

# **Parcours : DISCOVERY**

## **Module : Comment internet fonctionne**

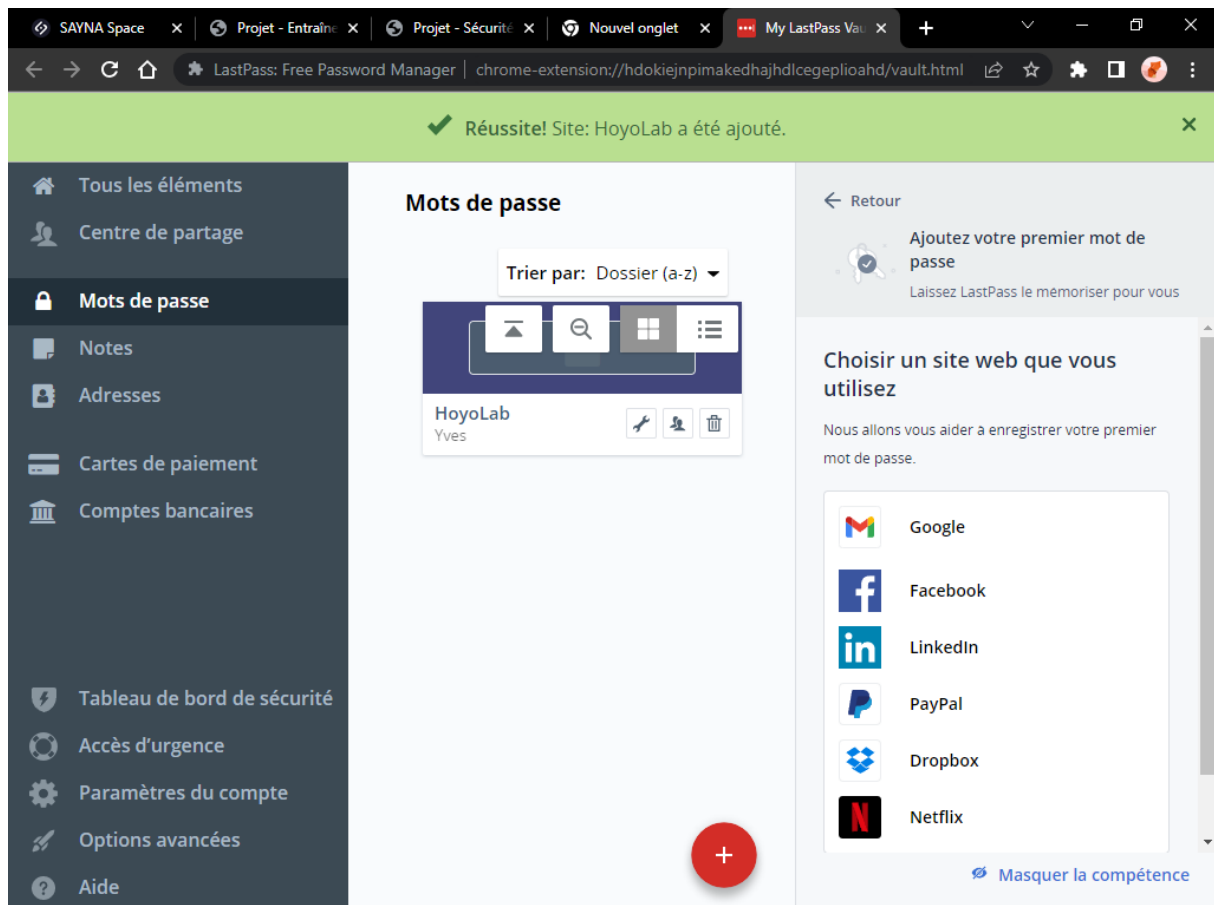
**Projet 1 - Un peu plus de sécurité, on n'en a  
jamais assez !**

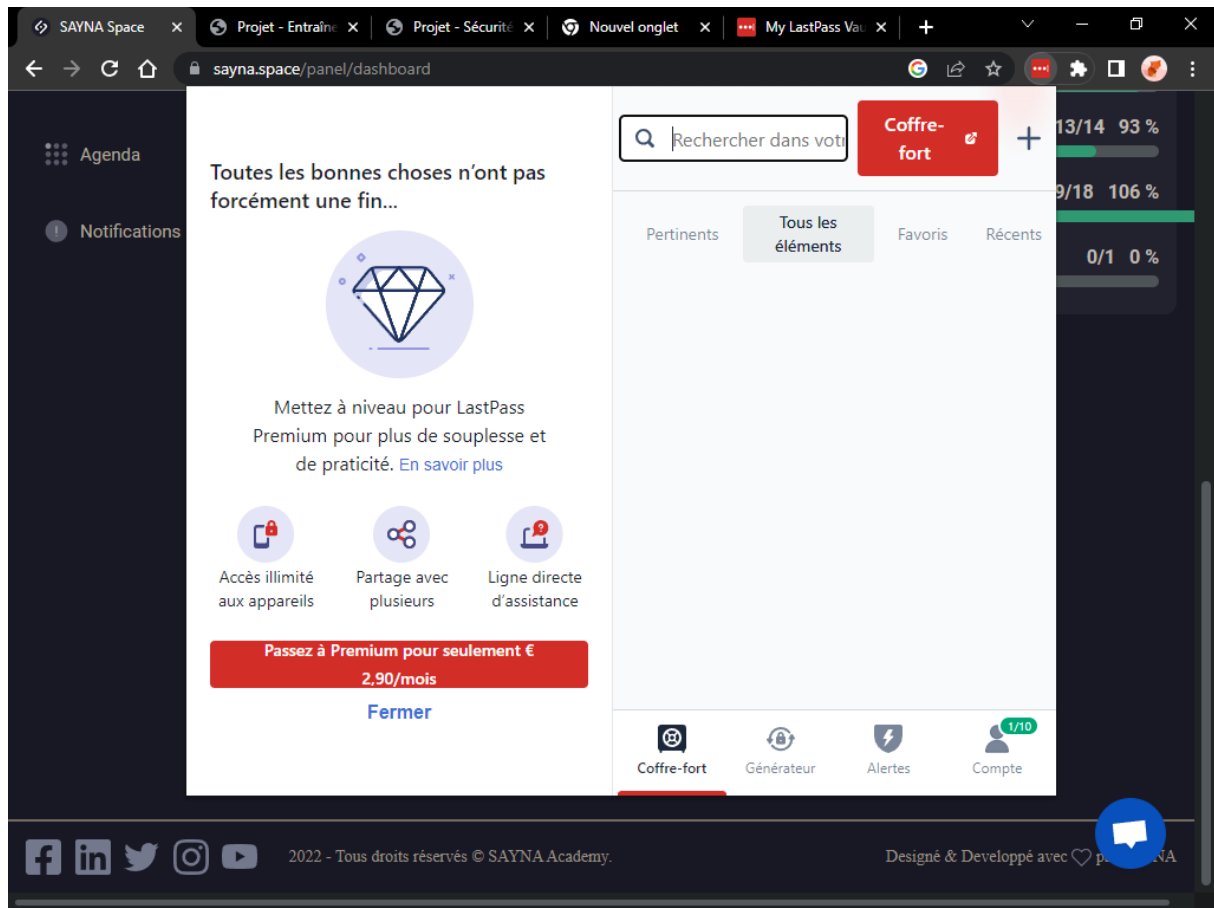
# 1 - Introduction à la sécurité sur Internet

