

Parcours : DISCOVERY

Module : Naviguer en toute sécurité

1 - Introduction à la sécurité sur Internet

Objectif : à la découverte de la sécurité sur internet

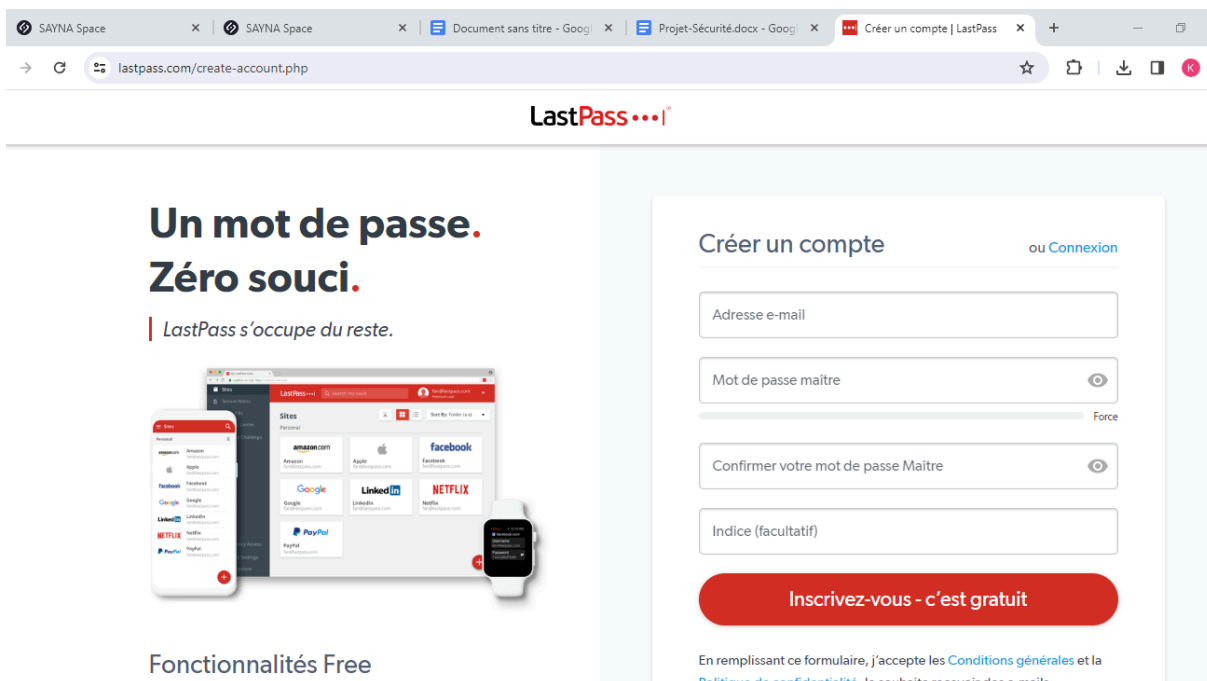
1/ En naviguant sur le web, consultez trois articles qui parlent de sécurité sur internet. Pensez à vérifier la source des informations et essayez de consulter des articles récents pour que les informations soient à jour. Saisissez le nom du site et de l'article.

- Article 1 = [lequipe.fr - VPN Surfshark](https://lequipe.fr/VPN-Surfshark) - Tout savoir sur le VPN Surfshark pour protéger vos données
- Article 2 = [BFMTV - VPN en ligne](https://BFMTV.com/VPN-en-ligne) - VPN en ligne : Quel logiciel pour naviguer en toute sécurité sur internet ?
- Article 3 = [salentolescarroz.fr - Sécurité de vos données en ligne](https://salentolescarroz.fr/Sécurité-de-vos-données-en-ligne) - Comment assurer la sécurité de vos données en ligne ?

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)



Un mot de passe.
Zéro souci.
LastPass s'occupe du reste.

