

Parcours : DISCOVERY

Module : Naviguer en toute sécurité

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

## **Sommaire**

- 1- Introduction à la sécurité 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 internet

Objectif : à la découverte de la sécurité sur internet

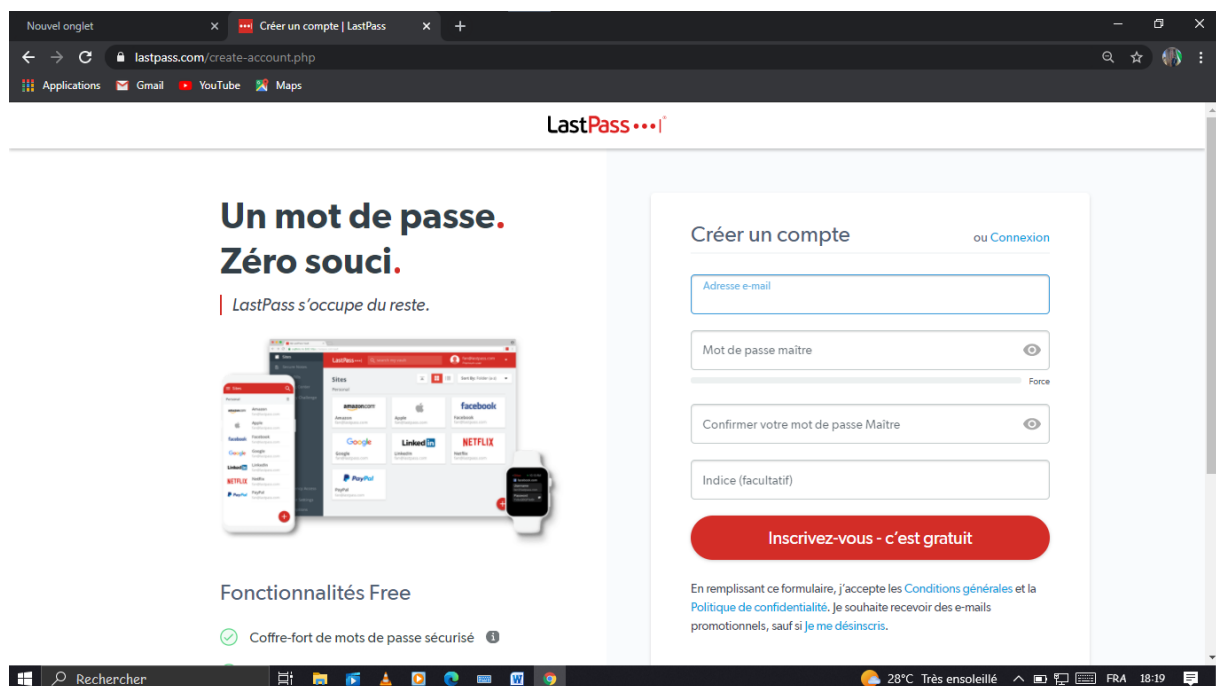
1/ En naviguant sur le web, consulte trois articles qui parlent de sécurité sur internet. Pense à vérifier la source des informations et essaie de consulter des articles récents pour que les informations soient à jour. Saisis le nom du site et de l'article.

- Article 1 = Kaspersky - définitions et significations de la sécurité sur internet
- Article 2 = Cybermalveillance - Comment se protéger sur Internet ?
- Article 3 = O'communication - Sécurité internet

## 2- Créer des mots de passe forts

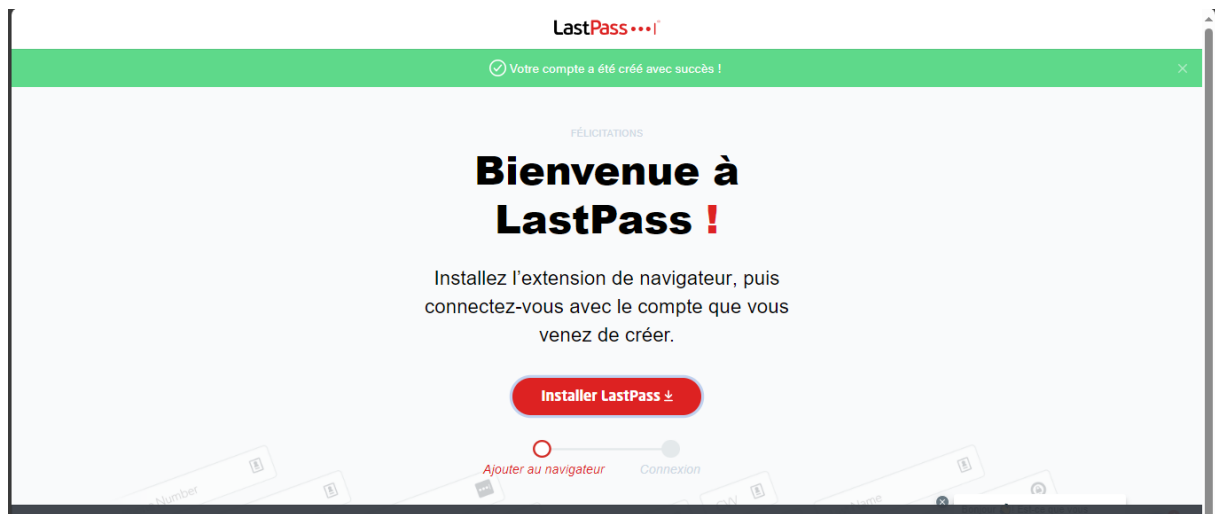
Objectif : utiliser un gestionnaire de mot de passe LastPass

- a) 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. Suis les étapes suivantes
- Accès au site de LastPass

