

Module : Naviguer en toute sécurité

1 - Introduction à la sécurité sur Internet

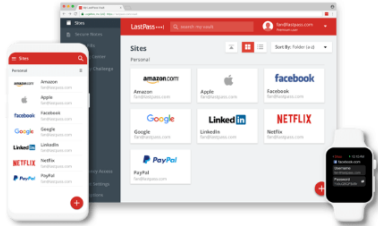
1/

- Article 1 = cyber malveillance gouv fr - Black Friday, fêtes de fin d'année : 7 conseils pour éviter les cyber-arnaques
- Article 2 = kaspersky- Sécurité Internet : Qu'est-ce que c'est et comment vous protéger en ligne ?
- Article 3 = youth.europa.eu - La sécurité sur internet

2 - Créer des mots de passe forts

Un mot de passe.
Zéro souci.

LastPass s'occupe du reste.



Fonctionnalités Free

Créer un compte

ou Connexion

Adresse e-mail

Mot de passe maître

Confirmer votre mot de passe Maître

Indice (facultatif)

Inscrivez-vous - c'est gratuit

En remplissant ce formulaire, j'accepte les [Conditions générales](#) et la [Politique de confidentialité](#). Je souhaite recevoir des e-mails

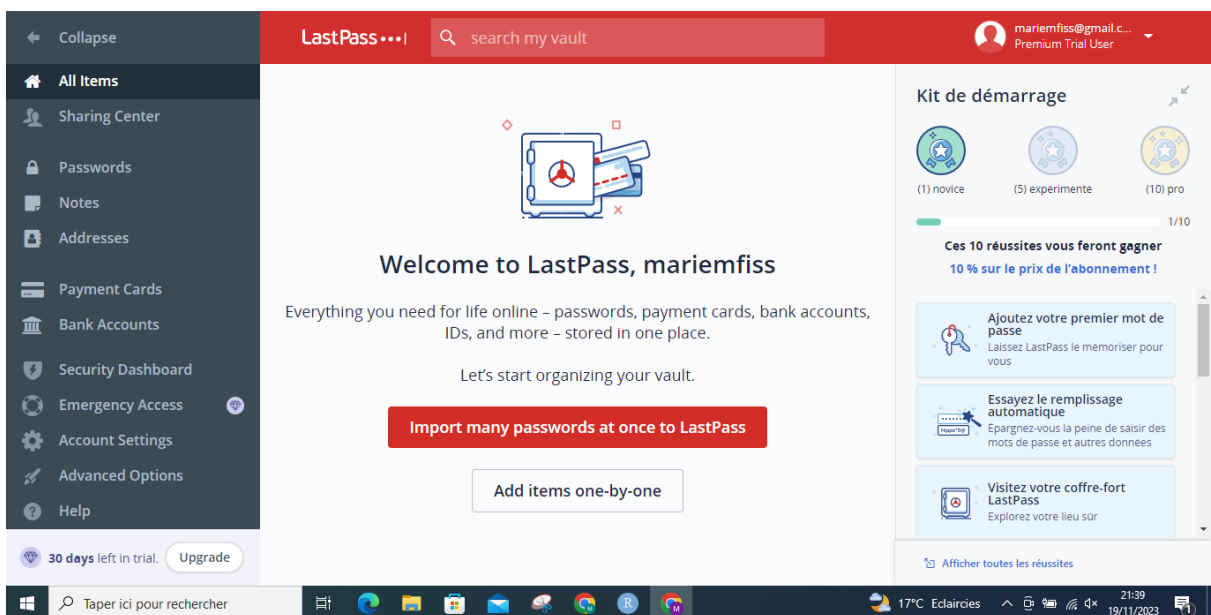
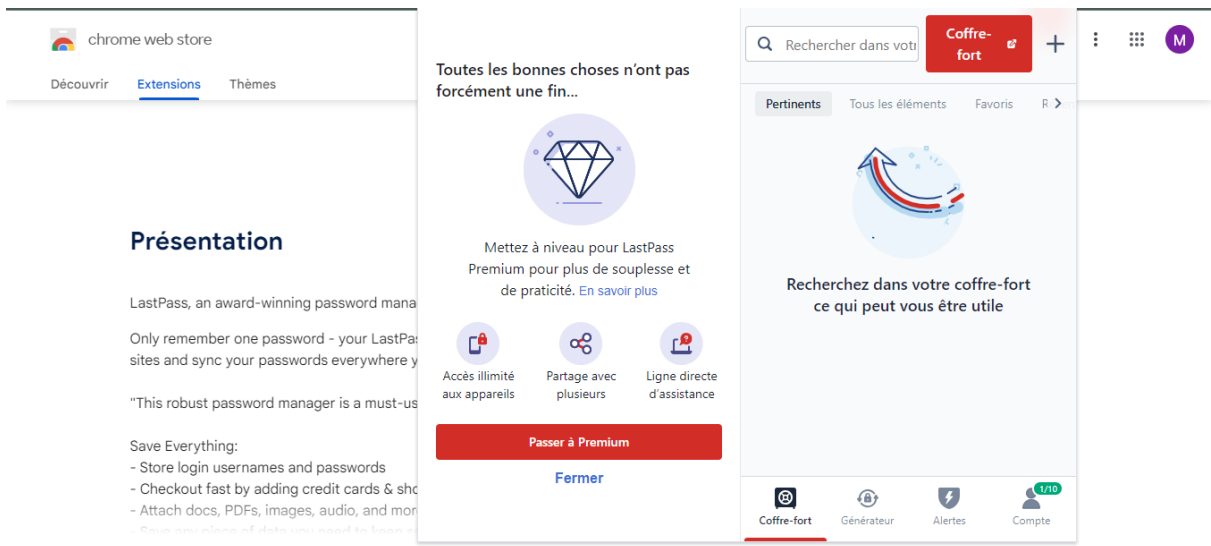
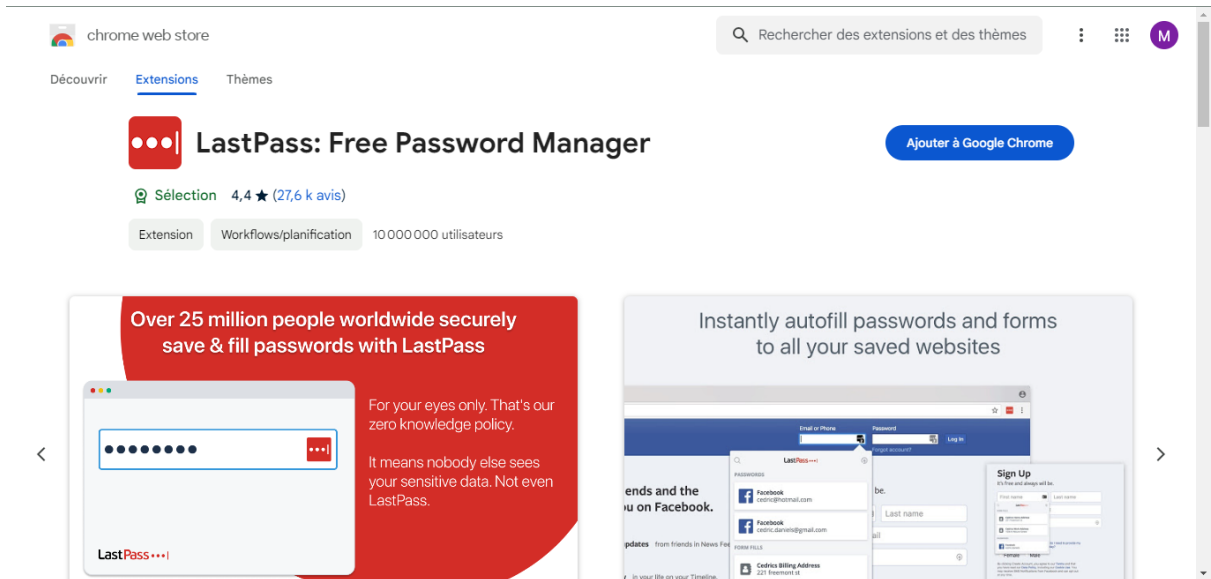
Votre compte a été créé avec succès !

FÉLICITATIONS

Bienvenue à
LastPass !

Installez l'extension de navigateur, puis connectez-vous avec le compte que vous venez de créer.

Ce site utilise des cookies et autres technologies pour entre autres l'exploitation du site, des analyses, pour améliorer l'interaction avec les utilisateurs ou pour de la publicité. Pour en savoir plus sur notre utilisation des cookies, consultez notre [Politique de confidentialité](#). Vous pouvez choisir d'y consentir ou de refuser l'utilisation et le partage de cookies et technologies comparables.