Fonctionnalités Free

Créer un compte ou Connexion

Adresse e-mail

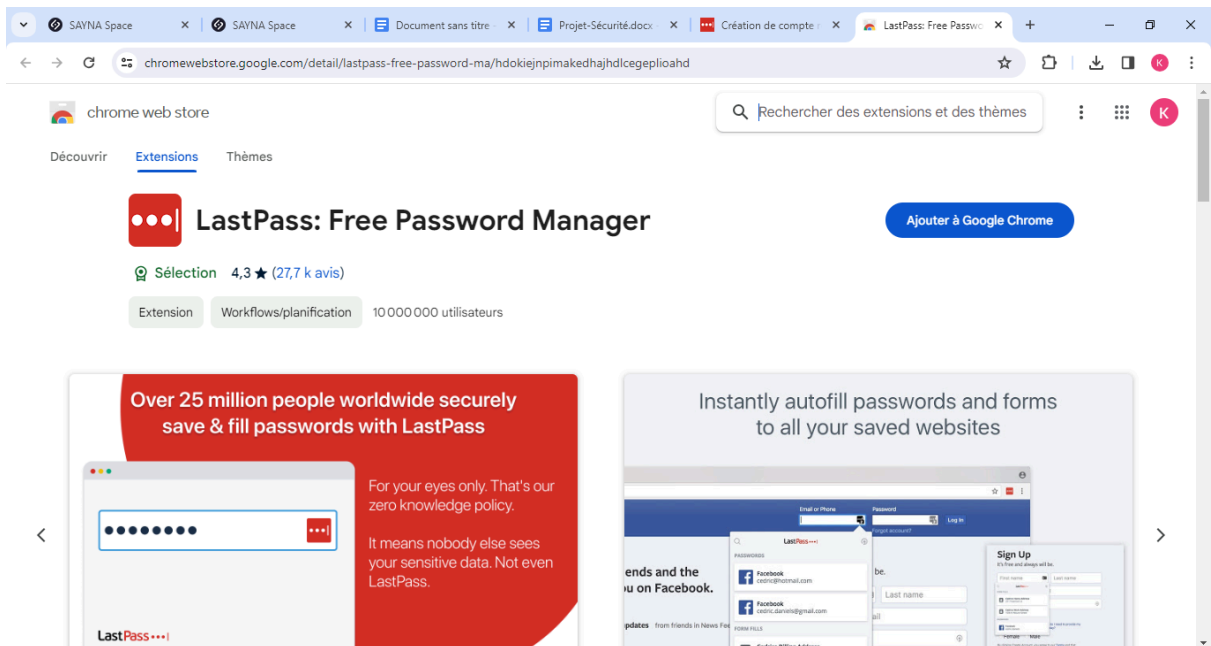
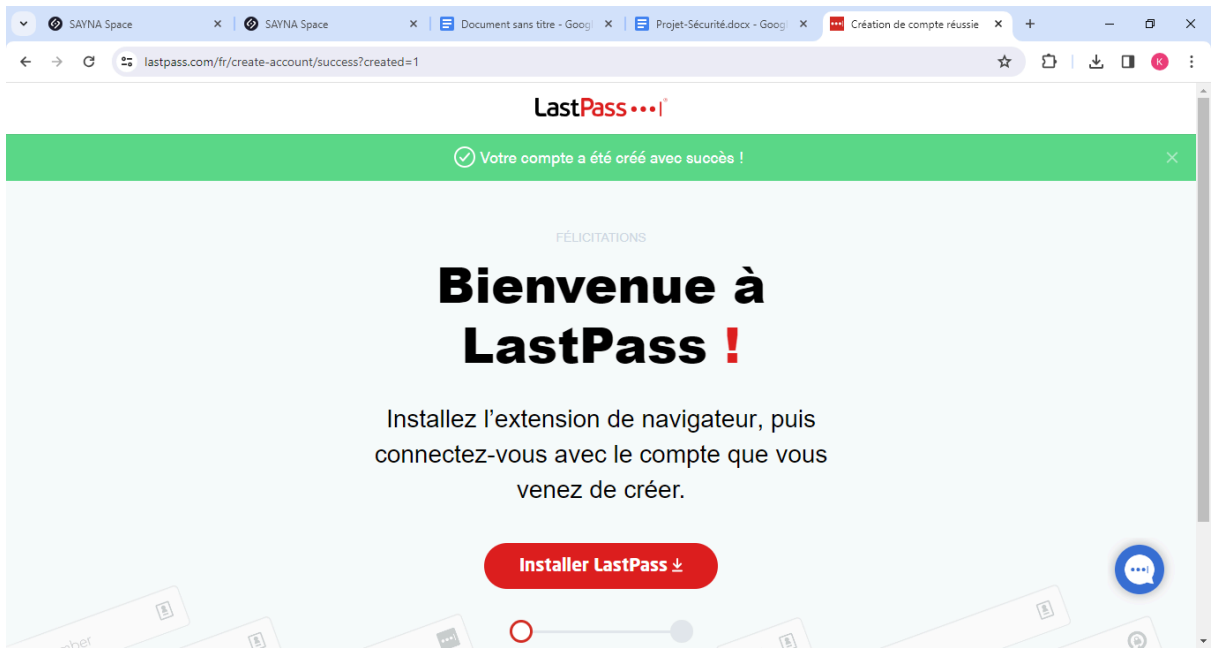
Mot de passe maître

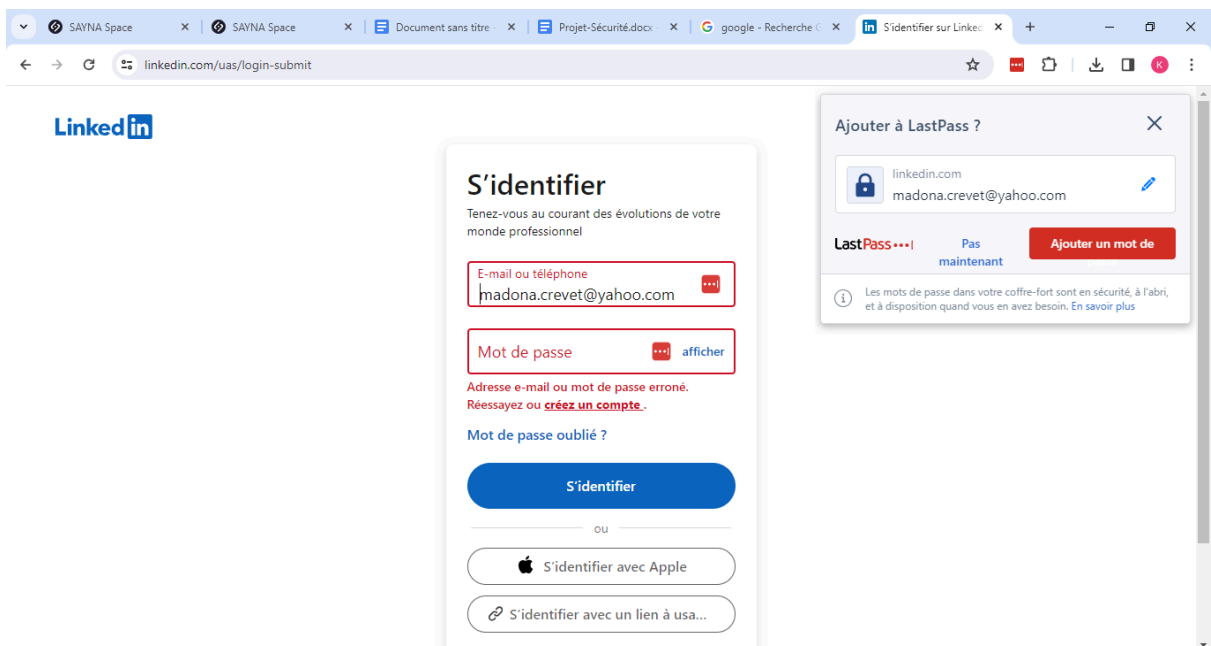
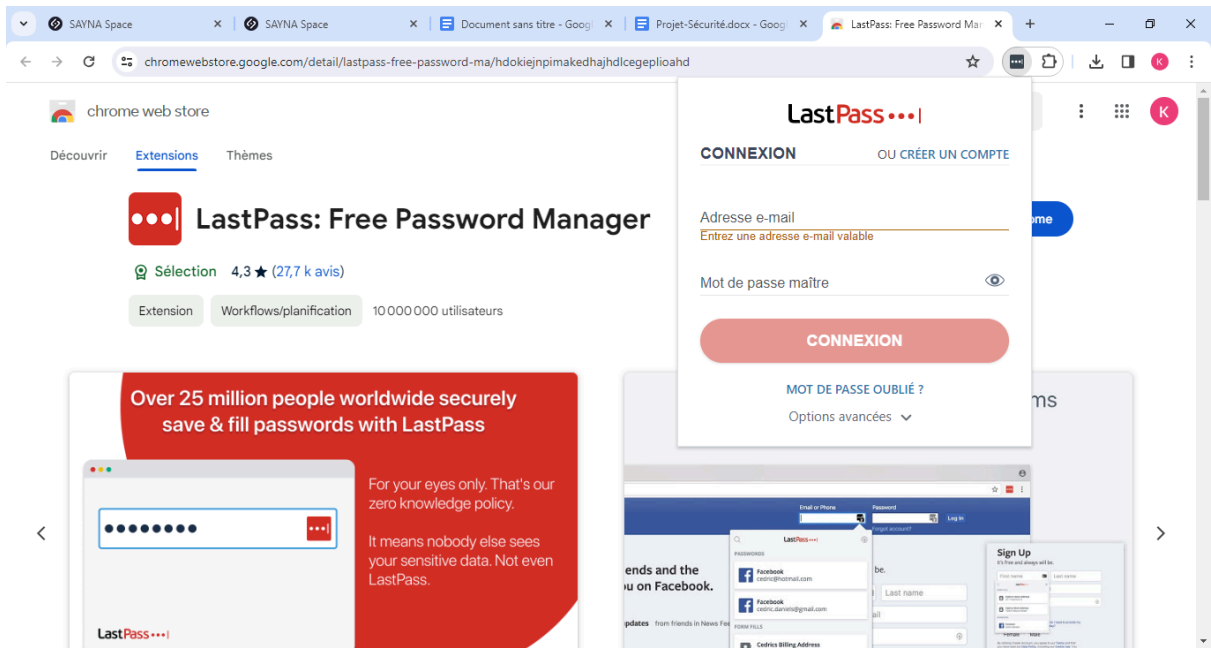
Confirmer votre mot de passe Maître

