

# 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

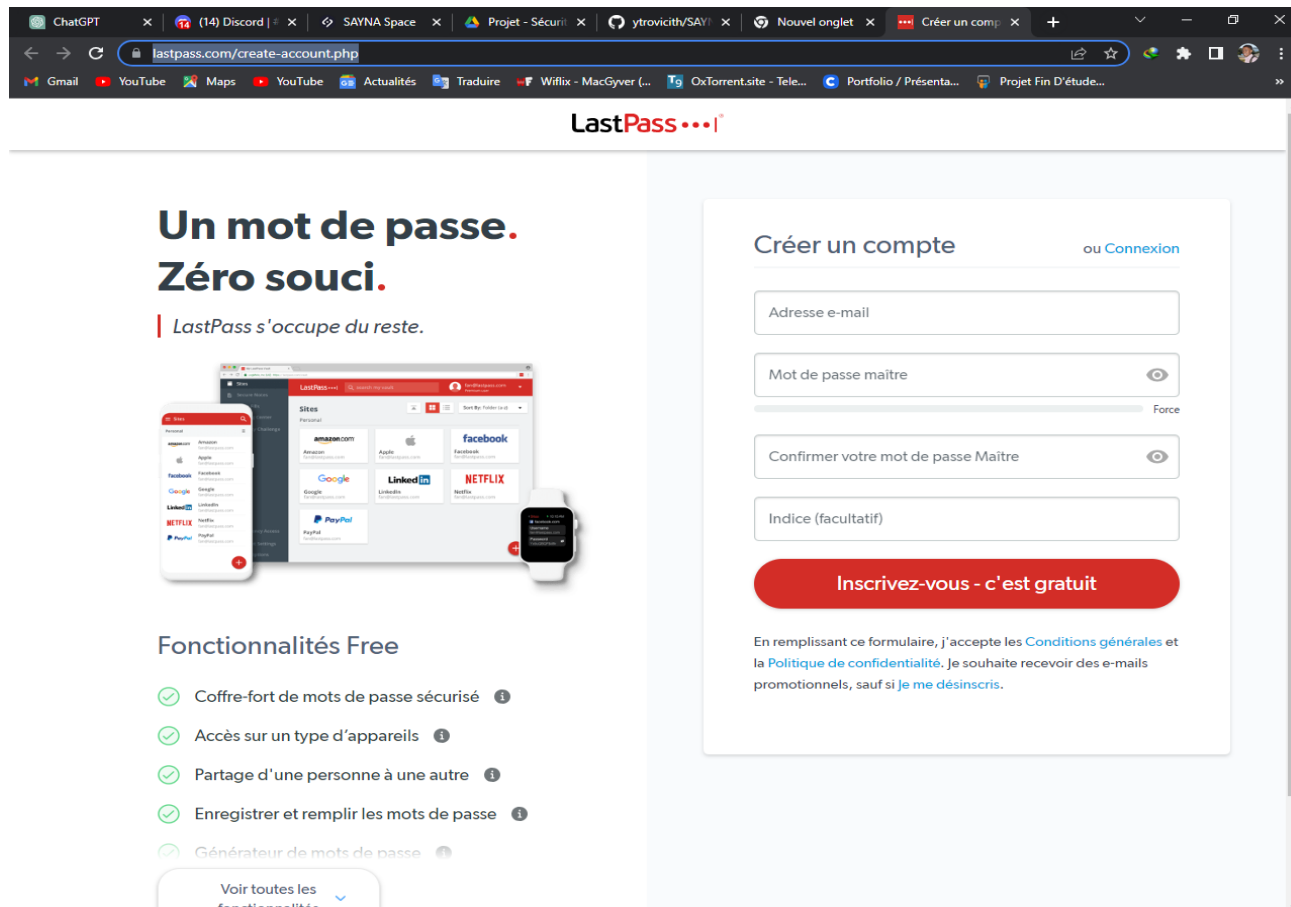
Voici les **trois articles** qui parlent de **sécurité sur internet**

- Article 1 = ANSSI - Dix règles de base
- Article 2 = Economie.gouv - Comment assurer votre sécurité numérique
- Article 3 = Site W - Naviguez en toute sécurité sur Internet

### 2 - Créer des mots de passe forts

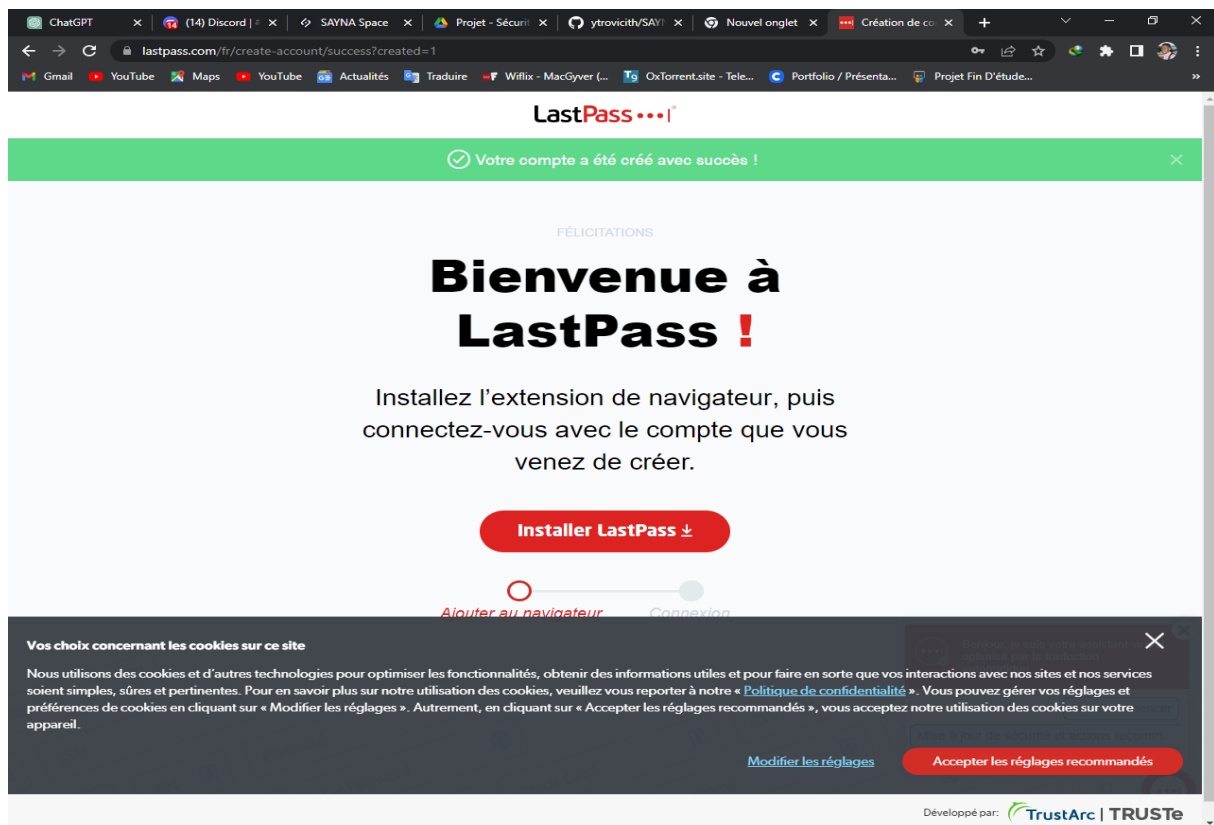
**1 / Dans cet exercice, nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Ce gestionnaire prend la forme d'une application web, accessible sur tous supports (PC, Mac, mobile).**

- Etape 1 : Accéder au site de LastPass

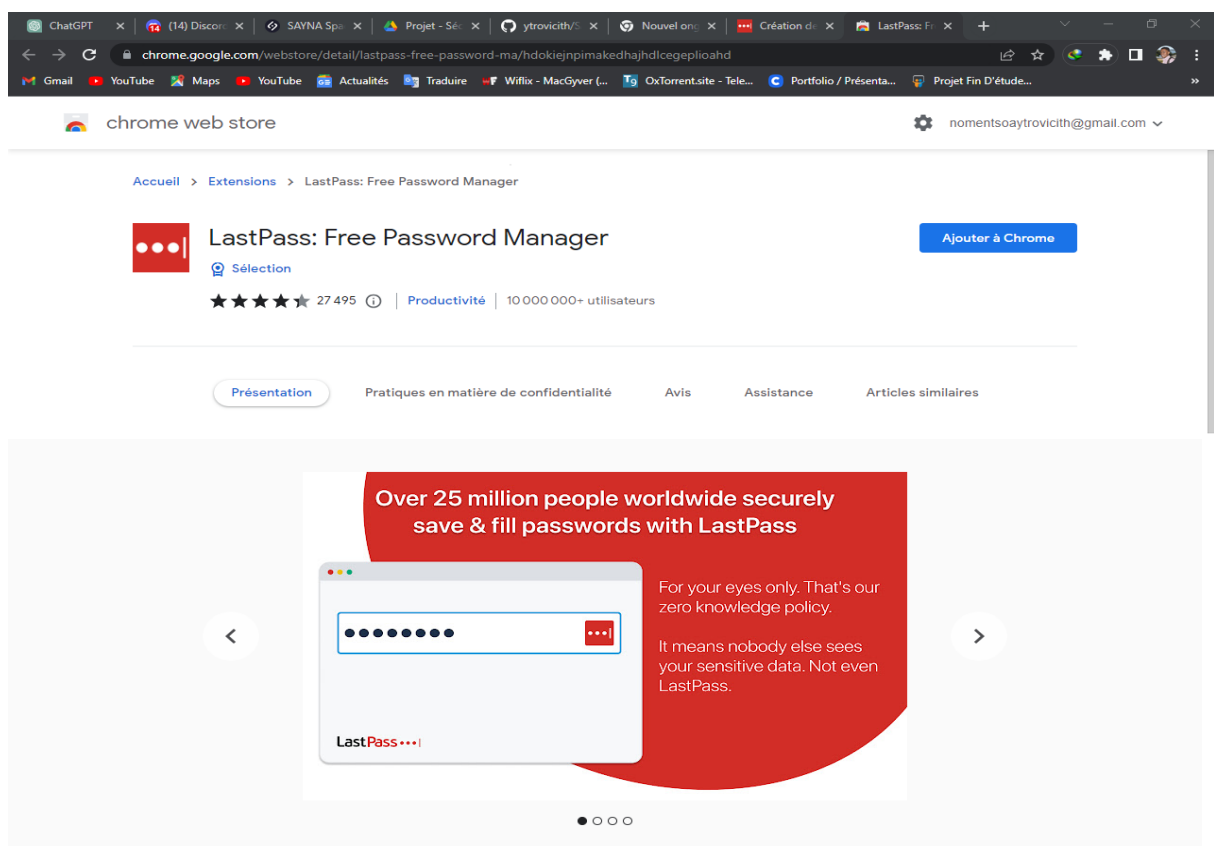


The screenshot shows the LastPass website in a web browser. The browser's address bar displays 'lastpass.com/create-account.php'. The page features the LastPass logo at the top. On the left, there's a section titled 'Un mot de passe. Zéro souci.' with the tagline 'LastPass s'occupe du reste.' Below this, there's an illustration of a smartphone, a tablet, and a smartwatch, all displaying the LastPass app interface. Underneath the illustration, the text 'Fonctionnalités Free' is followed by a list of features: 'Coffre-fort de mots de passe sécurisé', 'Accès sur un type d'appareils', 'Partage d'une personne à une autre', 'Enregistrer et remplir les mots de passe', and 'Générateur de mots de passe'. A link 'Voir toutes les fonctionnalités' is at the bottom of this list. On the right side of the page, there's a 'Créer un compte' form. It includes 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 at the bottom of the form. Below the button, there's a disclaimer: '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.'

