**Parcours : DISCOVERY**

**Module : Naviguer en toute sécurité**

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

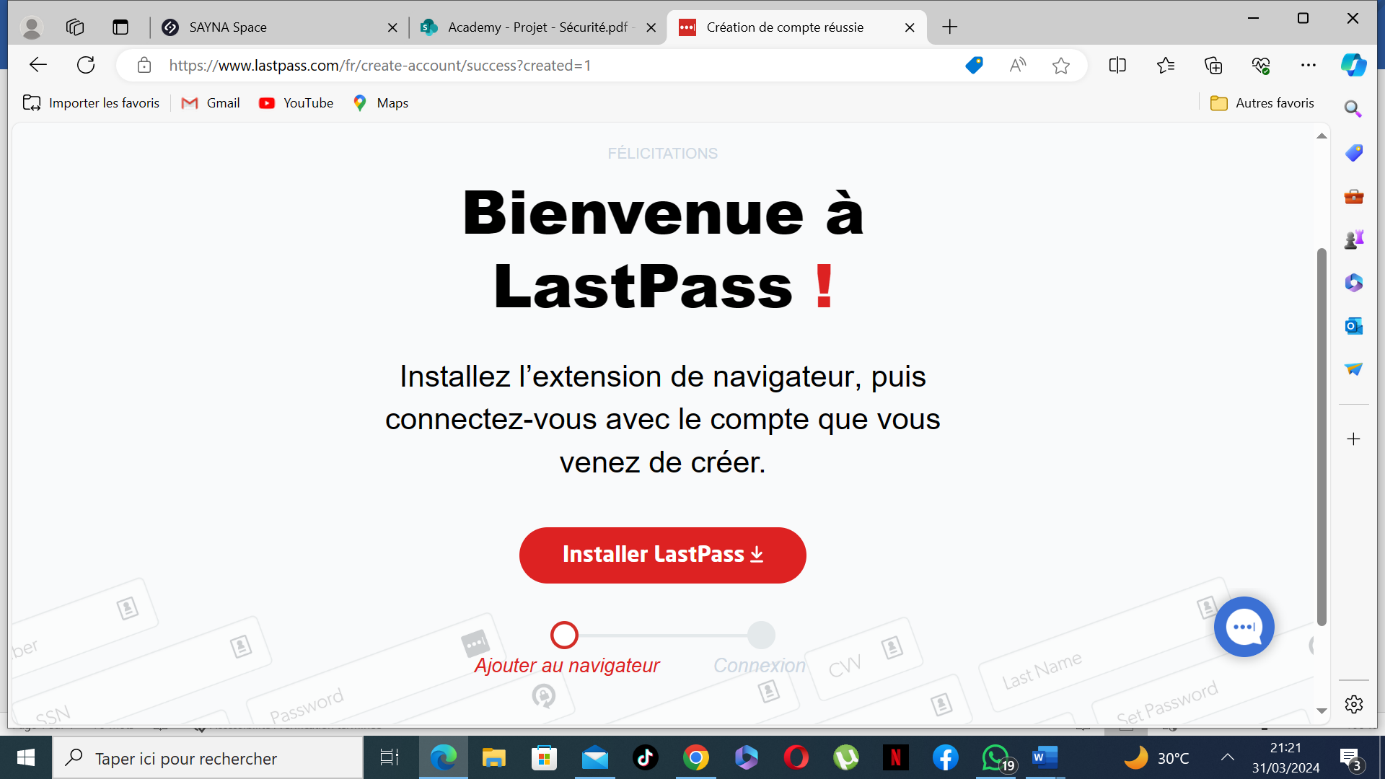
1. **Introduction à la sécurité sur internet**

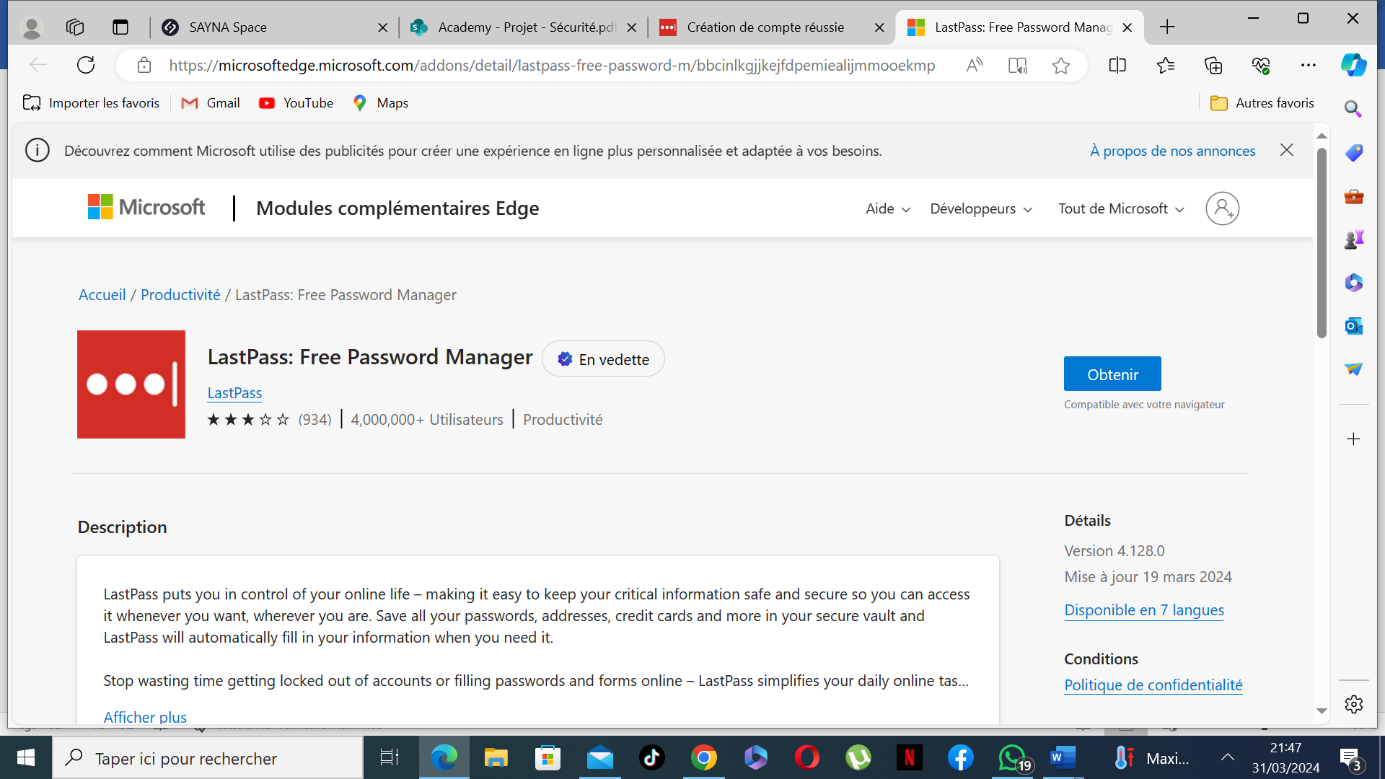
**1/ Cite trois articles récents qui parlent de sécurité sur internet**