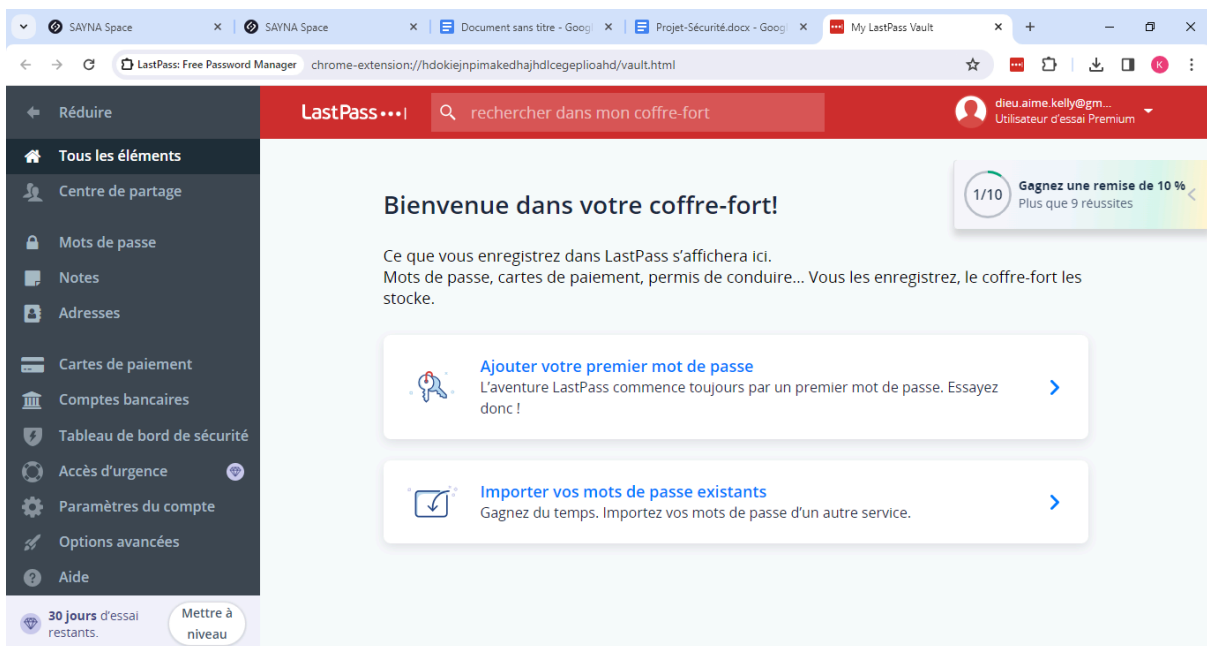
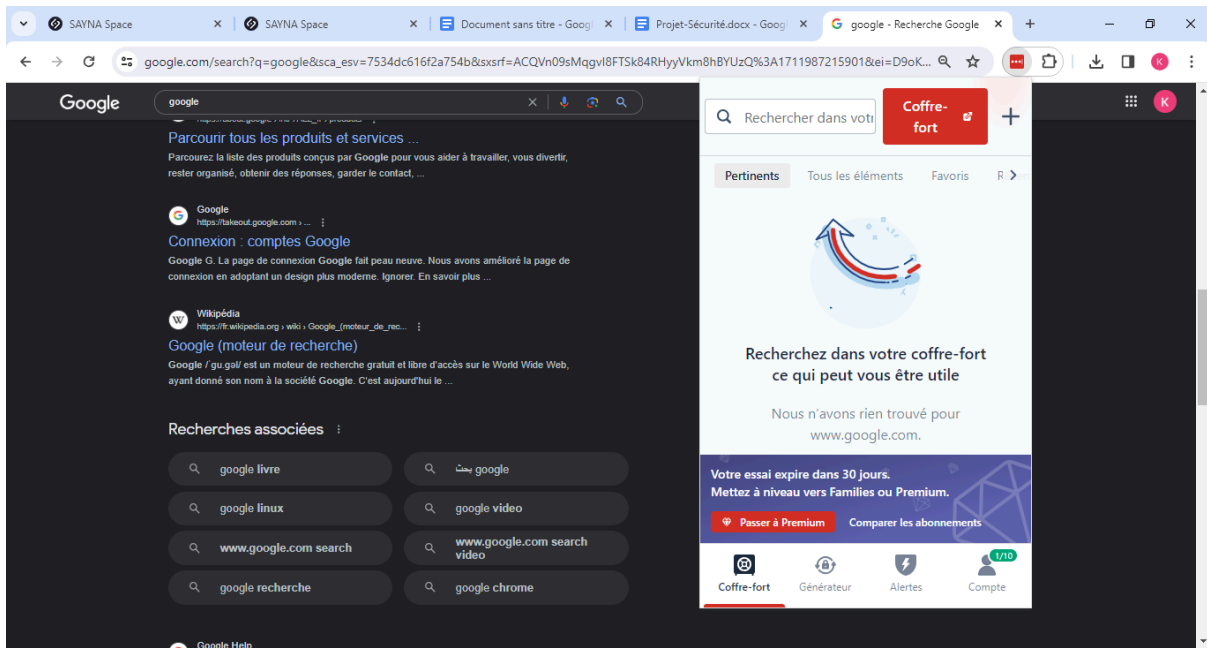
Indice (facultatif)