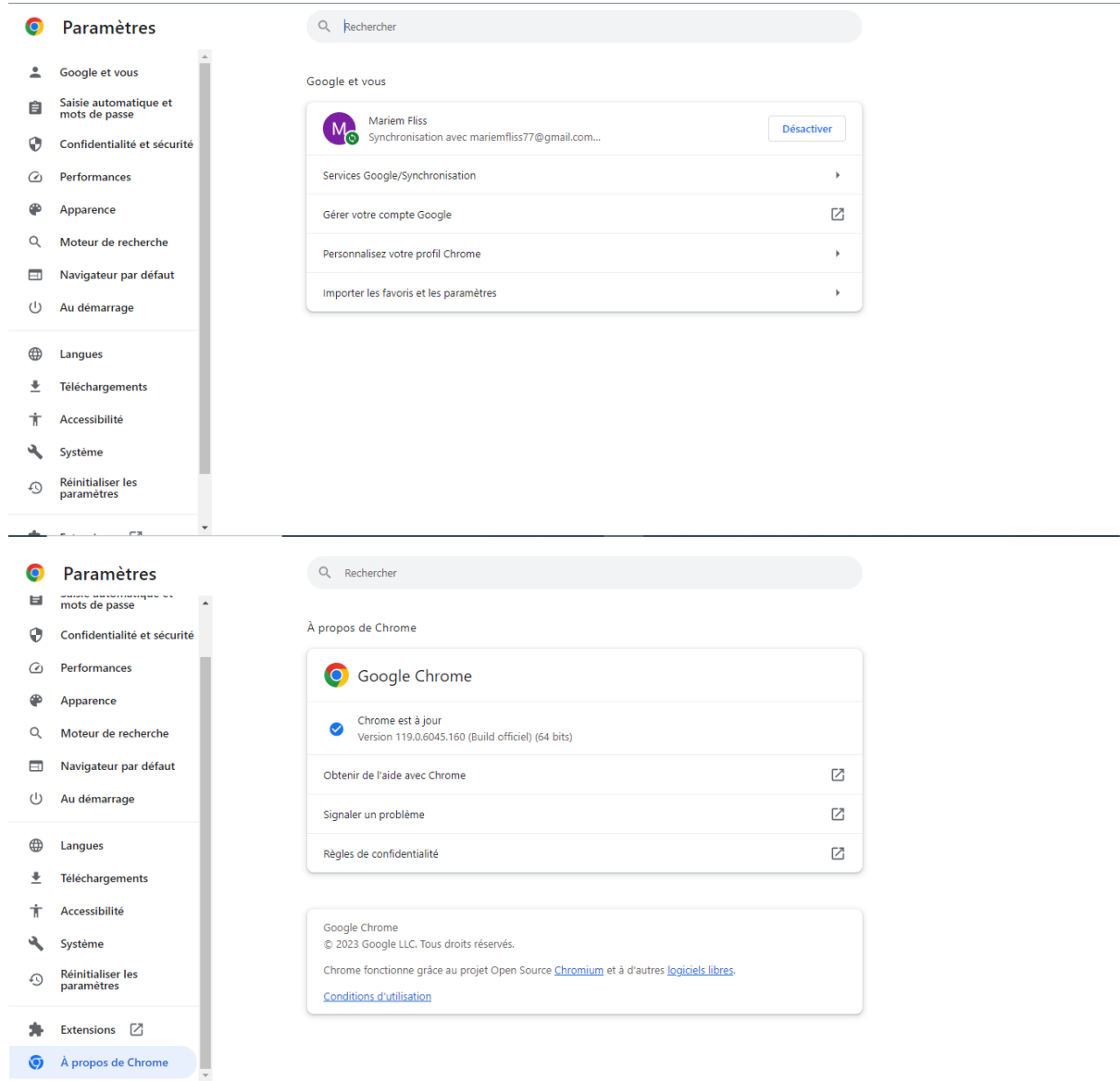


3 - Fonctionnalité de sécurité de votre navigateur :

1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants. (case à cocher)

- www.marvel.com -> marvel
- www.dccomics.com
- www.ironman.com
- www.fessebook.com ->facebook
- www.instagram.com->instagram

2/



4 - Éviter le spam et le phishing :

1/

8 / 8

Bon travail, Mariem
FLISS !
Vous avez obtenu un
score de 7/8.