Articles sur la sécurité internet.

- Articles 1 : [Kaspersky Confidentialité et sécurité sur Internet : 5 conseils de sécurité](#)
- Articles 2 : [O-communication Comment se protéger sur internet ?](#)
- Articles 3 : [GoDaddy les meilleurs outils pour sécuriser votre site web](#)

## 2 - Créer des mots de passe forts





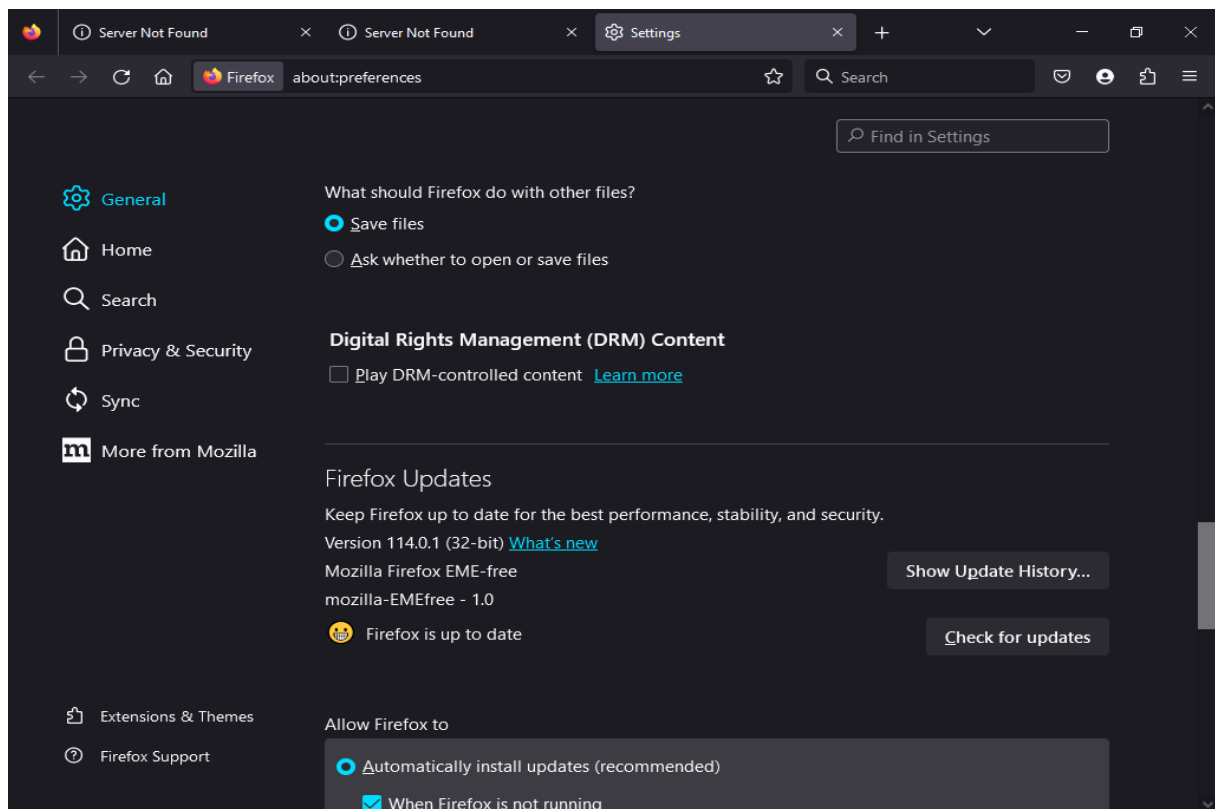
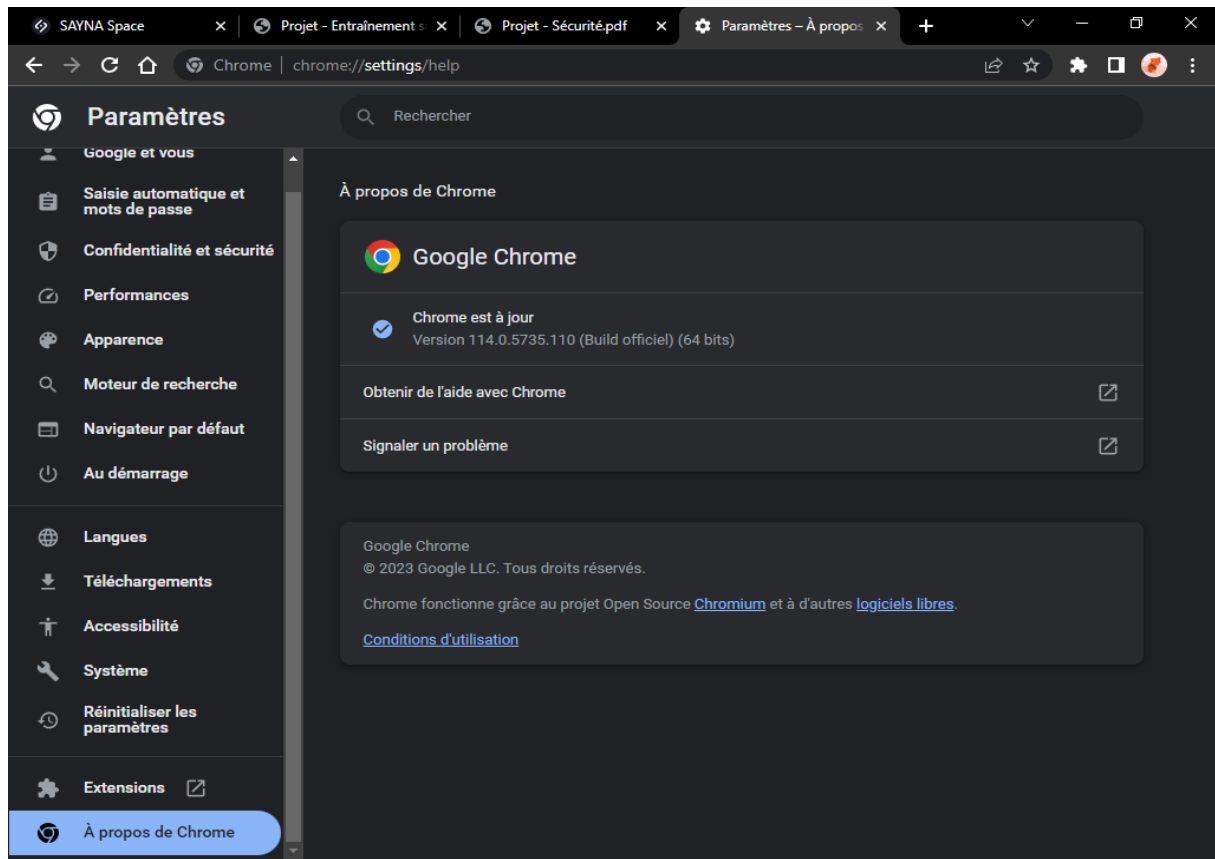
### 3 - Fonctionnalité de sécurité de votre navigateur

