



Parcours : DISCOVERY

Module : Naviguer en toute
sécurité

Projet 1 - Un peu plus de sécurité,
on n'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, consultez 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.

Réponse 1

Voici les articles

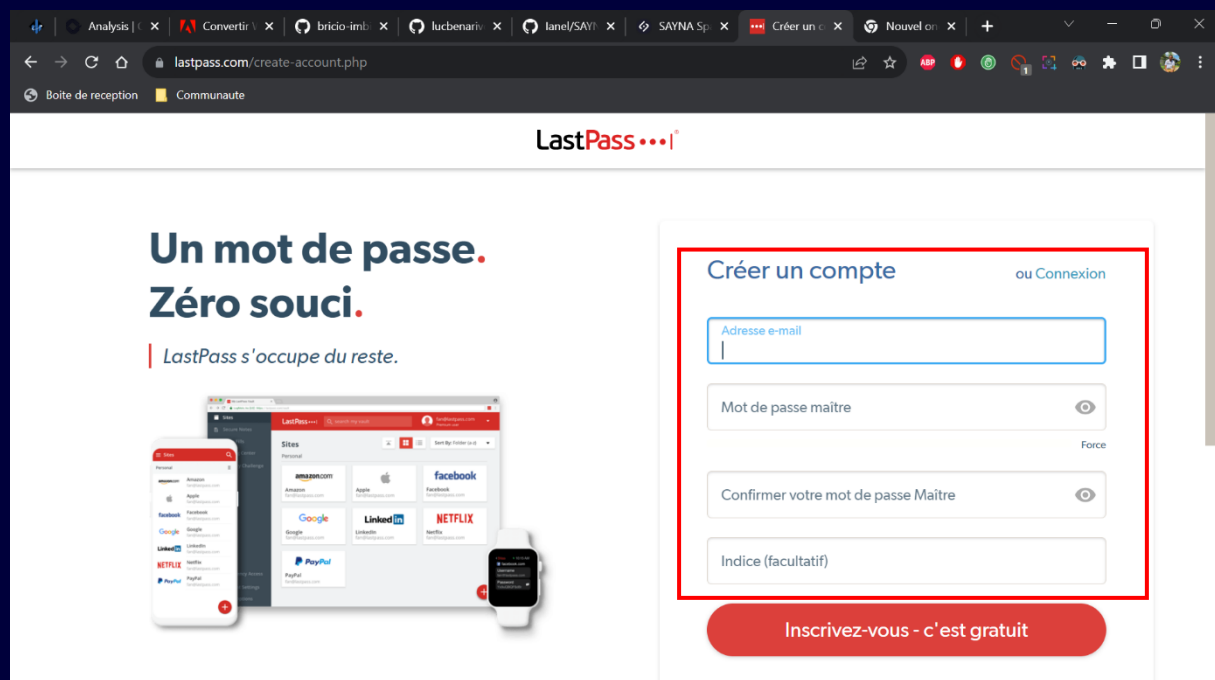
- Article 1 = Cybersécurité | CNIL - les technologies pour protéger son patrimoine informationnel et les personnes concernées des atteintes à leurs données.
- Article 2 = Confidentialité et sécurité sur Internet : 5 conseils de sécurité (kaspersky.fr) - 5 conseils de Confidentialité et sécurité sur Internet
- Article 3 = Cybersécurité 2022 : Principales cyberattaques menaçant votre entreprise| Insight FR - Principales cyberattaques menaçant votre entreprise.

2. Créer des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass

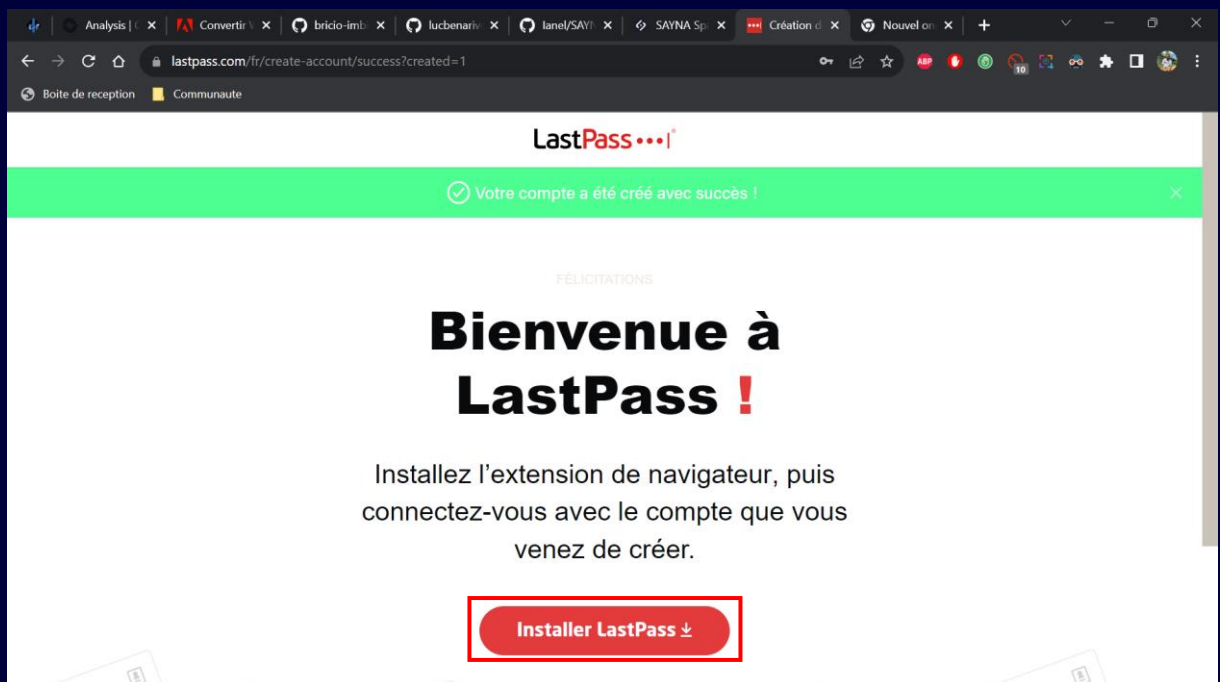
1/ Dans cet exercice, nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Ce gestionnaire prend la forme d'une application web, accessible sur tous supports (PC, Mac, mobile). Il est simple à prendre en main et propose un niveau de sécurité optimal.

- Accède au site de LastPass

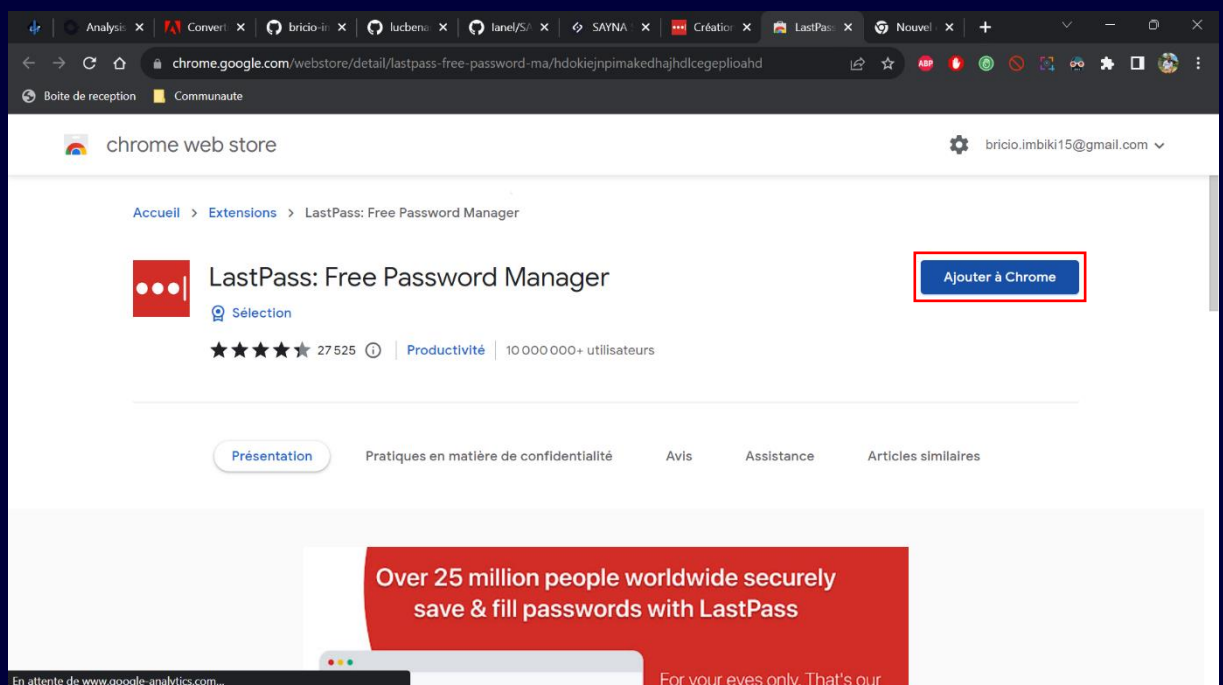


The screenshot shows the LastPass website in a web browser. The browser's address bar displays 'lastpass.com/create-account.php'. The page features the LastPass logo at the top. On the left, there is a promotional graphic with the text 'Un mot de passe. Zéro souci.' and 'LastPass s'occupe du reste.' Below this is an illustration of a smartphone, a laptop, and a smartwatch, all displaying the LastPass app interface. On the right side of the page, there is a 'Créer un compte' (Create an account) form, which is highlighted with a red rectangular border. The form includes the following fields: 'Adresse e-mail', 'Mot de passe maître' (Master password) with an eye icon to toggle visibility and a 'Force' label, 'Confirmer votre mot de passe Maître' (Confirm your Master password) with an eye icon, and 'Indice (facultatif)' (Optional hint). At the bottom of the form is a red button labeled 'Inscrivez-vous - c'est gratuit' (Sign up - it's free).