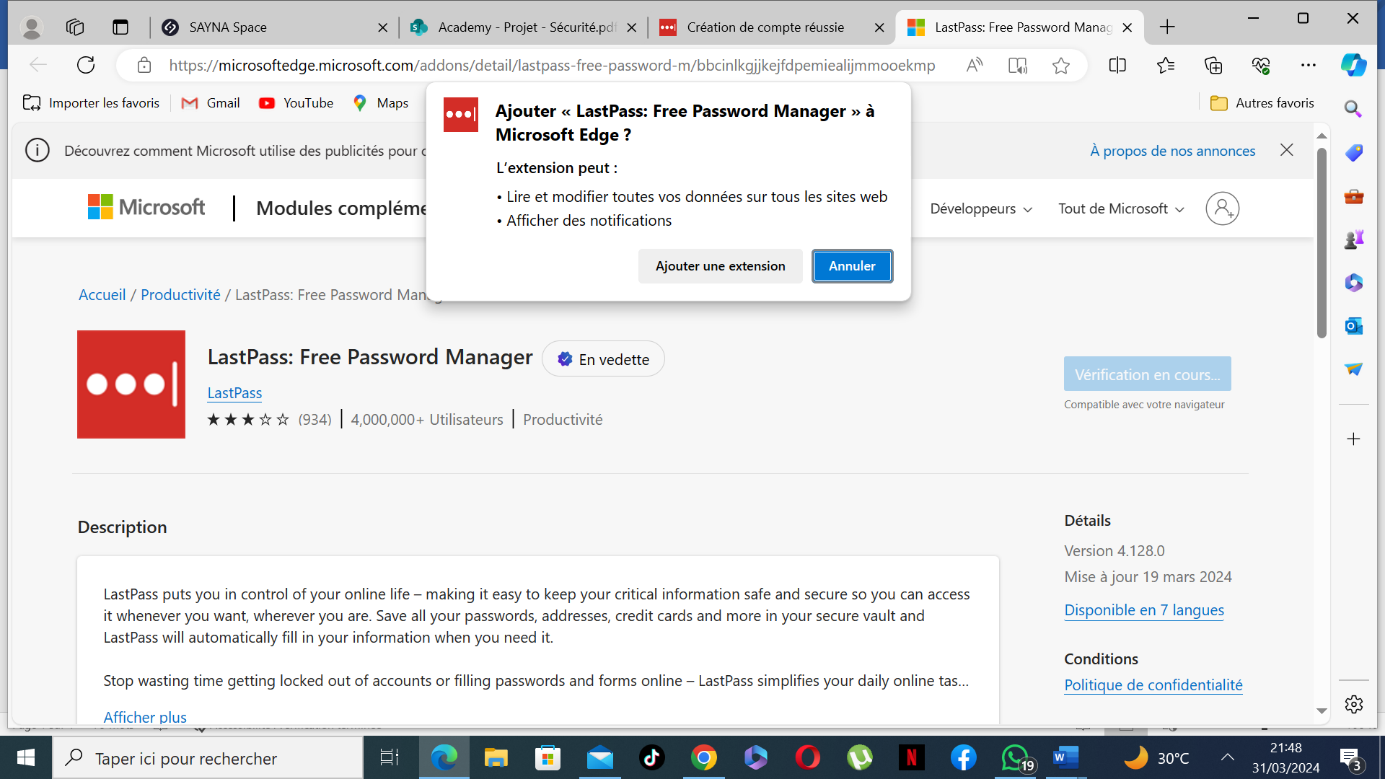
**Réponse 1**

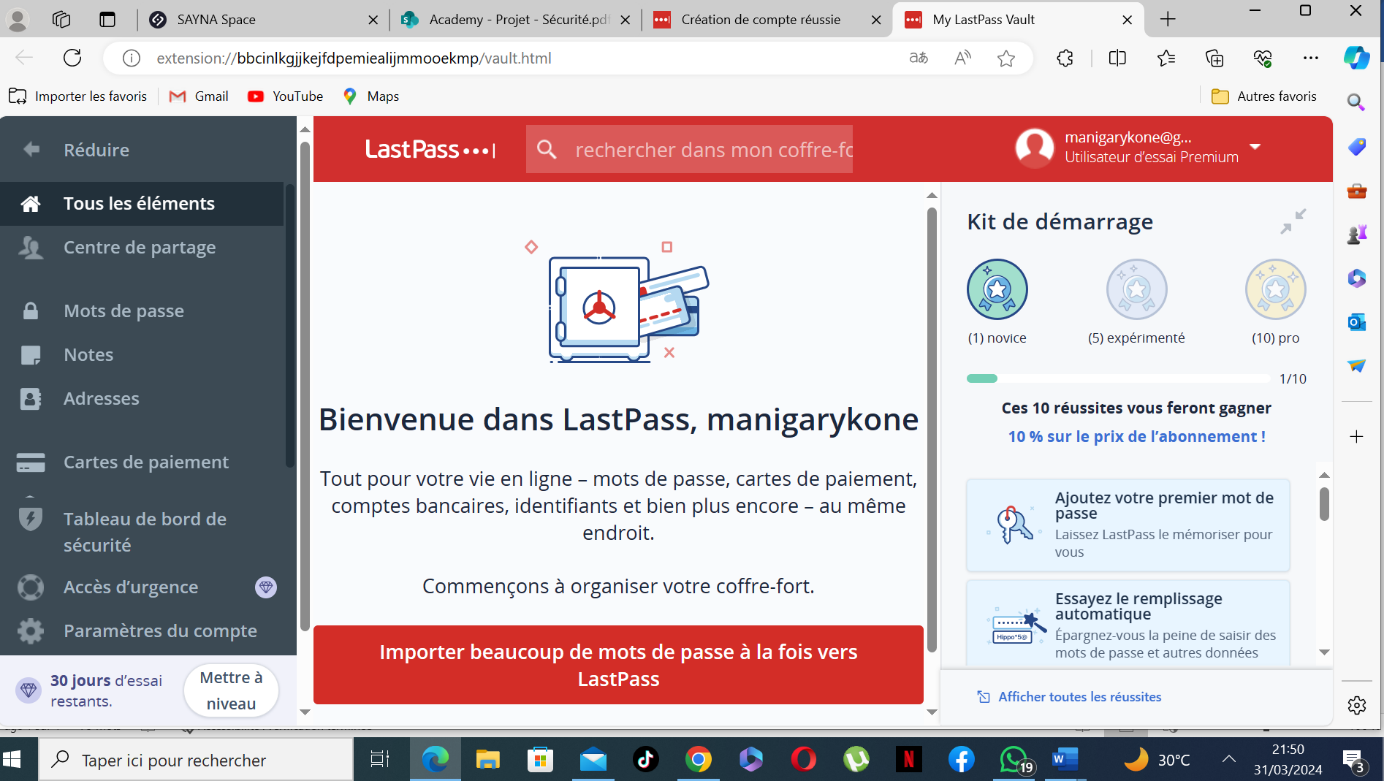
* Article 1 = ANSSI - Dix règles de base
* Article 2 =Economie.gouv - Comment assurer notre sécurité numérique
* Article 3 = Site W - Naviguer en toute sécurité sur internet