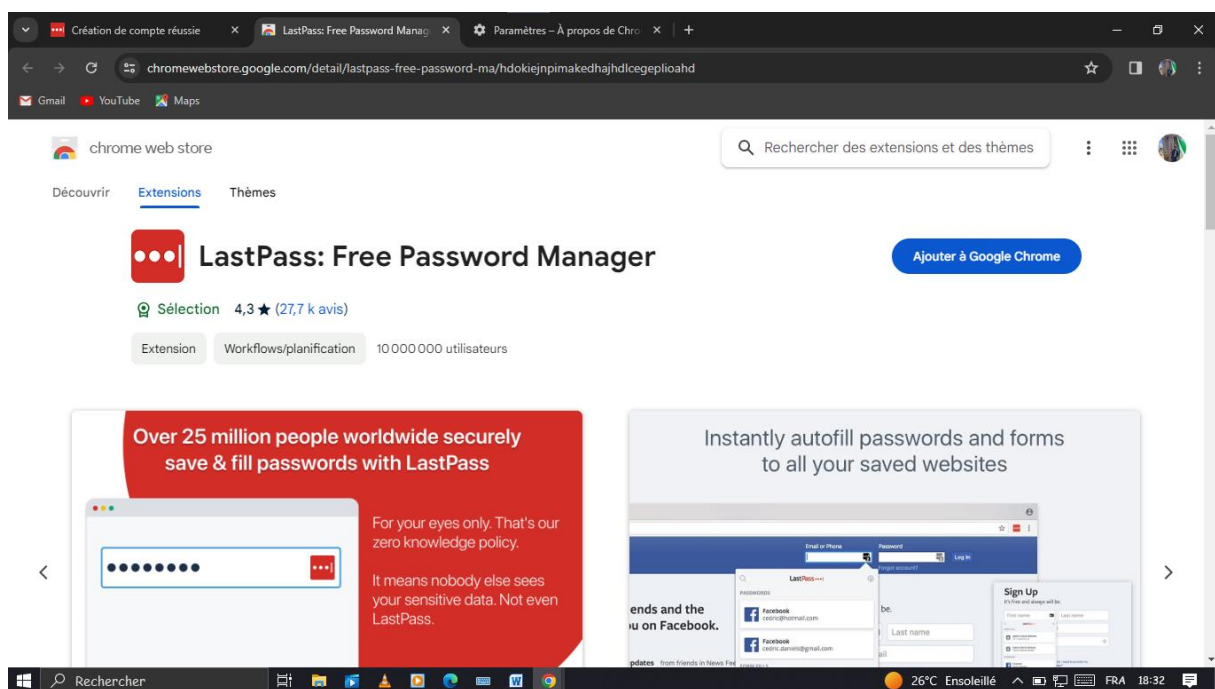


The screenshot shows a web browser window with the URL `lastpass.com/create-account.php`. The page features the LastPass logo and the headline "Un mot de passe. Zéro souci." with the tagline "LastPass s'occupe du reste." Below this is an illustration of a smartphone and a laptop displaying the LastPass interface. To the right, there is a "Créer un compte" (Create account) form with the following fields: "Adresse e-mail", "Mot de passe maître" (Master password) with a strength indicator, "Confirmer votre mot de passe Maître" (Confirm your master password), and "Indice (facultatif)" (Optional hint). A red button labeled "Inscrivez-vous - c'est gratuit" (Sign up - it's free) is at the bottom of the form. Below the button, 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." The browser's taskbar at the bottom shows the Windows logo, a search bar, and various application icons, along with system information: "28°C Très ensoleillé", "FRA", and "18:19".

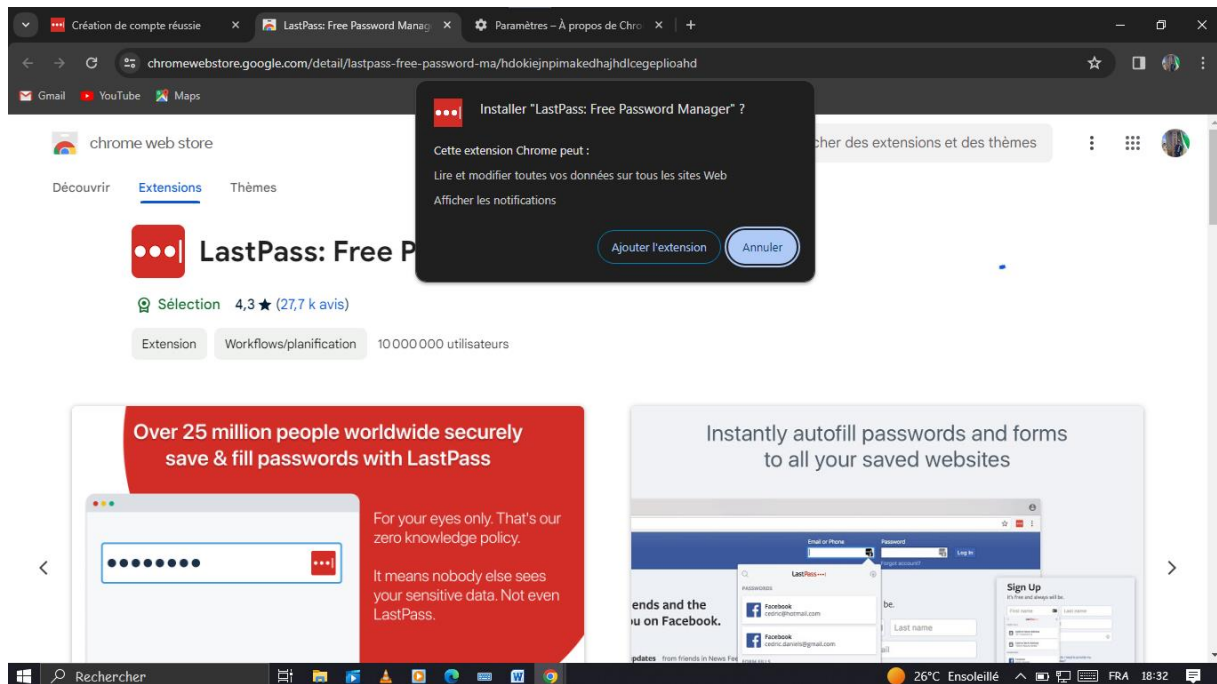
- Création d'un compte en remplissant le formulaire