- Création du compte effectuée

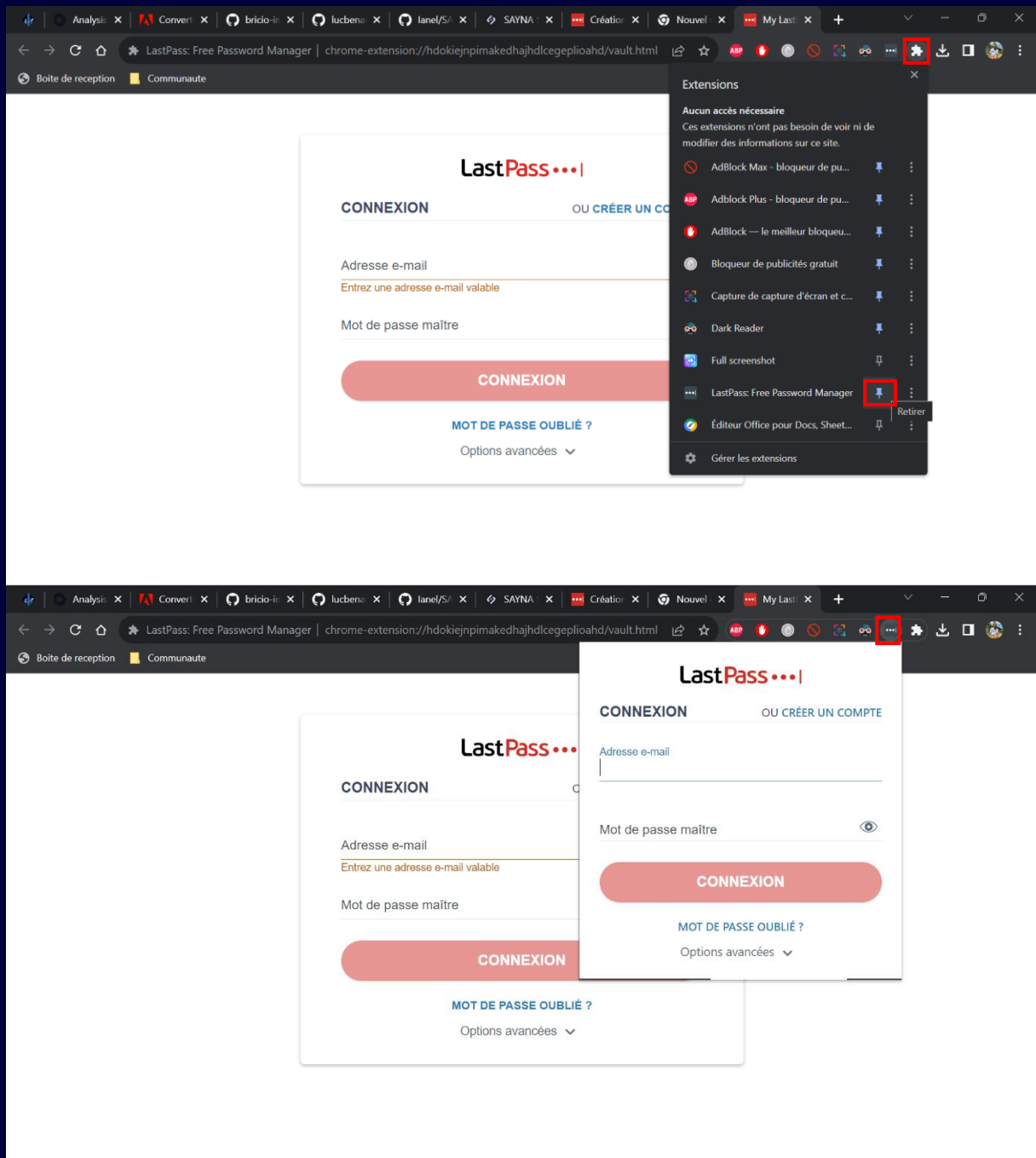


- Il te suffit de valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome"



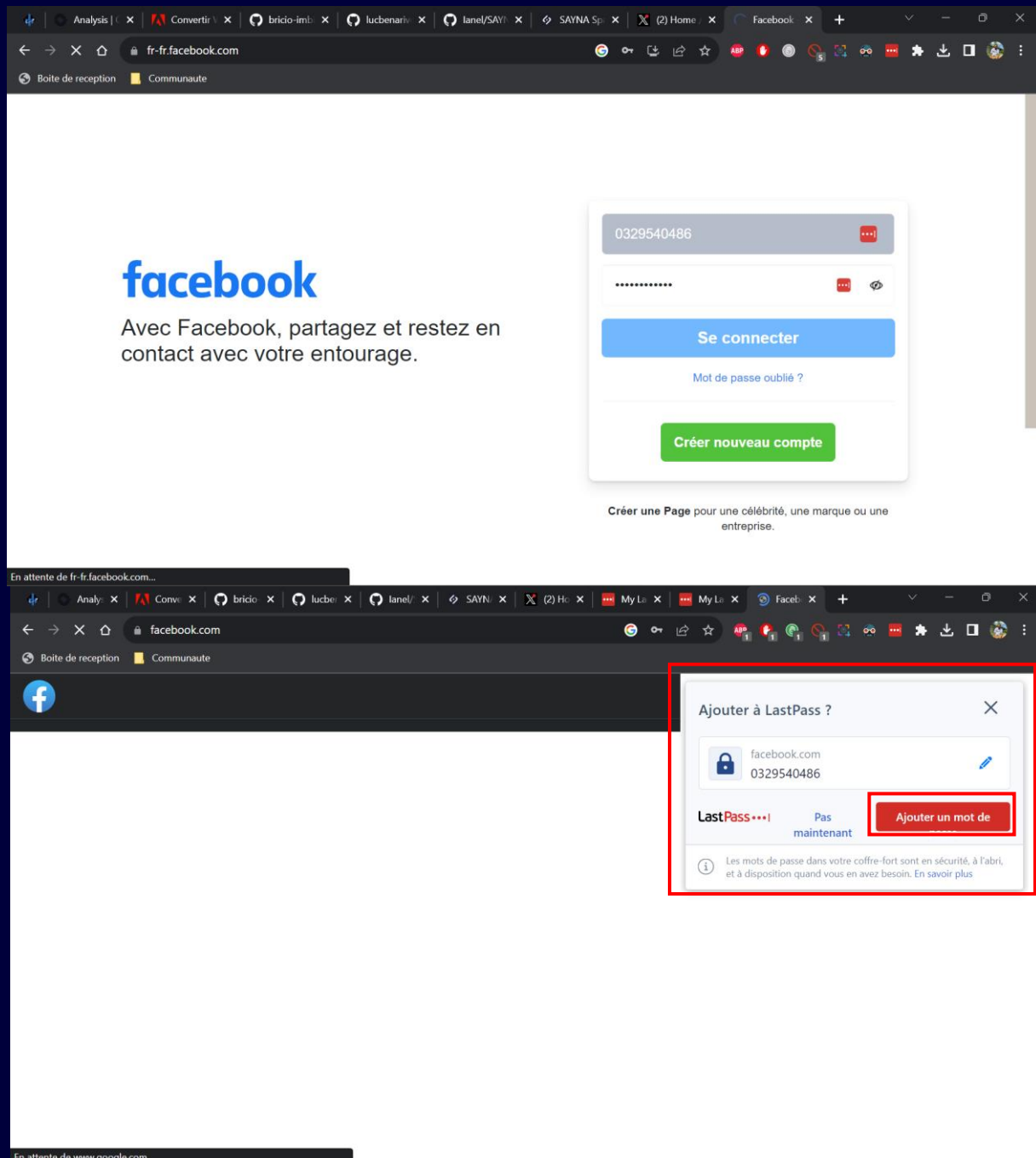
- Une fois installé, il te suffit d'accéder à cette extension et de t'y connecter