**2 – Créer des mots de passe forts**

****

****

****

****

**3 – Fonctionnalité de sécurité de votre navigateur**

**1/ Identifie les adresses internet qui te semblent provenir de sites Web malveillants**

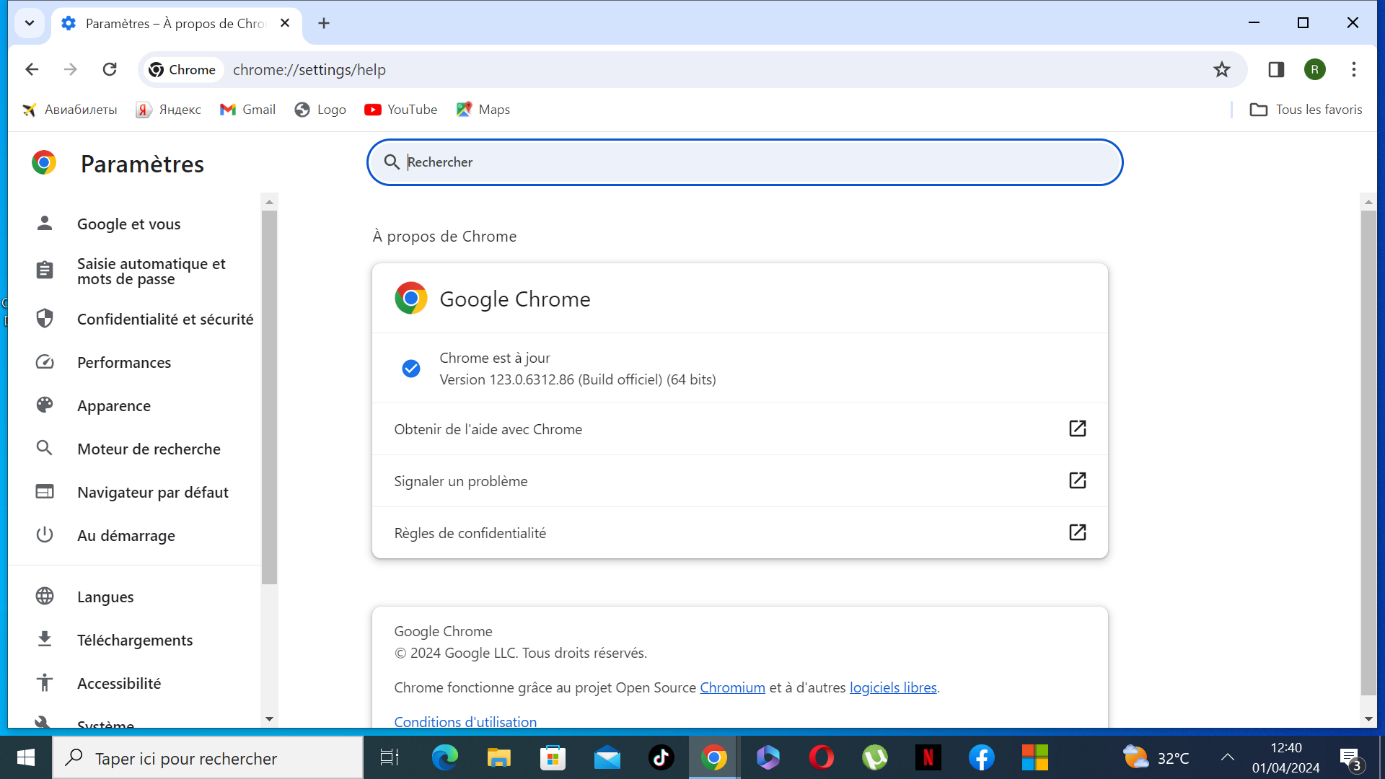
* www.morvel.com
* www.dccomics.com
* www.ironman.com
* www.fessebook.com
* www.instagam.com