**Les sites web qui semblent être malveillants sont :**

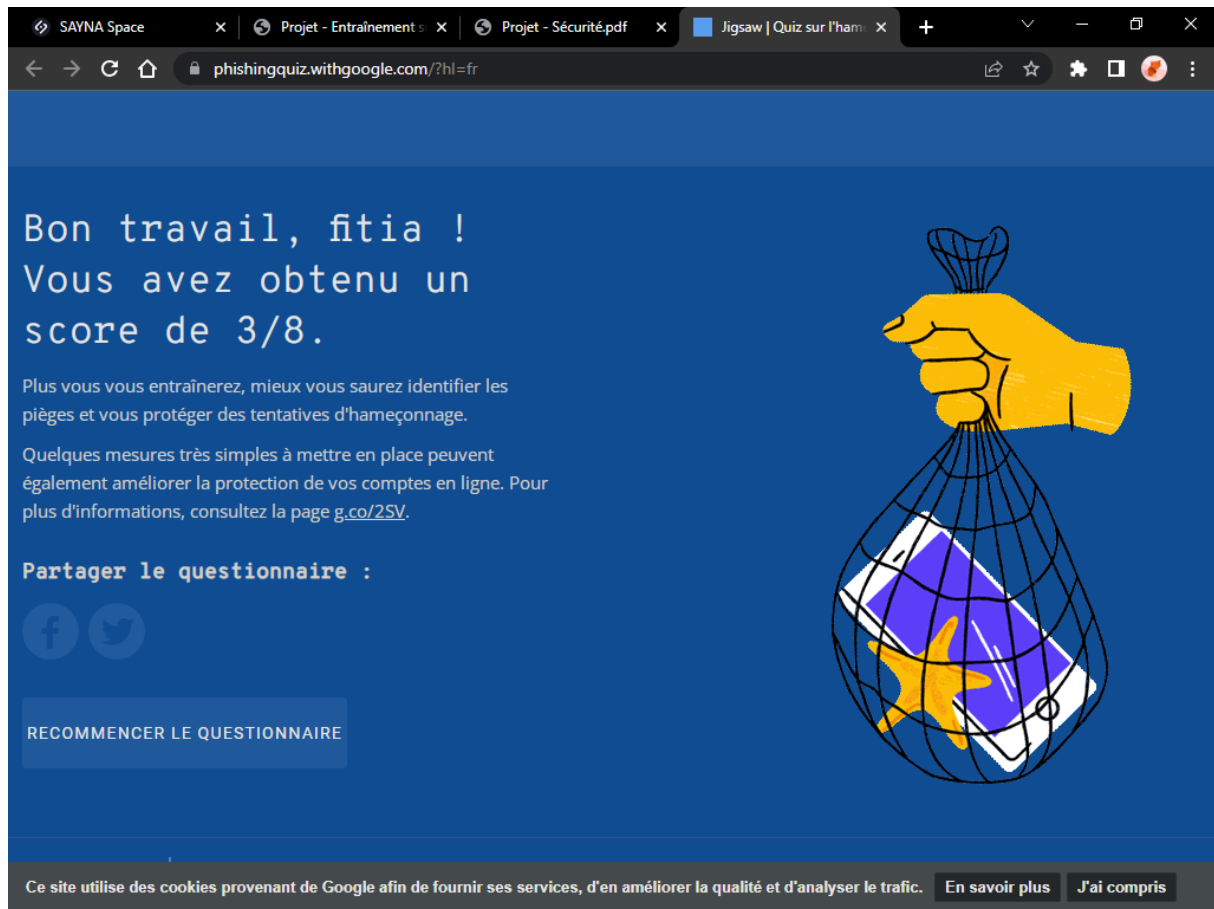
- [www.morvel.com](http://www.morvel.com), un dérivé de [www.marvel.com](http://www.marvel.com), le site web officiel de l'univers Marvel
- [www.fessebook.com](http://www.fessebook.com), un dérivé de [www.facebook.com](http://www.facebook.com), le plus grand réseau social du monde
- [www.instagram.com](http://www.instagram.com), un dérivé de [www.instagram.com](http://www.instagram.com), un autre réseau social très utilisé