Naviguer en toute sécurité

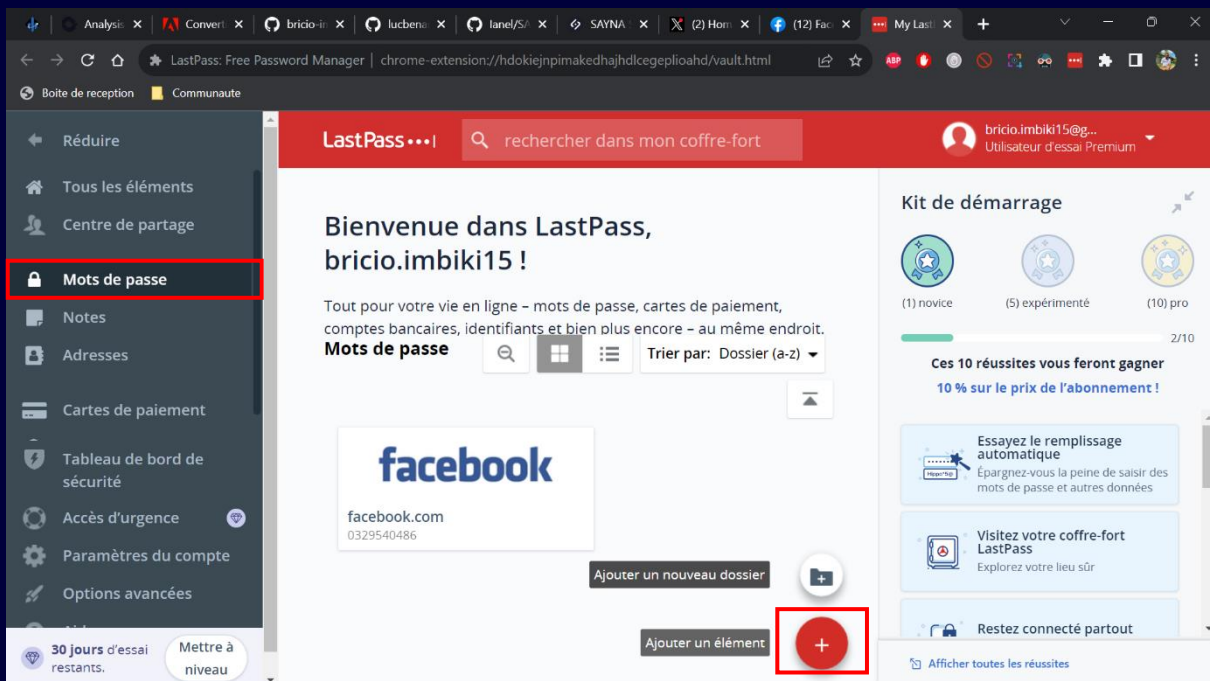
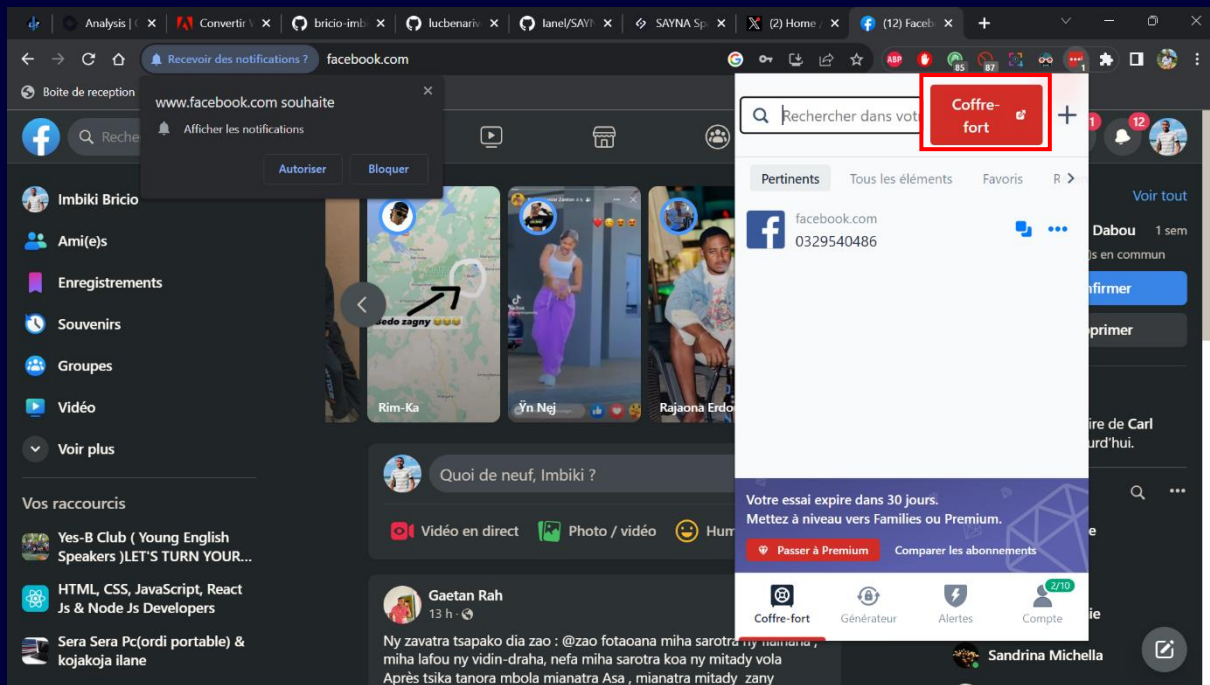


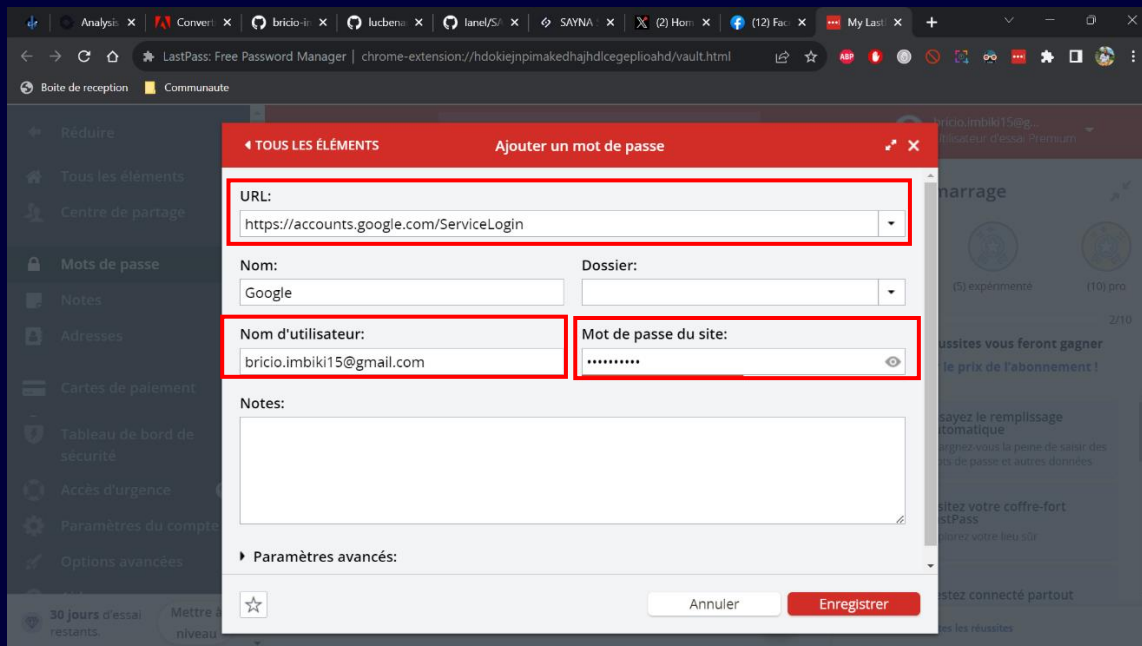
Réponse 1

Désormais, lorsque on peut enregistrer le mot de passe grâce à LastPass.



Naviguer en toute sécurité





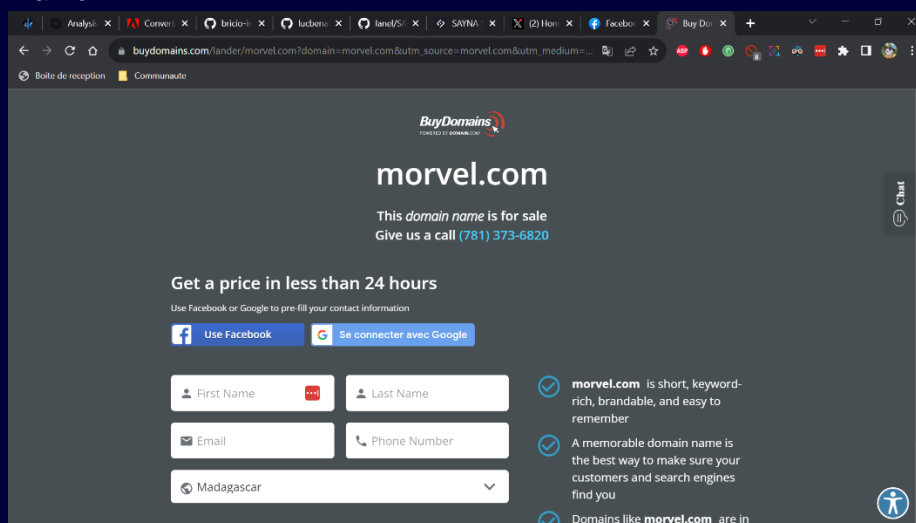
3. Fonctionnalité de sécurité de votre navigateur

1/ Identification adresses internet qui proviennent de sites web malveillants. (case à cocher)

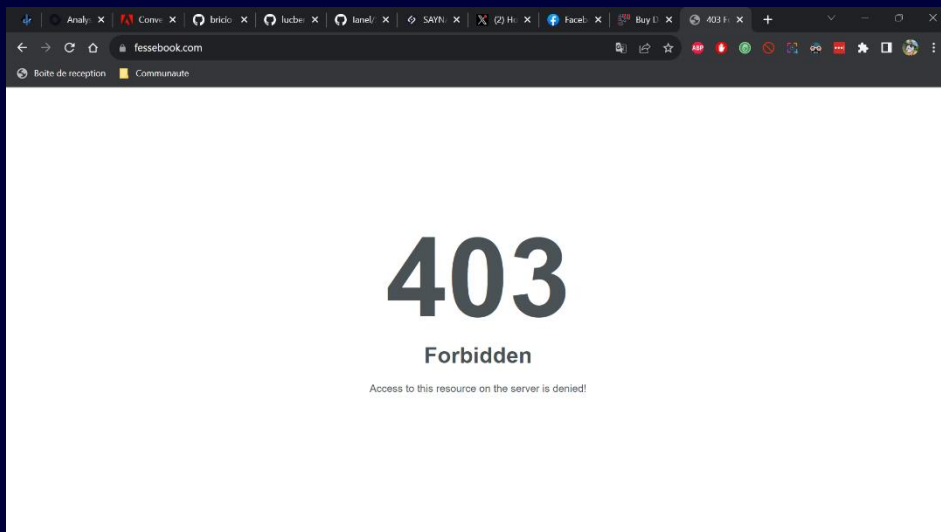
Réponse 1

Les sites web qui semblent être malveillants sont :