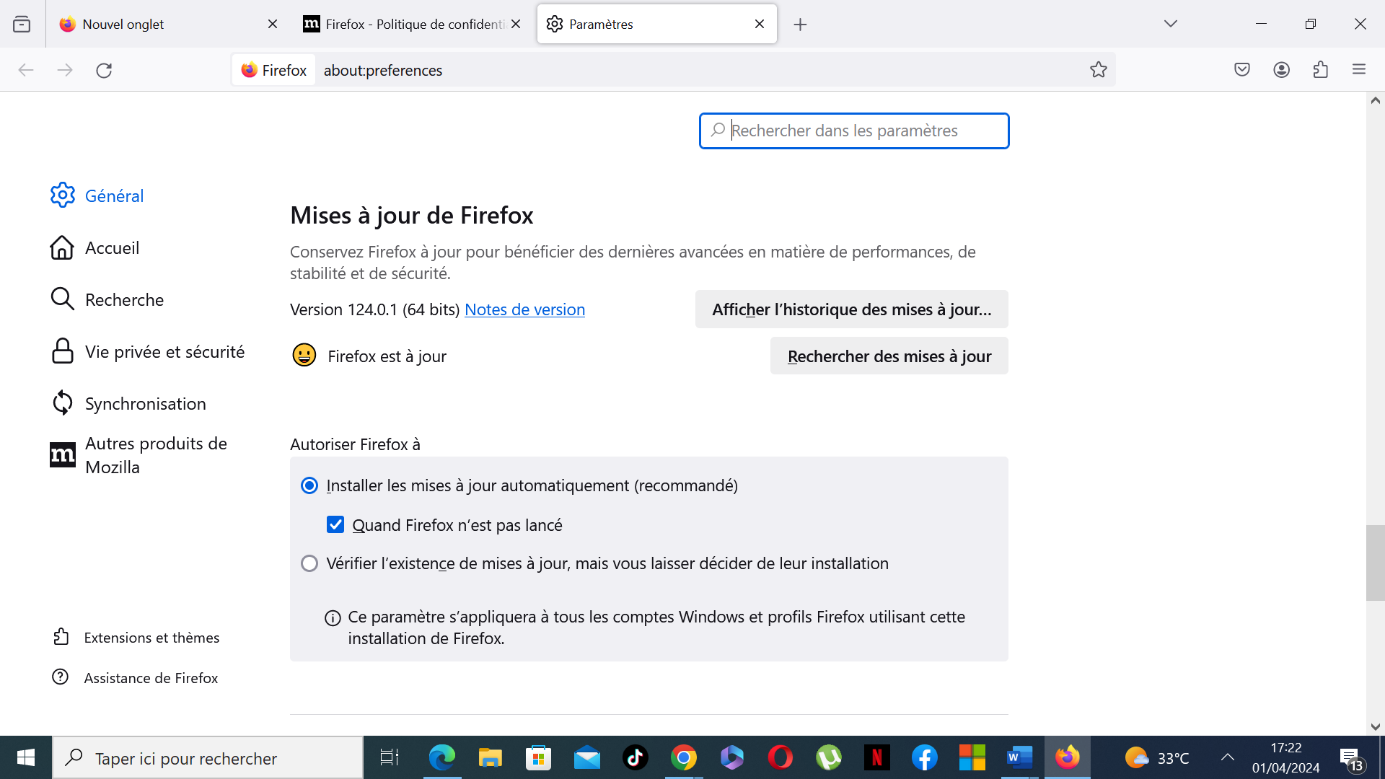
**Réponse 1**

Les sites web qui semblent être malveillants sont :

* www.morvel.com, un dérivé de www.marvel.com
* www.fessebook.com, un dérivé de www.facebook.com
* www.instagam.com, un dérivé de www.instagram.com

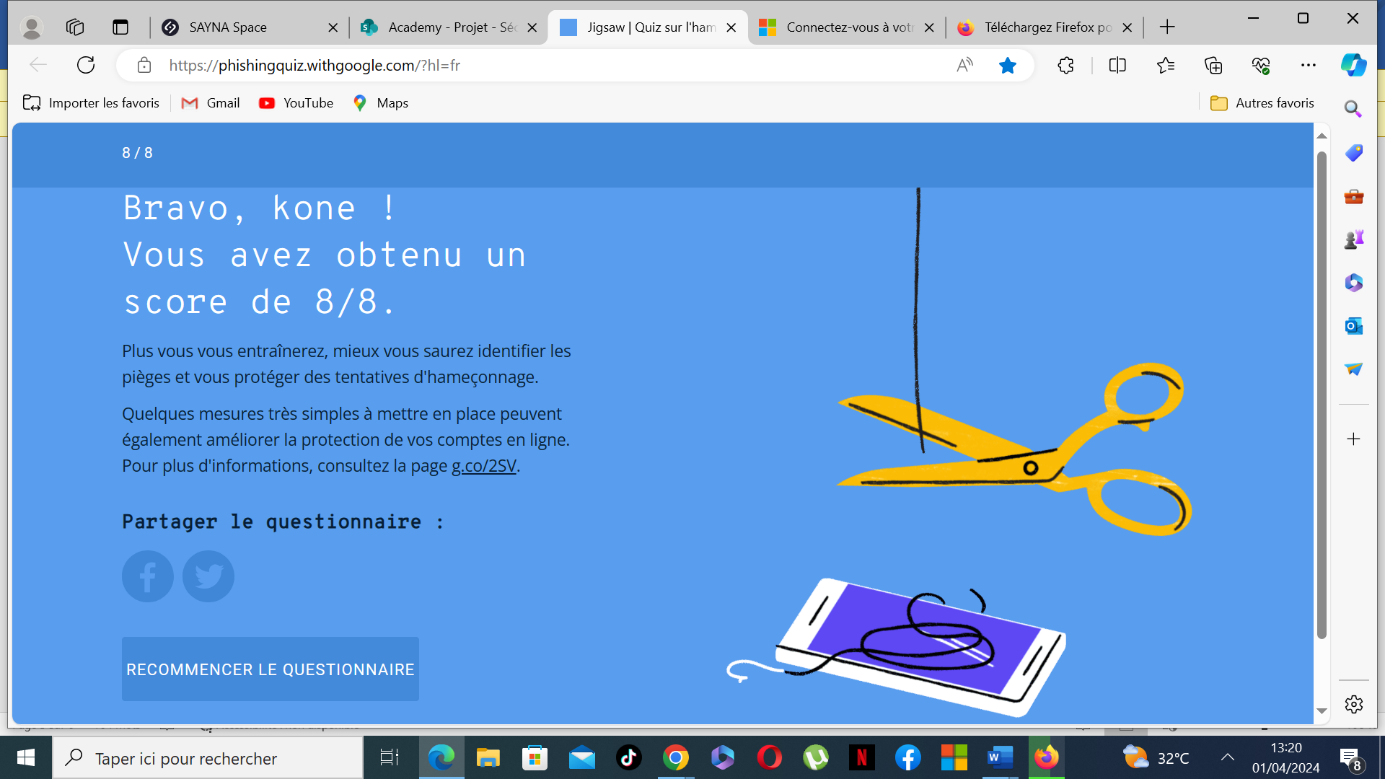
**2/ Vérifier si les navigateurs chrome et firefox sont à jour**