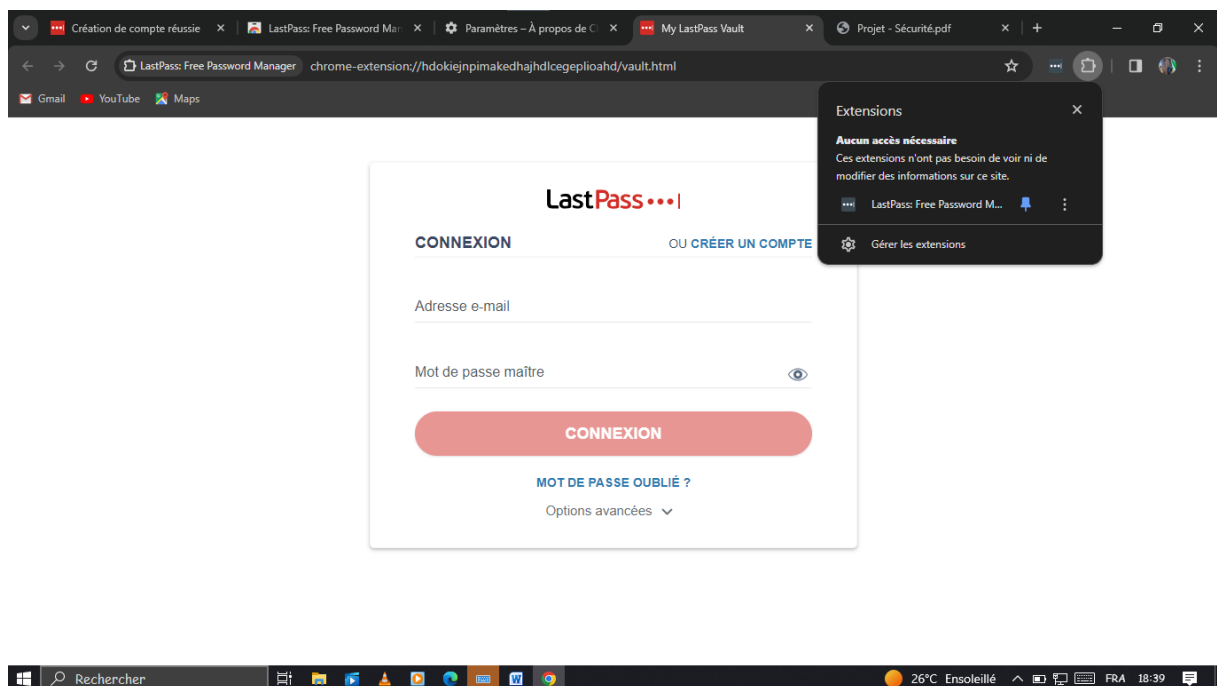
- Validation



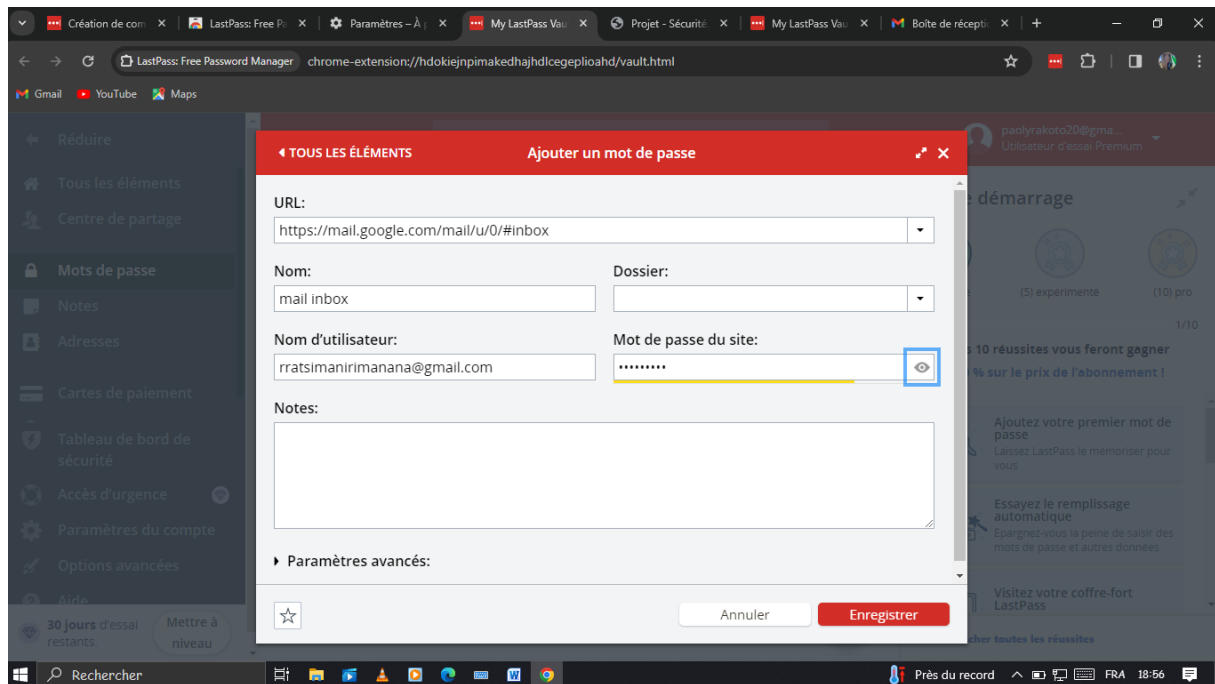
- Validation



- Accès et connexion à l'extension



- utilisation du gestionnaire de mot de passe



### 3- Fonctionnalité de sécurité de votre navigateur

Objectif : identifier les éléments à observer pour naviguer sur le web en toute sécurité

a- Identifie les adresses internet qui te 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