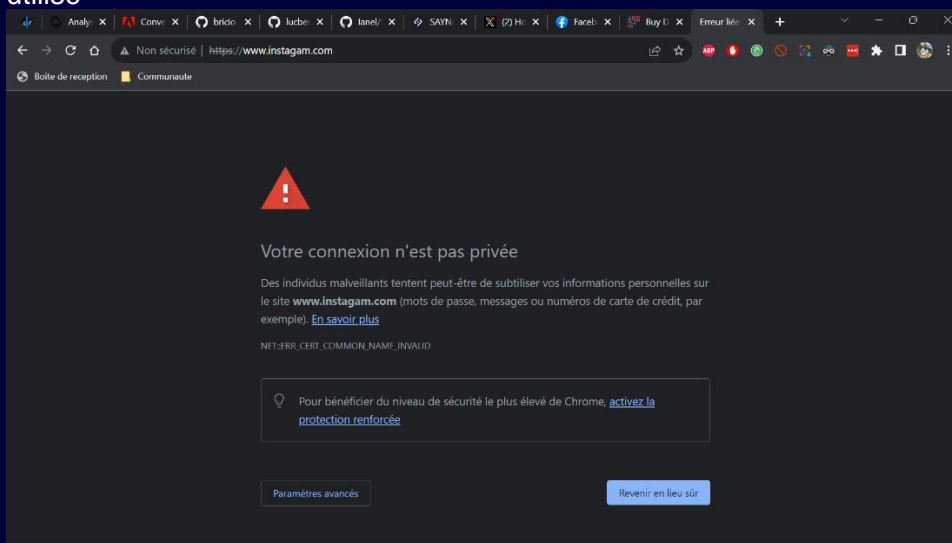
- www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel



- www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde

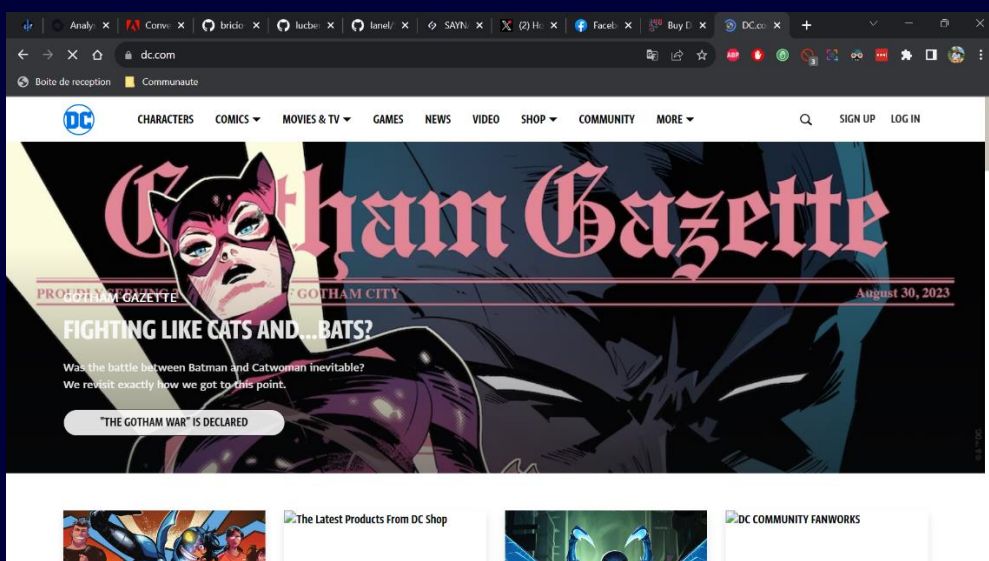


- www.instagram.com, un dérivé de www.instagram.com, un autre réseau social très utilisé



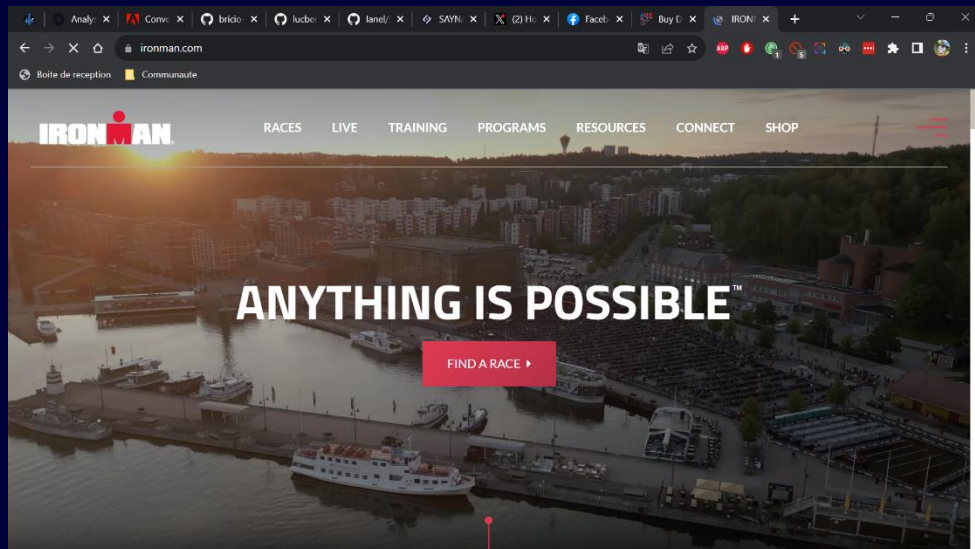
Les seuls sites qui semblaient être cohérents sont donc :

- www.dccomics.com, le site officiel de l'univers DC Comics



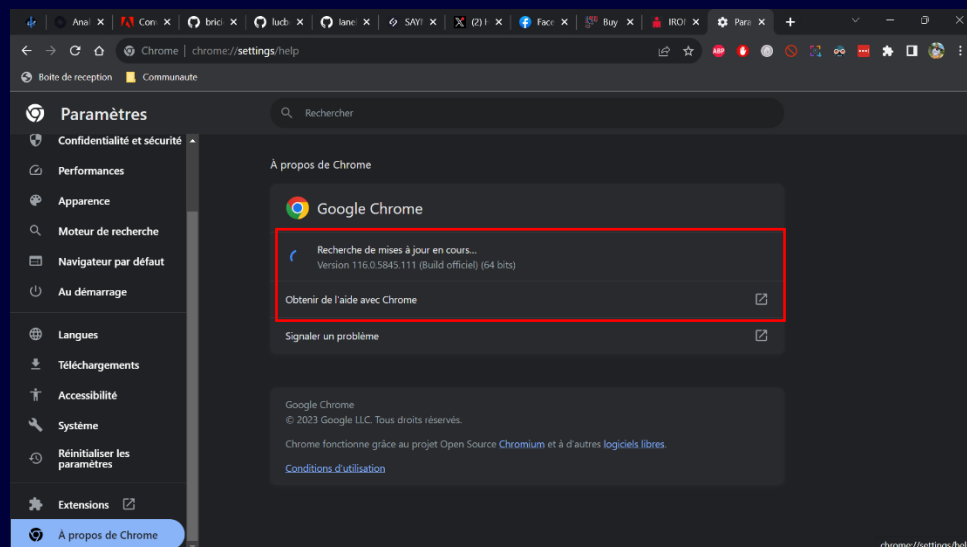
Naviguer en toute sécurité

- www.ironman.com, le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

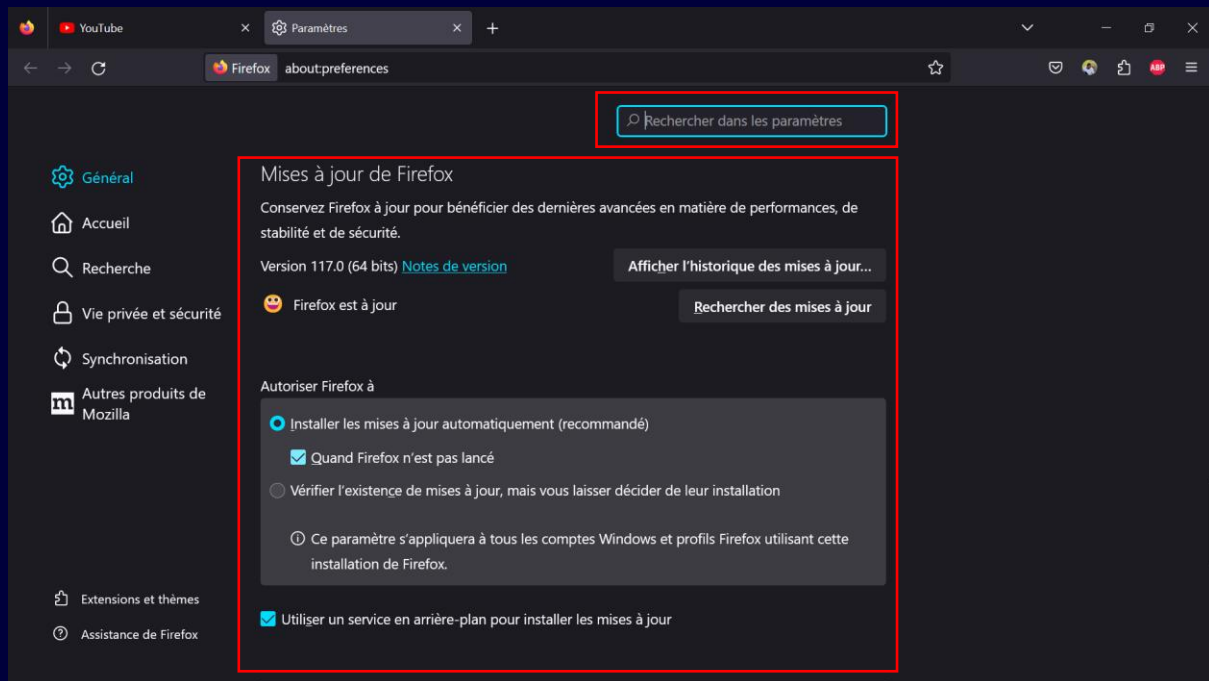


2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes. (case à cocher)

- Pour Chrome



- Pour Firefox



Réponse 2

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.