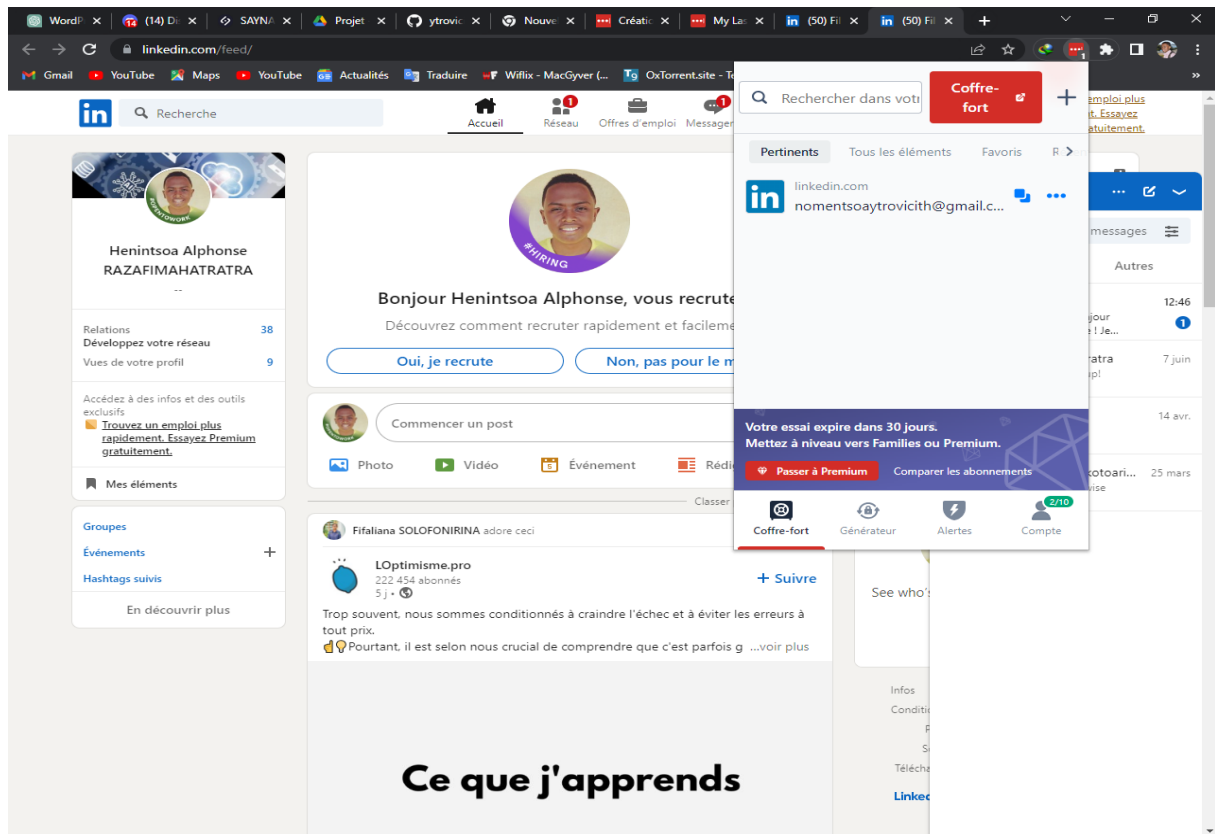
• Etape 2 : Créer un compte en remplissant le formulaire



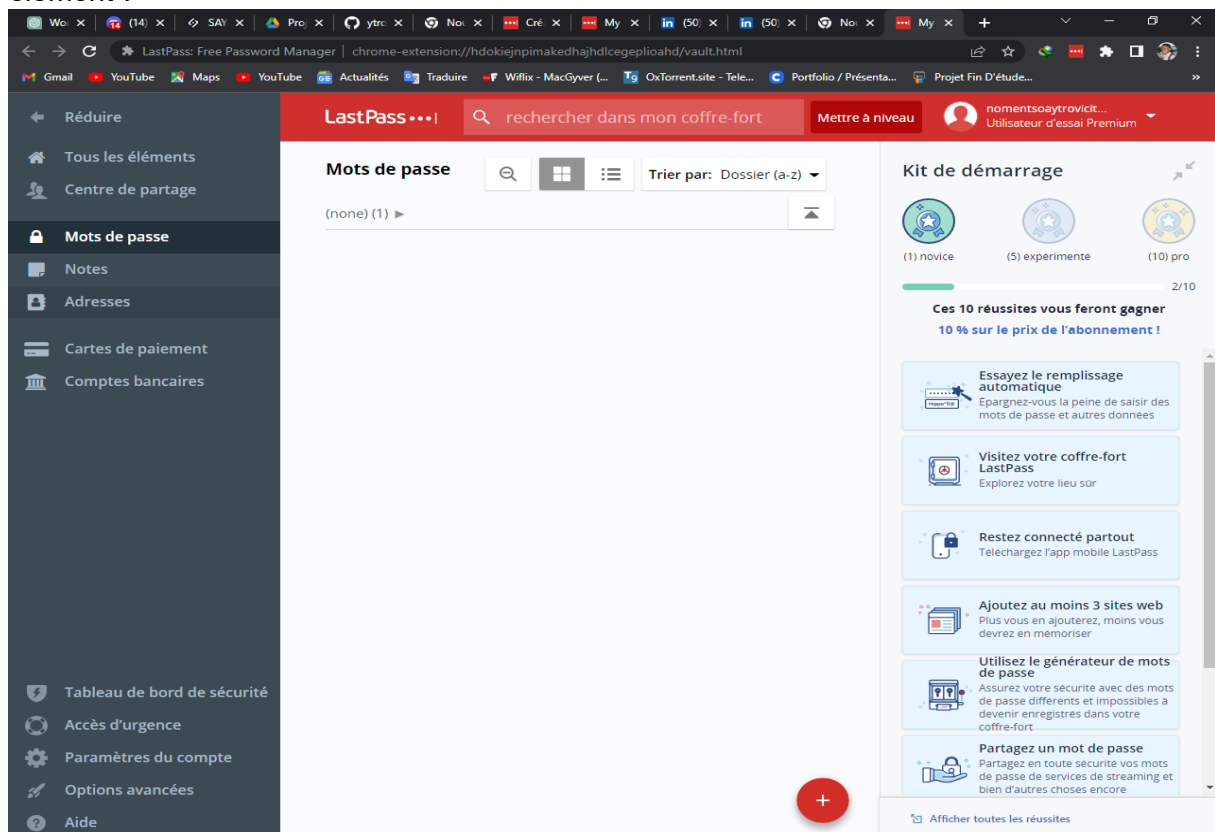
• Etape 3 : Valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome"



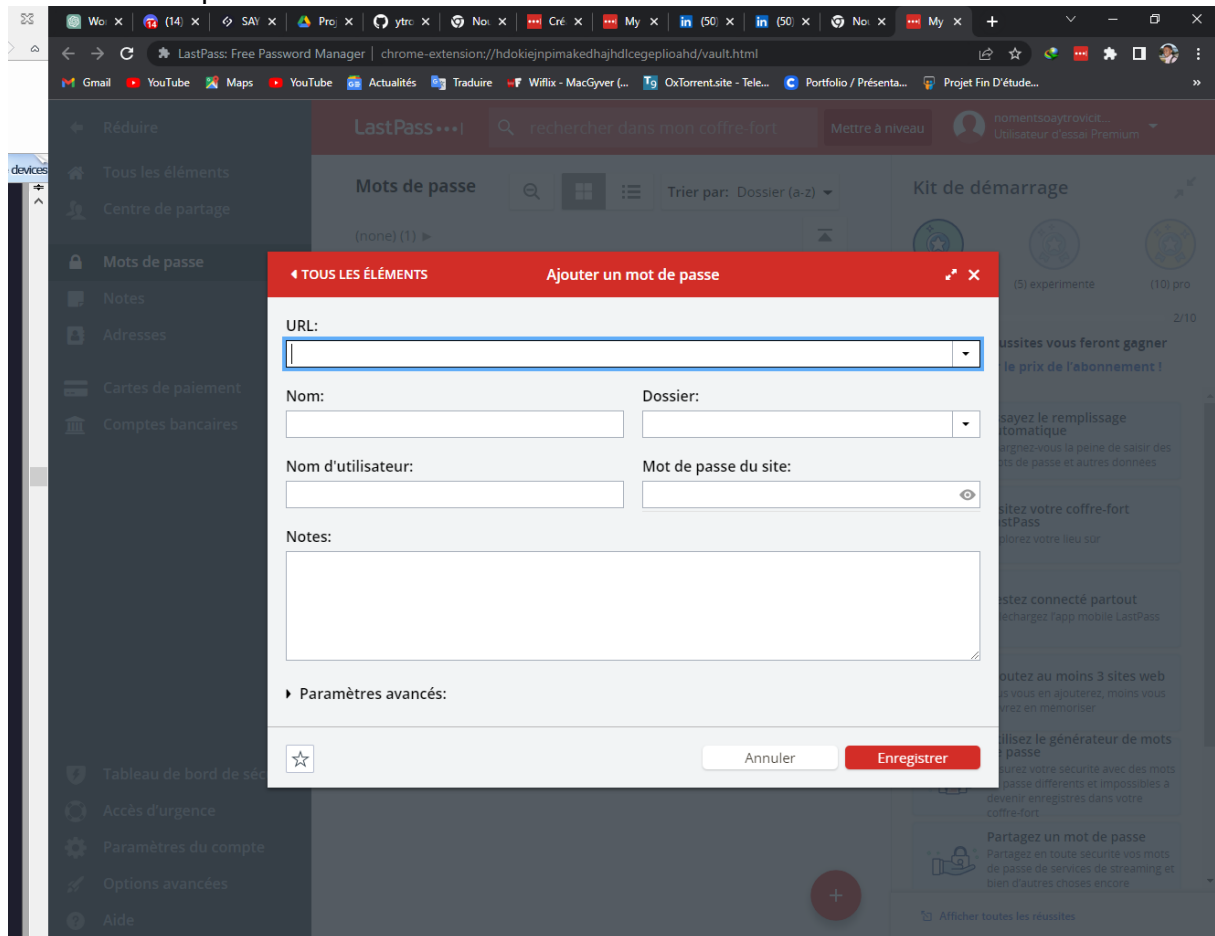
● Etape 4 : Connecter au compte déjà enregistré sur le LastPass.



