1 - Introduction à la sécurité sur Internet

1/ trois articles sur la sécurité sur internet

● Article 1 : Breizh-info - Sécurité internet : ces logiciels qui protègent votre réseau

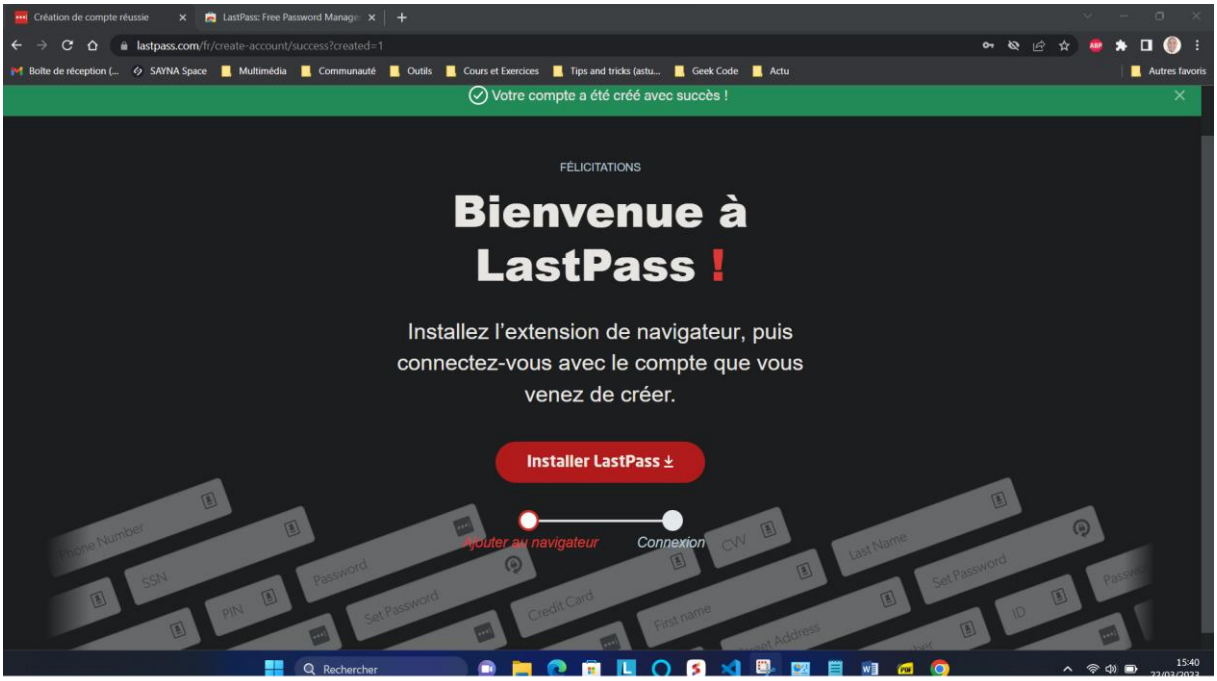
● Article 2 : Datagroup - Cyberattaque : 9 bonnes pratiques pour l'éviter

● Article 3 : Axido - Comment se protéger du piratage informatique ?