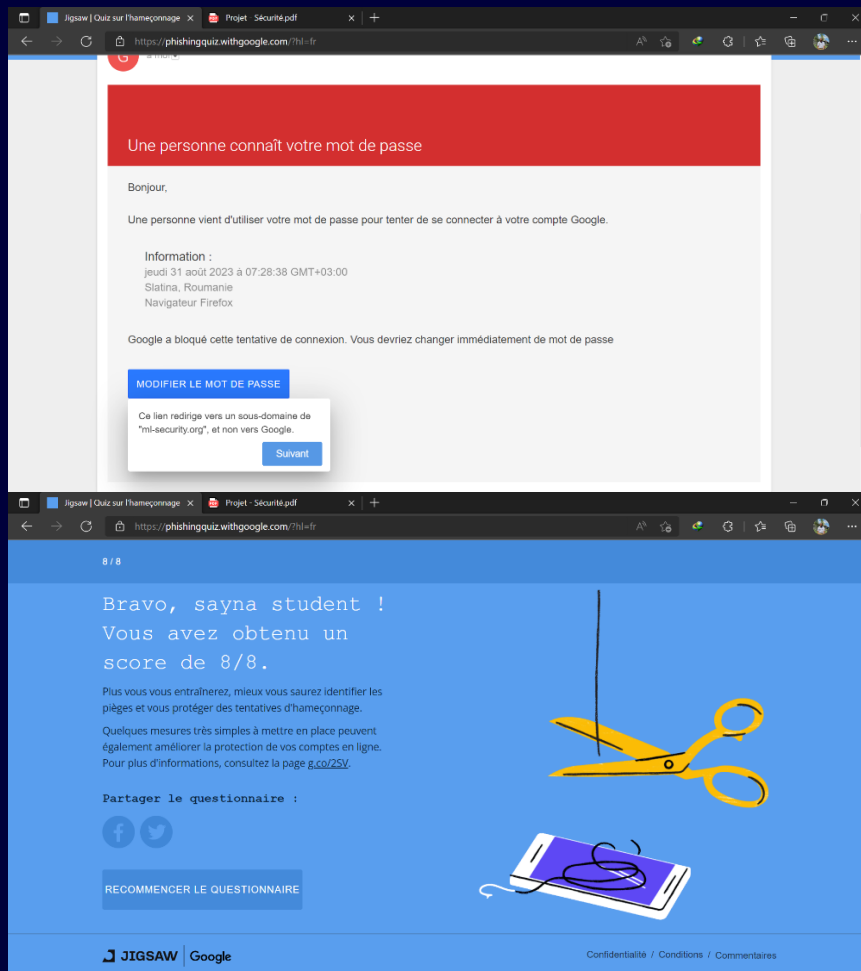
Pour ce faire accède au lien suivant et suis les étapes qui y sont décrites : Exercice 4 - Spam et Phishing

The image displays three sequential screenshots of a web browser showing the 'Phishing Quiz with Google' interface.

Top Screenshot: The main title screen. It features a blue header with 'Français' and a dropdown arrow. The main text asks 'Savez-vous reconnaître une tentative d'hameçonnage ?' (Do you know how to recognize a phishing attempt?). Below this, a paragraph explains that phishing is a malicious attempt to trick someone into providing personal information. A yellow hand icon is shown holding a fishing hook. A blue button labeled 'RÉPONDRE AU QUESTIONNAIRE' (Answer the questionnaire) is present. The footer includes the Google logo, 'Confidentialité / Conditions / Commentaires', and a small 'JIGSAW' logo.

Middle Screenshot: The registration step. It says 'Créer un nom et une adresse e-mail.' (Create a name and an email address). A paragraph explains that the quiz is realistic and that the information provided will not be used for anything. It includes a 'Plus d'infos' link. Below this is a form with two input fields: 'Nom' (Name) containing 'sayna student' and 'Adresse e-mail' (Email address) containing 'bricio.imbiki15@gmail.com'. A blue 'COMMENCER' (Start) button is at the bottom.

Bottom Screenshot: The phishing message preview. It shows a blue header with '0 / 8'. The main text says 'C'est exact. L'URL de ce message est trompeuse.' (That's correct. The URL of this message is deceptive). A paragraph explains that this attack is similar to one used to steal political campaign messages and advises checking URLs. A white button labeled 'MONTREZ-MOI' (Show me) is present. Below this is a simulated email from 'Google' to 'moi' at 07:28. The email body has a red header that says 'Une personne connaît votre mot de passe' (Someone knows your password) and begins with 'Bonjour,'.



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)

Réponse 1

- Site n°1
 - **Indicateur de sécurité**
 - Not secure
 - **Analyse Google**
 - Aucun contenu suspect

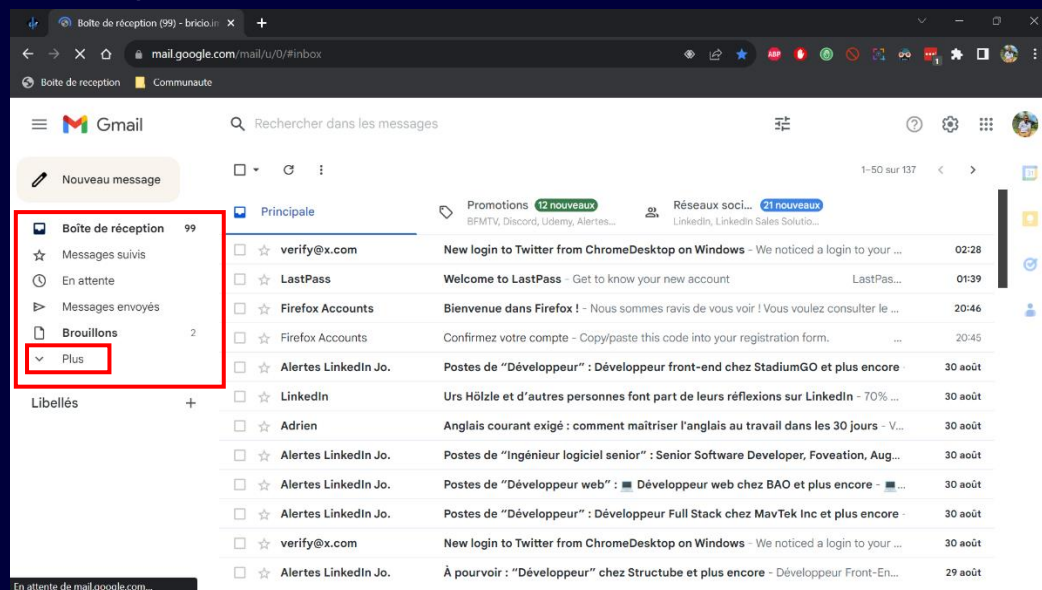
- Site n°2
 - Indicateur de sécurité
 - HTTPS 
 - Analyse Google
 - Aucun contenu suspect
- Site n°3
 - Indicateur de sécurité
 - Not secure
 - Analyse Google
 - Vérifier un URL en particulier (analyse trop générale)

