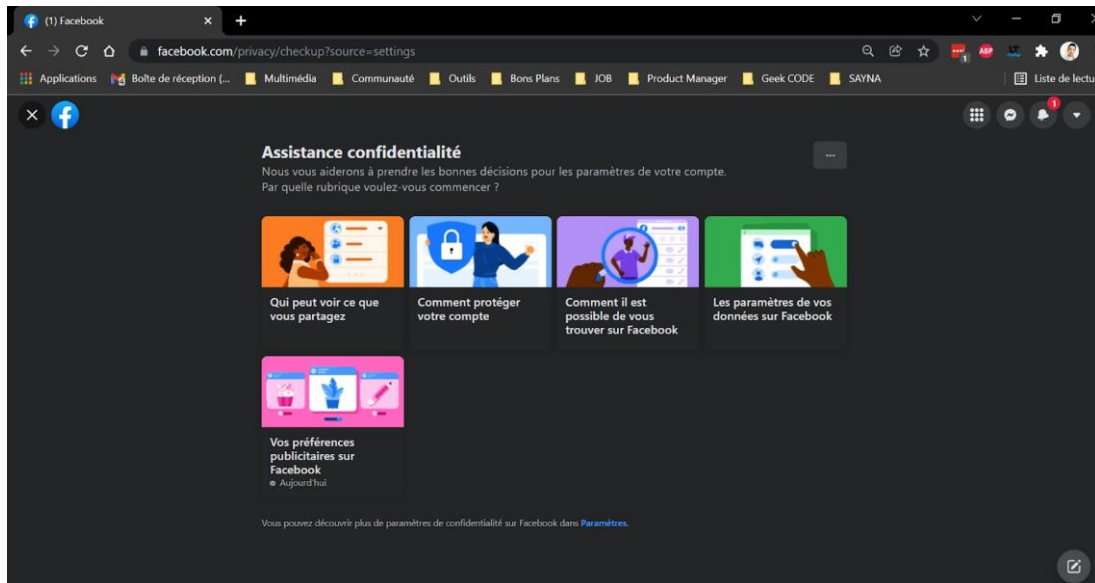
- Connecte-toi à ton compte Facebook
- Une fois sur la page d'accueil, ouvre le menu Facebook , puis effectue un clic sur "Paramètres et confidentialité". Pour finir, clic sur "Paramètres"



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



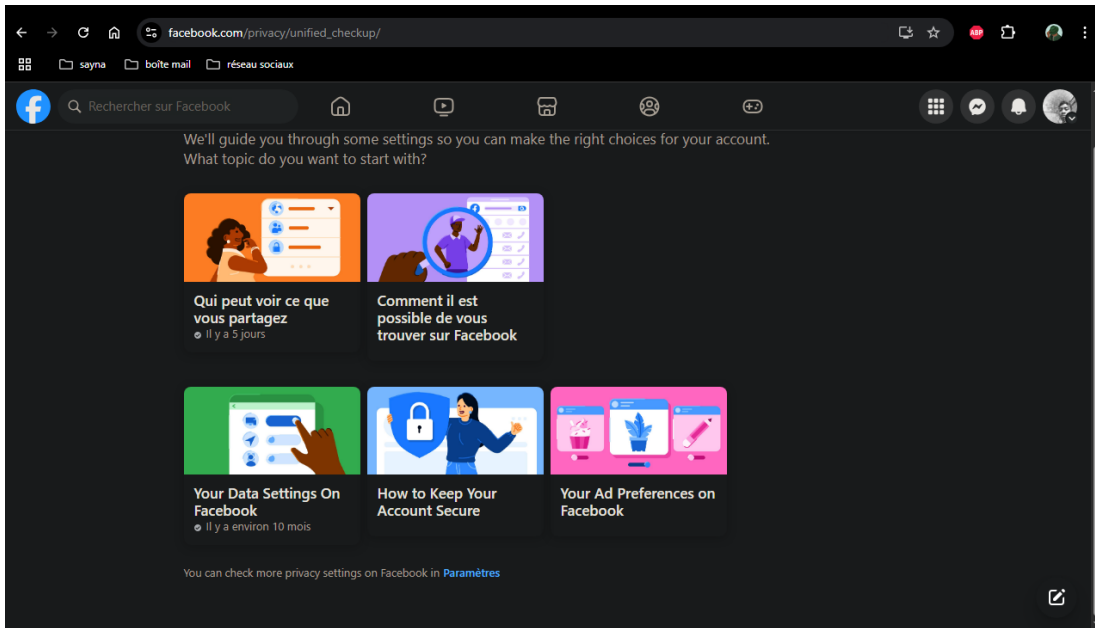
- Cette rubrique résume les grandes lignes de la confidentialité sur Facebook
 - La première rubrique (orange) te permettra de régler la visibilité de tes informations personnelles
 - La deuxième rubrique (bleu) te permet de changer ton mot de passe
 - La troisième rubrique (violet) te permet de gérer 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 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.