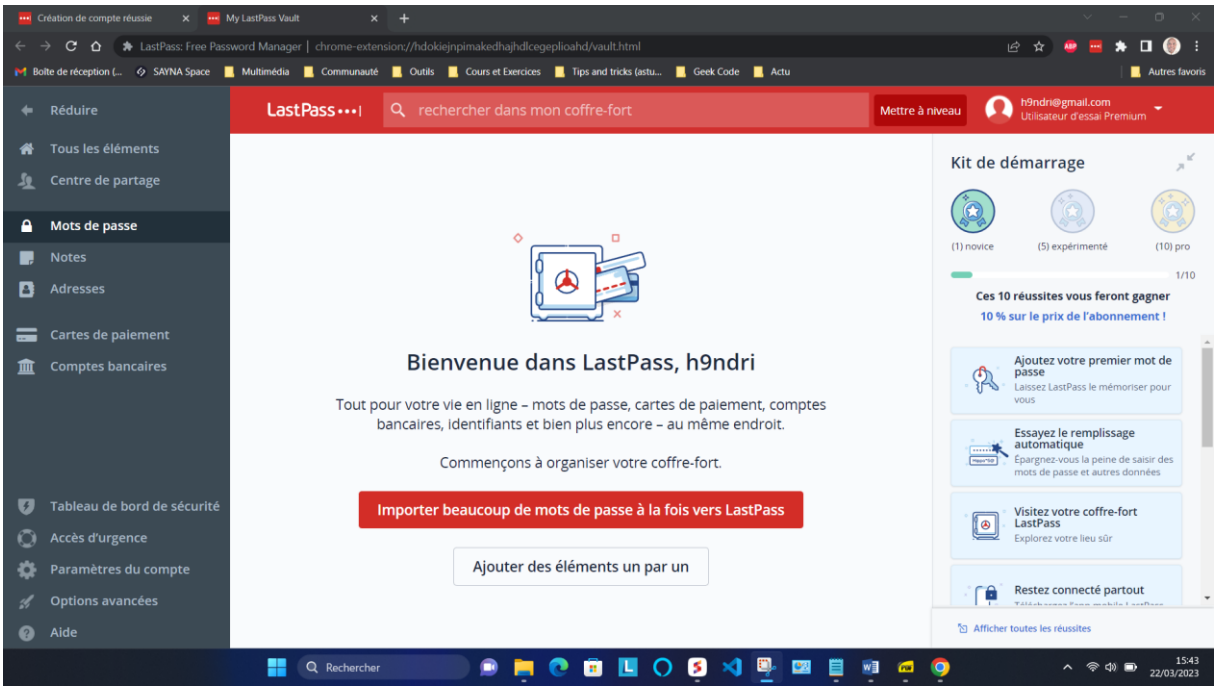
2 - Créer des mots de passe forts

1/

● Création d'un compte Lastpass



● Installation Lastpass sur Chrome



3 - Fonctionnalité de sécurité de votre navigateur

1/ Cocher les sites web qui semble être malveillants