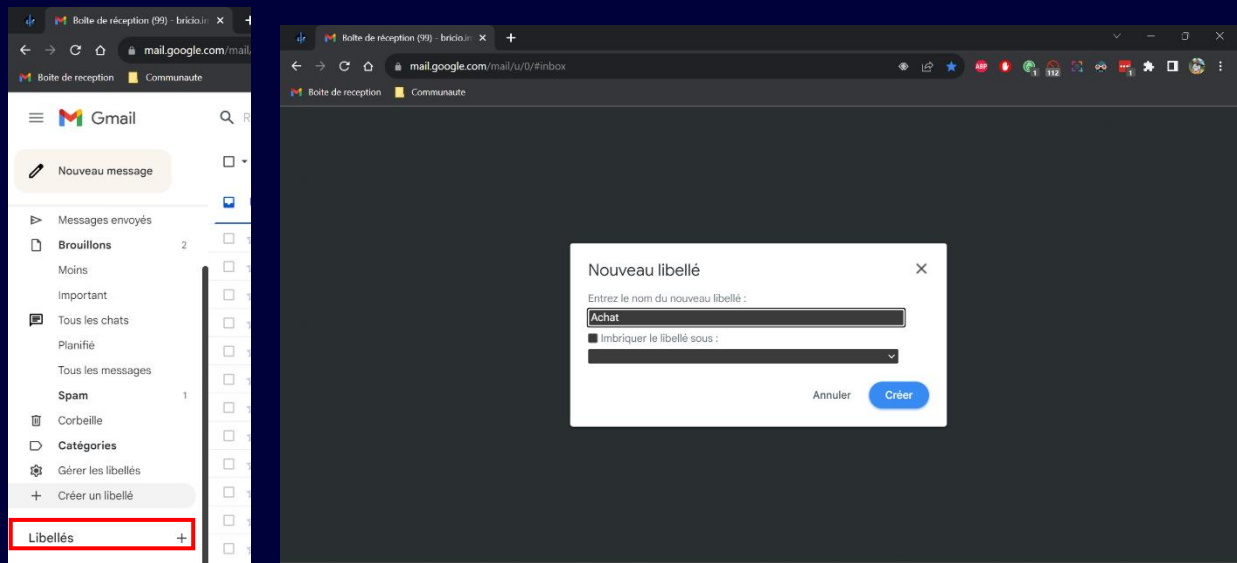
6. Achats en ligne sécurisés

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

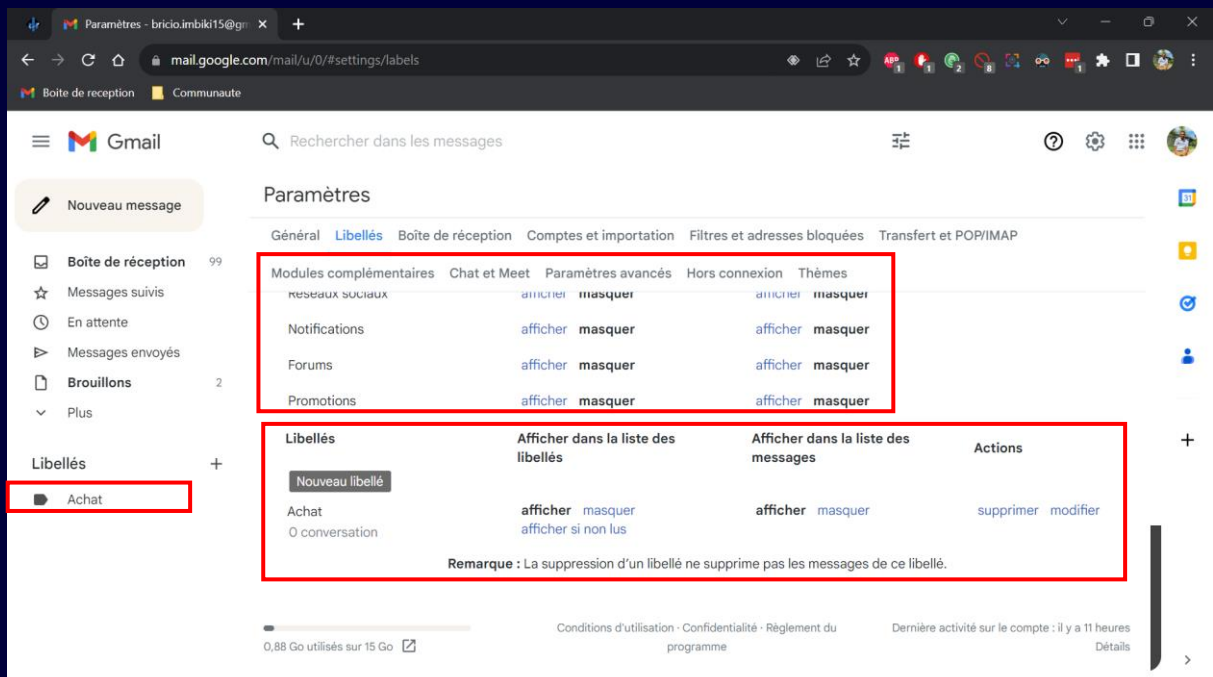
1/ Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le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





- Effectuer un clic sur le bouton “Créer” pour valider l’opération



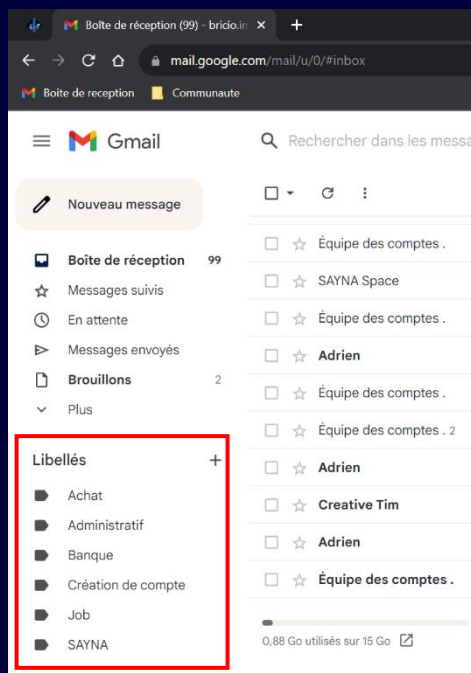
- Tu as maintenant un libellé pour stocker tous tes messages électroniques relatifs aux achats effectués sur internet : confirmation de l’achat, détail de la commande, modalités de livraison

Réponse 1

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

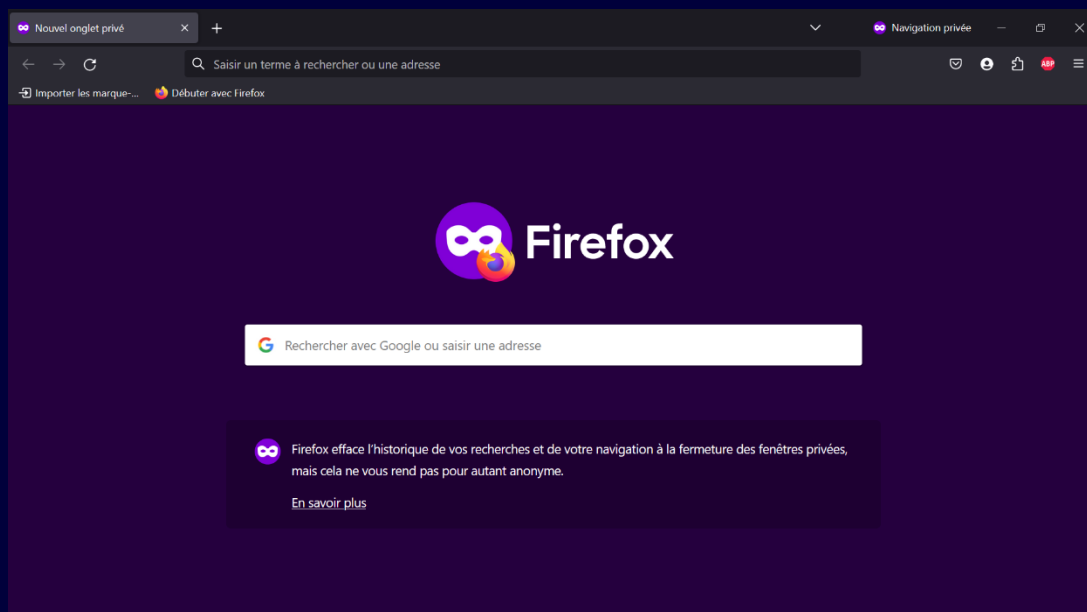
- Achats : historique, facture, conversations liés aux achats
- Administratif : toutes les démarches administratives
- Banque : tous les documents et les conversations liés à la banque personnelle
- Création de compte : tous les messages liés à la création d’un compte (message de bienvenue, résumé du 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*

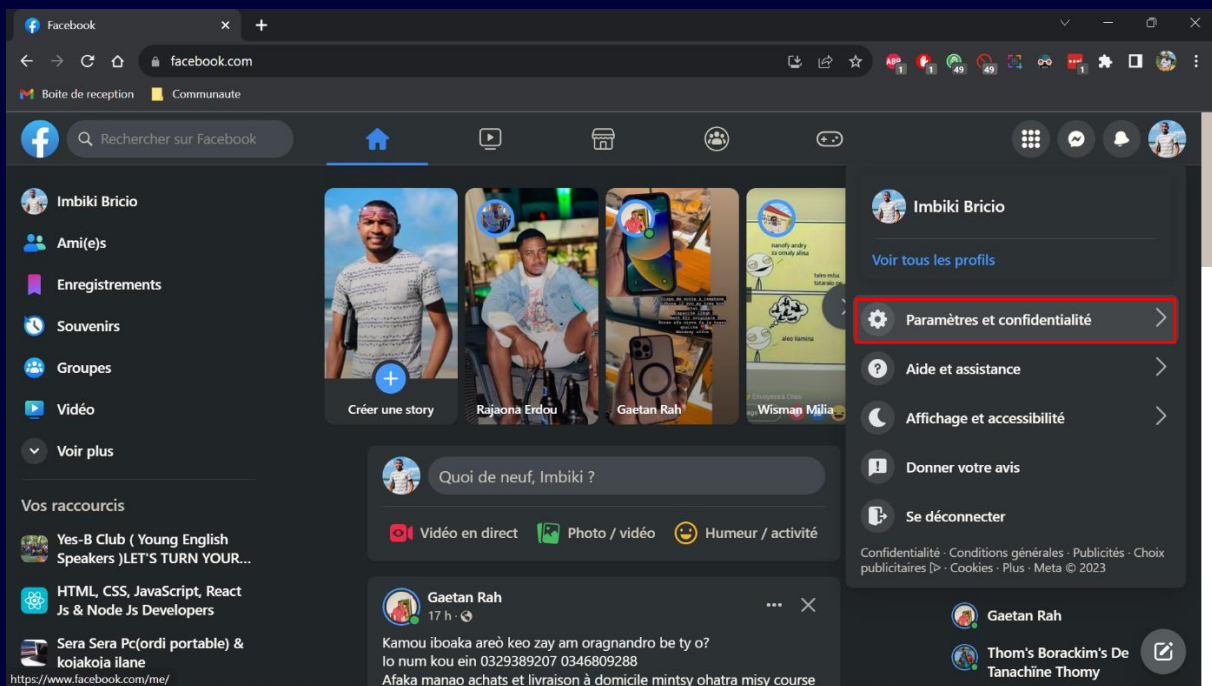


8. Principes de base de la confidentialité des médias sociaux

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"