Plus vous vous entraînez, mieux vous saurez identifier les
pièges et vous protégerez des tentatives d'hameçonnage.
Quelques mesures très simples à mettre en place peuvent
également améliorer la protection de vos comptes en ligne.
Pour plus d'informations, consultez la page g.co/2SV.

Partager le questionnaire :

RECOMMENCER LE QUESTIONNAIRE

Confidentialité / Conditions / Commentaires

5 - Comment éviter les logiciels malveillants :

- Site n°1:

État du site selon la navigation sécurisée

Grâce à la fonctionnalité de navigation sécurisée offerte par Google, des milliards d'URL sont analysées chaque jour afin de détecter les sites Web suspects. Nous découvrons ainsi des milliers de nouveaux sites douteux tous les jours, parmi lesquels figurent de nombreux sites Web légitimes ayant été infectés. Nous signalons ensuite ces sites par des avertissements dans la recherche Google et dans les navigateurs Web. Vous pouvez effectuer une recherche pour savoir si un site Web en particulier présente un danger.

Vérifier l'état du site

<https://henoo.fr/blog/10-meilleures-destination-europe-voyager-seul-2022/&hl=fr>

État actuel

✓ **Aucun contenu suspect détecté**

- Site n°2:

Grâce à la fonctionnalité de navigation sécurisée offerte par Google, des milliards d'URL sont analysées chaque jour afin de détecter les sites Web suspects. Nous découvrons ainsi des milliers de nouveaux sites douteux tous les jours, parmi lesquels figurent de nombreux sites Web légitimes ayant été infectés. Nous signalons ensuite ces sites par des avertissements dans la recherche Google et dans les navigateurs Web. Vous pouvez effectuer une recherche pour savoir si un site Web en particulier présente un danger.

Vérifier l'état du site

<https://www.kaggle.com/code/mariemfliss/notebookOf74f71f15/edit>

État actuel

Aucune donnée disponible

- Site n°3:

Vérifier l'état du site

<https://console.firebase.google.com/u/0/project/gestion-parc-info-3ff6f/overview?hl=fr&pli=1>