● Etape 5 : Gestion de compte LastPass. Pour ajouter un site et une connexion associée (identifiant + mot de passe), accéder à la rubrique “Mot de passe” puis cliquer sur “Ajouter un élément”.



- Etape 6 : Insérer toutes les informations à retenir à cette fenêtre qui s'ouvre pour automatiser la prochaine connexion .



### 3 - Fonctionnalité de sécurité de votre navigateur

1 / Soit à identifier les adresses internet qui semblent provenir de sites web malveillants.

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

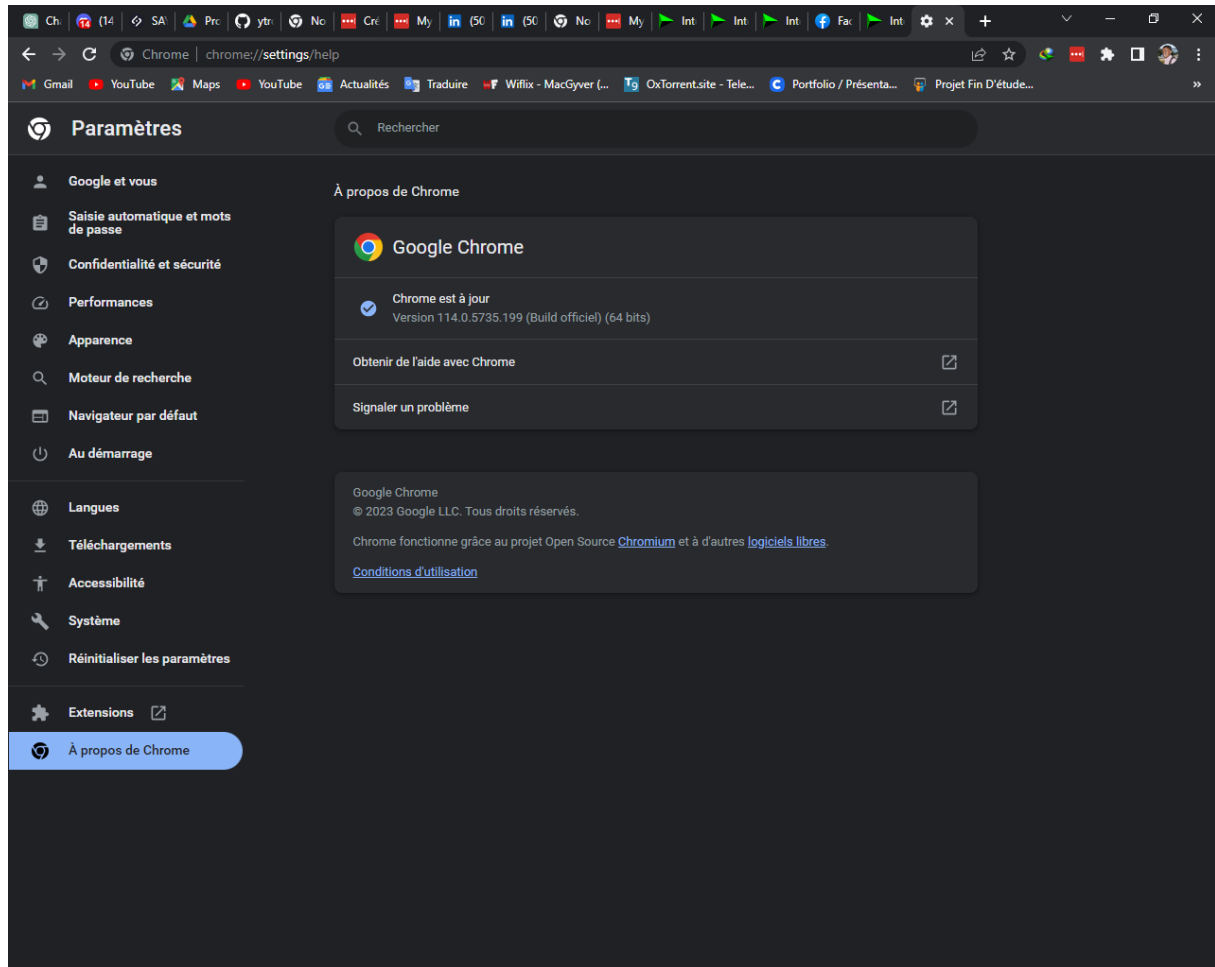
#### Réponse

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

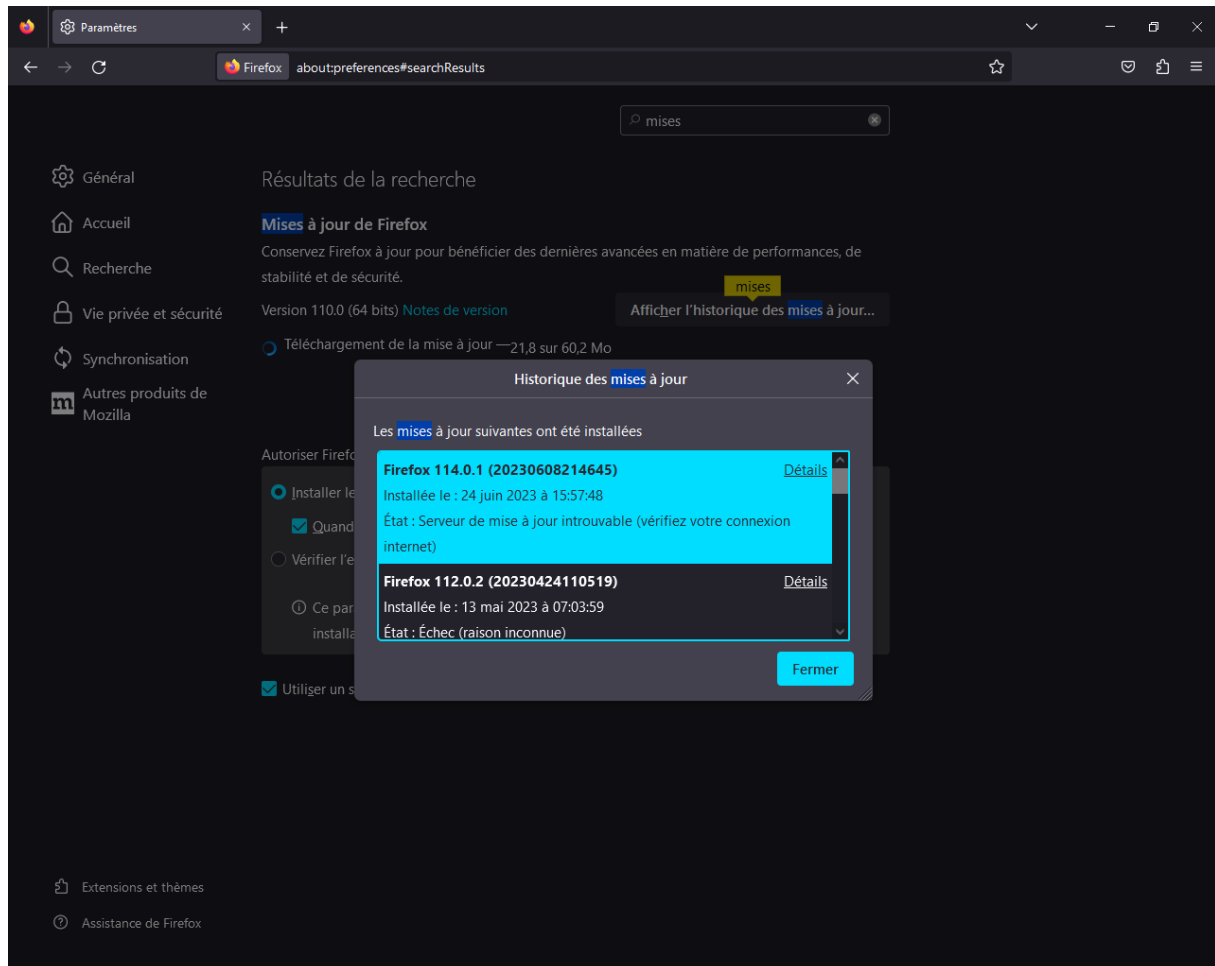
## 2/ Soit à vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour.

- Pour Chrome
  - On ouvre le menu du navigateur et accède aux “Paramètres”
  - On Clic sur la rubrique “A propos de Chrome”
  - Si on constate le message “Chrome est à jour”, c’est Ok



- Pour Firefox

- On ouvre le menu du navigateur et accède aux “Paramètres”
- Dans la rubrique “Général”, on fait défiler jusqu’à voir la section “Mise à jour de Firefox (astuce : on peut également saisir dans la barre de recherche “mises à jour” pour tomber directement dessus)



# 4 - Éviter le spam et le phishing

1 / Dans cet exercice, on va exercer à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.

## Exemple 1

The screenshot shows a web browser window displaying a phishing quiz. The URL in the address bar is [phishingquiz.withgoogle.com/?hl=fr](https://phishingquiz.withgoogle.com/?hl=fr). The page has a blue header with the text "1 / 8". Below the header, there is a large blue box with the text "Commençons par cet e-mail Google Docs." and a subtext: "Vérifiez bien le URL des liens en passant la souris ou en appuyant de manière prolongée dessus, et examinez les adresses e-mail. Ne vous inquiétez pas, aucun des liens ne fonctionne... Nous ne voudrions pas vous rediriger vers des pages louches !". There are two buttons: "HAMEÇONNAGE" and "LÉGITIME".

The email being analyzed is from "Luke Johnson" with the email address "<luke.json8000@gmail.com>". The email content shows a document link: "Budget département 2023.docx". Below the link, there is a message: "Bonjour. Voici le document demandé. N'hésitez pas à me contacter si vous avez besoin d'autre chose !". There is a button "Ouvrir dans Docs".

Below the email, there is a blue box with the text "C'est exact ! Il s'agit d'un e-mail d'hameçonnage." and a subtext: "Vous avez sans doute remarqué que l'URL ressemble à la véritable adresse. Prenez garde aux liens hypertextes et aux pièces jointes que vous ouvrez à partir des e-mails, car ils peuvent rediriger vers des sites Web frauduleux qui vous invitent à saisir des informations sensibles." There is a button "MONTREZ-MOI".