● www.morvel.com ☒

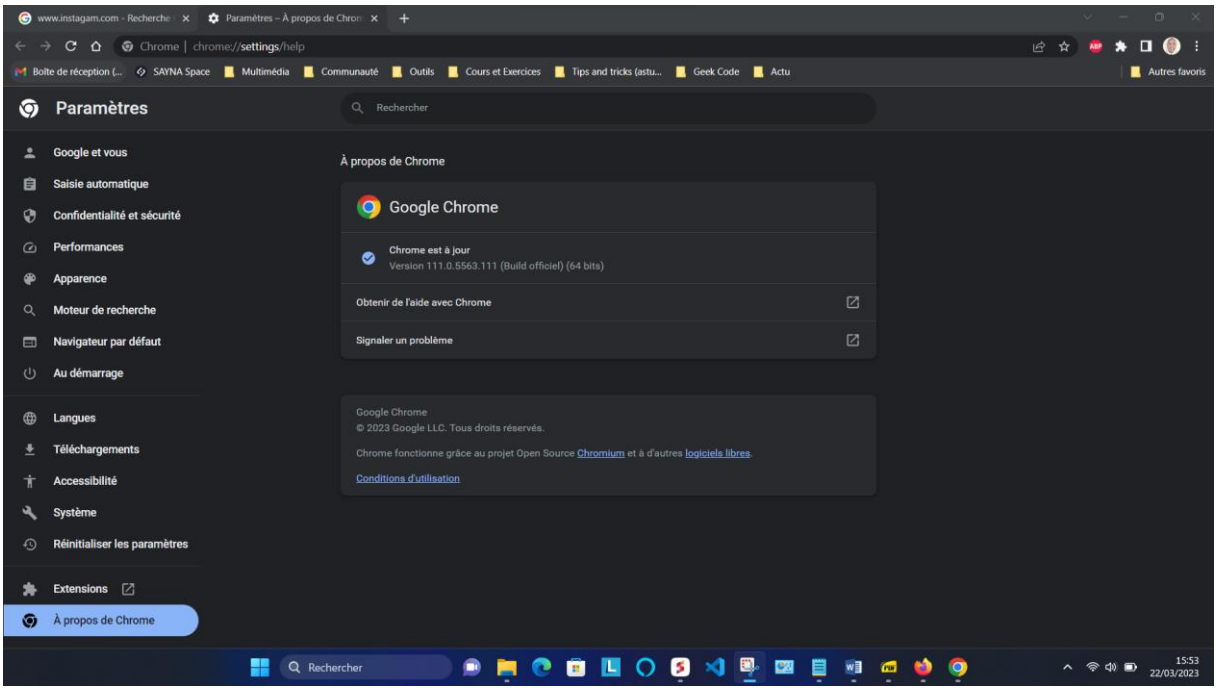
● www.dccomics.com

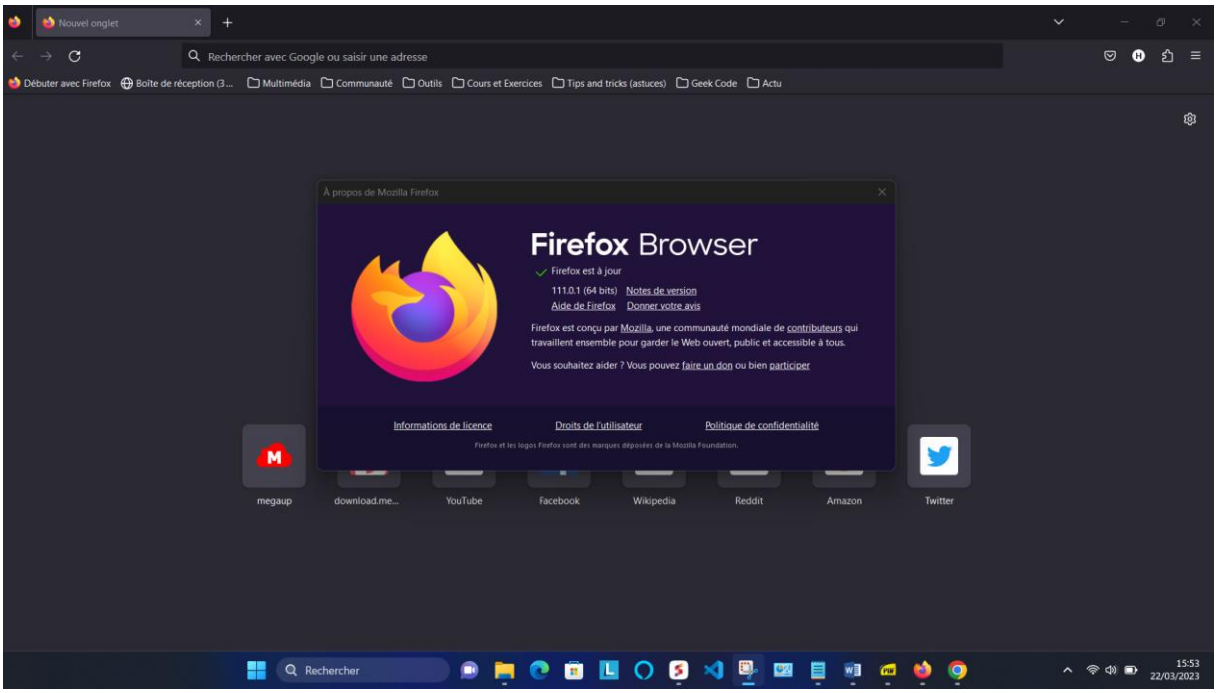
● www.ironman.com

● www.fessebook.com☒

● www.instagam.com☒

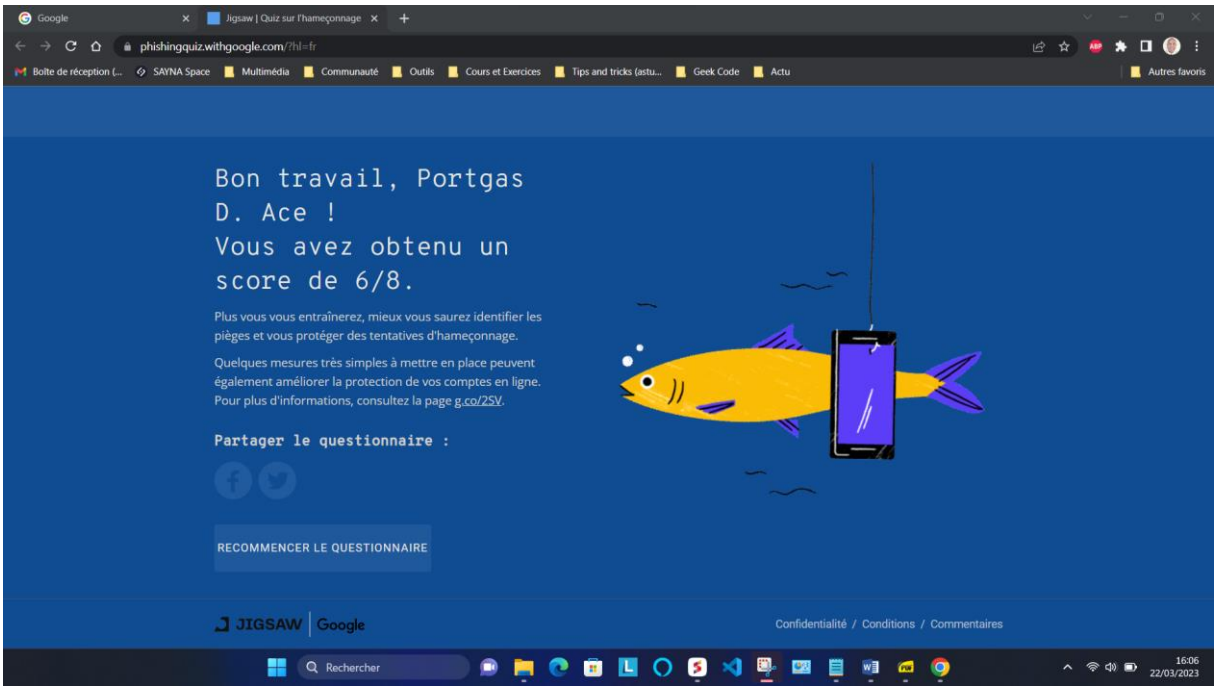
2/ Vérification des mises à jour des navigateurs Chrome et Firefox