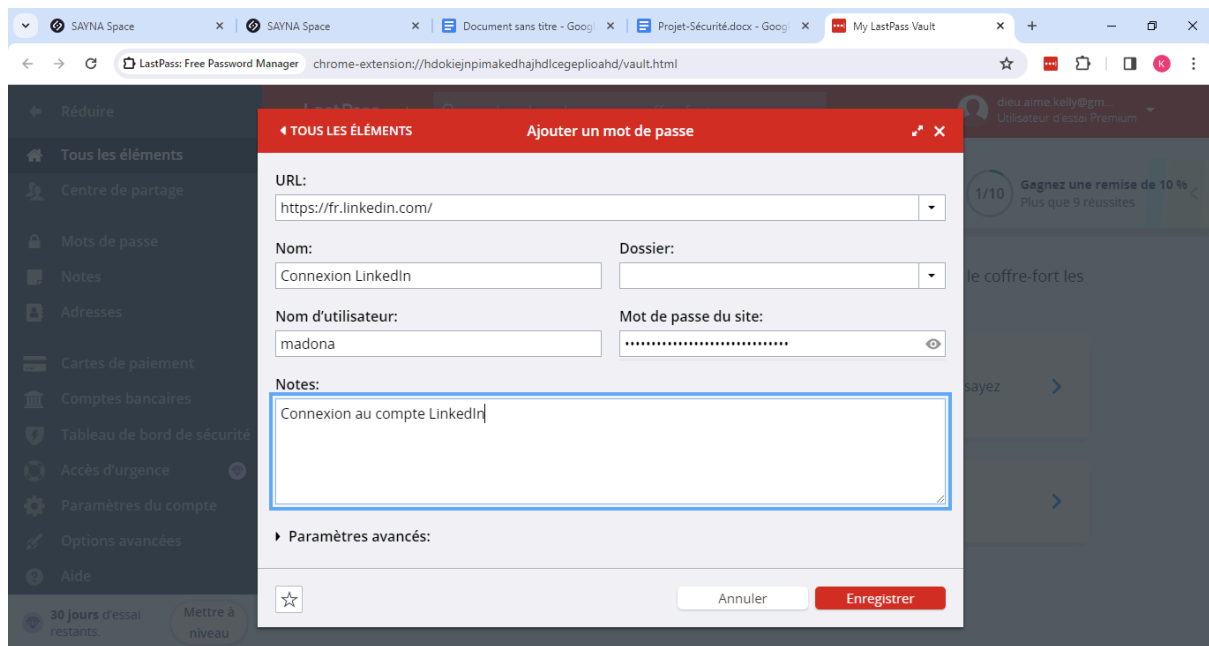
Inscrivez-vous - c'est gratuit

En remplissant ce formulaire, j'accepte les Conditions générales et la Politique de confidentialité. Je souhaite recevoir des e-mails









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

Les sites web qui semblent être malveillants sont :

- www.morvel.com : lorsqu'on clique sur ce lien, il est redirigé vers un autre site web, qui est le site web de BuyDomains, une société qui vend des noms de domaine. Cela peut être considéré comme normal, car le site web de BuyDomains est légitime et ne semble pas être un site web malveillant. Mais redirection vers un site de vente de domaine renforce l'idée que le site www.morvel.com peut ne pas être légitime et peut être associé à des activités malveillantes.
- www.fessebook.com : affiche un message d'erreur "403 Forbidden - L'accès à cette ressource sur le serveur est interdit". Cela indique que l'accès au site est refusé par le serveur. Ce type de message peut survenir pour diverses raisons, notamment si le site est configuré pour restreindre l'accès à certaines adresses IP, si l'utilisateur n'est pas autorisé à accéder au contenu, ou si le site est en panne ou mal configuré. Dans tous les cas..
- www.instagram.com : se dirige vers <https://www.instagram.com/> . Ce qui confirme que le site www.instagram.com est une tentative de contrefaçon du site légitime de

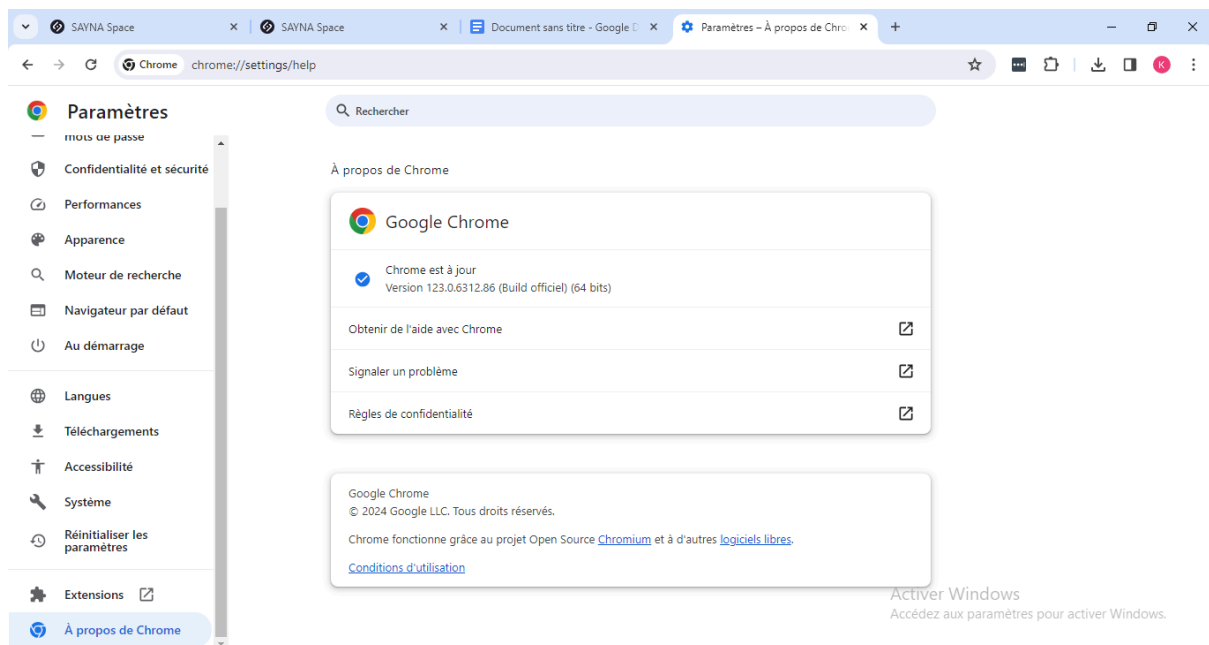
partage de photos "Instagram". Les sites qui tentent d'imiter des marques populaires peuvent être utilisés à des fins malveillantes, telles que le phishing, la collecte de données personnelles ou la distribution de logiciels malveillants.