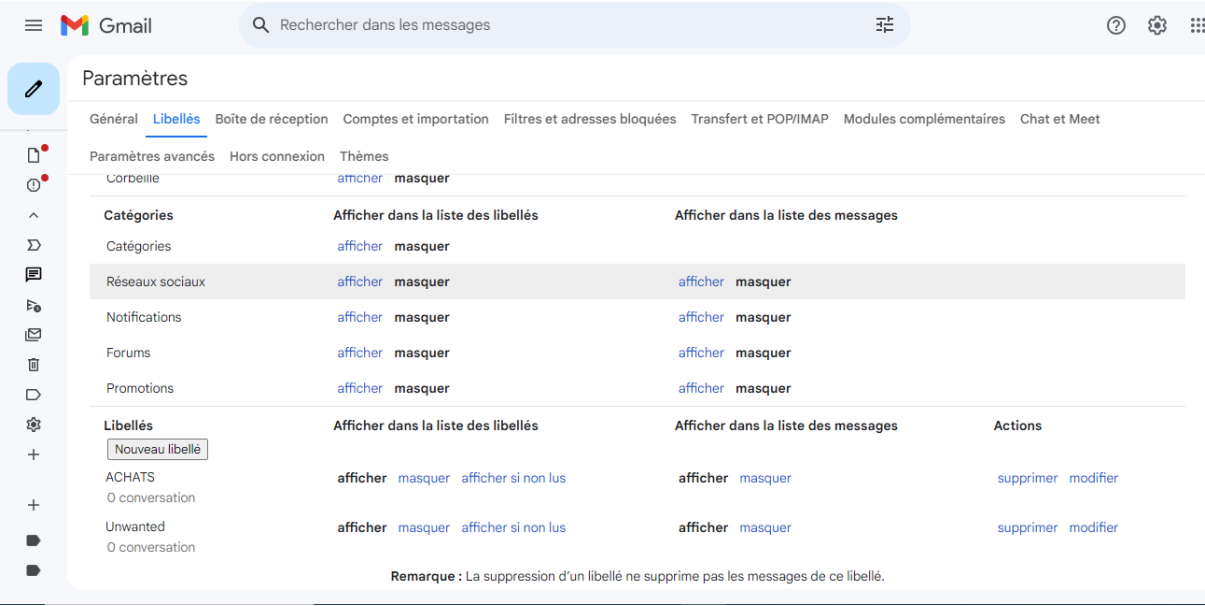
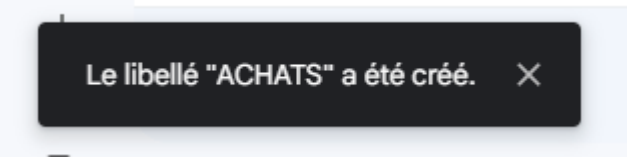
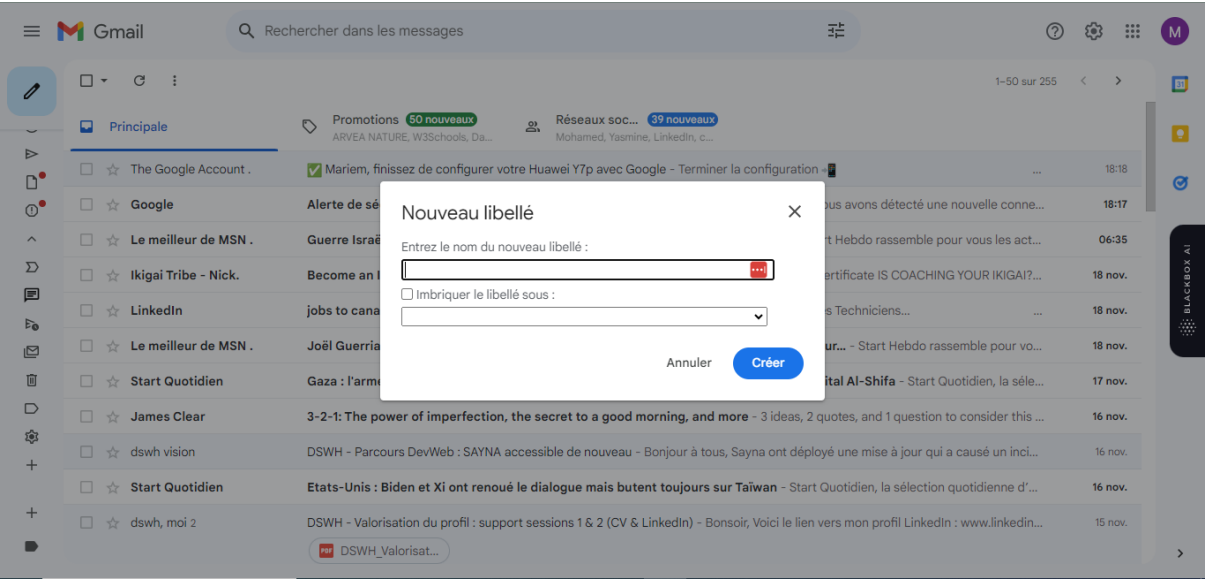