****

****

**4 - évite le spam et le pishing**

**1/ Capacité à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan**

****

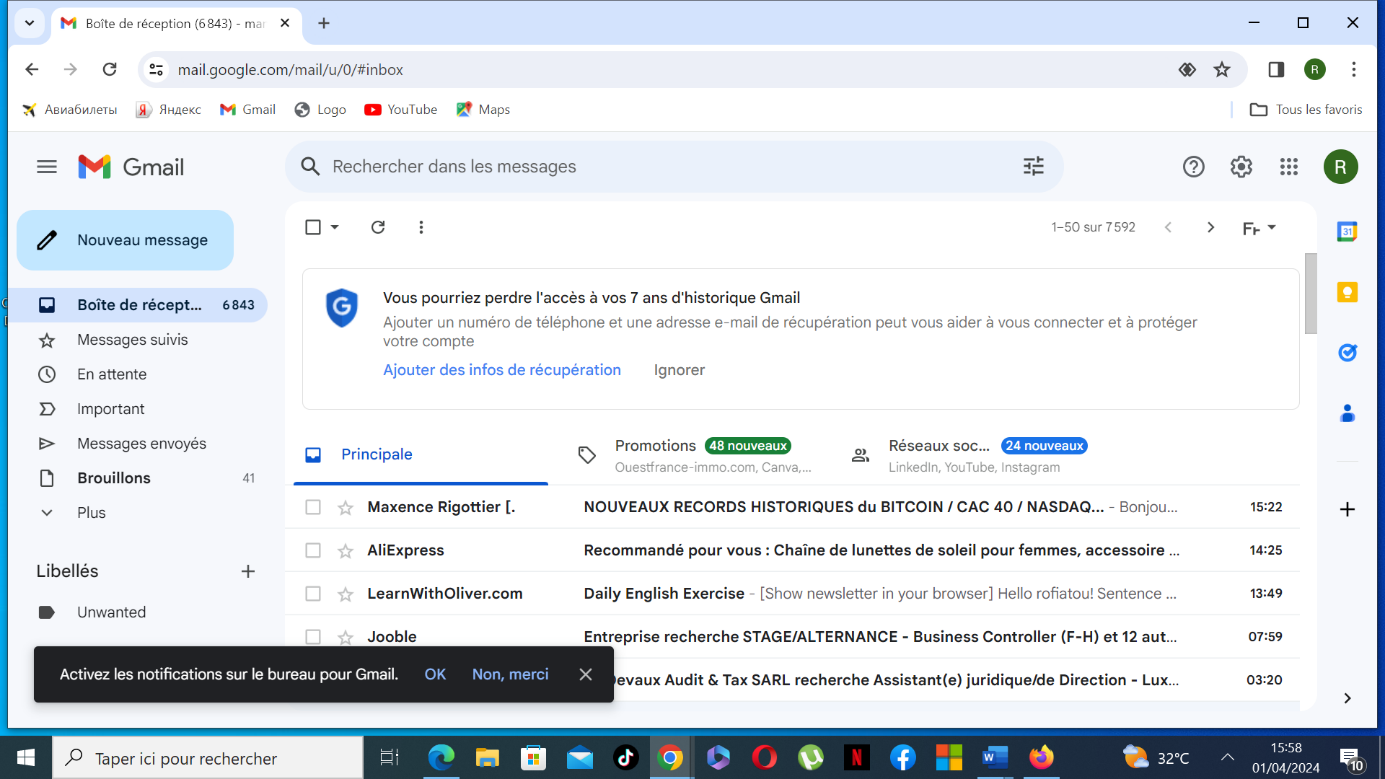
**5 – Comment éviter les logiciels malveillants**

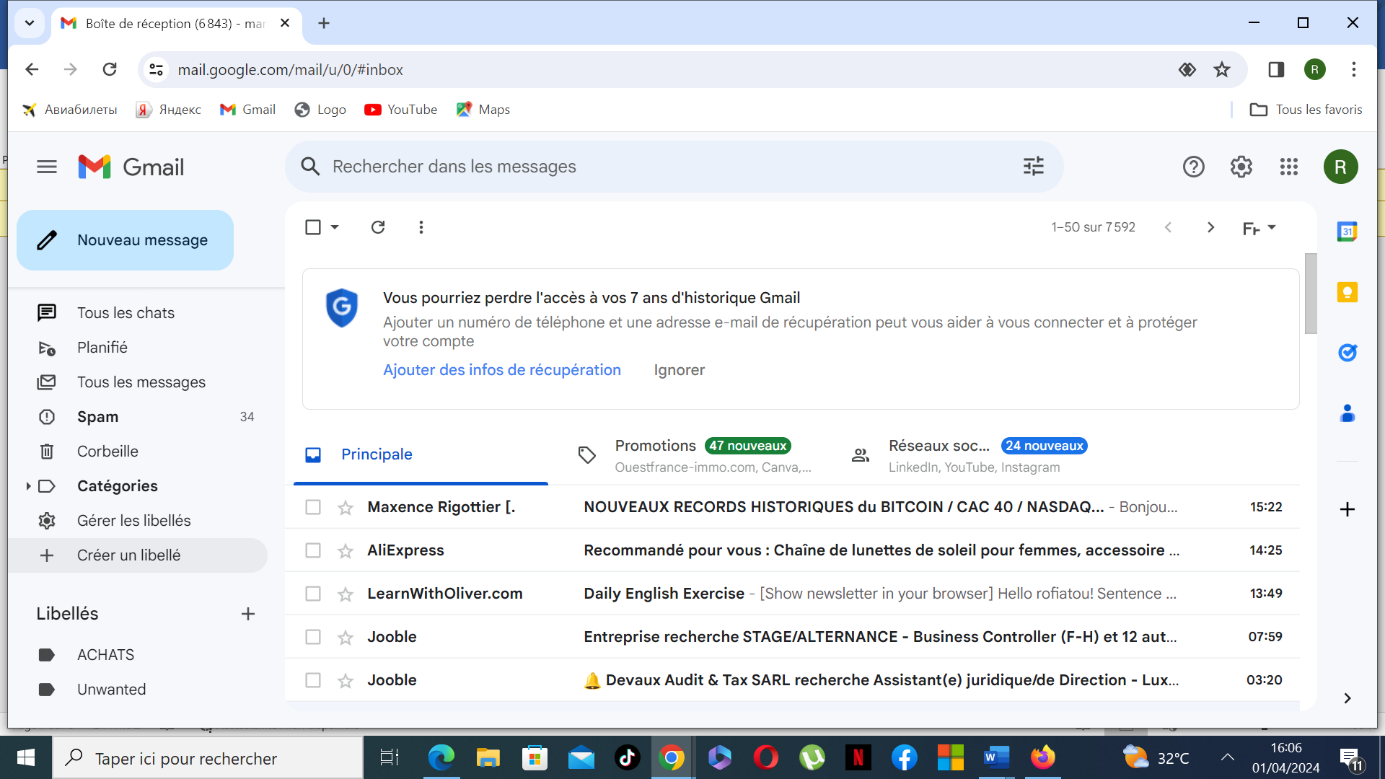
**3/ préciser l’indicateur de sécurité pour chaque site et le rapport d’analyse de l’outil google**