Les seuls sites qui semblaient être cohérents sont donc :

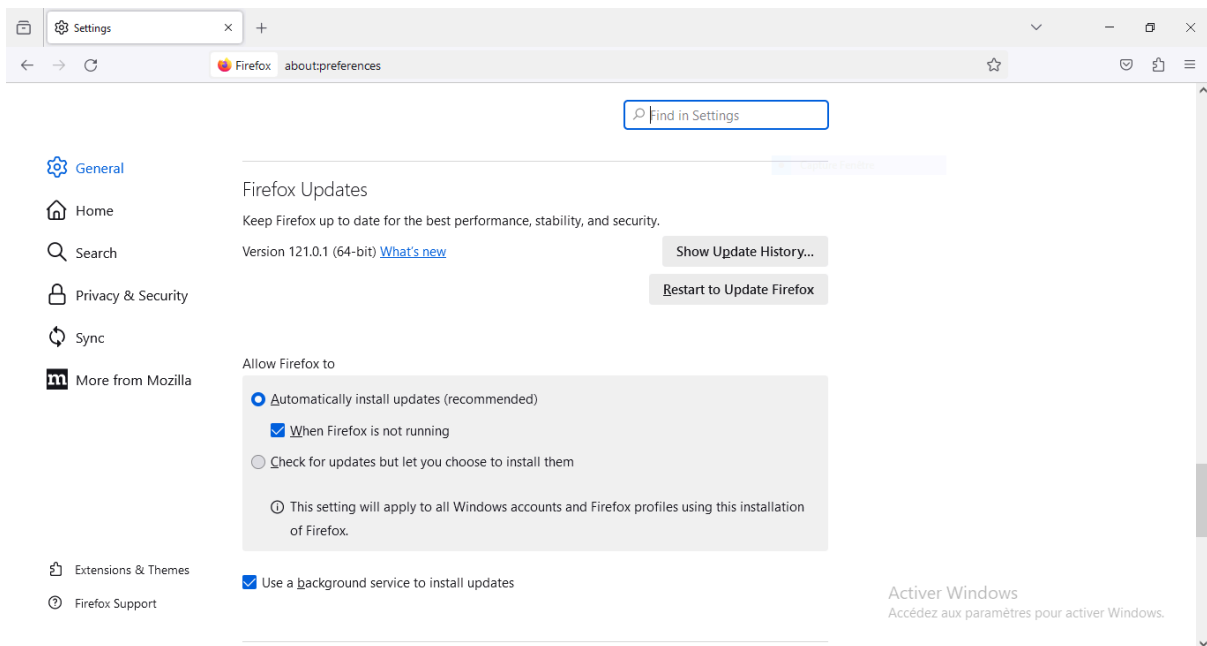
- www.dccomics.com le site officiel de l'univers DC Comics
- www.ironman.com le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

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)



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](#)



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
 - 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)

Reponse 1

- Site n°1 vostfree.tv
 - Indicateur de sécurité
 - HTTPS Not secure

- Analyse Google
 - Vérifier un URL en particulier
- Site n°2 tv5monde.com
 - Indicateur de sécurité
 - HTTPS
 - Analyse Google
 - Aucun contenu suspect
- Site n°3 baidu.com
 - Indicateur de sécurité
 - Not secure
 - Analyse Google
 - Vérifier un URL en particulier