**Les seuls sites qui semblaient être cohérents sont donc :**

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



## 4 - Éviter le spam et le phishing



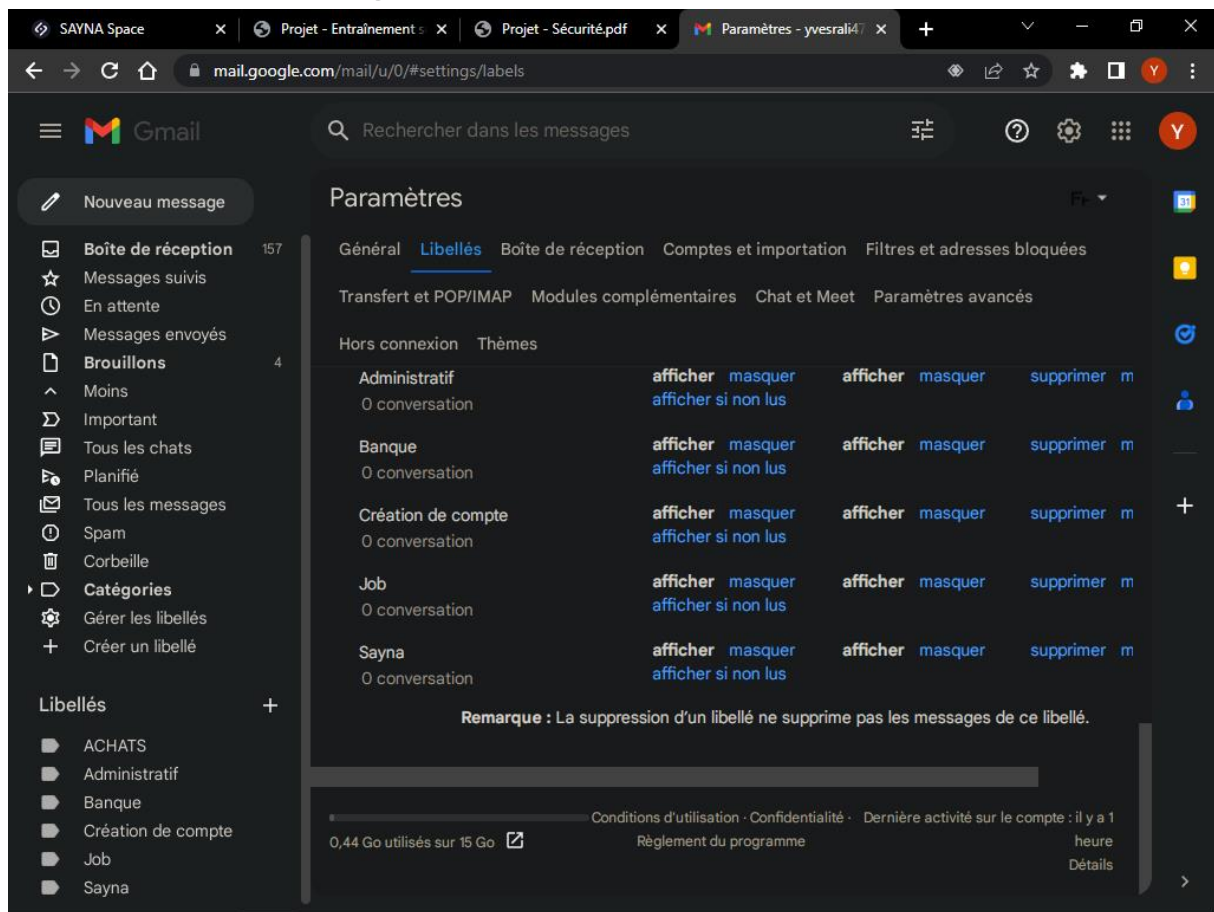
## 5 - Comment éviter les logiciels malveillants

- Site n°1
  - Domaine expiré.
- Site n°2
  - Indicateur de sécurité
    - Secure
  - Analyse Google
    - Aucun contenu suspect
- Site n°3
  - Indicateur de sécurité
    - Not Secure