Réponse 1

Lorsque j'ai suivi les instructions recommandées pour sécuriser mon compte Facebook, je l'ai bien fait et maintenant je sais comment sécuriser mon compte Facebook.



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 ????????

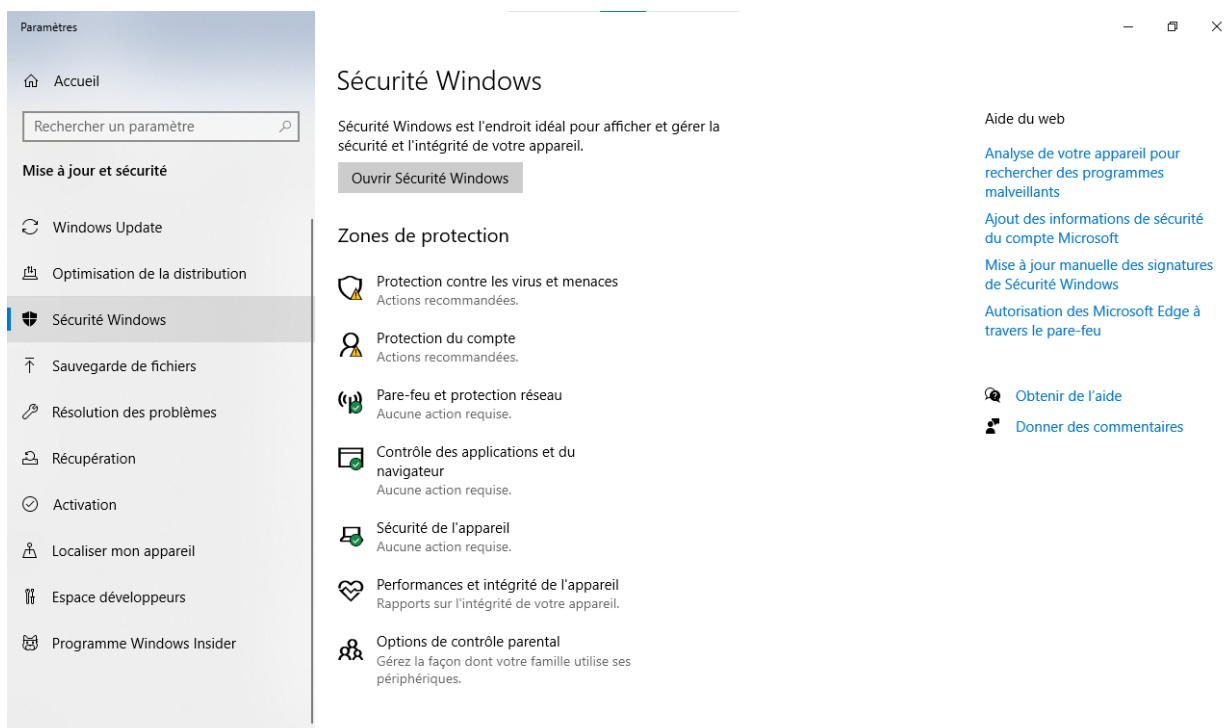
Réponse 1 :

Vérification de la sécurité en fonction de l'appareil utilisé

Vérification de la sécurité sur un PC Windows, voici les étapes à suivre :

1. Vérifier les mises à jour du système :

- Cliquez sur le bouton Démarrer.
- Va dans Paramètres.
- Cliquez sur Mise à jour et sécurité.