6 - Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

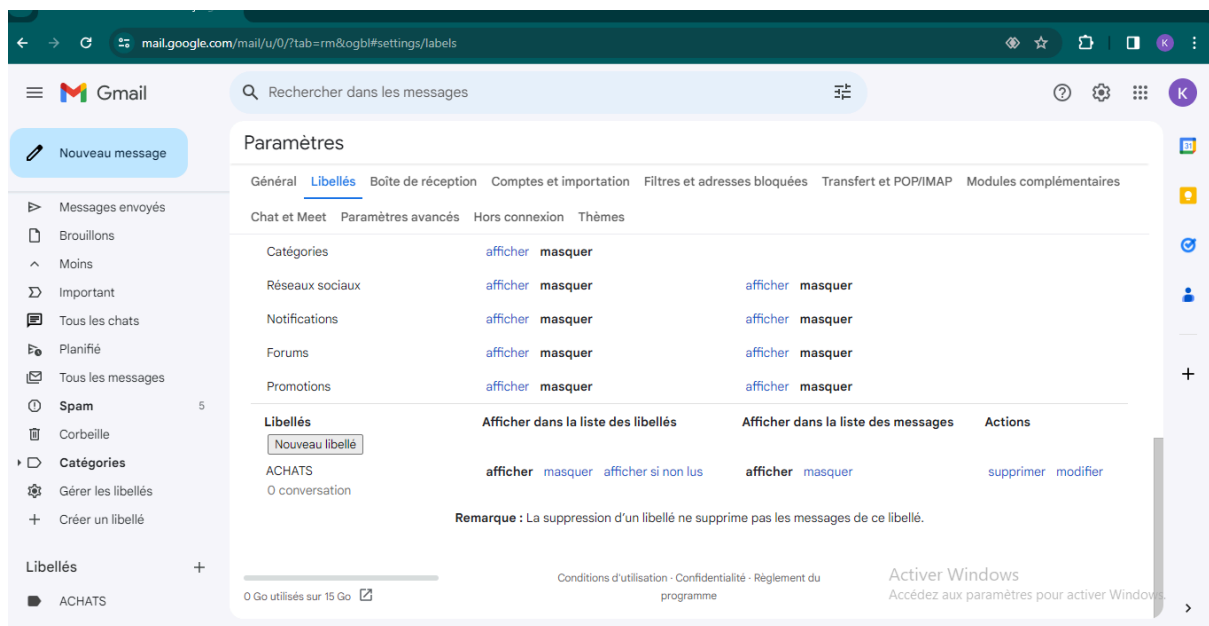
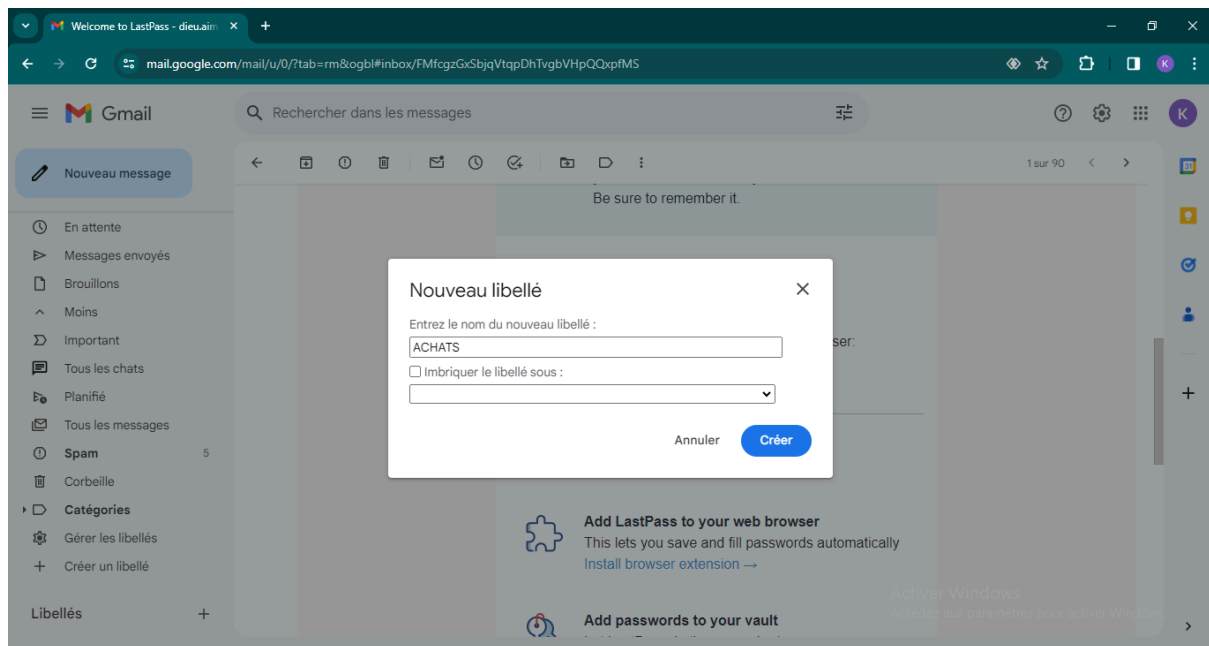
1/ Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le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

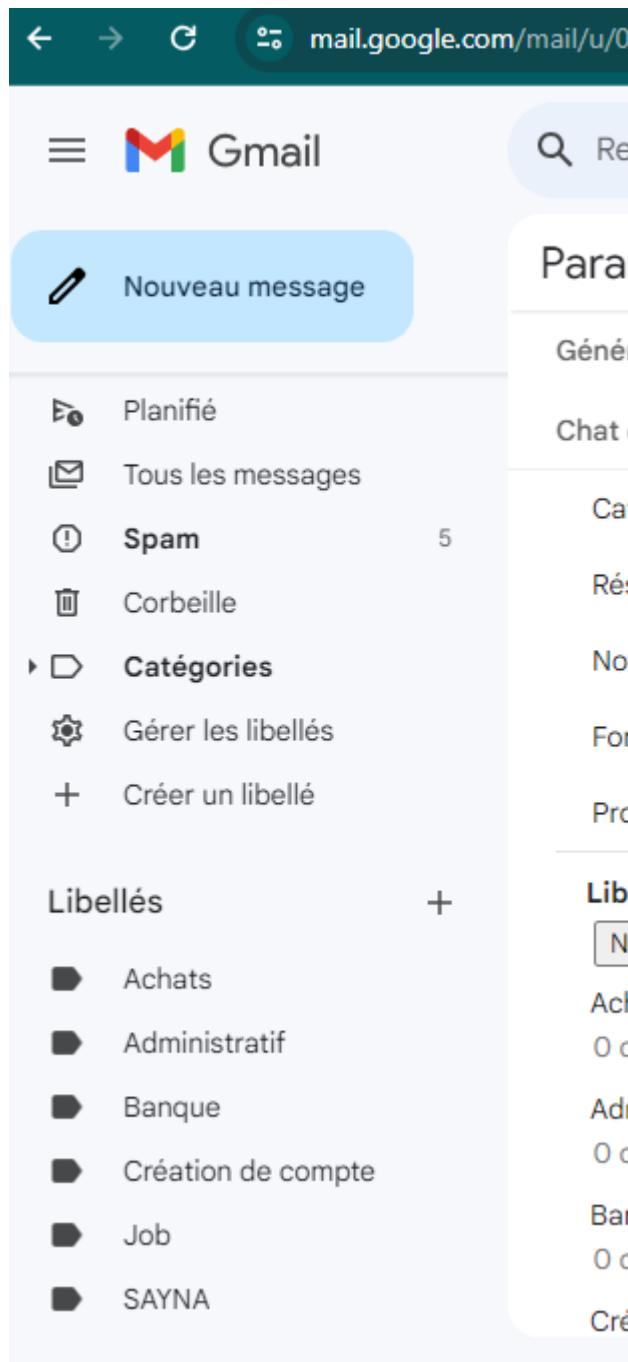
- Pour commencer, accède à ta messagerie électronique. Pour rappel, tu peux y accéder rapidement en ouvrant un nouvel onglet (dans la barre des favoris ou via le raccourci)