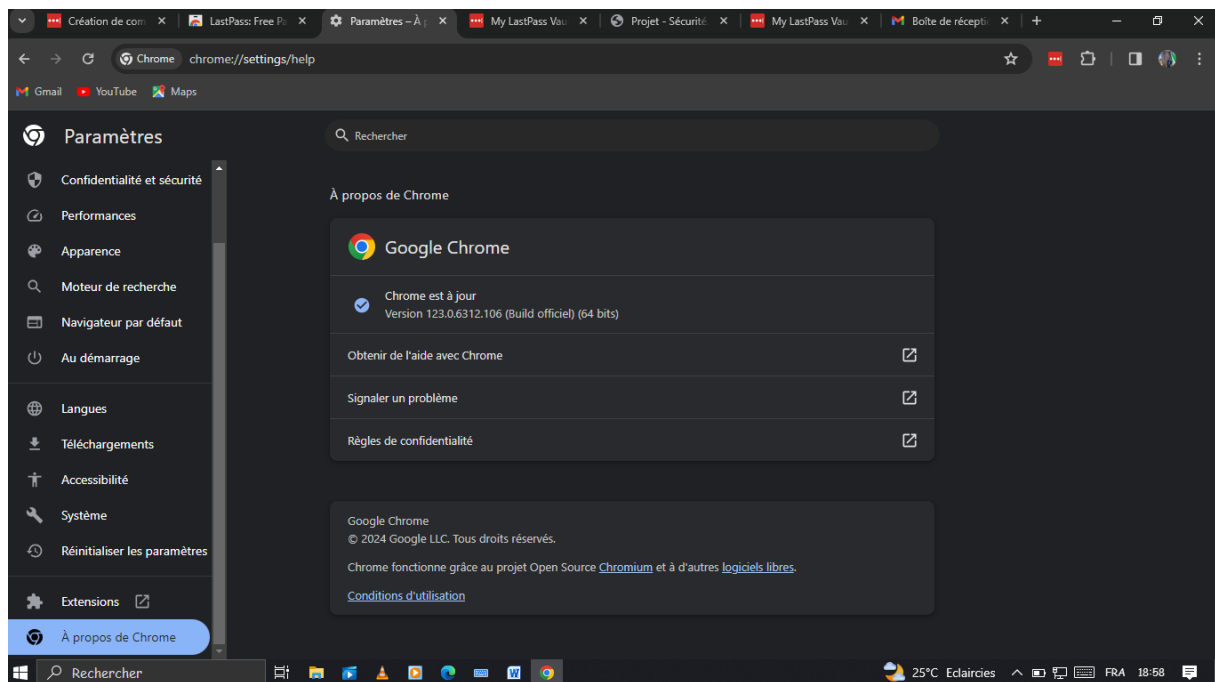
- [www.instagram.com](http://www.instagram.com), un dérivé de [www.instagram.com](http://www.instagram.com), un autre réseau social très utilisé

Les seuls sites qui semblaient être cohérents sont donc :

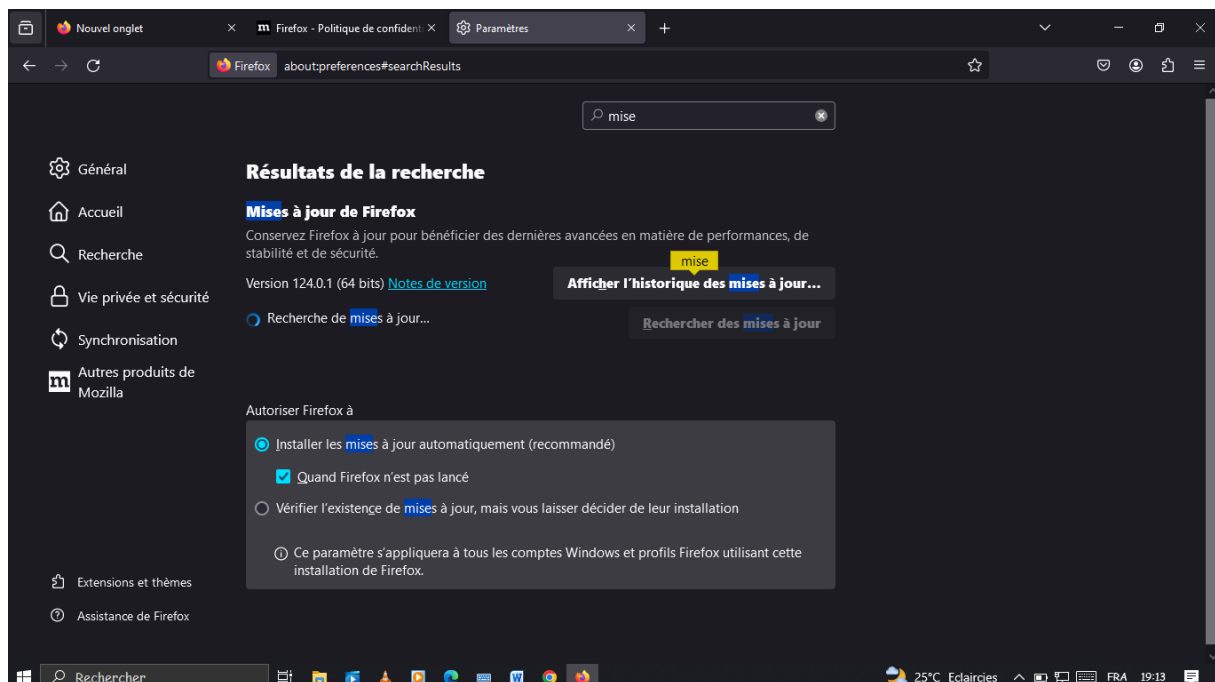
- [www.dccomics.com](http://www.dccomics.com), le site officiel de l'univers DC Comics
- [www.ironman.com](http://www.ironman.com), le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

b- Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour.