4 - Éviter le spam et le phishing

1/ Quiz pour vérification des spams et phishing



5 - Comment éviter les logiciels malveillants

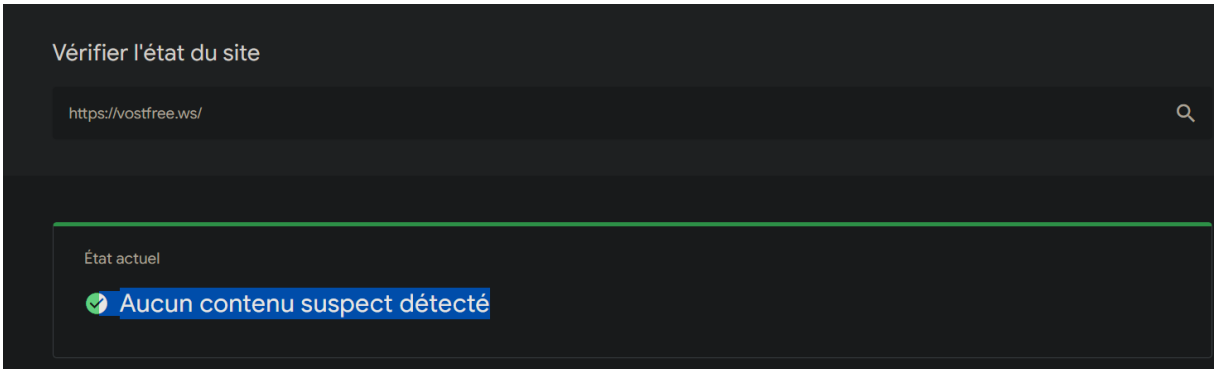
3/ Vérification des sites sur Google Transparence des informations