- Analyse Google

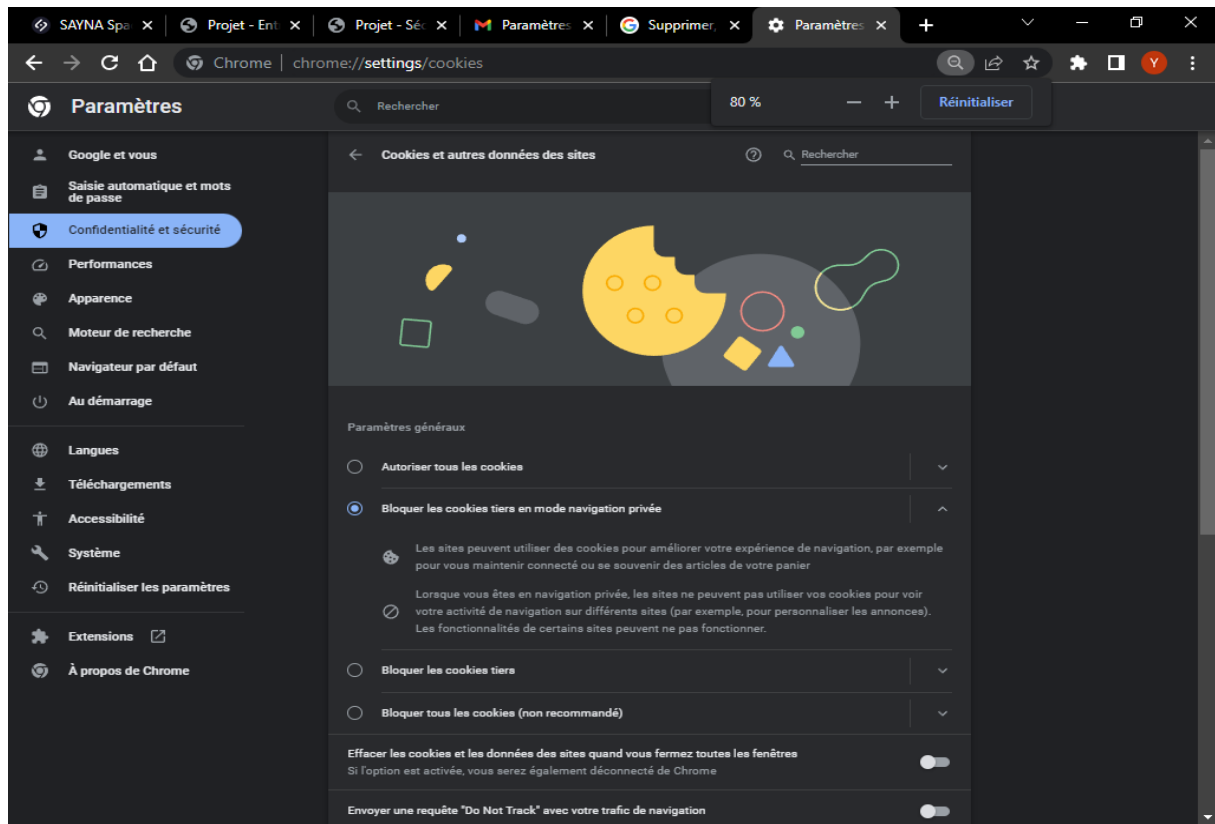
Il est difficile d'indiquer un simple niveau de sécurité pour les sites comme <http://www.baidu.com/>, qui comportent énormément de contenu. Des sites généralement considérés comme étant fiables présentent parfois du contenu suspect (par exemple, dans les blogs ou les commentaires). Pour obtenir des informations plus détaillées sur la sécurité, vérifiez un annuaire ou une page Web spécifique.