At the bottom of the page, there is a footer with the text: "Ce site utilise des cookies provenant de Google afin de fournir ses services, d'en améliorer la qualité et d'analyser le trafic." and two buttons: "En savoir plus" and "J'ai compris".

## Exemple 2

2 / 8


C'est exact ! Il s'agit d'un e-mail d'hameçonnage.

Bien vu ! Comme vous l'avez remarqué, le domaine de messagerie de l'expéditeur est mal orthographié ("efacks") et le lien redirige vers le site "mailru382.co". L'hameçonnage consiste généralement à vous induire en erreur avec des URL ressemblant à celle du site officiel.

MONTREZ-MOI

**Fax NoReply [admin]** <noreply@efacks.com> à moi 23:04

Vous avez reçu un fax d'une page le 08/07/2023 23:04  
[Cliquez ici pour afficher ce fax en ligne](#)



Merci d'avoir utilisé le service eFax ! Consultez le site [www.eFax.com/en/efax/page/help](http://www.eFax.com/en/efax/page/help) si vous avez des questions ou si vous pensez avoir reçu ce fax par erreur.  
eFax Inc (c) 2023

Ce site utilise des cookies provenant de Google afin de fournir ses services, d'en améliorer la qualité et d'analyser le trafic. [En savoir plus](#) [J'ai compris](#)

## Exemple 4


4 / 8

On dirait que vous n'avez plus d'espace de stockage disponible !

Je me demande combien coûte une mise à jour...

HAMEÇONNAGE LÉGITIME

**D** **Dropbox** <no-reply@dropboxmail.com> à moi 23:06



Bonjour,

Votre Dropbox est pleine, et les fichiers n'y sont plus synchronisés. Les nouveaux fichiers ajoutés à votre dossier Dropbox ne seront pas accessibles sur vos autres appareils ni sauvegardés en ligne.

Mettez à niveau votre Dropbox aujourd'hui pour obtenir un espace de stockage de 1 To (1 000 Go) et bénéficier de puissantes fonctionnalités de partage.

[Mettre à niveau votre Dropbox](#)

Pour découvrir d'autres moyens d'obtenir davantage d'espace, visitez notre page [Comment obtenir plus d'espace](#).

Profitez pleinement de votre Dropbox !

- L'équipe Dropbox

Ce site utilise des cookies provenant de Google afin de fournir ses services, d'en améliorer la qualité et d'analyser le trafic. [En savoir plus](#) [J'ai compris](#)



## Exemple 5

5 / 8

C'est exact ! Il s'agit d'un e-mail d'hameçonnage.

Cette tentative d'hameçonnage était difficile à repérer ! Les documents PDF peuvent contenir des logiciels malveillants ou des virus. Vérifiez toujours que l'expéditeur est digne de confiance, et utilisez votre navigateur ou un service en ligne comme Google Drive pour les ouvrir en toute sécurité.

MONTREZ-MOI

Sharon Mosley <sharon.mosley@westmountdayschool.org>  
à moi 23:07

Bonjour RAZAF,

Veuillez trouver ci-joint le rapport d'activité financière de 2023, à lire attentivement.

Cordialement,

Mme Sharon Mosley  
Westmount Day School

R.A.F. 2023.pdf

Ce site utilise des cookies provenant de Google afin de fournir ses services, d'en améliorer la qualité et d'analyser le trafic. [En savoir plus](#) [J'ai compris](#)

## Exemple 6

6 / 8

C'est exact. L'URL de ce message est trompeuse.

Cette attaque est semblable à celle qui a été employée pour pirater la messagerie de personnalités politiques. Vérifiez toujours attentivement les URL.

MONTREZ-MOI

Google <no-reply@google.support>  
à moi 23:08

Une personne connaît votre mot de passe

Bonjour,

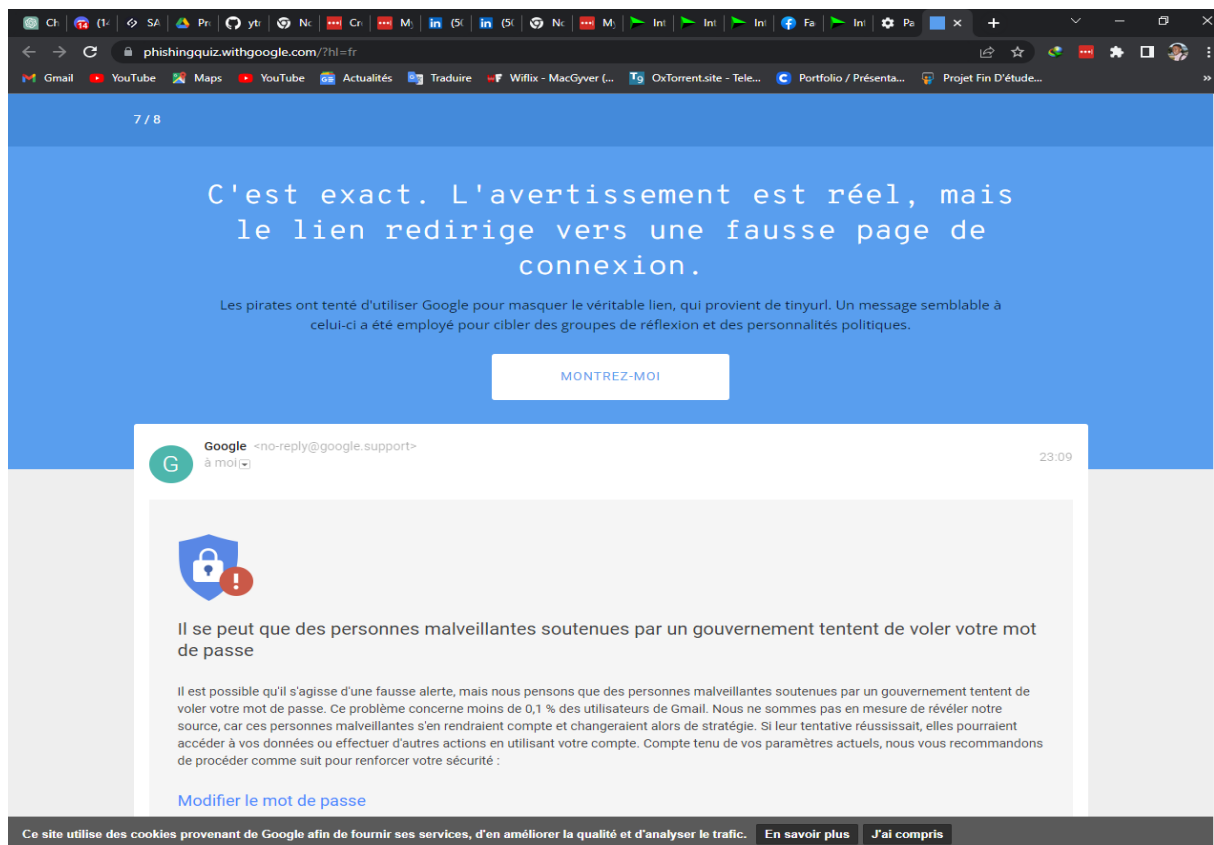
Une personne vient d'utiliser votre mot de passe pour tenter de se connecter à votre compte Google.

Information :  
samedi 8 juillet 2023 à 23:08:59 GMT+03:00  
Slatina, Roumanie  
Navigateur Firefox

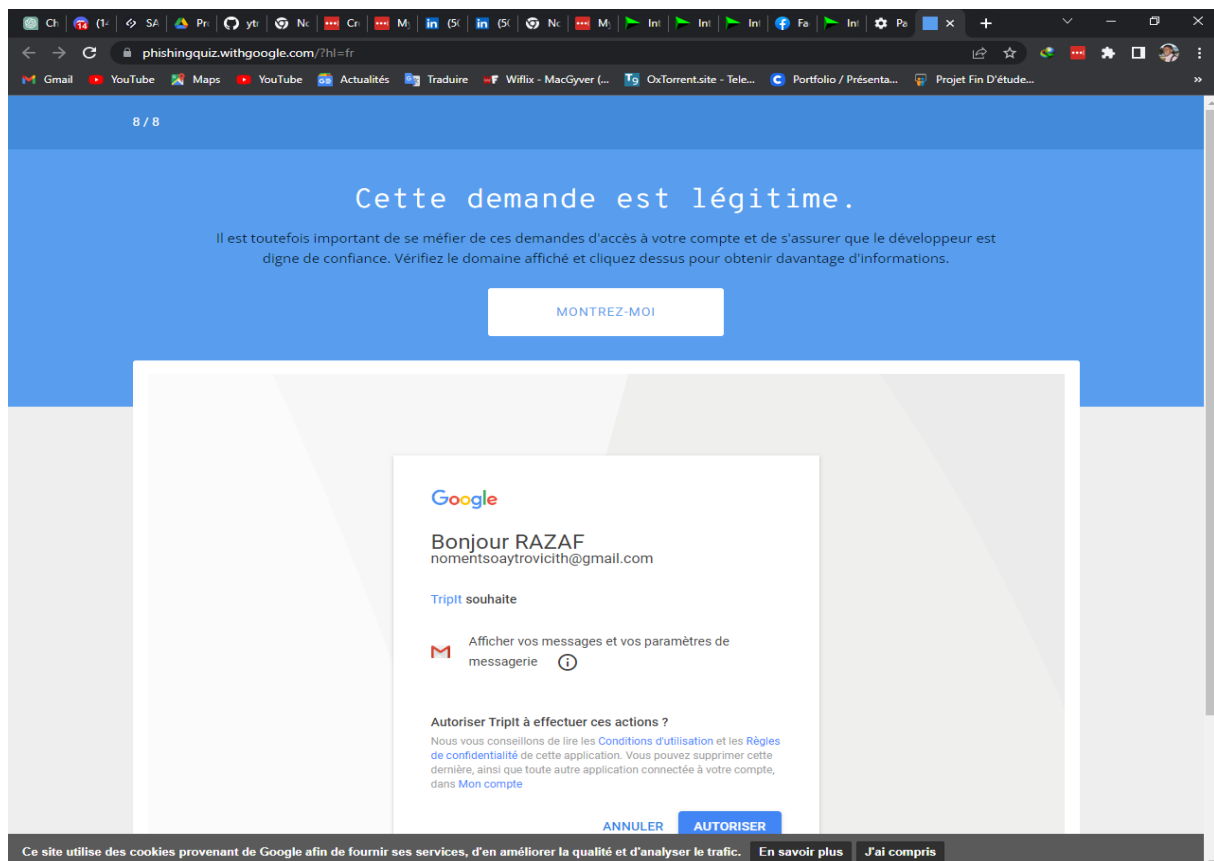
Google a bloqué cette tentative de connexion. Vous devriez changer immédiatement de mot de passe

Ce site utilise des cookies provenant de Google afin de fournir ses services, d'en améliorer la qualité et d'analyser le trafic. [En savoir plus](#) [J'ai compris](#)

## Exemple 7



## Exemple 8



## 5 - Comment éviter les logiciels malveillants

3/ Lors de la navigation sur le web, il arrive d'avoir des doutes sur la sécurité de certains sites. Comme on a 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 on peut s'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, on va devoir analyser les informations de plusieurs sites. Pour chaque site on devra préciser l'indicateur de sécurité et le rapport d'analyse de l'outil Google. Il 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.