Site 1 : https://vostfree.ws/

○ Indicateur de sécurité

■ HTTPS 🔒

○ Analyse Google

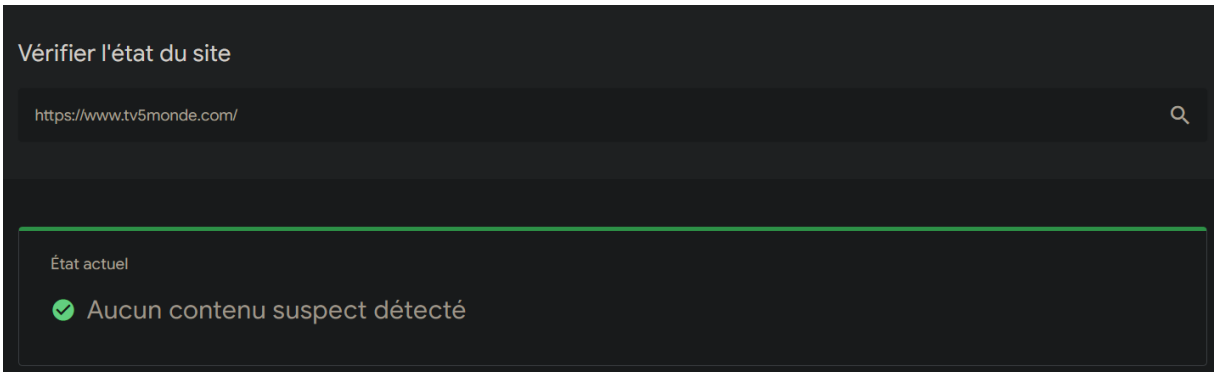


Site 2 : https://www.tv5monde.com/

○ Indicateur de sécurité

■ HTTPS 🔒

○ Analyse Google



Site 3 : http://www.baidu.com/

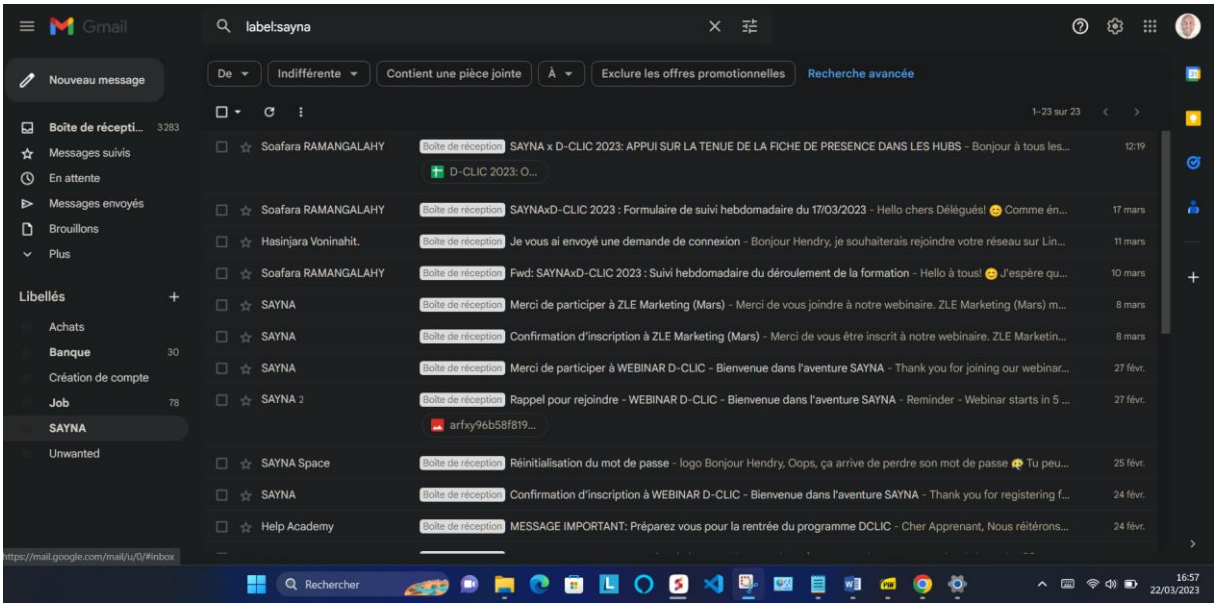
○ Indicateur de sécurité