Réponse 1

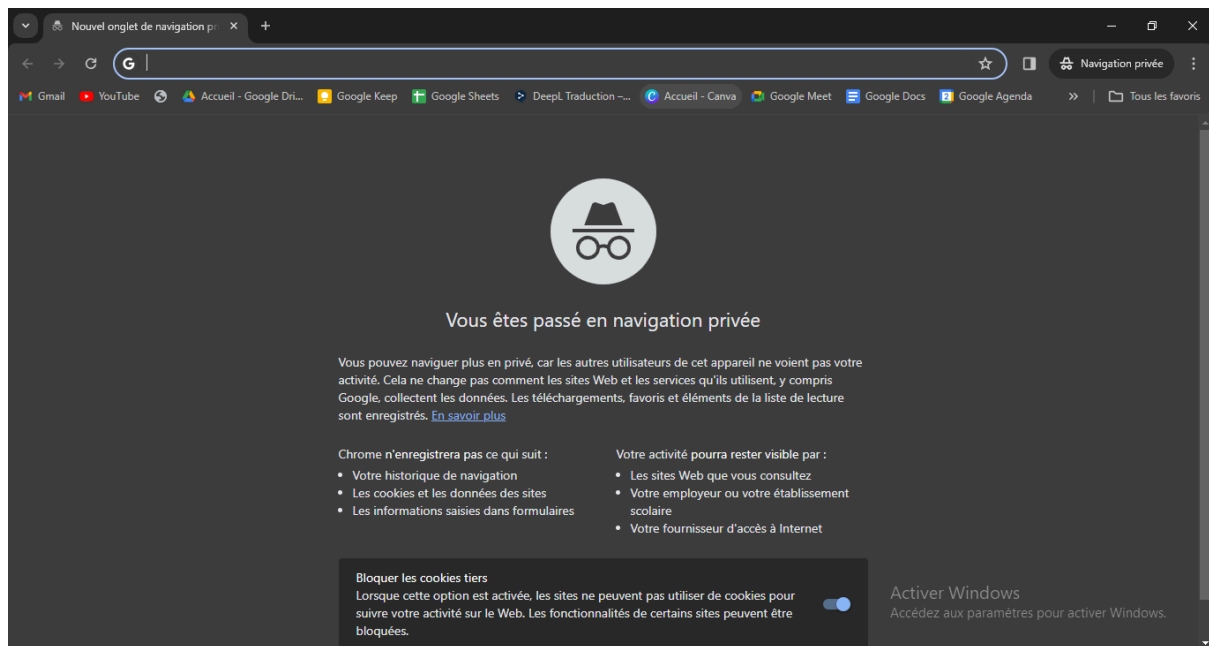
Voici un exemple d'organisation de libellé pour gérer sa messagerie électronique :

- 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.)



7 - Comprendre le suivi du navigateur

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

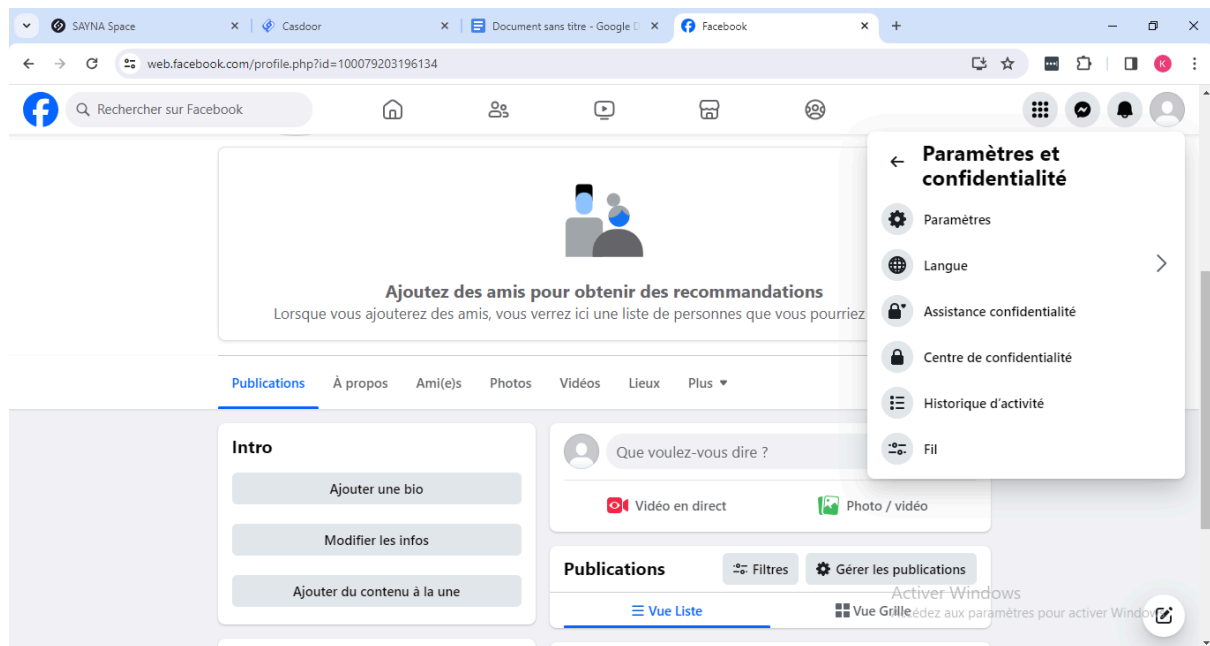


8 - Principes de base de la confidentialité des médias sociaux

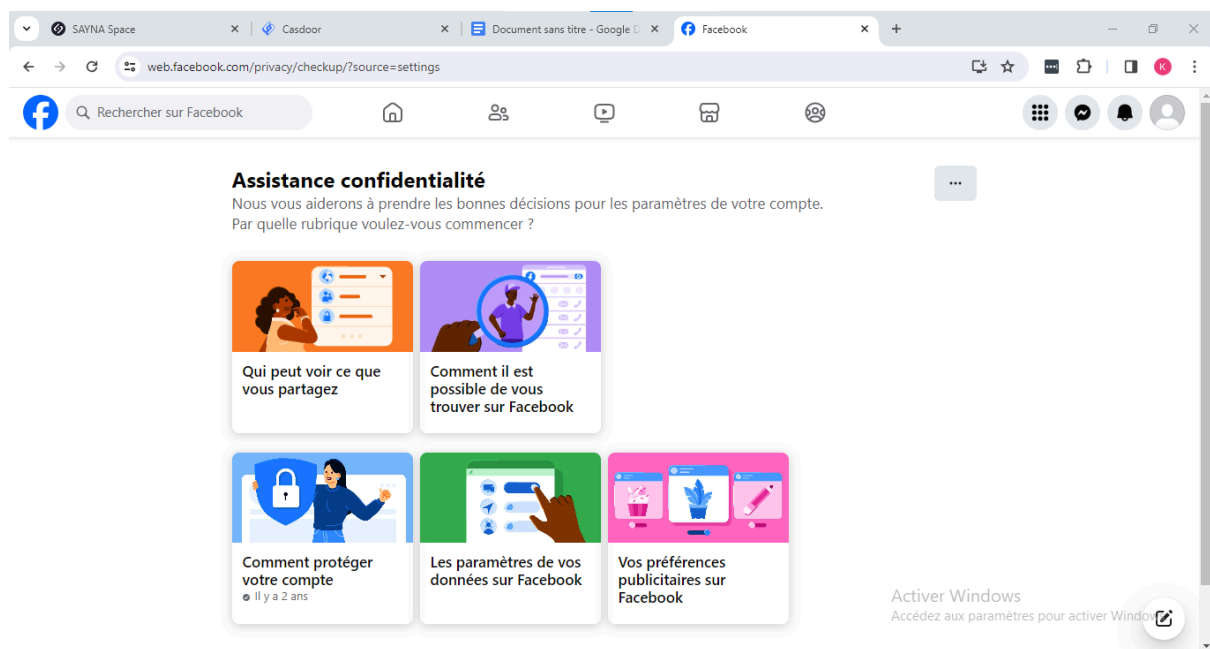
Objectif : Régler les paramètres de confidentialité de Facebook