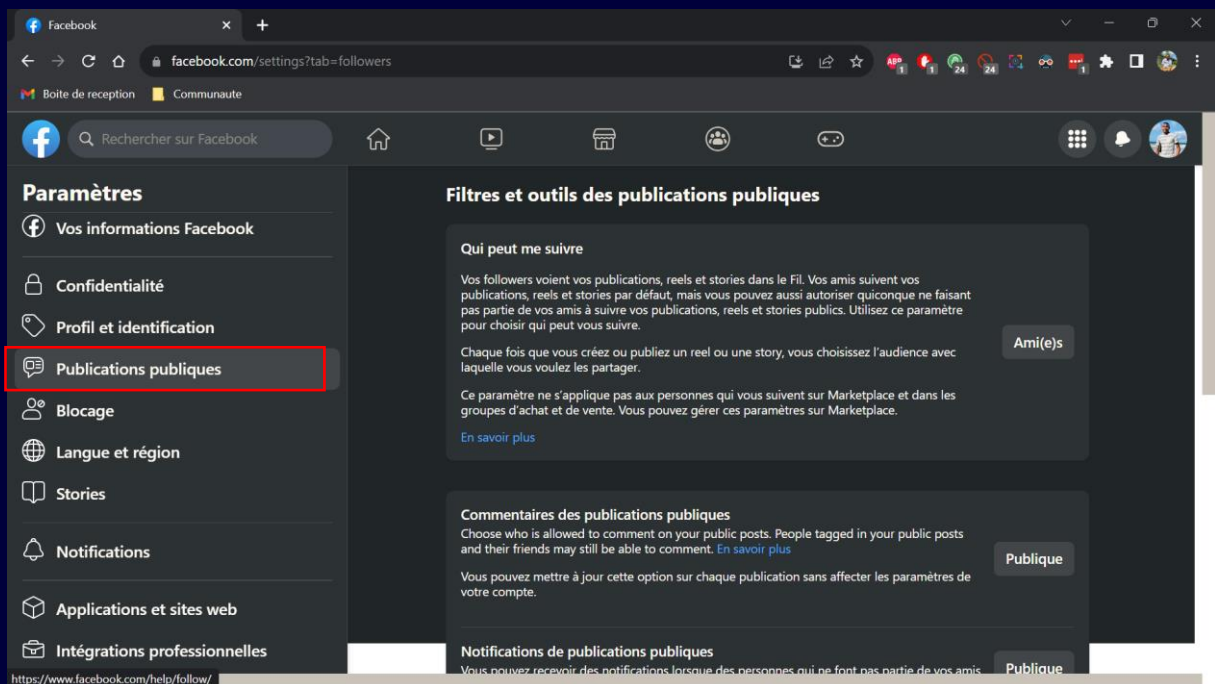
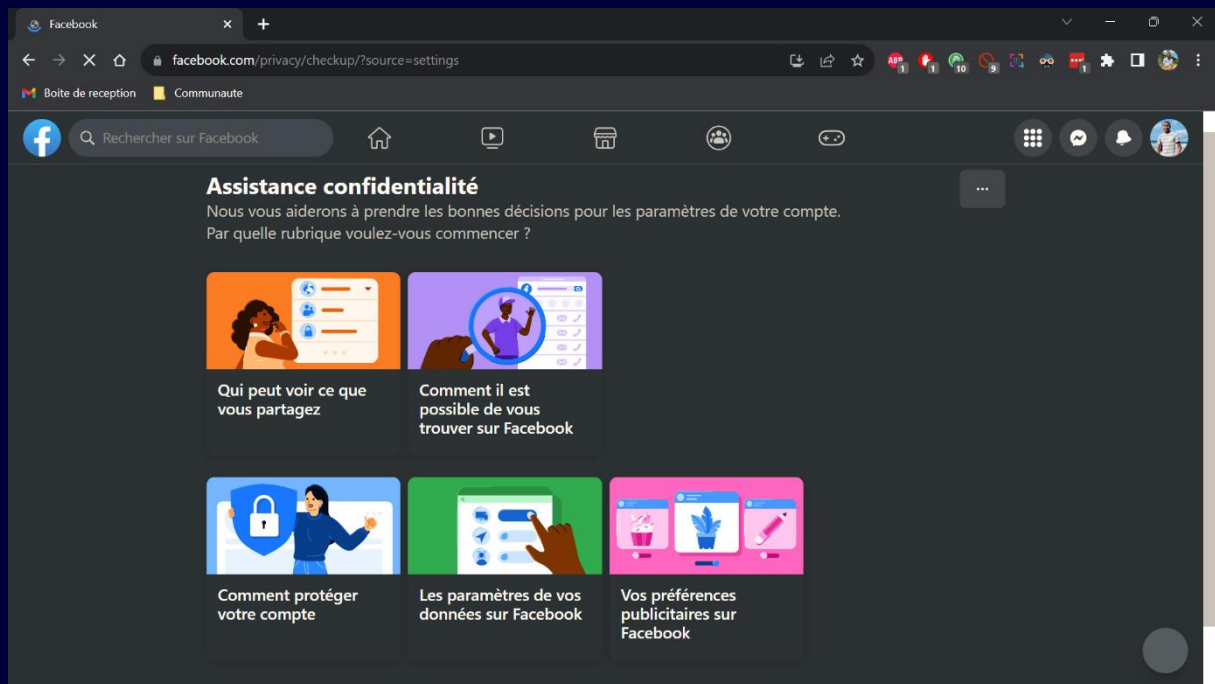
The image displays two screenshots of the Facebook interface, illustrating the steps to access privacy settings.

Screenshot 1: Facebook Home Page

- The browser address bar shows `facebook.com`.
- The left sidebar contains navigation options: Imbiki Brício, Ami(e)s, Enregistrements, Souvenirs, Groupes, Vidéo, and Voir plus.
- The main feed shows a post from Gaetan Rah with the text: "Kamou iboaka areò keo zay am oragnandro be ty o? lo num kou ein 0329389207 0346809288 Afaka manao achats et livraison à domicile mintsy ohatra misy course".
- The right sidebar shows the "Paramètres et confidentialité" (Settings and Privacy) menu, with "Paramètres" (Settings) highlighted by a red box.

Screenshot 2: Facebook Settings Page

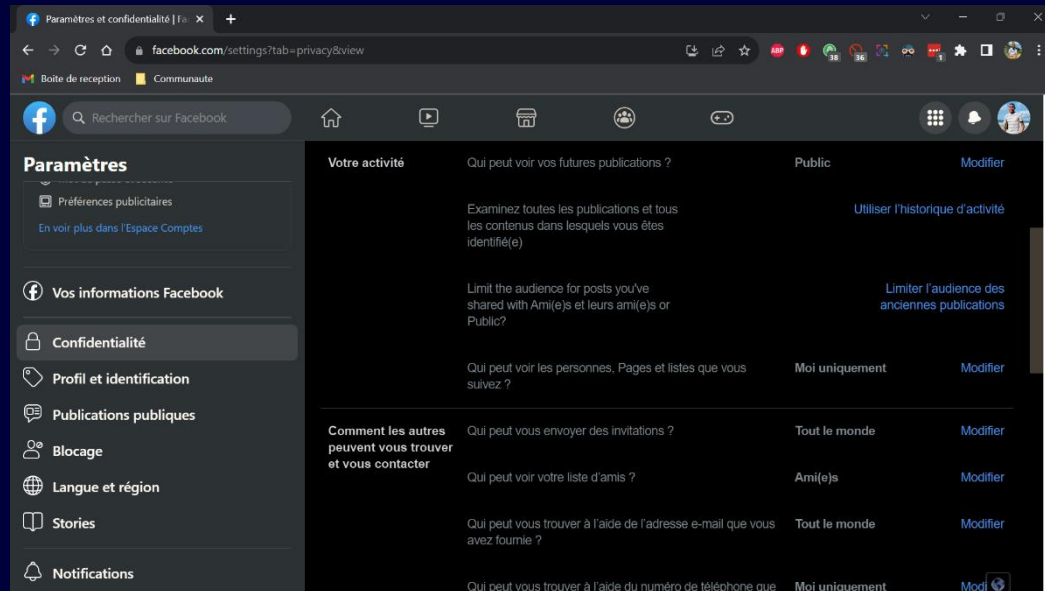
- The browser address bar shows `facebook.com/settings?tab=privacy`.
- The left sidebar contains the "Paramètres" (Settings) menu, with "Confidentialité" (Privacy) highlighted by a red box.
- The main content area is titled "Paramètres et outils de confidentialité" (Settings and Privacy Tools).
- The "Raccourcis de confidentialité" (Privacy Shortcuts) section is highlighted by a red box, containing the text: "Vérifiez certains paramètres importants. Passez en revue rapidement quelques paramètres importants pour vous assurer que vous partagez bien avec les personnes souhaitées."
- Below this, there are sections for "Gérez votre profil" (Manage your profile), "En savoir plus sur le Centre de confidentialité" (Learn more about the Privacy Center), and "Votre activité" (Your activity).
- The "Votre activité" section shows a table with columns for "Qui peut voir vos futures publications ?" (Who can see your future posts?) and "Modifier" (Edit). The current setting is "Public".
- At the bottom, there is a link to "Utiliser l'historique d'activité" (Use activity log).