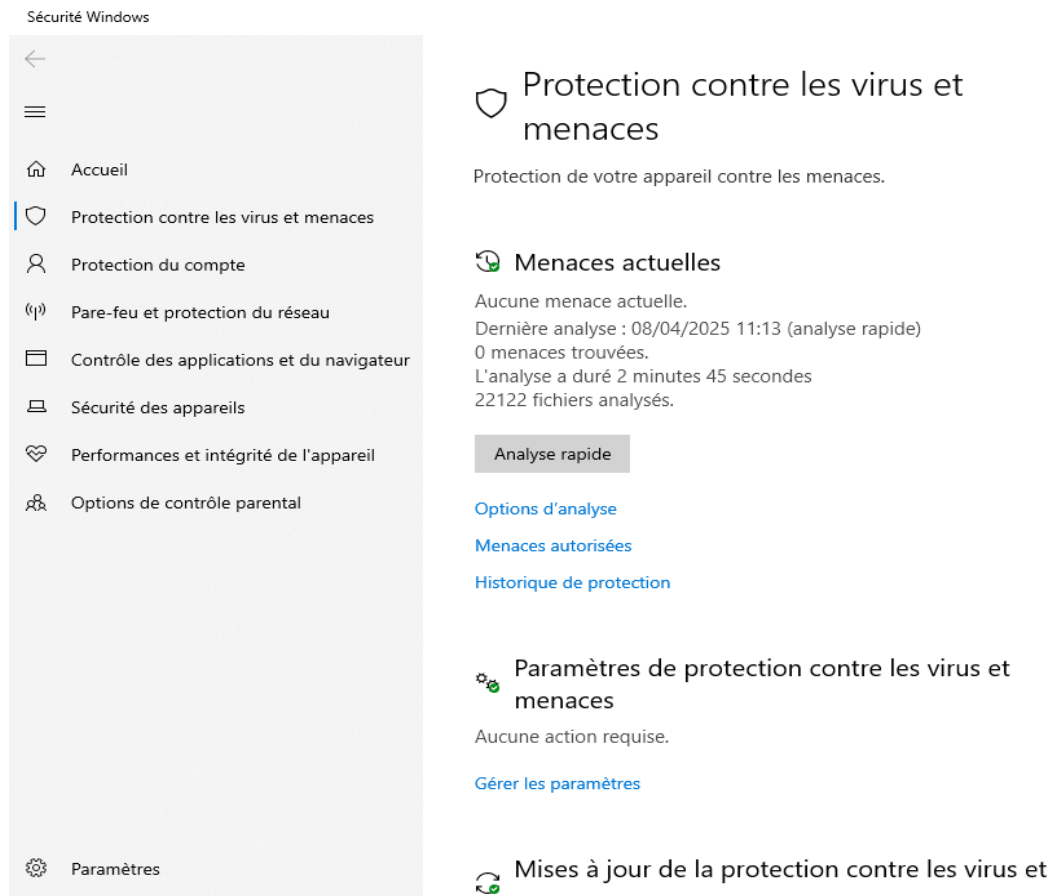
- Sélectionne Windows Update et clique sur Rechercher des mises à jour.



- Si des mises à jour sont disponibles, installe-les. Cela corrige souvent des failles de sécurité.

2. Vérifier que Windows Defender est activé :

- Toujours dans Paramètres, va dans Mise à jour et sécurité > Sécurité Windows.
- Vérifie que Protection contre les virus et menaces est activée.
- Clique sur Analyse rapide pour vérifier rapidement si ton PC est infecté par un virus.



3. Vérifier les programmes suspects :

- Appuie sur Ctrl + Maj + Échap pour ouvrir le Gestionnaire des tâches.
- Vérifie les processus qui tournent. Si tu vois un programme inconnu ou suspect, fais des recherches sur Internet pour savoir s'il s'agit d'un virus.