- 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)

## Réponse :

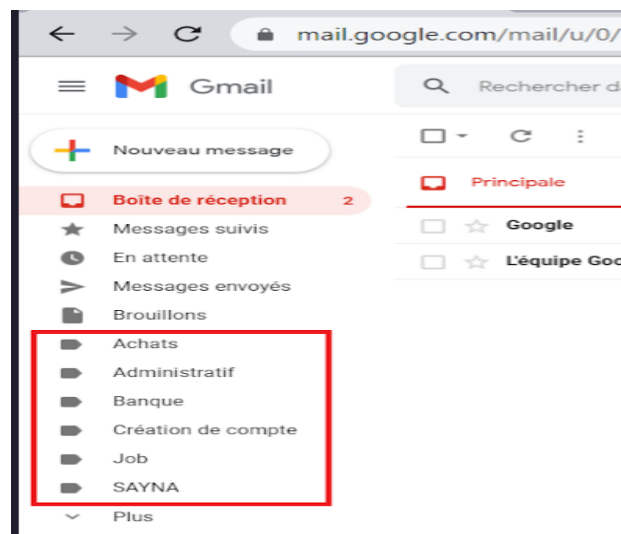
- Site n°1
  - **Indicateur de sécurité**
    - HTTPS
  - **Analyse Google**
    - Aucun contenu suspect
- Site n°2
  - **Indicateur de sécurité**
    - Not secure
  - **Analyse Google**
    - Aucun contenu suspect
- Site n°3
  - **Indicateur de sécurité**
    - Not secure
  - **Analyse Google**
    - Vérifier un URL en particulier (analyse trop générale)

## 6 - Achats en ligne sécurisés

### 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

Qu'est-ce qu'un cookie dans le contexte d'Internet ?

Un petit fichier texte stocké sur votre appareil par un site web.

Quel est le rôle principal des cookies ?

Améliorer l'expérience utilisateur sur un site web.

Quelles informations peuvent être stockées dans un cookie ?

Votre historique de navigation et vos préférences sur un site web.

Quelles sont les conséquences de la désactivation des cookies ?

Certaines fonctionnalités des sites web pourraient ne pas fonctionner correctement.

Qu'est-ce que la navigation privée (ou le mode incognito) ?

Un moyen de naviguer sur Internet sans que les cookies soient stockés.

Quelles informations sont supprimées lorsque vous utilisez la navigation privée ?

Votre historique de navigation et les cookies.

Quelle est la principale différence entre la navigation privée et la désactivation des cookies ?

La désactivation des cookies affecte tous les sites web, tandis que la navigation privée n'affecte que la session en cours.

**Voici une étape pour voir et gérer les cookies sur Google Chrome :**

1. On ouvre Google Chrome sur notre ordinateur.
2. On clique sur les trois points verticaux en haut à droite de la fenêtre du navigateur pour ouvrir le menu.
3. Dans le menu déroulant, on sélectionne "Paramètres".
4. On fait défiler la page vers le bas et on clique sur "Paramètres avancés".
5. Dans la section "Confidentialité et sécurité", on clique sur "Paramètres de contenu".
6. Dans la nouvelle fenêtre, on clique sur "Cookies".
7. Maintenant, on peut voir tous les cookies stockés sur notre navigateur Chrome. Les cookies sont répertoriés par nom, domaine, chemin, taille et date d'expiration.

**Pour gérer les cookies, on a plusieurs options :**

- Pour supprimer un cookie spécifique, on clique sur l'icône de la corbeille à droite du cookie.
- Pour supprimer tous les cookies, on clique sur "Tout supprimer" en haut de la liste.
- On peut également bloquer les cookies de certains sites en cliquant sur "Ajouter" à côté de "Bloquer" et en saisissant l'adresse du site.
- Si on souhaite bloquer tous les cookies par défaut, on active l'interrupteur à côté de "Bloquer tous les cookies".

## Voici une étape pour voir et gérer l'utilisation de la navigation privée sur Google Chrome :

1. On ouvre Google Chrome sur notre ordinateur.
2. On clique sur les trois points verticaux en haut à droite de la fenêtre du navigateur pour ouvrir le menu.
3. Dans le menu déroulant, on sélectionne "Nouvelle fenêtre de navigation privée" ou on utilise le raccourci clavier "Ctrl+Shift+N".
4. Une nouvelle fenêtre de navigation privée s'ouvre. On peut l'identifier par l'icône d'un chapeau et d'une loupe sombres dans le coin supérieur gauche de la fenêtre.
5. On est maintenant en mode de navigation privée. Toutes les pages qu'on visite dans cette fenêtre ne seront pas enregistrées dans l'historique de navigation, les cookies et les données de formulaire ne seront pas sauvegardés, et on sera déconnecté des comptes qu'on a utilisés pendant cette session privée.

## Pour gérer l'utilisation de la navigation privée :

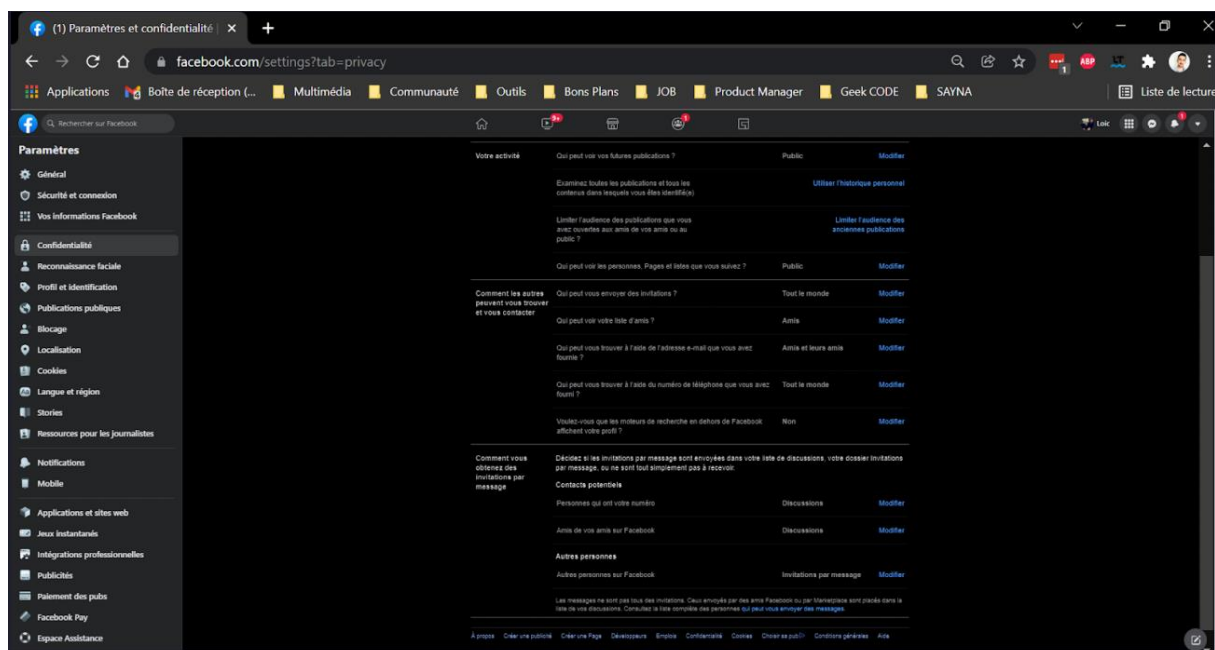
- Pour ouvrir une nouvelle fenêtre de navigation privée, on peut répéter les étapes 2 et 3.
- Pour quitter la navigation privée et revenir à la navigation normale, on ferme simplement la fenêtre de navigation privée.

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

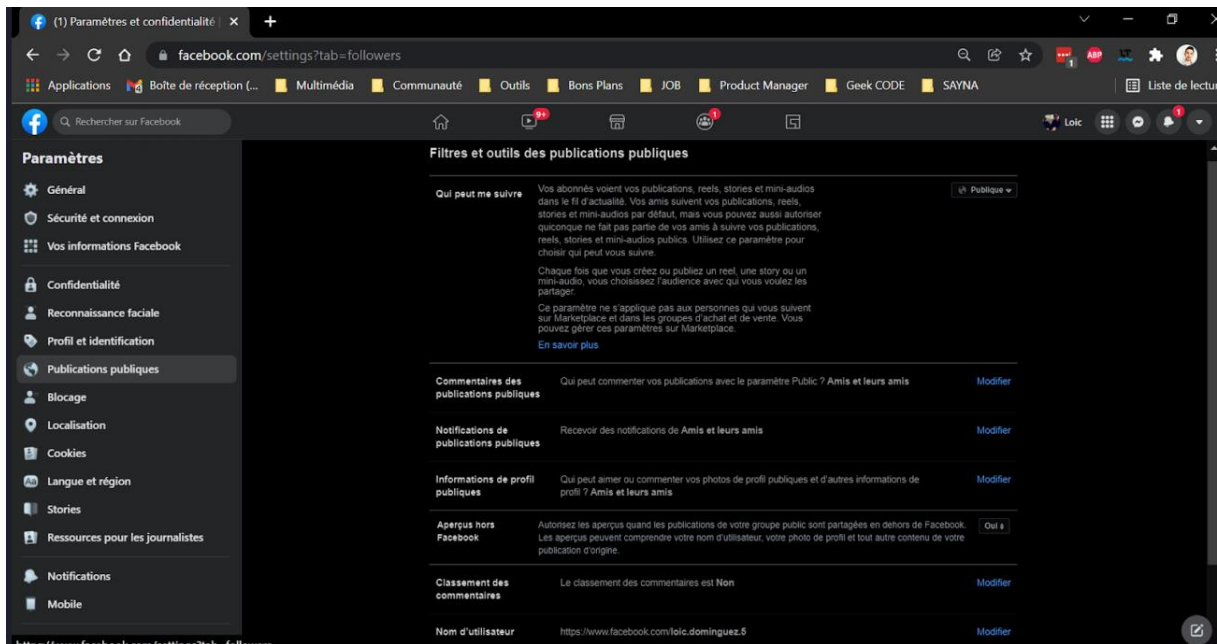
## Réponse

Voici un exemple de paramétrage de compte Facebook pour une utilisation privilégiant les échanges avec les amis, mais autorisant le contact avec des inconnus

- Confidentialité



- Publications publiques



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

1 /soit à proposer des exercices pour vérifier la sécurité en fonction de l'appareil utilisé ??????? Comment faire ????????