■ Non sécurisé

○ Analyse Google

6 - Achats en ligne sécurisés

1/ Création et organisation de plusieurs libellés sur Gmail

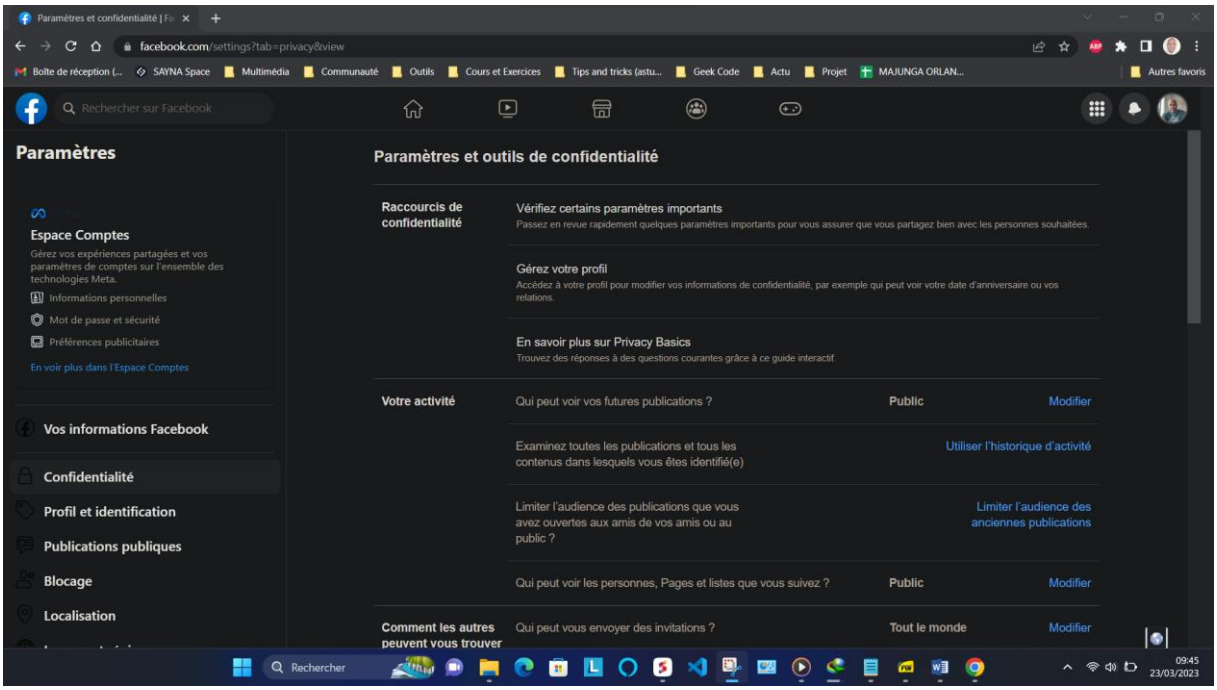


7 - Comprendre le suivi du navigateur

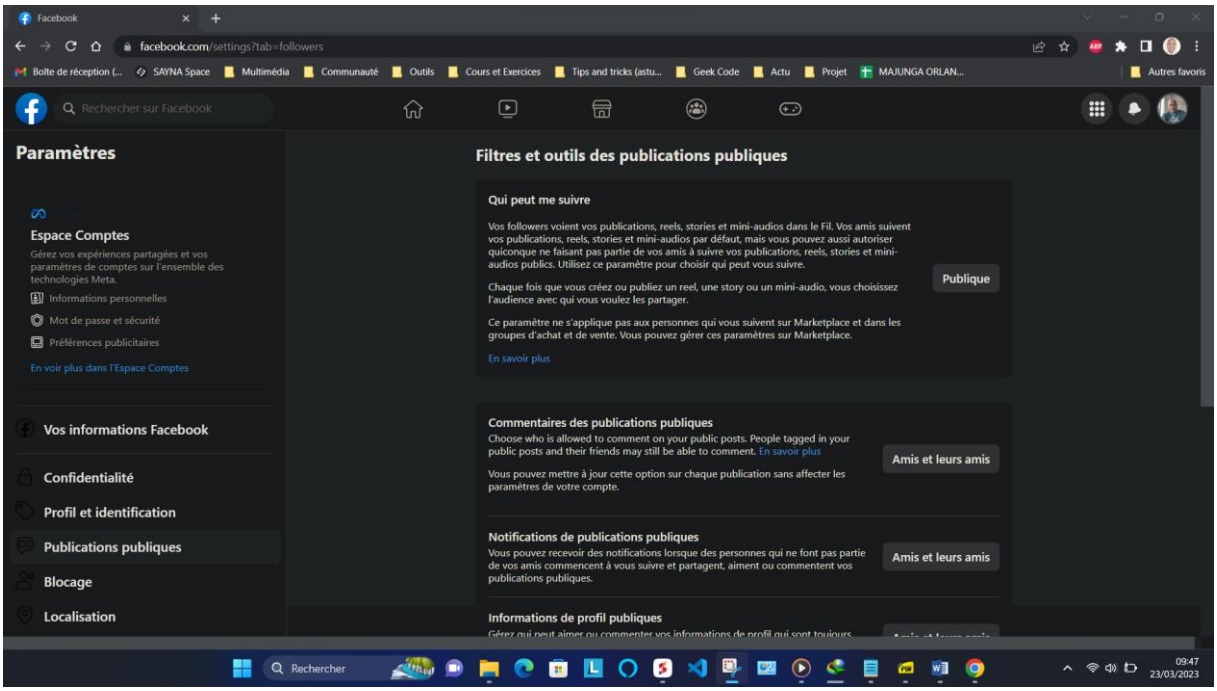
Exercice sur la gestion des cookies et l'utilisation de la navigation privée☒