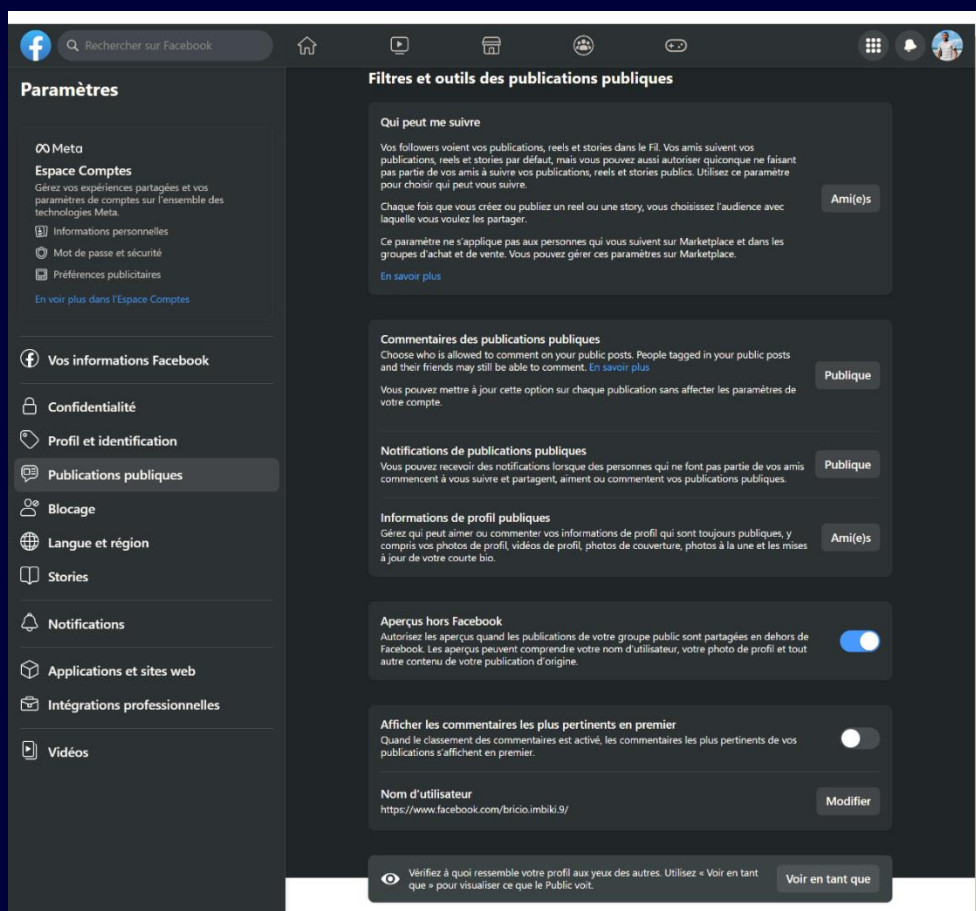
Réponse 1

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



- Publications publiques



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

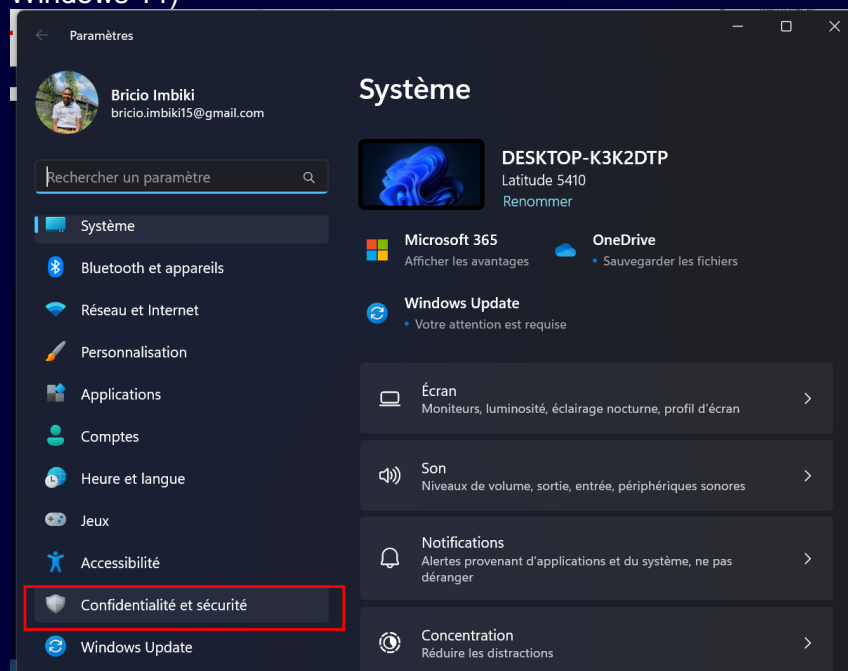
Objectif :

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

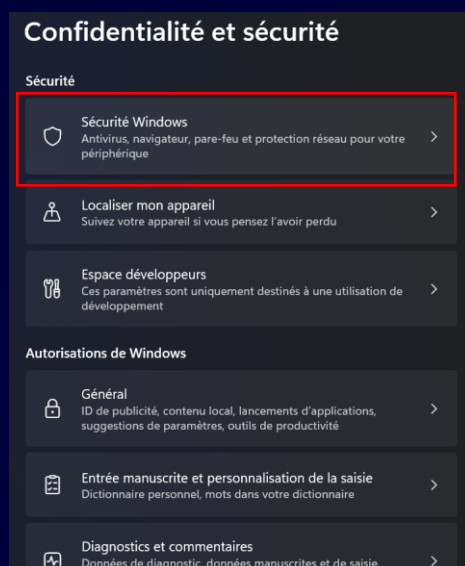
Réponse 1 :

Accéder au paramètre sécurité de l'appareil utilisé (moi, j'utilise l'ordinateur avec un système d'exploitation

Windows 11)



- Clic sur « **Confidentialité et Sécurité** » ensuite clic sur « **Sécurité Windows** » et puis clic sur « **Protection contre virus et menace** »



- Le système montre le statut de la sécurité de l'appareil et on peut faire l'analyse si nécessaire.



Autre solution :

Si votre ordinateur est infecté par un virus, il est important de prendre des mesures pour protéger vos données et votre vie privée. Pour vérifier la sécurité de votre ordinateur, vous pouvez effectuer les exercices suivants:

1. Exécutez une analyse antivirus complète de votre système à l'aide d'un programme antivirus tel que Microsoft Defender, Malwarebytes ou un autre programme antivirus .
2. Ouvrez le Gestionnaire des tâches en appuyant sur Ctrl + Maj + Échap ou en cliquant avec le bouton droit sur la barre des tâches Windows et en sélectionnant "Gestionnaire des tâches". Recherchez les processus inhabituels qui utilisent beaucoup de ressources .
3. Vérifiez que votre système d'exploitation, les logiciels et les applications installés sont à jour .
4. Évaluez l'impact et l'étendue de l'infection. Vérifiez que le virus ne s'est pas propagé à d'autres appareils ou équipements de votre réseau informatique. Mesurez les conséquences de l'infection et identifiez les éventuelles informations perdues ou compromises .

J'espère que cela vous aidera à vérifier la sécurité de votre ordinateur.

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

Réponse 2 :

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

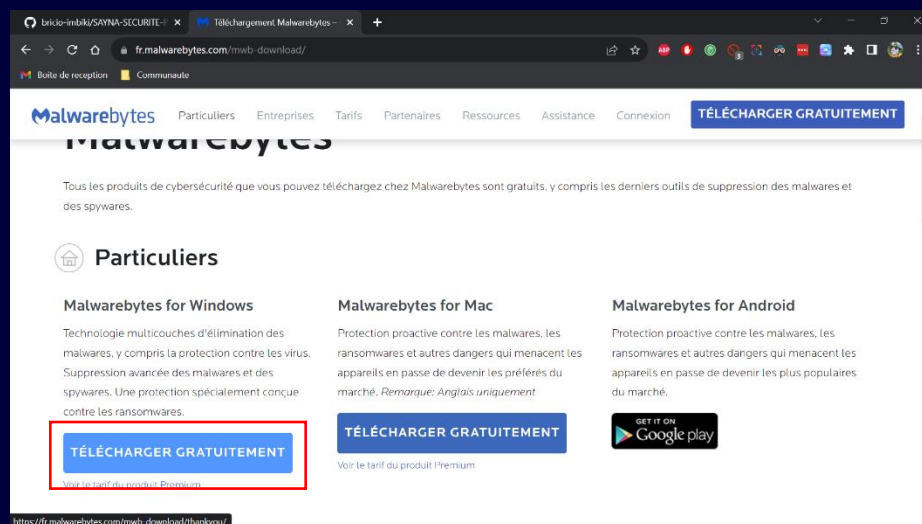
Voici les étapes générales pour installer et utiliser un antivirus et un antimalware sur votre appareil:

Tout d'abord, vous devez télécharger un logiciel antivirus et antimalware fiable. Il existe de nombreux logiciels disponibles sur Internet, tels que Malwarebytes .

On va télécharger d'abord un logiciel d'antivirus par exemple smadav

1. Pour télécharger Malwarebytes clic sur ce lien.

<https://fr.malwarebytes.com/mwb-download/>



2. Une fois que vous avez téléchargé le logiciel selon votre appareil, ouvrez le fichier d'installation et suivez les instructions à l'écran pour installer le logiciel sur votre appareil.
3. Après l'installation, ouvrez le logiciel antivirus et antimalware et effectuez une analyse complète de votre appareil. Cela permettra de détecter tout virus ou malware qui pourrait être présent sur votre appareil.
4. Si le logiciel détecte des menaces, suivez les instructions à l'écran pour supprimer les menaces détectées.
5. Pour une protection continue, assurez-vous de mettre à jour régulièrement votre logiciel antivirus et antimalware pour vous protéger contre les dernières menaces et votre appareil peut être sécurisé.