Exercice 1: Sécurité des ordinateurs personnels

- Quelles sont les mesures de sécurité recommandées pour protéger un ordinateur personnel ?
- Enumérez cinq bonnes pratiques pour maintenir la sécurité d'un ordinateur.
- Quels sont les signes révélateurs d'une infection par un logiciel malveillant sur un ordinateur ?

Exercice 2: Sécurité des appareils mobiles

- Quelles sont les principales menaces auxquelles les appareils mobiles sont confrontés en matière de sécurité ?
- Nommez trois mesures de sécurité que vous pouvez prendre pour protéger votre appareil mobile.
- Expliquez ce qu'est l'authentification à deux facteurs et pourquoi elle est importante pour la sécurité des appareils mobiles.

**Réponse :**

Exercice 1: Sécurité des ordinateurs personnels

- Les mesures de sécurité recommandées pour protéger un ordinateur personnel incluent :
  - Utiliser un logiciel antivirus et le maintenir à jour.

- Installer les mises à jour de sécurité du système d'exploitation et des applications.
- Utiliser des mots de passe forts et uniques pour les comptes utilisateur.
- Éviter de télécharger des logiciels provenant de sources non fiables.
- Sauvegarder régulièrement les données importantes.

b) Cinq bonnes pratiques pour maintenir la sécurité d'un ordinateur sont :

- Utiliser un pare-feu pour bloquer les connexions non autorisées.
- Activer la fonctionnalité de chiffrement pour protéger les données sensibles.
- Utiliser une connexion Wi-Fi sécurisée et éviter les réseaux publics non sécurisés.
- Être vigilant face aux tentatives de phishing et ne pas cliquer sur des liens suspects.
- Limiter les privilèges d'accès pour les comptes utilisateurs et utiliser un compte administrateur distinct.

c) Les signes révélateurs d'une infection par un logiciel malveillant sur un ordinateur peuvent inclure :

- Ralentissement soudain de la performance de l'ordinateur.
- Apparition de fenêtres publicitaires intempestives.
- Modifications non autorisées des paramètres du navigateur.
- Perte ou modification de fichiers sans raison apparente.
- Activité du disque dur ou du réseau excessive en l'absence d'utilisation de l'ordinateur.

## Exercice 2: Sécurité des appareils mobiles

a) Les principales menaces auxquelles les appareils mobiles sont confrontés en matière de sécurité sont :

- Logiciels malveillants ciblant les appareils mobiles.
- Applications non sécurisées ou contenant des logiciels malveillants.
- Perte ou vol de l'appareil.
- Attaques de phishing via des messages ou des liens suspects.
- Connexions Wi-Fi non sécurisées.

b) Trois mesures de sécurité que vous pouvez prendre pour protéger votre appareil mobile sont :

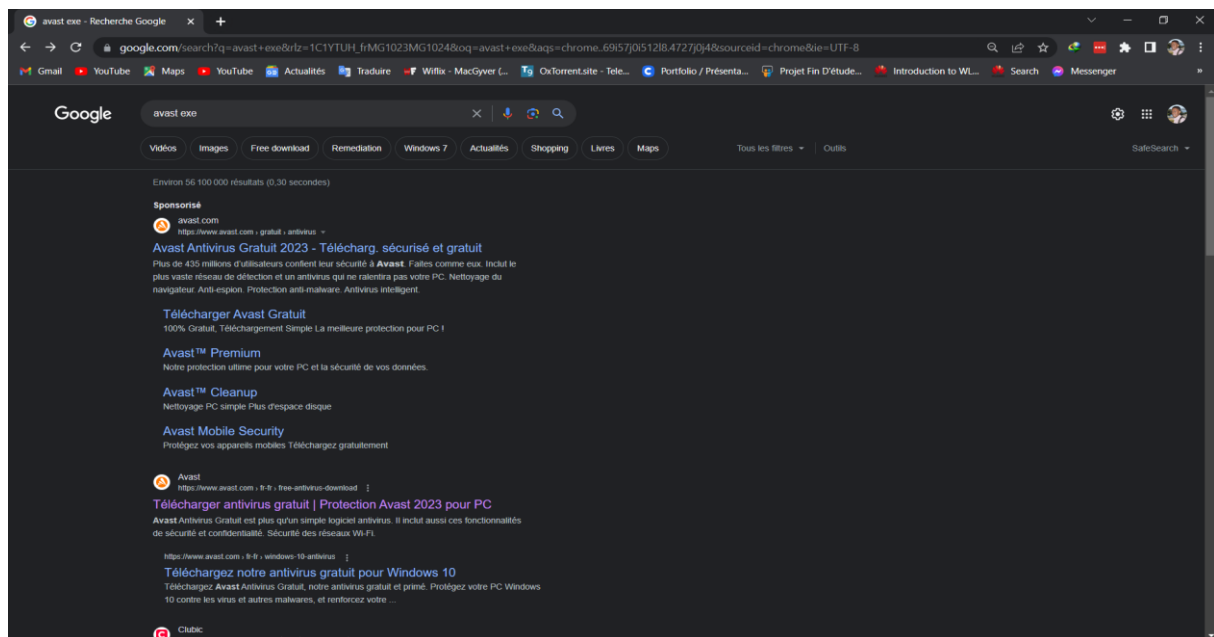
- Utiliser un code PIN, un schéma de verrouillage ou la reconnaissance biométrique pour protéger l'accès à l'appareil.
- Installer uniquement des applications provenant de sources officielles et vérifier les autorisations demandées.
- Activer le suivi à distance ou une fonctionnalité antivol pour localiser et verrouiller l'appareil en cas de perte ou de vol.

c) L'authentification à deux facteurs est une méthode de sécurité qui demande deux éléments d'identification différents pour accéder à un compte ou à un appareil. Cela ajoute une couche de sécurité supplémentaire en nécessitant, par exemple, un mot de passe et un code de vérification envoyé sur votre appareil mobile. Cela réduit le risque d'accès non autorisé, même si le mot de passe est compromis.