État actuel

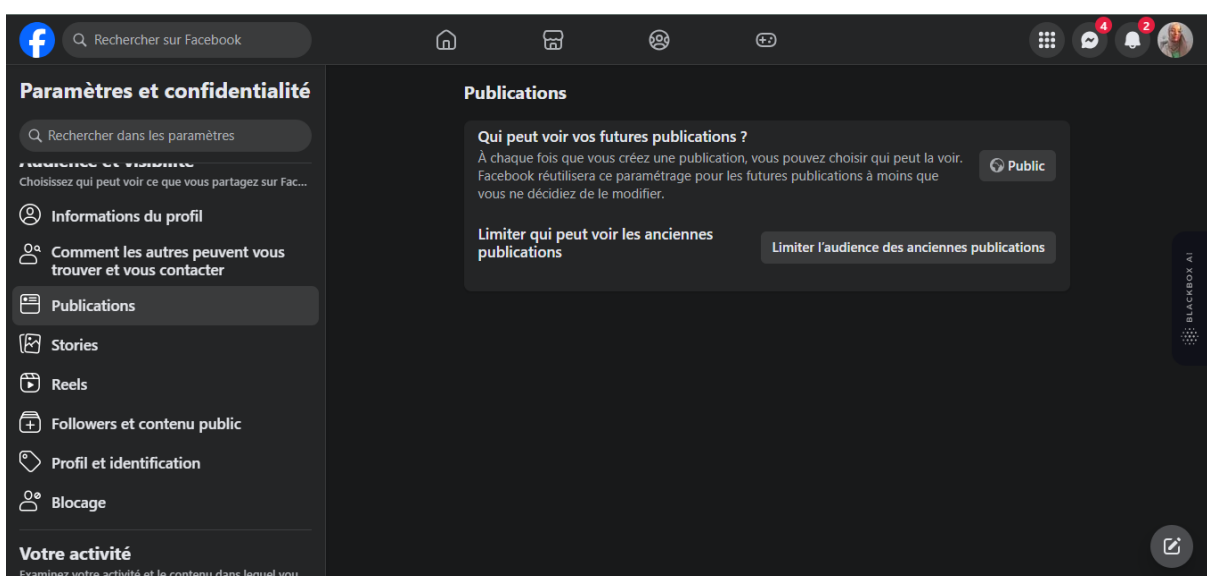
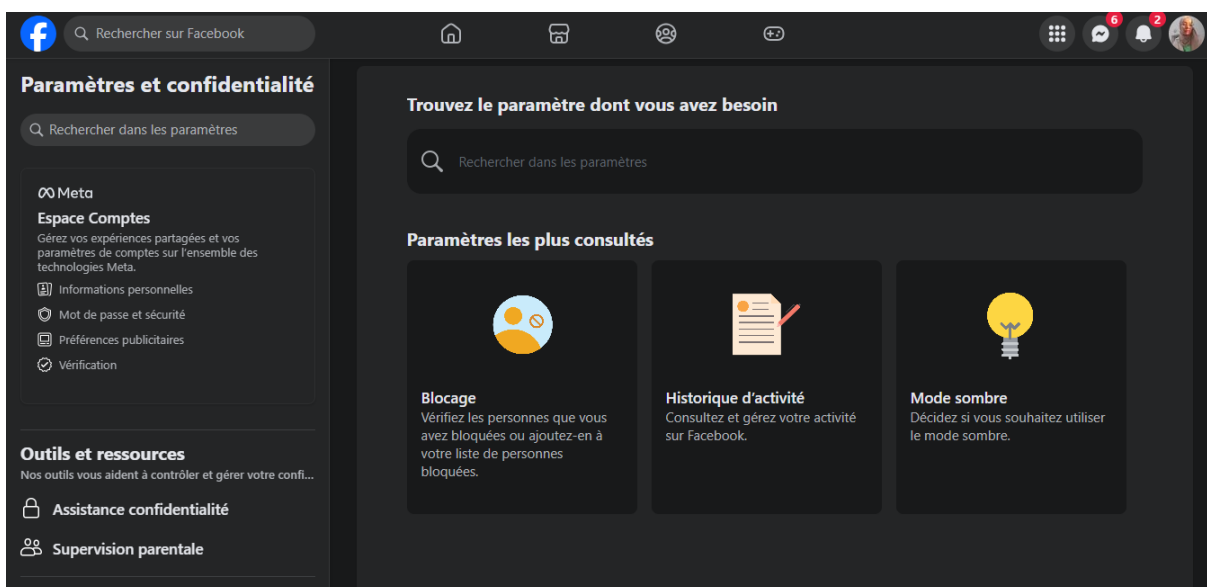
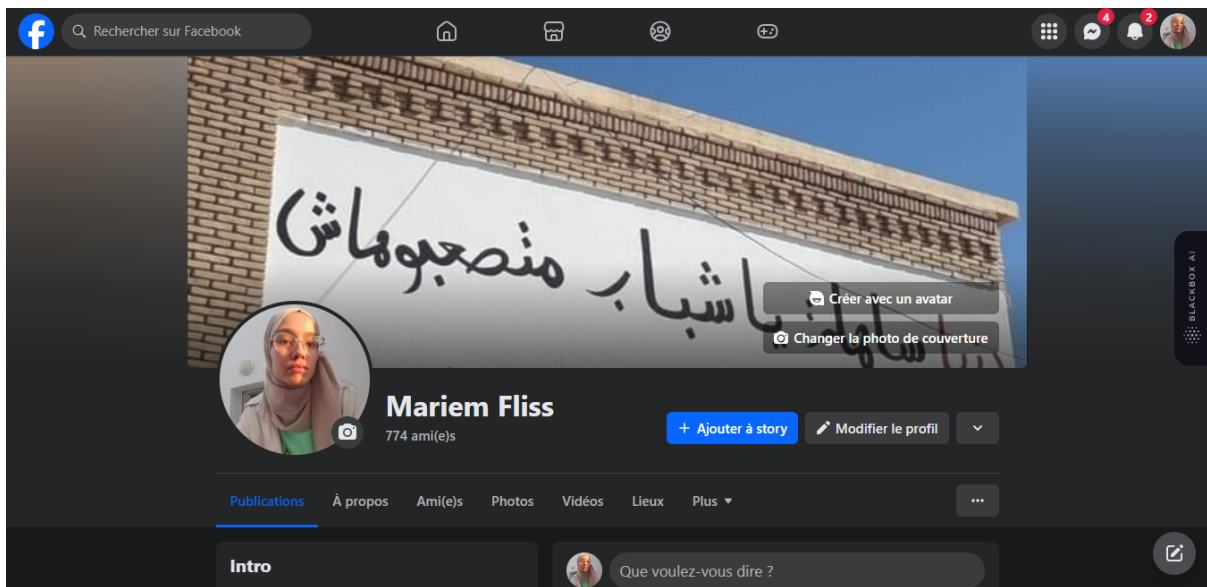
Vérifier une URL en particulier