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

Réponse 2 :

Installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé

Installer un antivirus sur un PC Windows, voici les étapes à suivre :

1. Choisir un antivirus :

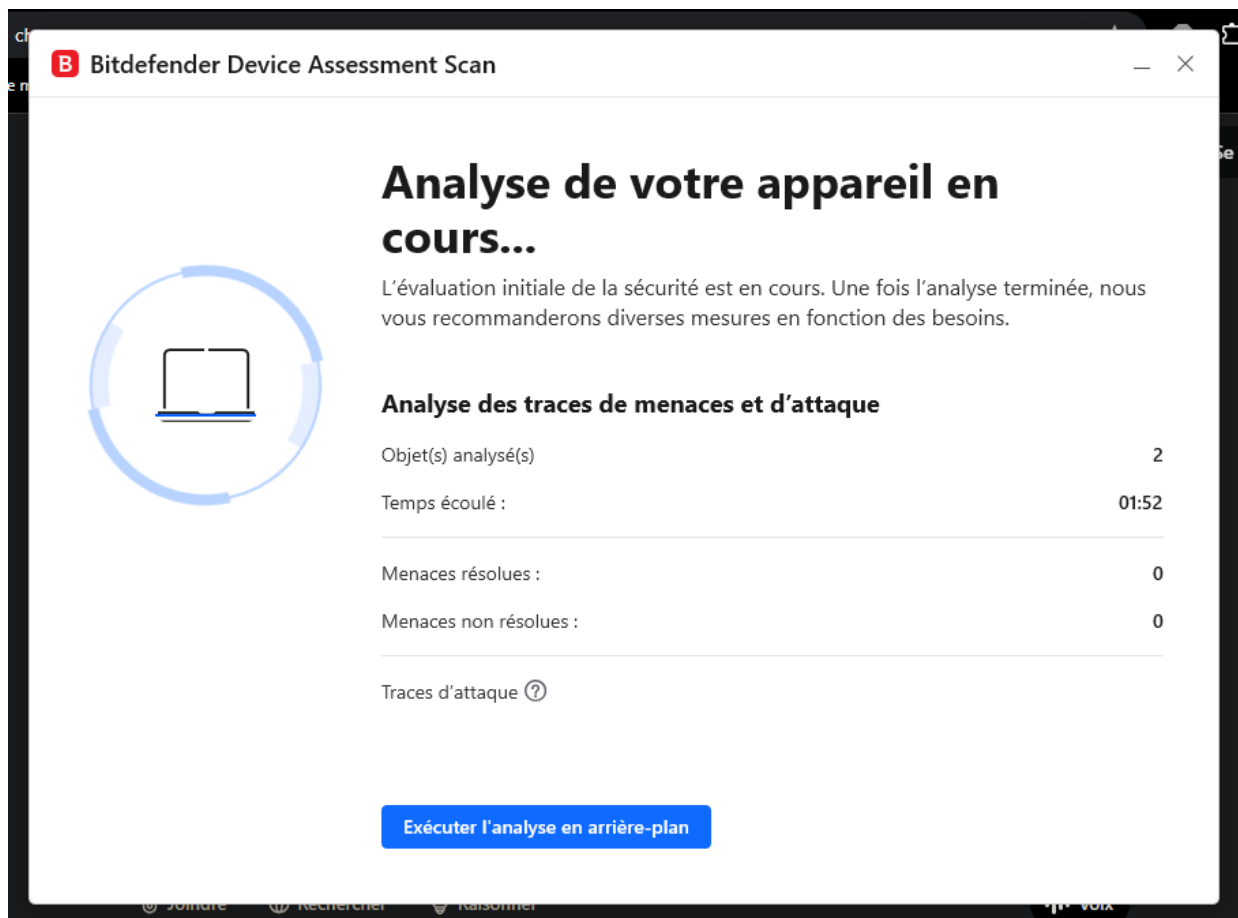
- Télécharge un antivirus de confiance comme Avast, Bitdefender, ou Kaspersky.

2. Installer l'antivirus :

- Va sur le site officiel de l'antivirus que tu as choisi
- Télécharge le fichier d'installation et double-clique dessus pour démarrer l'installation.
- Suis les instructions à l'écran pour terminer l'installation.

3. Effectuer une analyse complète :

- Ouvre l'antivirus que tu viens d'installer.
- Cherche l'option Analyse complète ou Scan complet et clique dessus.
- Laisse l'antivirus analyser ton PC pour détecter d'éventuels virus ou malwares.



- Si des menaces sont détectées, suis les instructions pour les supprimer.