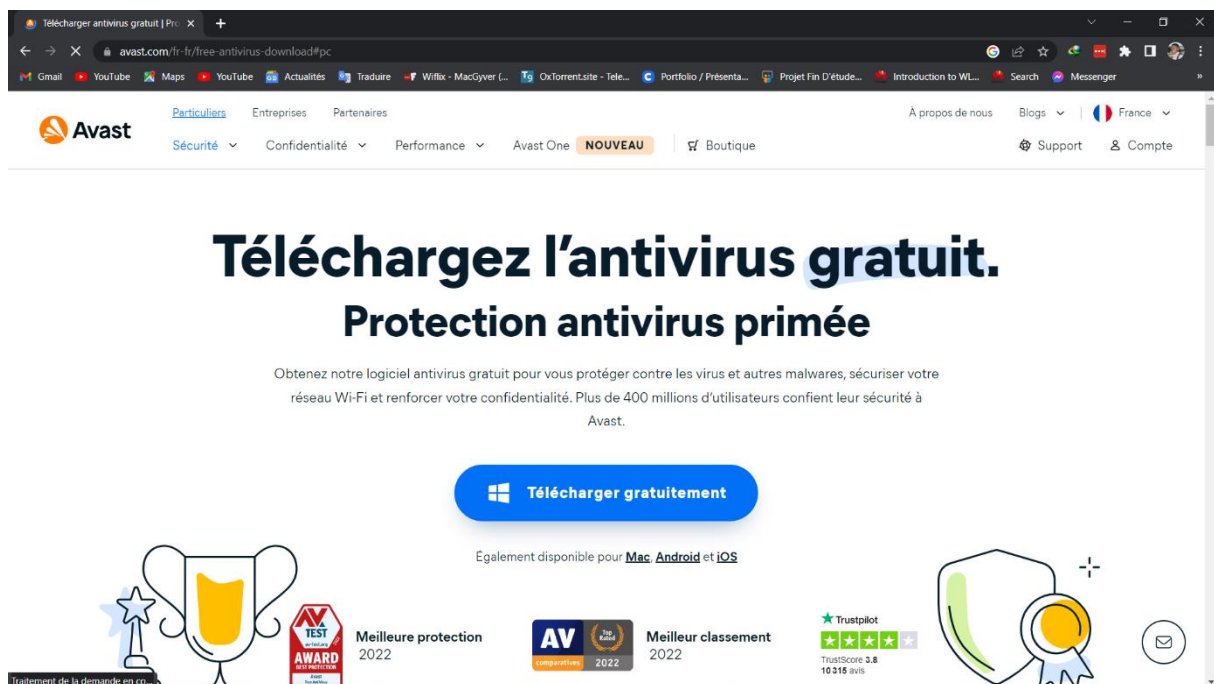


**2/ Soit à proposer un exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé.**

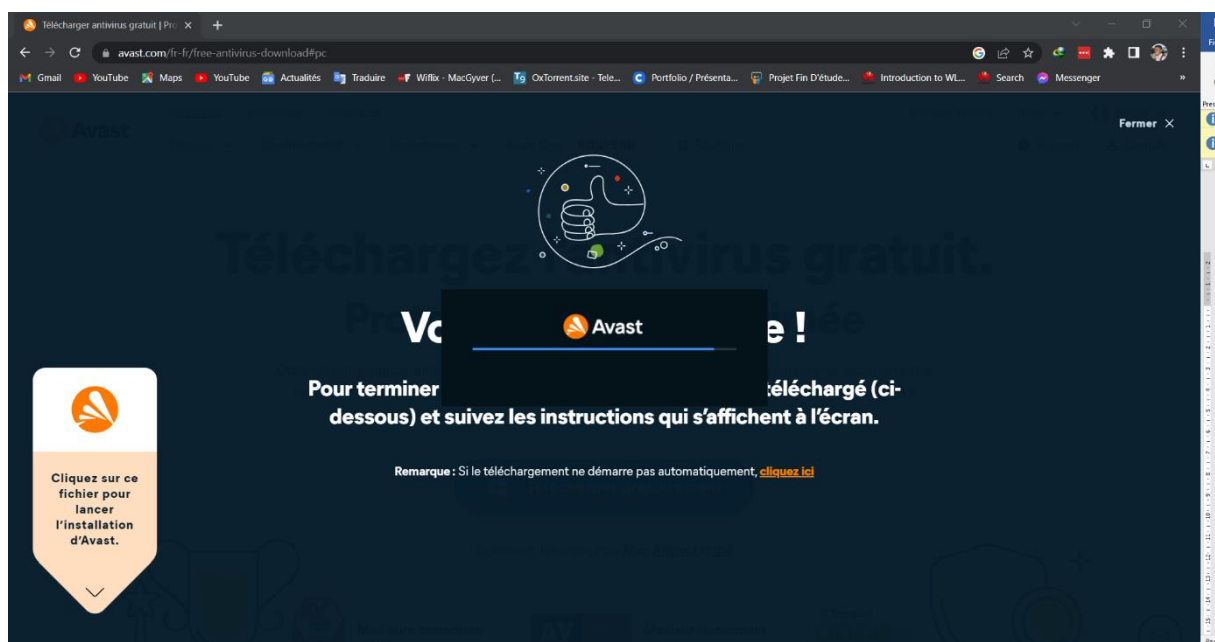
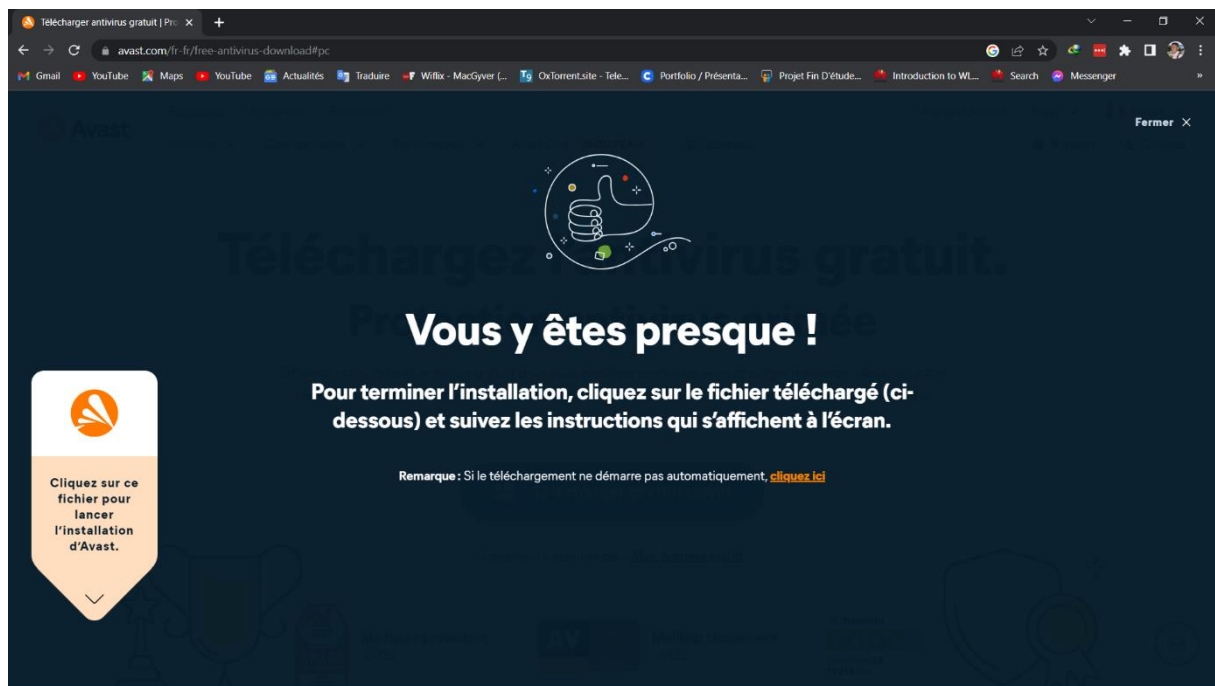
**Etape1 : Télécharger le logiciel d'antivirus et antimalware « AVAST on line »**