Il est difficile d'indiquer un simple niveau de sécurité pour les sites comme <https://console.firebase.google.com/u/0/project/gestion-parc-info-3ff6f/overview?hl=fr&pli=1>, 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 spécifiques.

6 - Achats en ligne sécurisés :



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



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

Exercice pour Vérifier la Sécurité en Fonction de l'Appareil Utilisé:

Objectif: Tester la sécurité d'un appareil en identifiant les vulnérabilités potentielles.

Exercice: Analyse de Sécurité

Ordinateur personnel (PC ou Mac):

- Tâche: Vérifiez les paramètres de sécurité de votre système d'exploitation.
- Actions:
 - Examinez les paramètres du pare-feu et assurez-vous qu'il est activé.
 - Vérifiez les mises à jour du système d'exploitation et des logiciels.
 - Utilisez un scanner de vulnérabilité pour identifier d'éventuelles failles de sécurité.
 - Assurez-vous que votre antivirus est à jour et effectuez une analyse complète du système.

Smartphone (iOS ou Android):

- Tâche: Évaluer la sécurité des applications et des paramètres du téléphone.
- Actions:
 - Examinez les autorisations des applications et révoquez celles qui semblent excessives.
 - Assurez-vous que le verrouillage par mot de passe ou empreinte digitale est activé.
 - Vérifiez les mises à jour du système d'exploitation et des applications.
 - Installez une application de sécurité mobile pour scanner les applications et détecter les menaces.

Réseau Domestique:

- Tâche: Évaluer la sécurité de votre réseau Wi-Fi.
- Actions:
 - Changez le mot de passe par défaut de votre routeur.
 - Activez le chiffrement WPA3 pour votre réseau Wi-Fi.
 - Vérifiez la liste des appareils connectés au réseau et identifiez les éventuels intrus.
 - Mettez à jour le firmware de votre routeur.

Exercice pour Installer et Utiliser un Antivirus + Antimalware:

Objectif: Installer un programme de sécurité pour protéger l'appareil contre les menaces informatiques.

Exercice: Installation d'un Antivirus + Antimalware

Ordinateur personnel (PC ou Mac):

- Tâche: Installer un antivirus et un antimalware.
- Actions:
 - Choisissez un logiciel antivirus réputé et téléchargez-le depuis le site officiel.
 - Suivez les instructions d'installation et effectuez une mise à jour de la base de données de définitions.
 - Configurez des analyses planifiées pour vérifier régulièrement votre système.
 - Testez la capacité de l'antivirus à détecter et mettre en quarantaine des menaces en simulant une infection (avec un fichier test).

Smartphone (iOS ou Android):

- Tâche: Installer une application de sécurité mobile.
- Actions:
 - Choisissez une application de sécurité bien notée sur la boutique d'applications.
 - Installez l'application et effectuez une analyse complète du téléphone.
 - Configurez des analyses régulières et assurez-vous que l'application est activée en arrière-plan.
 - Simulez une menace en téléchargeant un fichier test et vérifiez la réaction de l'application.