- Pour Chrome



- Pour Firefox



## 4- Éviter le spam et le phishing

Objectif : Reconnaître plus facilement les messages frauduleux

## 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
- Analyse Google : Aucun contenu suspect

➤ Site n°2

- Indicateur de sécurité : Not secured
- Analyse Google : Aucun contenu suspect

➤ ● Site n°3

- Indicateur de sécurité : Not secured
- Analyse Google : Vérifier un URL en particulier (analyse trop générale)

## **6- Achats en ligne sécurisés**

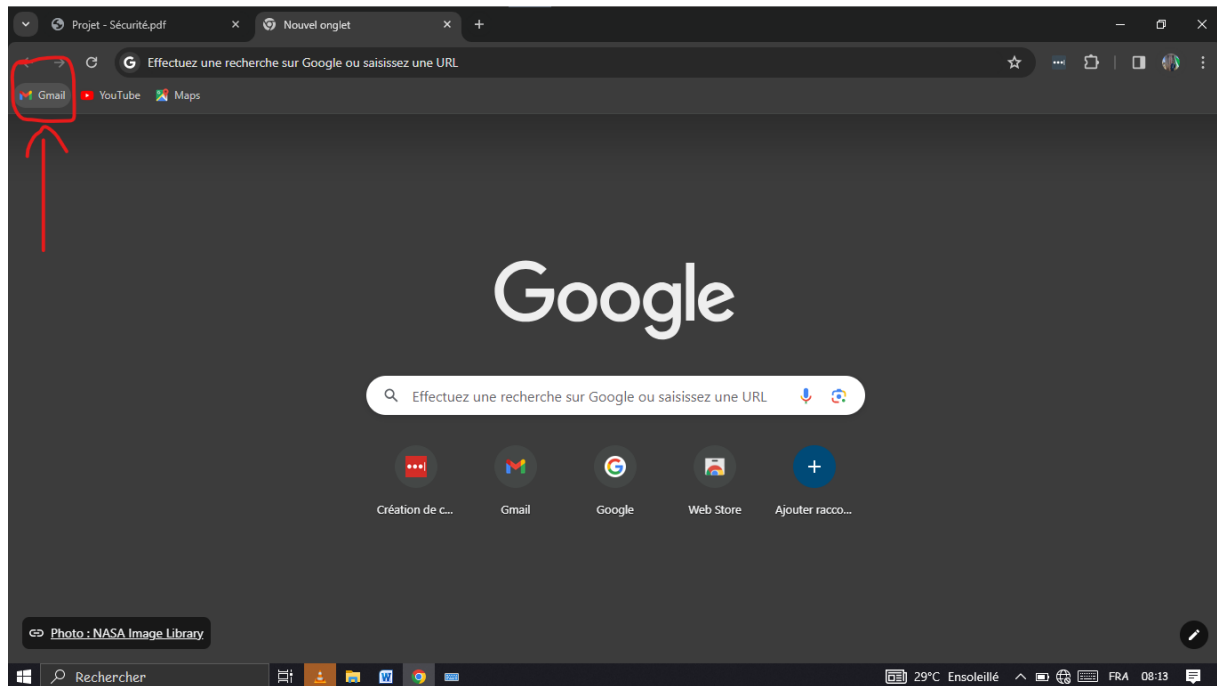
Objectif : créer un registre des achats effectués sur internet

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.

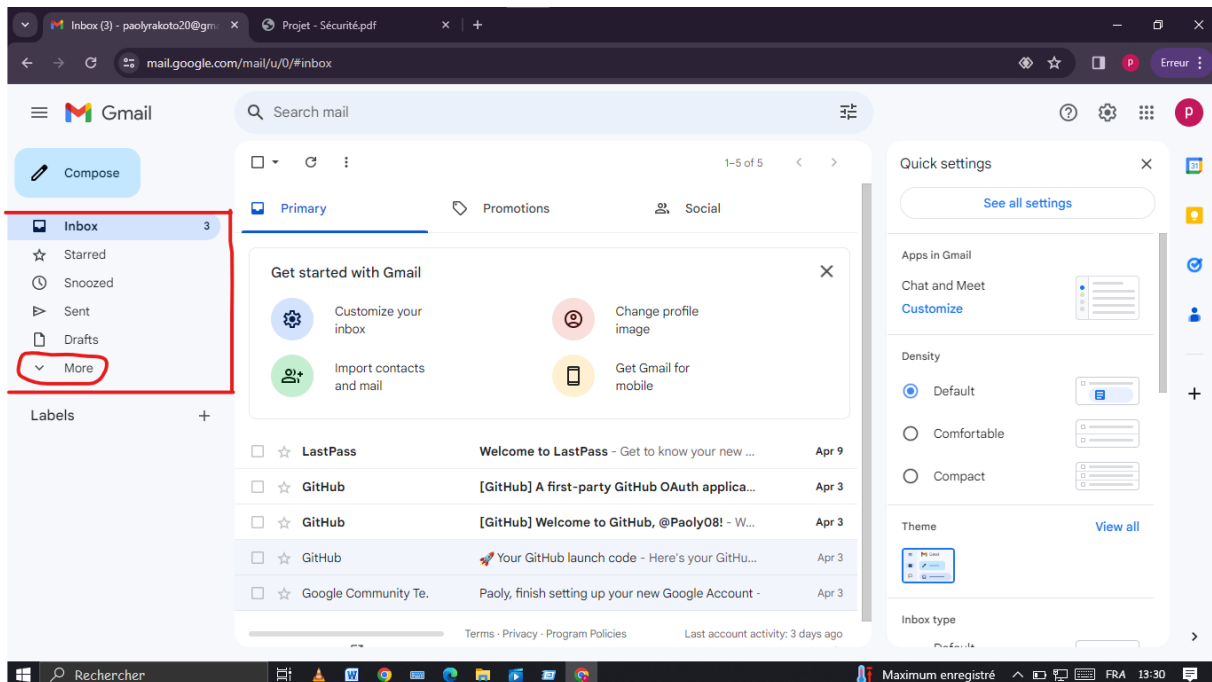
Deux possibilités s'offrent à toi pour organiser ce registre :