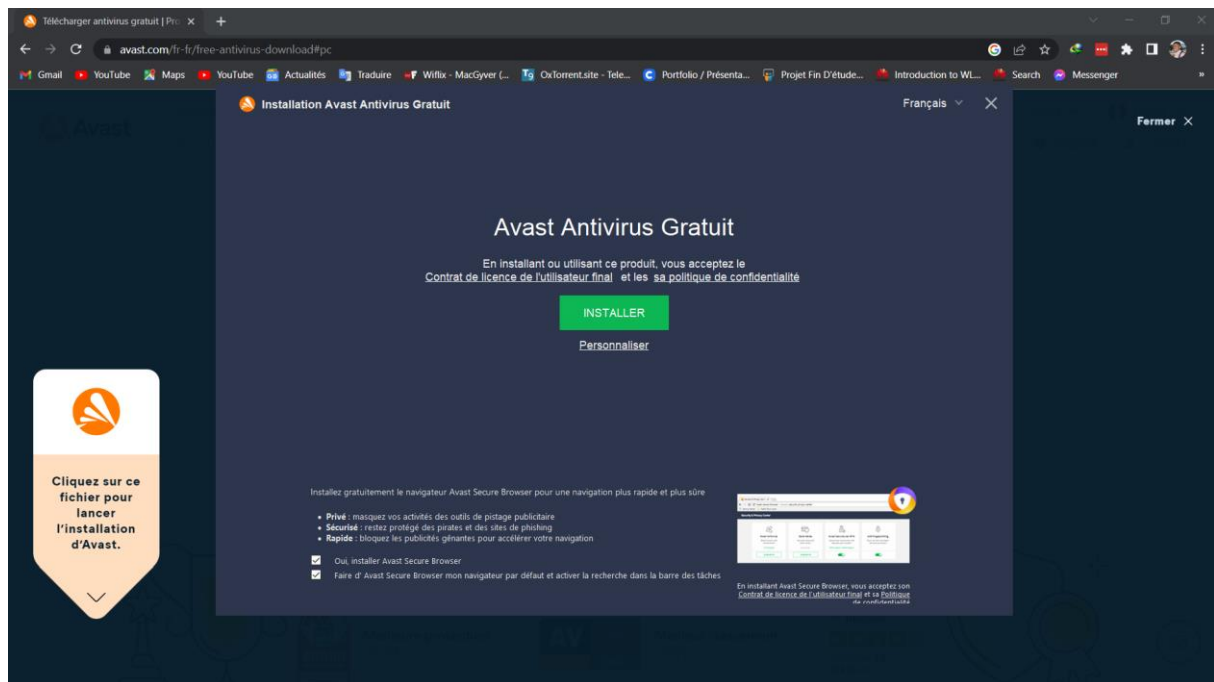


**Etape2 : Cliquer sur le bouton téléchargement**

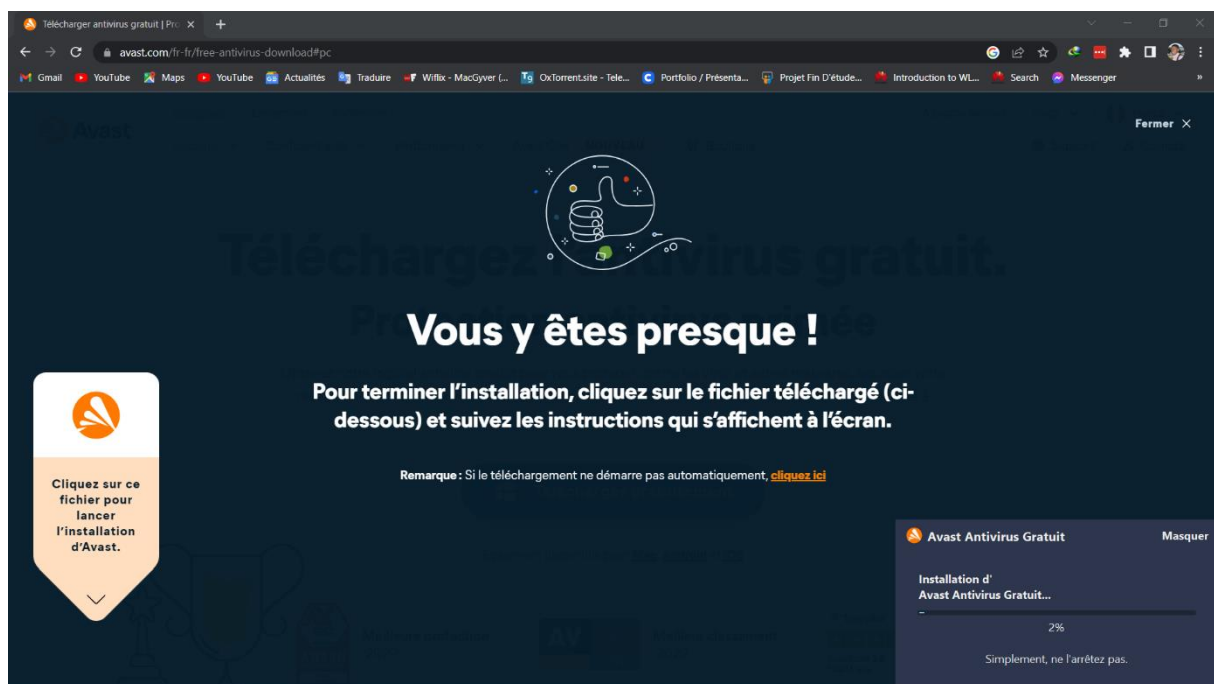


### Etape3 : Attendre le lancement du téléchargement

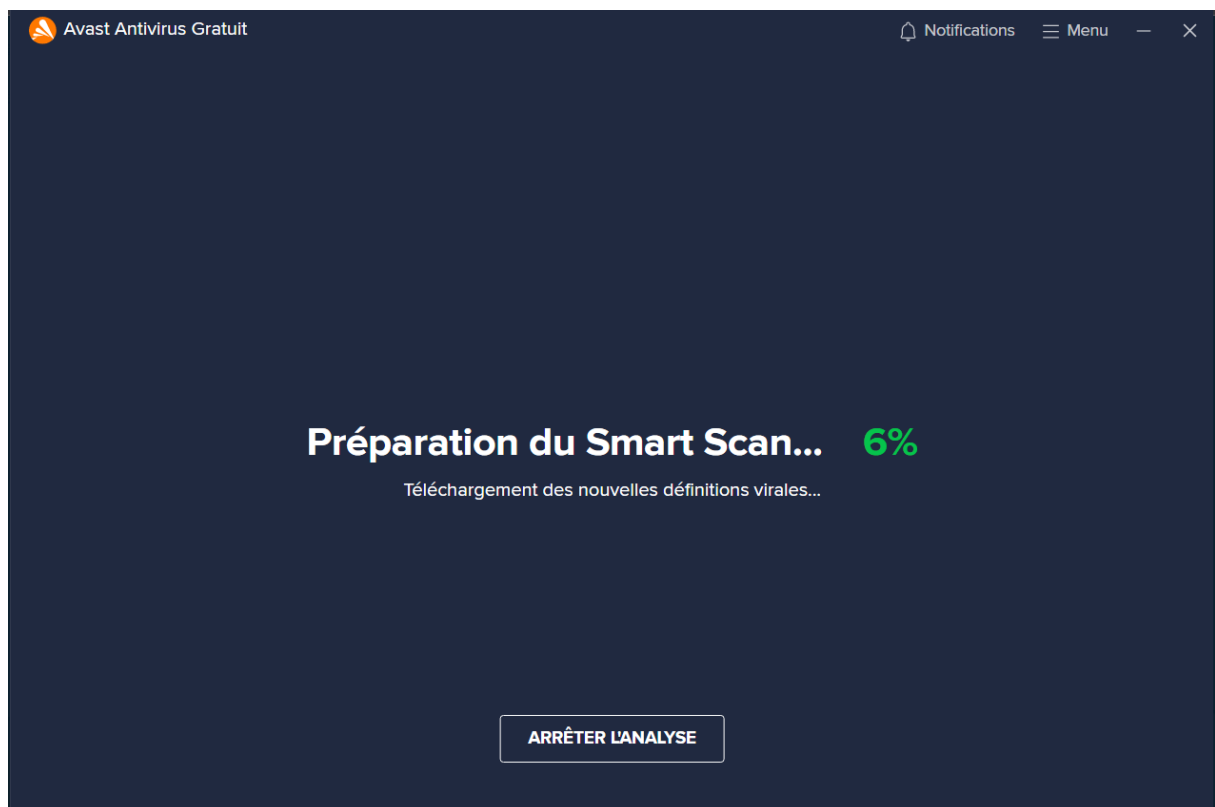
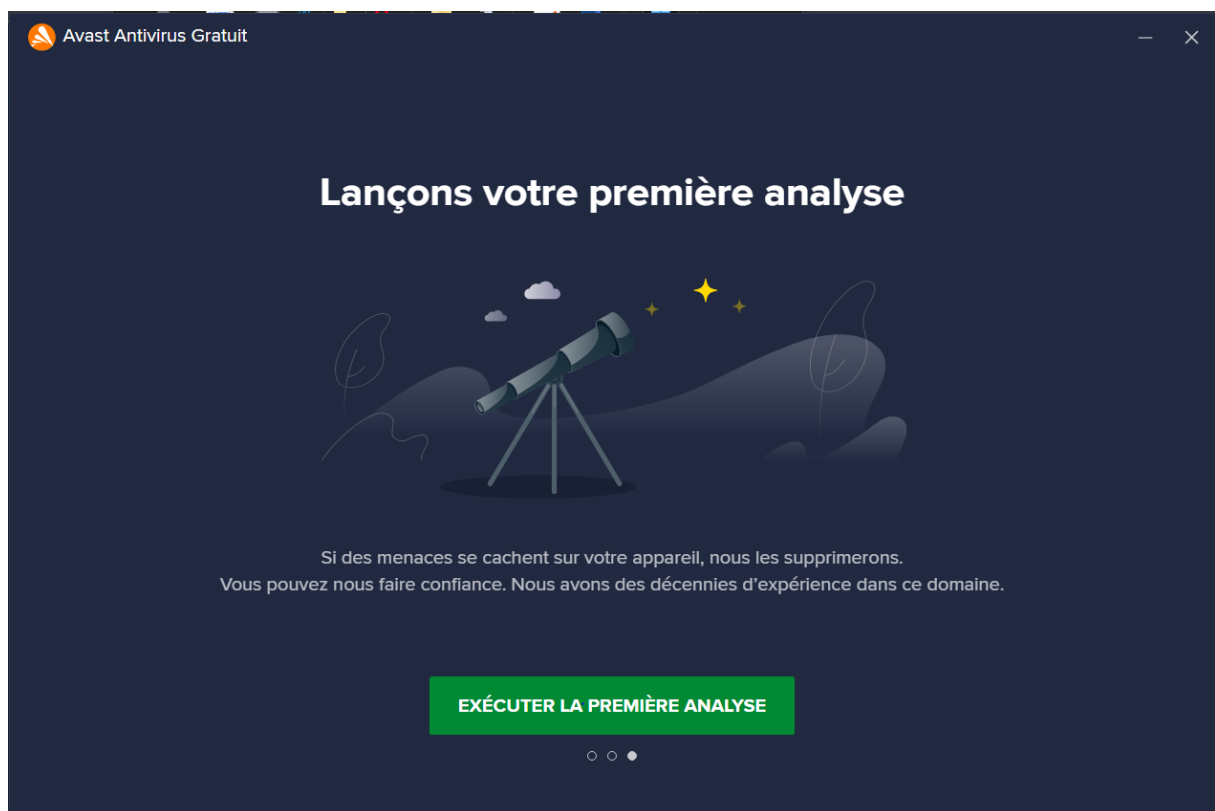


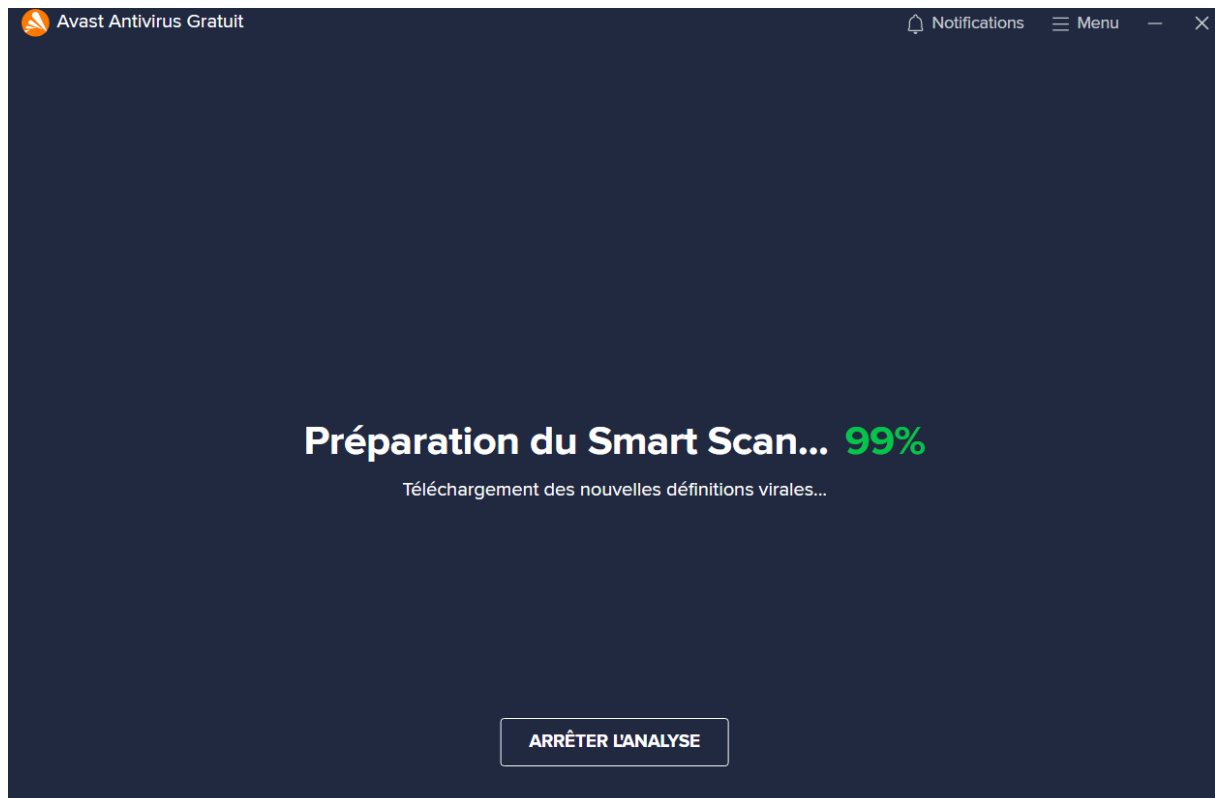


#### Etape4 : Attendre la fin du téléchargement

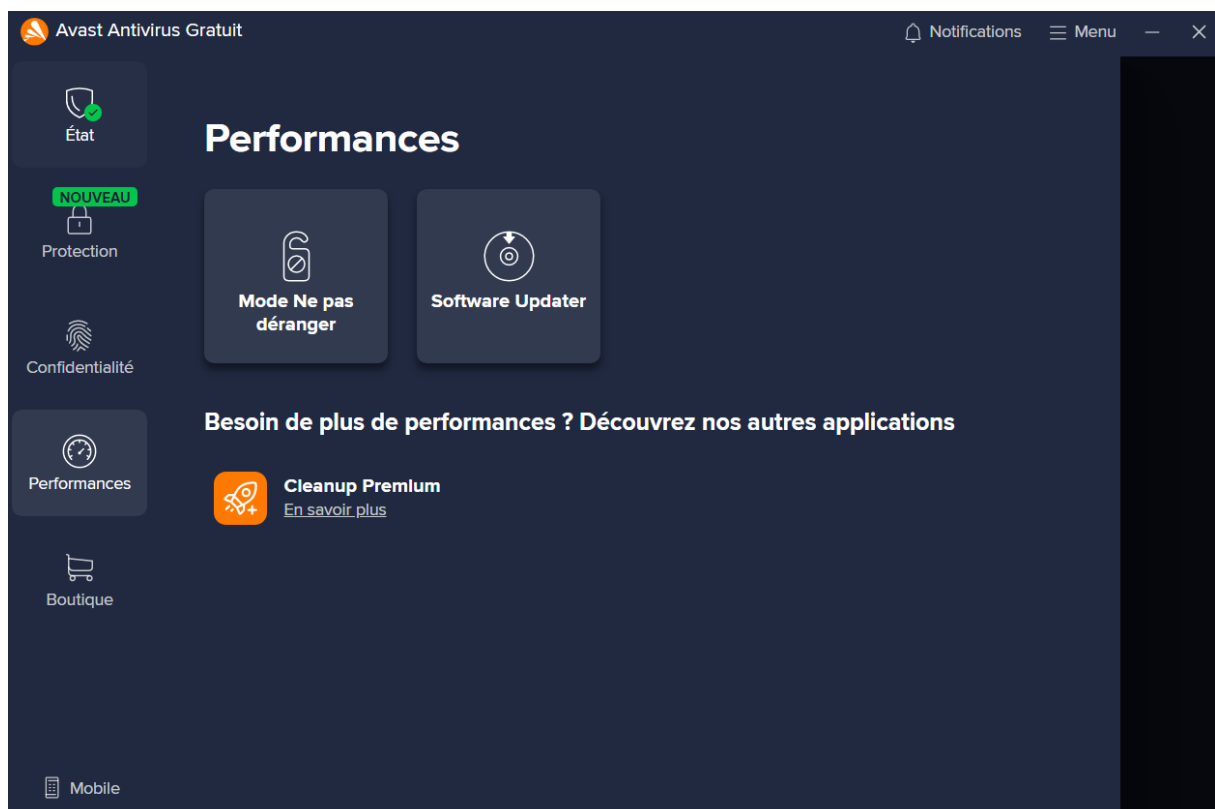


## Etape5 : Exécuter l'analyse





## Etape6 :Après avoir fini l'Analyse





État

## Protection

NOUVEAU



Protection



Confidentialité



Performances



Boutique

Mobile



Analyse antivirus



Agents de sécurité



Quarantaine



Inspecteur réseau



Agent anti-ransomware



Pare-feu



NOUVEAU

Mode bancaire



Agent contre l'accès distant



Real Site



Sandbox