8 - Principes de base de la confidentialité des médias sociaux

1/ Réglage des paramètres de confidentialité de Facebook



● Publications publiques



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

1/ Pour vérifier la sécurité d'un ordinateur

Windows	MacOs	Linux
1. Mettre l'ordinateur hors connexion internet 2. Exécuter Microsoft Defender hors connexion 3. Supprimer manuellement le logiciel de sécurité non fiable 4. Utilisez la Scanner de sécurité Microsoft gratuite 5. Installer les dernières mises à jour de Microsoft Update 6. Vérifier que le pare-feu Windows est activé	1. Mettre à jour votre système d'exploitation et les différents programmes utilisés 2. Sauvegarder le contenu de votre Mac sur un disque externe via Time Machine 3. N'installer que des logiciels provenant d'App Store 4. Installer des programmes comme Bitdefender Virus Scanner (gratuit), MacAfee ou encore Kaspersky (payant) pour scanner le contenu des disques dure	1. Effectuer une analyse de sécurité sur votre ordinateur Linux avec Lynis[1]

Il faut noter que MacOs est un système d'exploitation beaucoup moins propice aux attaques virales que Windows. Et donc ces exercices sont davantage de la prévention pour l'utilisateur MacOs.

Egalement, Linux a pendant longtemps été considéré comme le système d'exploitation le plus sécurisé sur le marché.

2/ Installation et utilisation d'un antivirus + antimalware sur un ordinateur

Système d'exploitation	Windows	MacOs	Linux
Exemple d'antivirus + antimalware	Avast Software Symantec Bitdefender Kaspersky Lab. McAfee Microsoft Corporation	Bitdefender Intego Norton McAfee AVG Avast	AntiVir for Linux AVG Bitdefender Linux Edition McAfee Avast

[1] Lynis exécute une série de tests automatisés qui vérifient minutieusement de nombreux composants système et paramètres de votre système d'exploitation Linux. Il présente ses conclusions dans un rapport ASCII codé par couleur sous la forme d'une liste d'avertissements, de suggestions et d'actions à plusieurs niveaux à entreprendre.

	ESET		
Installation	Rechercher un antivirus de confiance qui convient à vos besoins et télécharger le à partir du site Web du fournisseur d'antivirus. Une fois le fichier d'installation téléchargé, double-cliquez dessus pour lancer le processus d'installation. Suivre les instructions à l'écran pour installer l'antivirus sur votre ordinateur. Si l'antivirus demande un redémarrage de l'ordinateur après l'installation, faites-le.	Rechercher un antivirus de confiance qui convient à vos besoins et télécharger le à partir du site Web du fournisseur d'antivirus. Une fois le fichier d'installation téléchargé, double-cliquez dessus pour monter l'image disque de l'antivirus. Ouvrir le fichier .pkg contenu dans l'image disque en double-cliquant dessus. Suivre les instructions à l'écran pour installer l'antivirus sur votre ordinateur. Si l'antivirus demande un redémarrage de l'ordinateur après l'installation, faites-le.	Installer Clamav par ligne de commande. Trouver Clam sur votre pc. Sélectionner les fichiers à installer. Pour accéder à votre logiciel d'antivirus, Dans l'onglet « Applications », cliquez sur « Accessoires », puis « Scanner de Virus ».
Utilisation	S'assurer que l'antivirus est configuré pour s'exécuter au démarrage de votre ordinateur. De cette façon, il sera actif dès que vous allumez votre ordinateur. Mettre à jour régulièrement l'antivirus pour vous assurer qu'il est à jour avec les dernières définitions de virus. Exécuter régulièrement des analyses complètes de votre système pour détecter et supprimer les virus, les logiciels malveillants et autres menaces potentielles.	S'assurer que l'antivirus est configuré pour s'exécuter au démarrage de votre ordinateur. De cette façon, il sera actif dès que vous allumez votre ordinateur. Mettre à jour régulièrement l'antivirus pour vous assurer qu'il est à jour avec les dernières définitions de virus. Exécuter régulièrement des analyses complètes de votre système pour détecter et supprimer les virus, les logiciels malveillants et autres menaces potentielles.	Mettre à jour Clam. Renseigner votre antivirus sur les fichiers à scanner. Dans le barre de menu, cliquez sur « Avancé » puis sur « Préférences ».