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

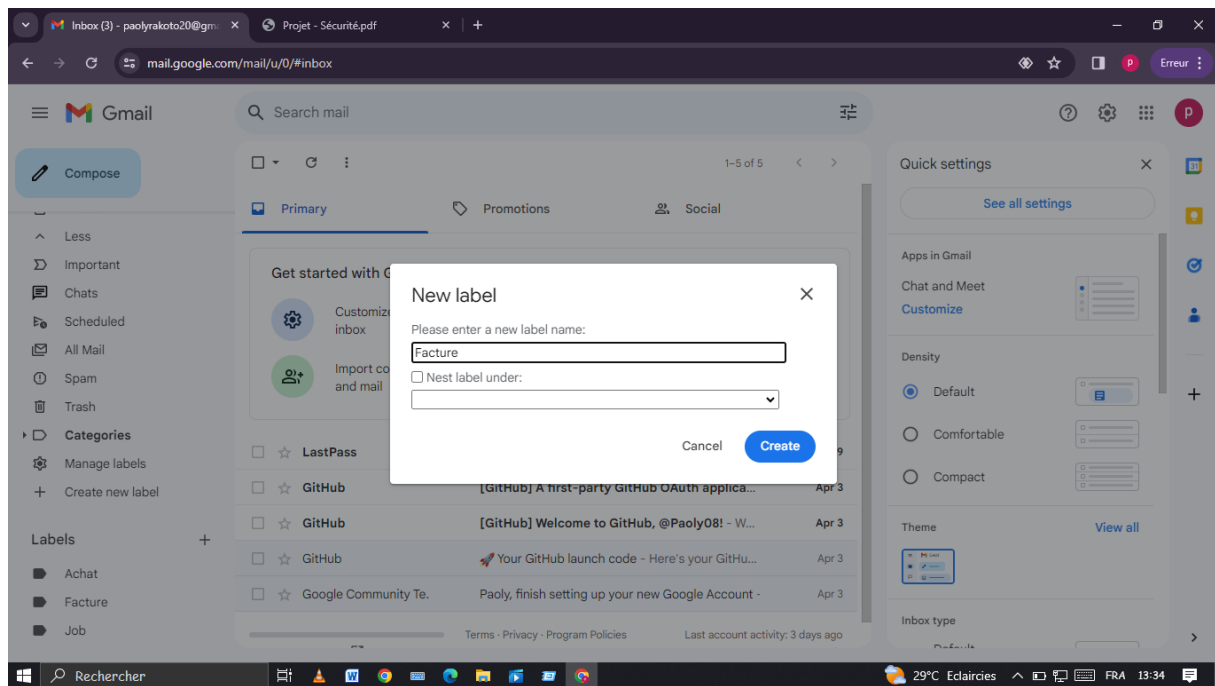
## ➤ Accès à la messagerie électronique



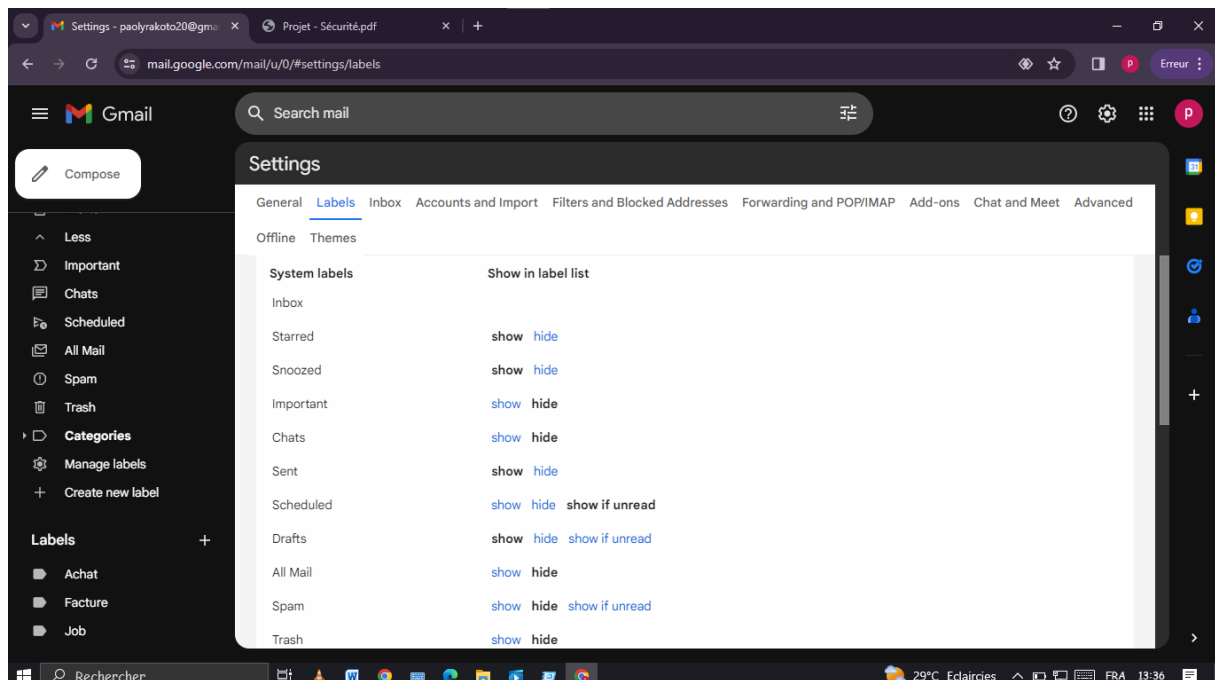
## ➤ Page d'accueil



## ➤ Création de