* 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

**6 – Achats en ligne sécurisés**

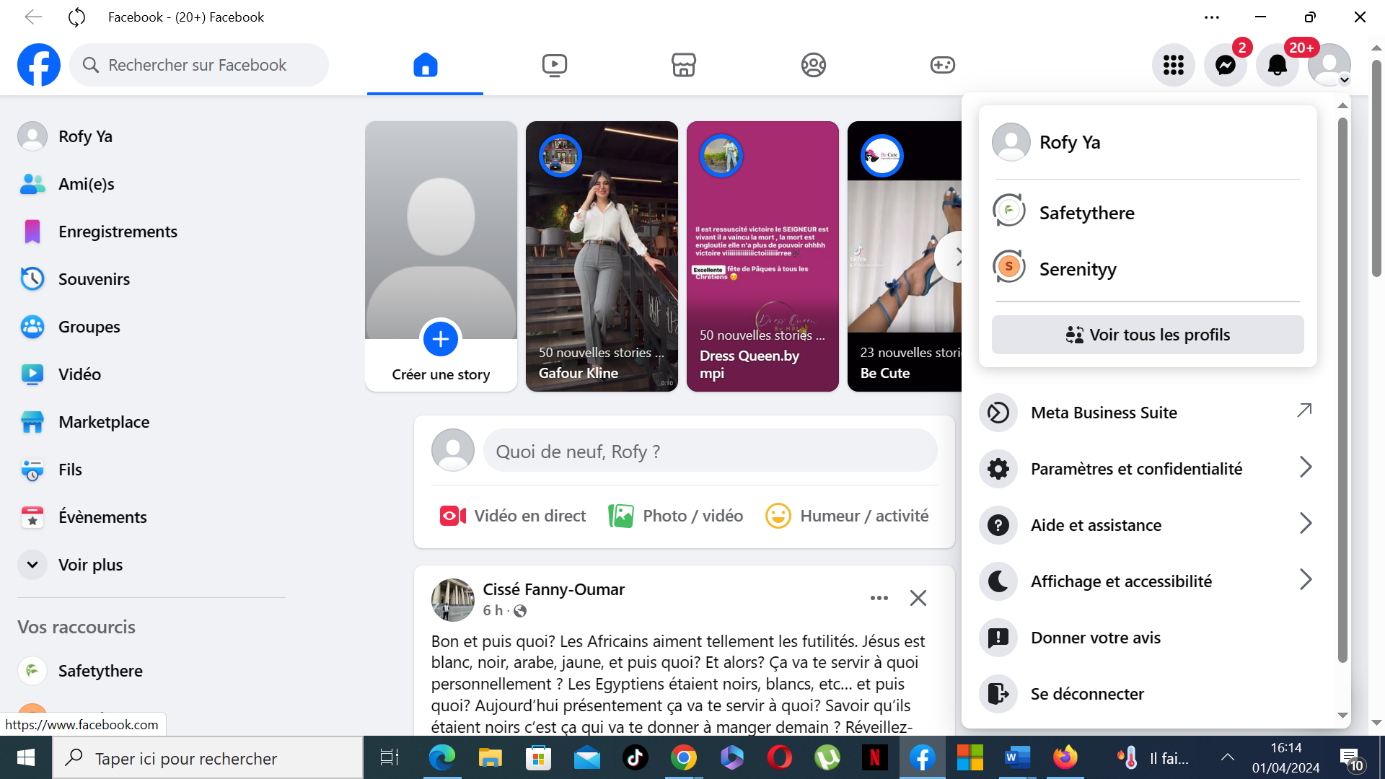
**1/Créer un registre des achats**