## 6 - Achats en ligne sécurisés

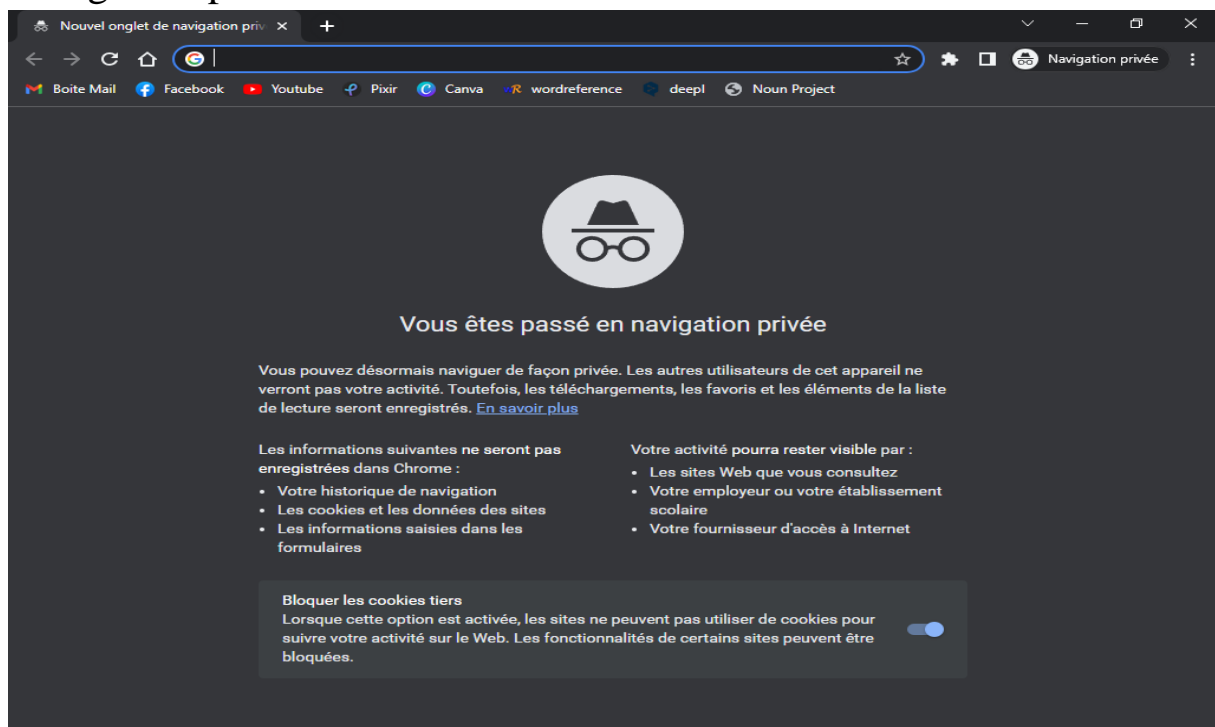


# 7 - Comprendre le suivi du navigateur

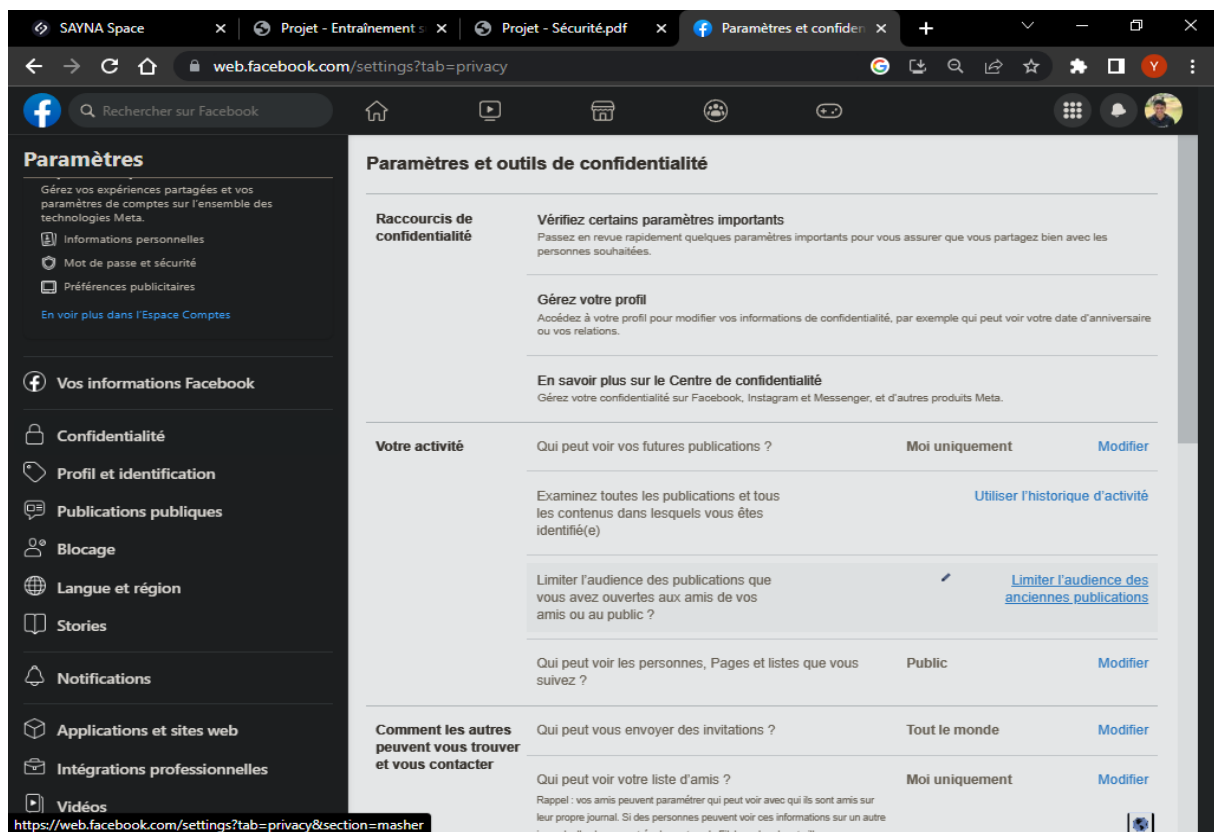
## Gérer les cookies



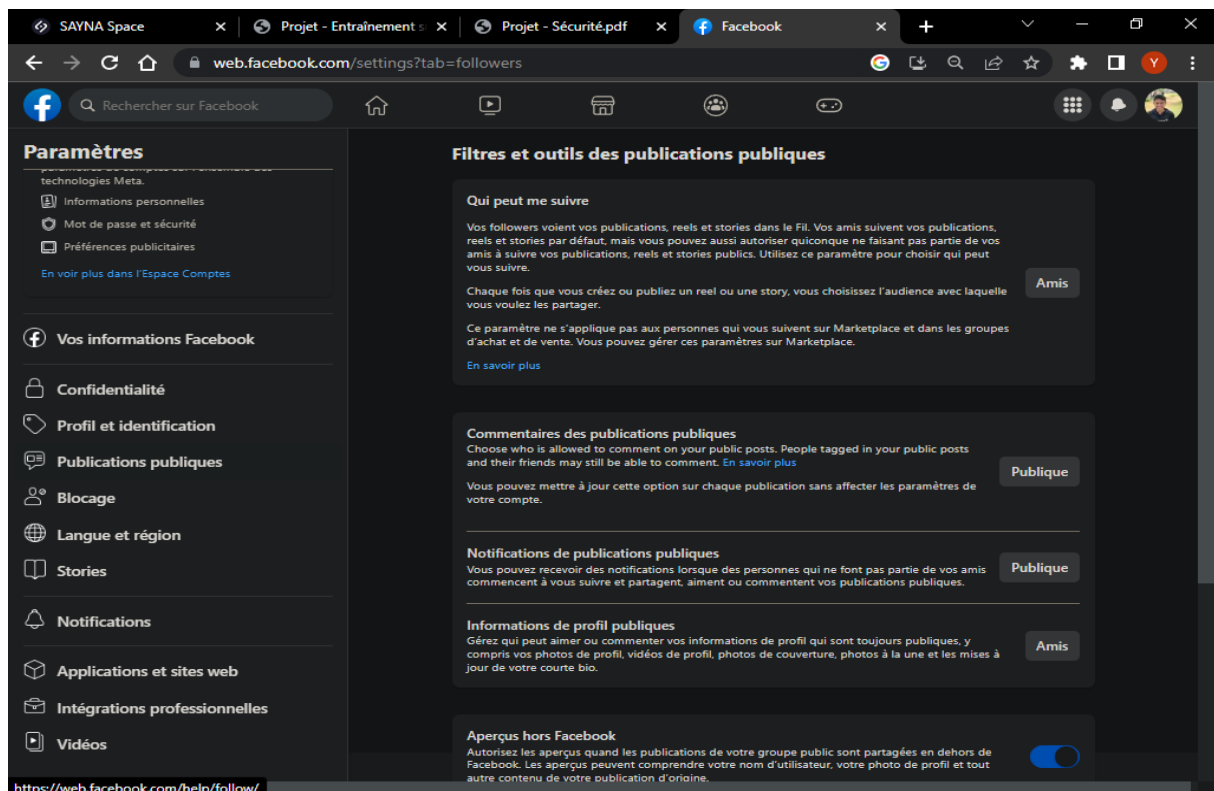
## Navigation privée



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



The screenshot shows the Facebook 'Paramètres et outils de confidentialité' (Privacy and Security Settings) page. The left sidebar contains a menu with options like 'Informations personnelles', 'Mot de passe et sécurité', 'Préférences publicitaires', ' Vos informations Facebook', 'Confidentialité', 'Profil et identification', 'Publications publiques', 'Blocage', 'Langue et région', 'Stories', 'Notifications', 'Applications et sites web', 'Intégrations professionnelles', and 'Vidéos'. The main content area is titled 'Paramètres et outils de confidentialité' and includes sections for 'Raccourcis de confidentialité', 'Vérifiez certains paramètres importants', 'Gérez votre profil', 'En savoir plus sur le Centre de confidentialité', 'Votre activité', and 'Comment les autres peuvent vous trouver et vous contacter'. The 'Votre activité' section shows settings for 'Qui peut voir vos futures publications ?' (set to 'Moi uniquement') and 'Examinez toutes les publications et tous les contenus dans lesquels vous êtes identifié(e)' (with a link to 'Utiliser l'historique d'activité'). The 'Comment les autres peuvent vous trouver et vous contacter' section shows settings for 'Qui peut vous envoyer des invitations ?' (set to 'Tout le monde') and 'Qui peut voir votre liste d'amis ?' (set to 'Moi uniquement').



The screenshot shows the Facebook 'Filtres et outils des publications publiques' (Public Post Filters and Tools) page. The left sidebar is identical to the previous screenshot. The main content area is titled 'Filtres et outils des publications publiques' and includes sections for 'Qui peut me suivre', 'Commentaires des publications publiques', 'Notifications de publications publiques', 'Informations de profil publiques', and 'Aperçus hors Facebook'. The 'Qui peut me suivre' section shows settings for 'Vos followers voient vos publications, reels et stories dans le Fil' (set to 'Amis') and 'Chaque fois que vous créez ou publiez un reel ou une story, vous choisissez l'audience avec laquelle vous voulez les partager'. The 'Commentaires des publications publiques' section shows settings for 'Choisissez qui peut commenter vos publications publiques' (set to 'Publique'). The 'Notifications de publications publiques' section shows settings for 'Vous pouvez recevoir des notifications lorsque des personnes qui ne font pas partie de vos amis commencent à vous suivre et partagent, aiment ou commentent vos publications publiques' (set to 'Publique'). The 'Informations de profil publiques' section shows settings for 'Gérez qui peut aimer ou commenter vos informations de profil qui sont toujours publiques, y compris vos photos de profil, vidéos de profil, photos de couverture, photos à la une et les mises à jour de votre courte bio' (set to 'Amis'). The 'Aperçus hors Facebook' section shows a toggle switch for 'Autorisez les aperçus quand les publications de votre groupe public sont partagées en dehors de Facebook' (set to 'On').