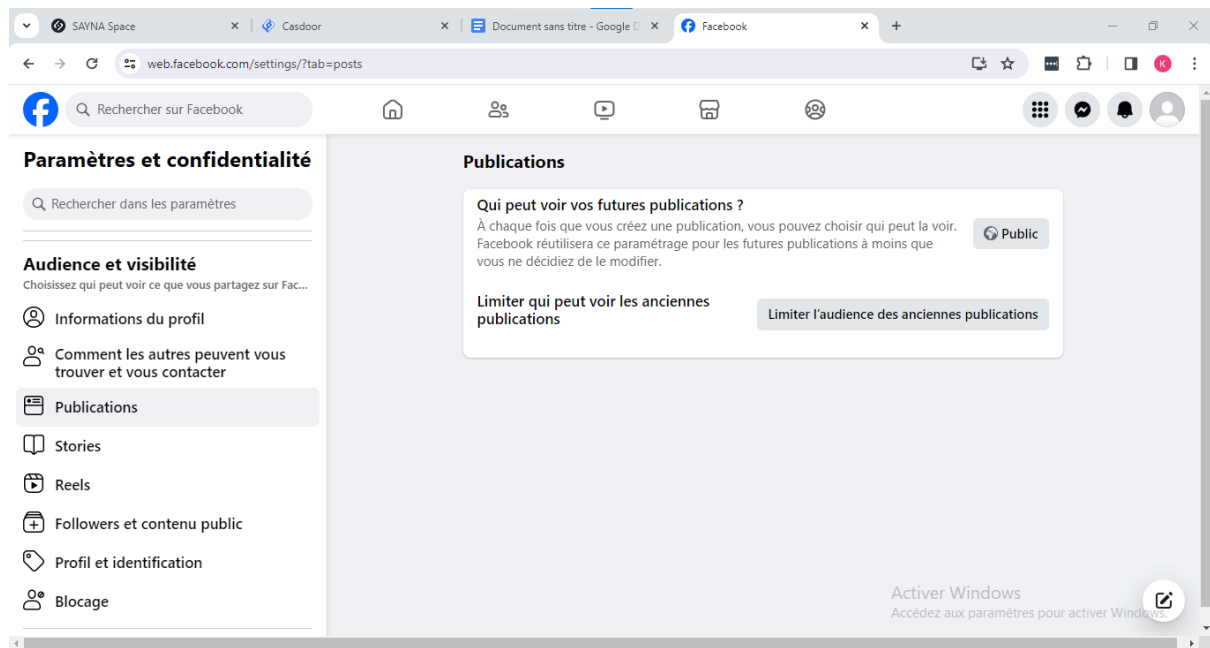
1/ Plus tôt dans le cours (Internet de base) tu as déjà été amené à utiliser ce réseau social en partageant une publication. Dans cet exercice on va te montrer le réglage des paramètres de confidentialité pour Facebook. Suis les étapes suivantes. (case à cocher)

- 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"



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





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 ????????

Exercices:

- Exercice 1 : Analyse antivirus complète
 - Si vous n'avez pas déjà installé un antivirus, téléchargez-en un à partir d'une source fiable.
 - Effectuez une analyse complète de votre système à l'aide de l'antivirus nouvellement installé.
 - Notez tous les fichiers ou programmes signalés comme infectés ou suspects.
- Exercice 2 : Analyse avec un logiciel anti-malware
 - Téléchargez et installez un logiciel anti-malware reconnu et fiable.
 - Effectuez une analyse complète de votre système à l'aide de ce logiciel.
 - Notez les éventuelles infections ou programmes malveillants détectés.
- Exercice 3 : Mise à jour des logiciels
 - Assurez-vous que tous vos logiciels, y compris votre système d'exploitation, sont à jour avec les derniers correctifs de sécurité.
 - Vérifiez régulièrement les mises à jour disponibles et installez-les dès qu'elles sont disponibles.
- Exercice 4 : Vérification des paramètres de sécurité

- Passez en revue les paramètres de sécurité de votre navigateur web, de votre pare-feu et d'autres applications critiques.
- Assurez-vous que les pare-feu sont activés et correctement configurés pour bloquer les activités suspectes.
- Exercice : Éducation à la sécurité informatique
 - Familiarisez-vous avec les signes courants d'une infection par un virus ou un logiciel malveillant.
 - Enseignez à d'autres personnes de votre environnement de travail les meilleures pratiques en matière de sécurité informatique.

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

Exercice:

- Sur un ordinateur Windows :
 - Téléchargez un antivirus reconnu comme Avast, Bitdefender ou Kaspersky depuis leur site officiel.
 - Suivez les instructions d'installation.
 - Une fois installé, exécutez une analyse complète de votre système.
 - Pour un logiciel anti-malware, vous pouvez utiliser des outils comme Malwarebytes.
 - Exécutez régulièrement des analyses avec ces logiciels pour détecter et supprimer les menaces potentielles.
- Sur un Mac :
 - Utilisez l'antivirus intégré à macOS, appelé XProtect.
 - Vous pouvez également opter pour des solutions tierces comme Avast ou Sophos.
 - Installez l'antivirus et suivez les instructions pour configurer et effectuer une analyse complète du système.
- Sur un appareil mobile (Android ou iOS) :
 - Téléchargez et installez une application antivirus à partir du Google Play Store (pour Android) ou de l'App Store (pour iOS).
 - Des options populaires incluent Avast, AVG ou Bitdefender pour Android, et Avira ou Norton pour iOS.
 - Suivez les instructions pour configurer l'application et effectuer une analyse complète de votre appareil.