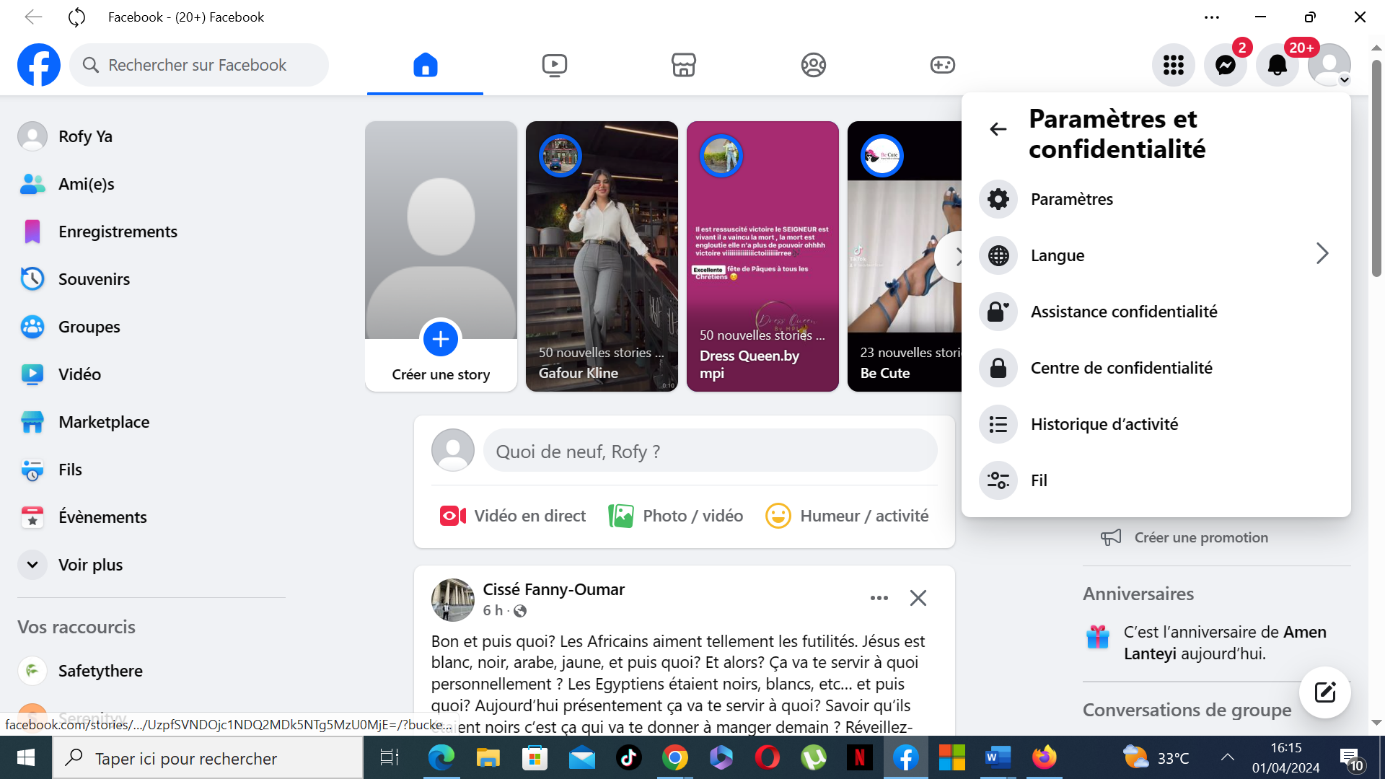


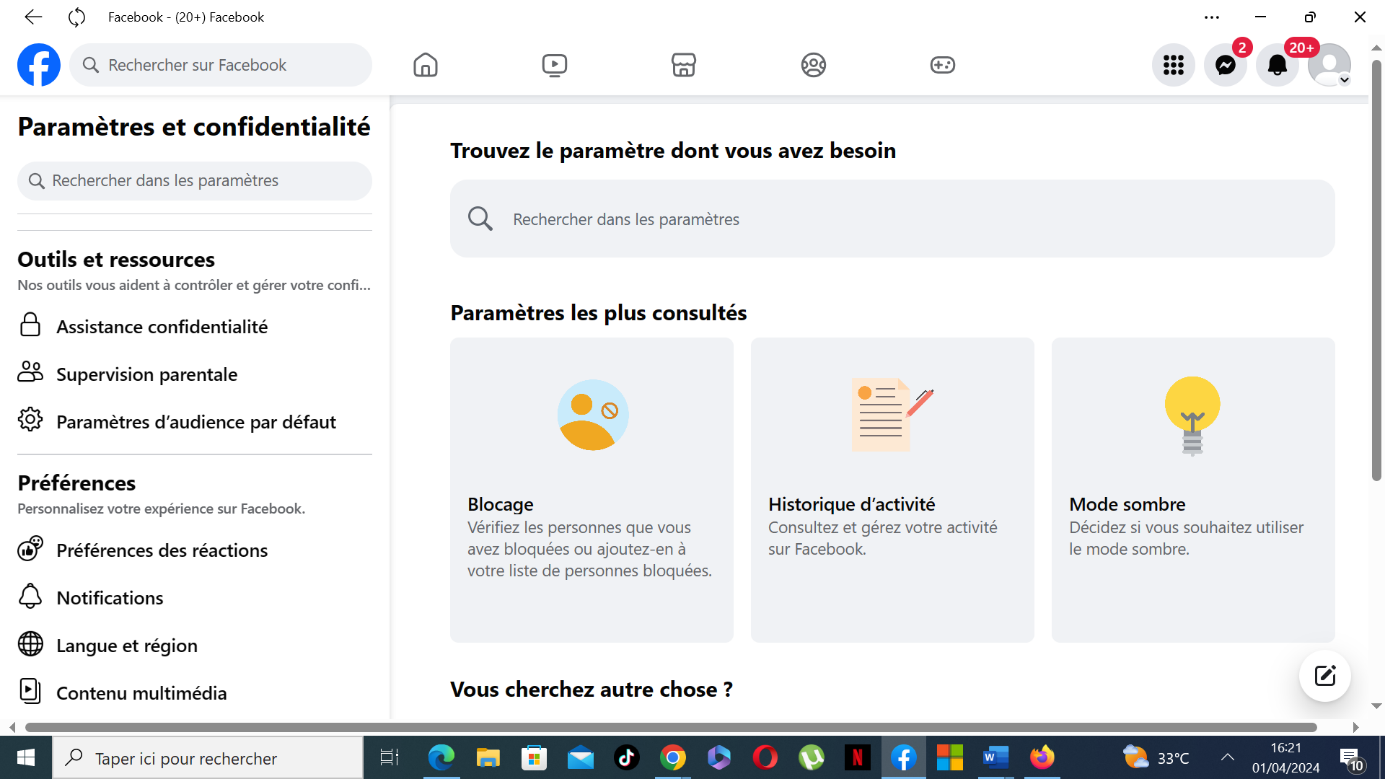


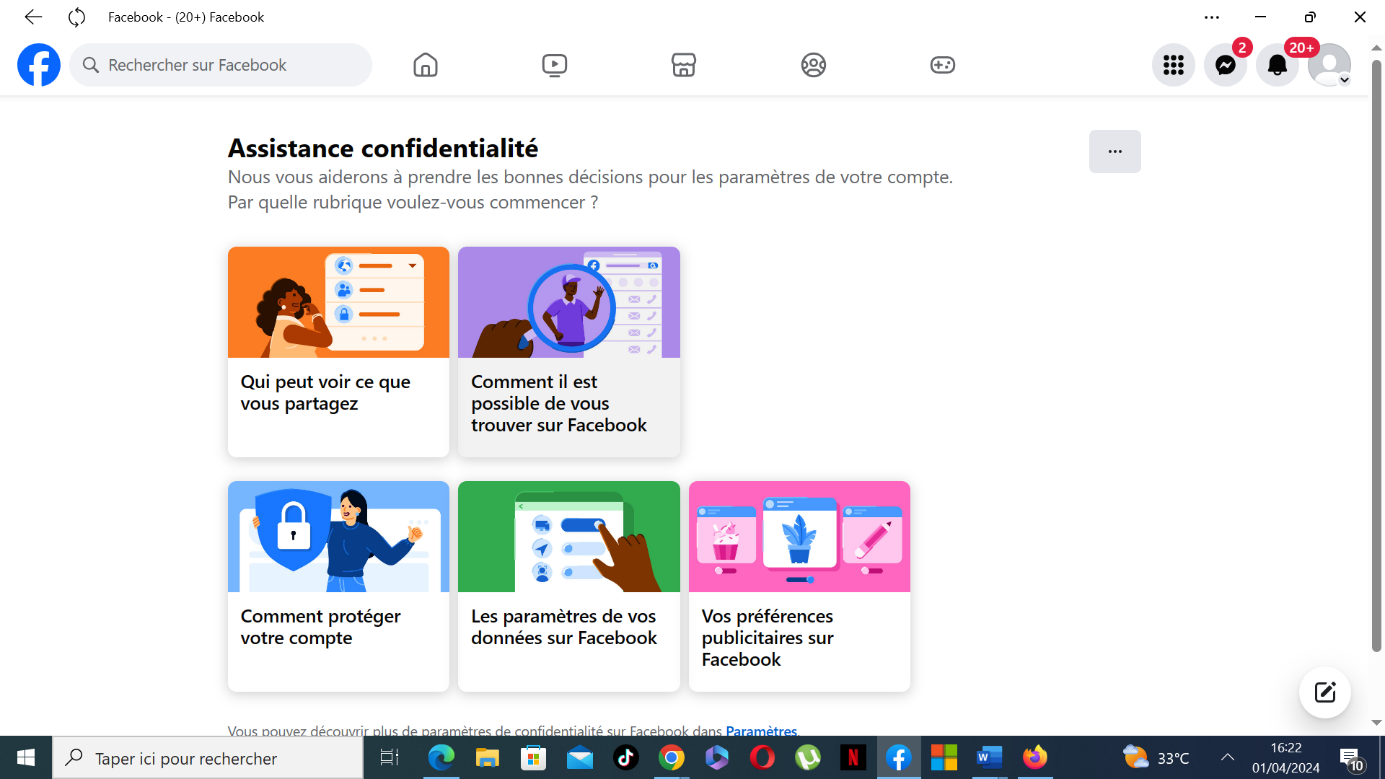
**7 - Comprendre le suivi du navigateur**