libellé

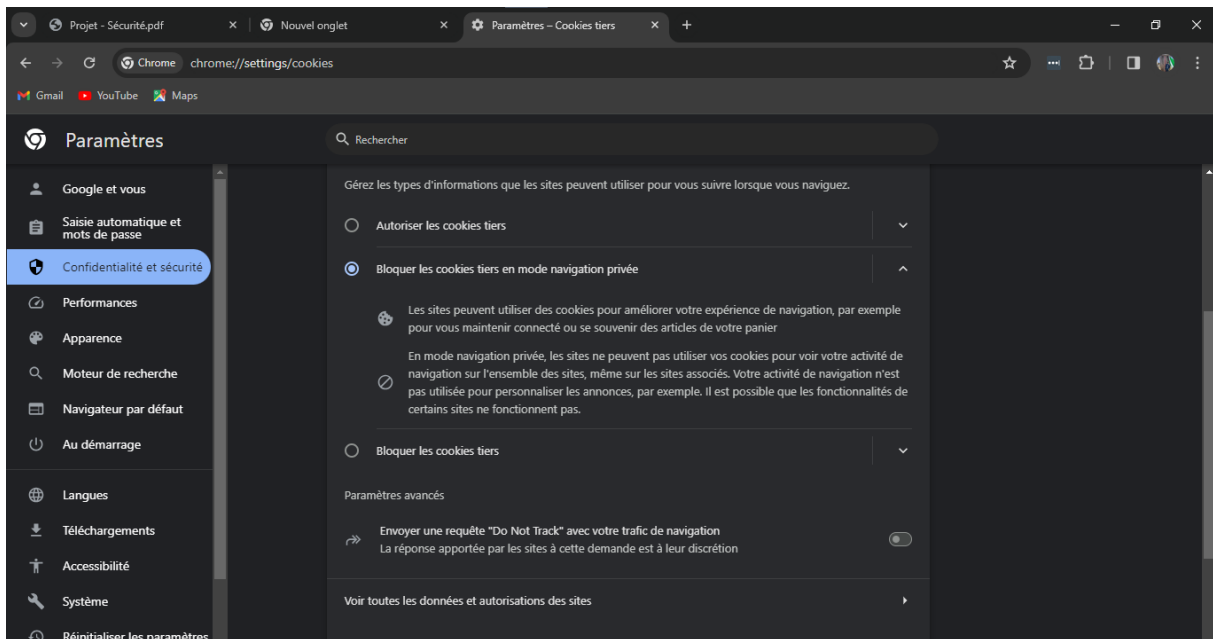


## ➤ Gérer le libellé



## 7- Comprendre le suivi du navigateur

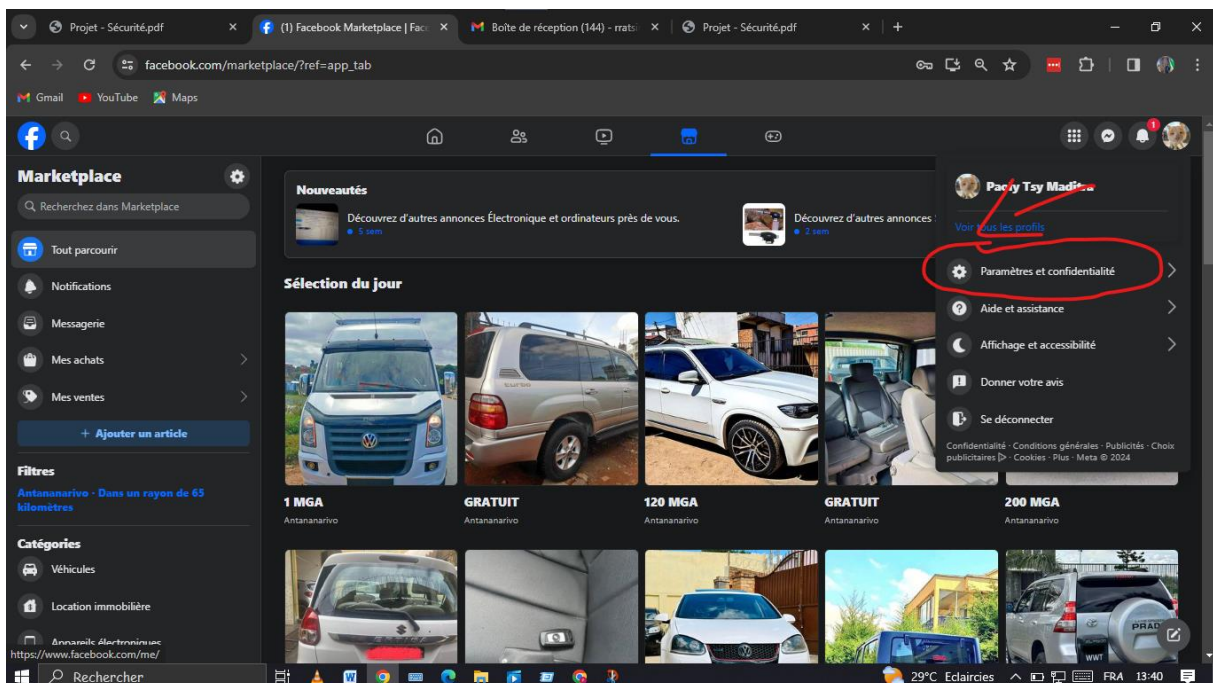
Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée