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

### Windows

Utiliser une application anti-programme malveillant : l'installation d'une application anti-programme malveillant et sa mise à jour peuvent aider à protéger votre PC contre les virus et autres programmes malveillants (logiciels malveillants).

Microsoft Defender est un logiciel anti-programme malveillant gratuit inclus avec Windows, et il est mis à jour automatiquement via Windows Update. Il existe également des produits anti-programme malveillant fabriqués par d'autres entreprises parmi lesquelles vous pouvez choisir.

#### 1. Installer les dernières mises à jour de Microsoft Update

Notez qu'un virus informatique peut vous empêcher d'accéder au site web Microsoft Update pour installer les dernières mises à jour. Nous vous recommandons de configurer l'exécution automatique du service des mises à jour automatiques de façon à ce que l'ordinateur ne manque aucune mise à jour importante.

#### 2. Utilisez la Scanner de sécurité Microsoft gratuite

Microsoft propose un outil en ligne gratuit qui analyse les menaces potentielles et vous permet de les supprimer de votre ordinateur.

#### 3. Utiliser l'outil de suppression de logiciels malveillants Windows

#### 4. Supprimer manuellement le logiciel de sécurité non fiable

Si le logiciel de sécurité non autorisé ne peut pas être détecté ou supprimé à l'aide de Scanner de sécurité Microsoft ou de l'outil de suppression de logiciels malveillants Windows, procédez comme suit :

- Notez le nom du logiciel de sécurité non autorisé. Pour cet exemple, nous l'appellerons XP Security Agent 2020.
- Redémarrez votre ordinateur.
- Lorsque le logo du fabricant de l'ordinateur s'affiche, appuyez plusieurs fois sur la touche F8.
- Lorsque vous y êtes invité, mettez l'option Mode sans échec avec prise en charge réseau en surbrillance à l'aide des touches de direction, puis appuyez sur Entrée.
- Cliquez sur le bouton Démarrer et vérifiez si le logiciel de sécurité non fiable apparaît dans le menu Démarrer. Si ce n'est pas le cas, cliquez sur Tous les programmes et faites défiler jusqu'à ce que vous trouviez le nom du logiciel de sécurité non autorisé.

- Cliquez avec le bouton droit sur le nom du logiciel de sécurité non autorisé, puis cliquez sur Propriétés.
- Cliquez sur l'onglet Raccourci .
- Dans la boîte de dialogue Propriétés , cochez le chemin du programme logiciel de sécurité non autorisé répertorié dans Target. Par exemple, C:\Program Files\XP Security Agent 2020.
- Cliquez sur Ouvrir l'emplacement du fichier.
- Dans la fenêtre Program Files, cliquez sur Program Files dans la barre d'adresse.
- Faites défiler jusqu'à ce que vous trouviez le logiciel de sécurité non autorisé. Par exemple, XP Security Agent 2020.
- Cliquez avec le bouton droit sur le dossier, puis cliquez sur Supprimer.
- Redémarrez votre ordinateur.
- Accédez au site web Scanner de sécurité Microsoft.
- Cliquez sur le bouton Télécharger maintenant, puis cliquez sur Exécuter.
- Suivez les instructions pour analyser votre ordinateur et vous aider à supprimer le logiciel de sécurité non autorisé.