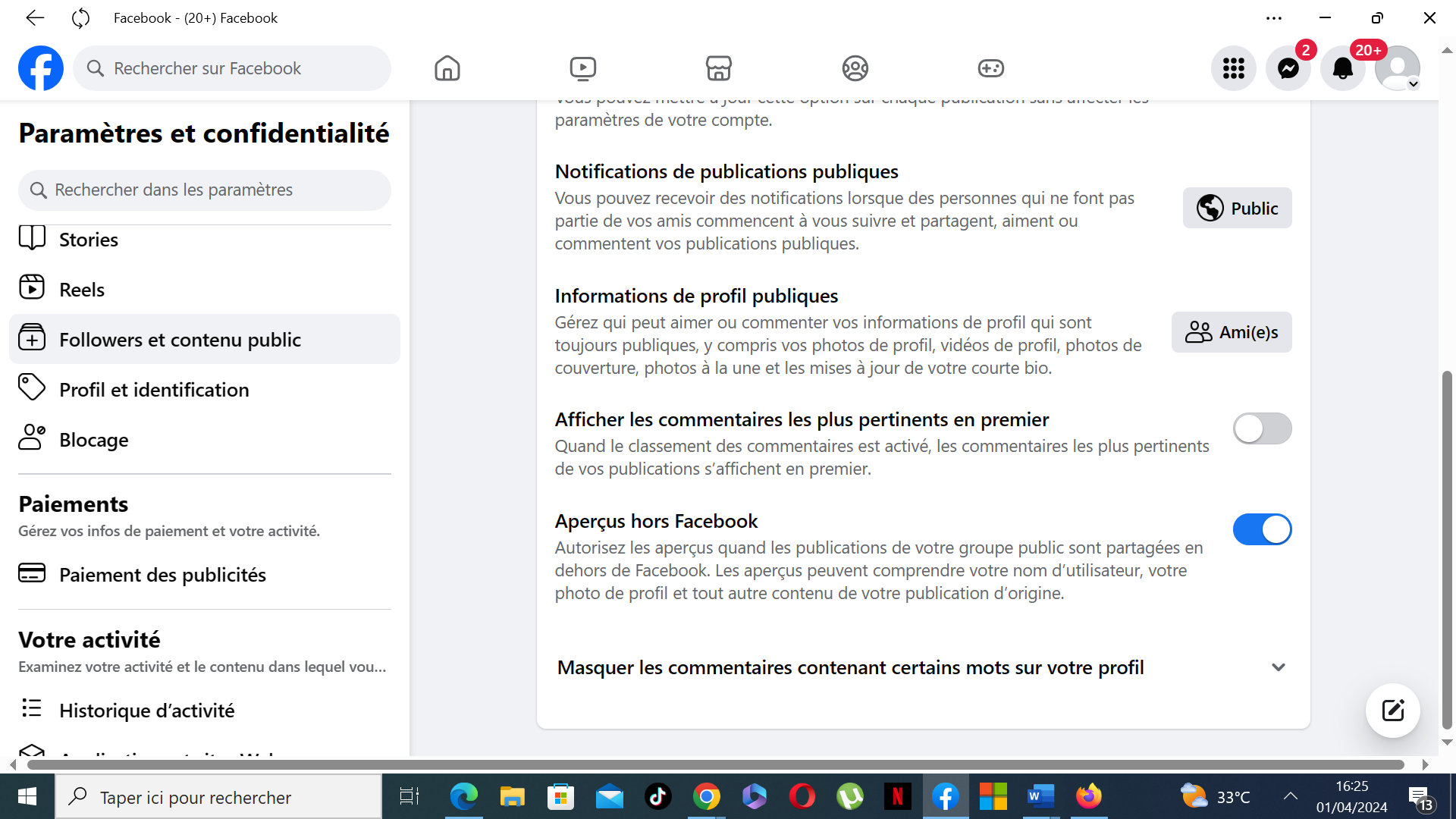
**8 – Principes de bases de la confidentialité des médias sociaux**

****

****

****

****

****

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

**1/ Proposer un ou plusieurs exercices pour vérifier la sécurité de votre ordinateur**

-Il faut vérifier les performances et l'intégrité de votre appareil dans Sécurité Windows

Dans la zone de recherche de la barre des tâches, il faut saisir Sécurité Windows, puis le sélectionner dans les résultats.

Ensuite, il faut sélectionner « Performances et intégrité de l'appareil pour afficher le rapport d'intégrité ».

Le Rapport d’intégrité commence en vous affichant la dernière fois qu’une analyse d’intégrité de l’appareil a été exécutée. L’heure affichée doit en principe être l’heure actuelle, car Sécurité Windows tente d’exécuter une analyse d’intégrité de l’appareil lorsque vous ouvrez la page « Performances et intégrité de l’appareil ».

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

- I l faut se procurer un antivirus. Certains antivirus populaires gratuits sont particulièrement efficaces pour protéger l’ordinateur contre les virus et les maliciels. Ils offrent des mises à jour constantes afin de vous protéger contre les virus et les maliciels les plus récents. Avira est gratuit et très bon, il en existe d'autres gratuits et efficaces.

Il faut télécharger l’antivirus depuis le site officiel du programme et choisir un programme reconnu, qu'il soit gratuit ou payant.

Sur Windows 8 et 10, il y a Windows Defender, un antimalware gratuit fourni par Microsoft.

Ensuite il faut installer l’antivirus. Il faut être connecté à internet pour télécharger et installer le programme et les actualisations récentes. Avant d'installer l’antivirus sur l’ordinateur, il faut fermer tous les programmes qui sont en cours d'exécution.

Certains antivirus gratuits qu’on télécharge offrent l'option d'installer une barre d'outils dans votre moteur de recherche. Ceci peut quelquefois vous apporter une meilleure protection, mais peut également altérer nos préférences et si on a une machine un peu ancienne, cela peut nous poser des problèmes. Durant l'installation de l'antivirus, on a la possibilité d'accepter ou non.

En outre, il faut mettre l'antivirus à jour. Après avoir installé notre antivirus, il faut installer les dernières mises à jour. L'antivirus ne contient généralement pas les dernières mises à jour. S'il ne le fait pas automatiquement, le programme nous suggère généralement d'installer les mises à jour récentes, il faut acceptez ou cliquez sur l'option « mise à jour » pour se connecter au serveur du programme. La plupart des antivirus ont une icône dans la barre des taches (en bas à droite de l'écran) sur laquelle on peut cliquer avec le bouton droit de la souris afin d'ouvrir un petit menu offrant différentes actions possibles, entre autres la mise à jour.

Les antivirus ont généralement l'option « mise à jour automatique » présélectionnée. Il faut vérifier si c'est le cas en se rendant dans le menu « options » de notre antivirus. Si on ne souhaite pas activer la mise à jour automatique, il faut faire les mises à jour manuellement au moins une fois par semaine.

Par ailleurs, il faut planifier les analyses automatiques. Il est préférable de programmer l'antivirus pour qu'il effectue automatiquement des analyses de l’ordinateur. Il faut chercher l'option « configurer l'antivirus » et programmer le logiciel afin qu'il réalise des analyses automatiques à un moment de la journée ou de la nuit durant lequel on n'utilise pas l'ordinateur. Une analyse hebdomadaire est suffisante pour une utilisation normale. Si on télécharge de nombreux fichiers et programmes ou si on va sur des sites internet à risques, il faut programmer des analyses plus fréquentes.

Et il faut télécharger les mises à jour de Windows régulièrement. Windows offre des mises à jour de sécurité constantes. Certaines de ces mises à jour sont destinées à renforcer la sécurité de notre système en corrigeant des vulnérabilités exploitables du programme. Si on fait les mises à jour de Windows avec régularité, notre ordinateur est mieux protégé.