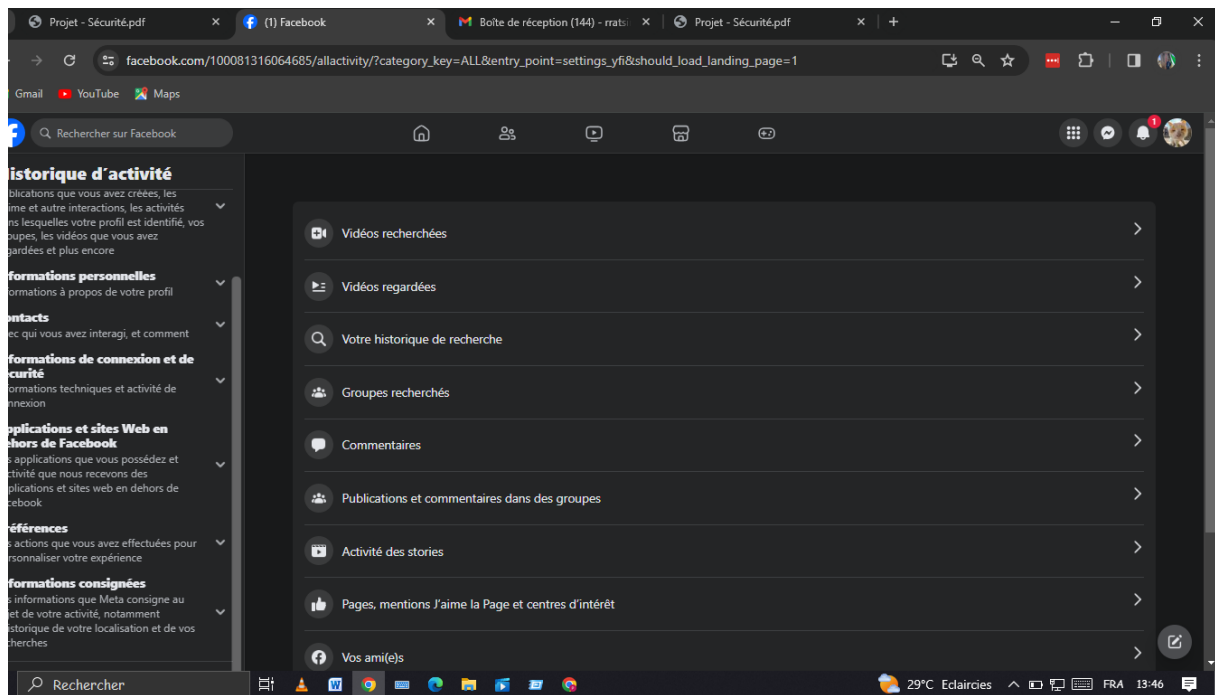
## 8- Principes de base de la confidentialité des médias sociaux

Objectif : Régler les paramètres de confidentialité de Facebook

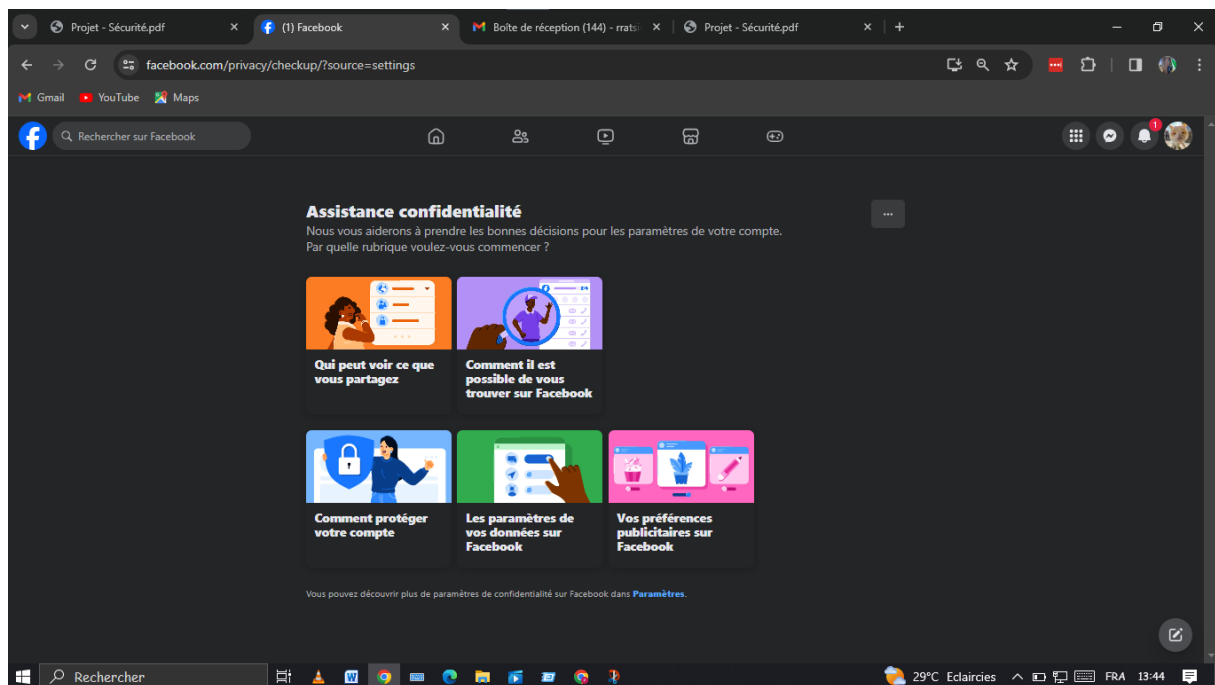
➤ Paramètres



## ➤ Paramètre de Confidentialité



## ➤ Assistance de confidentialité



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

Objectif :

1/ exercice pour vérifier la sécurité de l'appareil utilisé

Pour un ordinateur :

- Analyse des vulnérabilités : Utilisez des outils d'analyse des vulnérabilités pour rechercher les failles de sécurité potentielles dans le système d'exploitation, les applications installées et les services en cours d'exécution.
- Scan antivirus et anti-malware : Exécutez des analyses antivirus et anti-malware pour détecter et éliminer les logiciels malveillants, les virus et autres menaces potentielles.

Pour un smartphone :

- Analyse des applications : Examinez les applications installées sur le smartphone pour détecter les applications malveillantes ou suspectes. Utilisez des outils antivirus ou anti-malware spécifiquement conçus pour les smartphones.
- Mises à jour du système d'exploitation et des applications : Assurez-vous que le système d'exploitation du smartphone ainsi que toutes les applications sont régulièrement mises à jour avec les derniers correctifs de sécurité pour remédier aux vulnérabilités connues.

2/ exercice pour installer et utiliser un antivirus + antimalware

➤ Pour un smartphone :

- Recherchez une application fiable
- Téléchargez et installez l'application
- Configurez l'application
- Effectuez une analyse initiale
- Activez les fonctions de protection en temps réel
- Mettez à jour régulièrement

- Pour un ordinateur
  - Choix du logiciel
  - Téléchargement
  - Installation
  - Configuration
  - Mise à jour
  - Analyse initial
  - Protection en temps réel
  - Planification des analyses
  - Utilisation continue