#### 5. Exécuter Microsoft Defender hors connexion

Microsoft Defender hors connexion est un outil anti-programme malveillant qui permet de supprimer les virus difficiles à éliminer qui démarrent avant le démarrage de Windows. À compter de Windows 10, Microsoft Defender hors connexion est intégré.

## Mac Os

### Partie 3: Comment se débarrasser d'un virus sur Mac

Si votre Mac présente l'un des signes mentionnés ci-dessus ou si un outil tiers a détecté un virus sur votre Mac, vous devez être vigilant. Voici quelques suggestions de techniques pour se débarrasser des logiciels malveillants sur Mac que vous pouvez également appliquer.

#### **Solution 1: Quitter toute application malveillante**

Tout d'abord, vous devez vous assurer qu'aucune application malveillante ne fonctionne sur votre Mac. Pour ce faire, vous pouvez utiliser le moniteur d'activité de Mac et quitter de force l'application.

Pour obtenir le moniteur d'activité, vous pouvez aller sur le bureau et visiter Applications > Utilitaires > Moniteur d'activité pour l'ouvrir. Vous pouvez également le rechercher dans la recherche Spotlight de Mac.

Une fois la fenêtre du moniteur d'activité lancée, essayez de rechercher toute entité malveillante. Il peut s'agir de toute application que vous n'avez pas installée auparavant.

Il suffit de la sélectionner et de cliquer sur le bouton "Forcer la sortie" qui lui est adjacent pour empêcher l'application de fonctionner en arrière-plan.

## **Solution 2: Supprimer les applications indésirables**

Quitter une application malveillante du système n'est pas suffisant. Si vous voulez supprimer le virus sur Mac, pensez à désinstaller complètement l'application.

Il suffit d'aller dans le Finder > Applications et de jeter un coup d'œil à la liste complète des applications installées. À partir de là, essayez d'identifier toutes les applications suspectes ou provenant de sources non fiables.

Ensuite, il suffit de sélectionner l'application, de faire un clic droit et de cliquer sur l'option "Déplacer vers la corbeille" dans le menu contextuel. Confirmez votre choix pour supprimer définitivement l'application.

## **Solution 3: Supprimer les fichiers infectés et nettoyer la corbeille du Mac**

Outre les applications, une entité malveillante peut également être présente dans n'importe quel dossier. De plus, si un fichier a été infecté, le malveillant peut se propager à d'autres sources également. Pour résoudre ce problème et apprendre à se débarrasser du virus sur le Mac, faites le choix difficile de supprimer le contenu infecté.

Il suffit d'aller dans le Finder et de naviguer jusqu'à l'emplacement où se trouvent les fichiers ou dossiers infectés.

Sélectionnez les données infectées, faites un clic droit et déplacez-les vers la corbeille.

Ensuite, allez sur le bureau et, dans le Finder, choisissez de "Vider la corbeille". Vous pouvez également cliquer avec le bouton droit de la souris sur l'icône de la corbeille dans le dock et la vider à partir de là.

## **Solution 5: Créer un nouveau profil d'utilisateur**

Si vous n'êtes pas en mesure de procéder à une suppression complète du virus Mac, envisagez plutôt de le fuir. Pour ce faire, il vous suffit de créer un nouveau profil utilisateur sur votre Mac. Cependant, assurez-vous de supprimer au préalable tous les éléments de connexion afin que le virus ne dispose pas des autorisations nécessaires. Voici comment se débarrasser du virus sur Mac en créant un nouveau profil.

Dans le Finder de Mac, allez dans Préférences du système > Utilisateurs et groupes.

Cliquez ensuite sur l'icône représentant un cadenas et saisissez les informations d'identification du compte administrateur pour accéder à ces paramètres.

Ensuite, cliquez sur le bouton Ajouter un utilisateur et entrez les détails pertinents pour créer un nouveau profil. Je vous recommande de donner au nouveau compte des droits d'administration puisque vous n'utiliserez plus le profil actuel

En outre, dans la fenêtre Utilisateurs et groupes, vous pouvez visiter la section Éléments de connexion. Sélectionnez les éléments de connexion enregistrés et supprimez-les du profil correspondant

### **Solution 6: Réparer le disque**

Apple n'a peut-être pas inclus beaucoup d'outils intégrés pour fournir une protection antivirus complète pour Mac, mais elle dispose d'une solution intelligente pour réparer le disque. Avec l'aide de son application Utilitaire de disque, vous pouvez effectuer une opération de premier secours sur le disque dur du système. Il s'agit également d'une solution idéale pour supprimer gratuitement les virus sur Mac.

Allez dans le Finder de Mac et visitez Applications > Utilitaires > Utilitaire de disque.

Lorsque la fenêtre de l'utilitaire de disque s'ouvre, sélectionnez votre disque dur dans la barre latérale. La plupart du temps, il s'agit du disque dur de Macintosh.

Sur la droite, vous pouvez voir toutes sortes d'opérations que vous pouvez effectuer sur le disque. Il suffit de cliquer sur le bouton "Premier secours" pour analyser votre disque et le réparer en cas de dommages indésirables.

## **Installation Anti-virus**

### **Windows – Mac Os**

- **Télécharger et installer Avast sur votre appareil.**
  - **Faite une Analyse de disque.**
  - **Réparer le disque si besoins.**
  - **Redémarrer l'ordinateur après réparation.**
- 
- **Avast** : Antivirus de renommée mondiale, pour tous les appareils
- Forts de plus de 30 ans d'expérience, nous avons créé un logiciel antivirus à la fois simple d'utilisation et doté du plus grand réseau de détection des menaces au monde, alimenté par le machine Learning et offrant une sécurité réseau qui ne ralentit aucun appareil (PC, Mac, Android ou iPhone).