02/01/2025

SAYNA-SECURITE-PROJET1

kévin kowouvi
kowouvikossi3335@gmail.com

SAYNA-SECURITE-PROJET1

Parcours : DISCOVERY

Module : Naviguer en toute sécurité

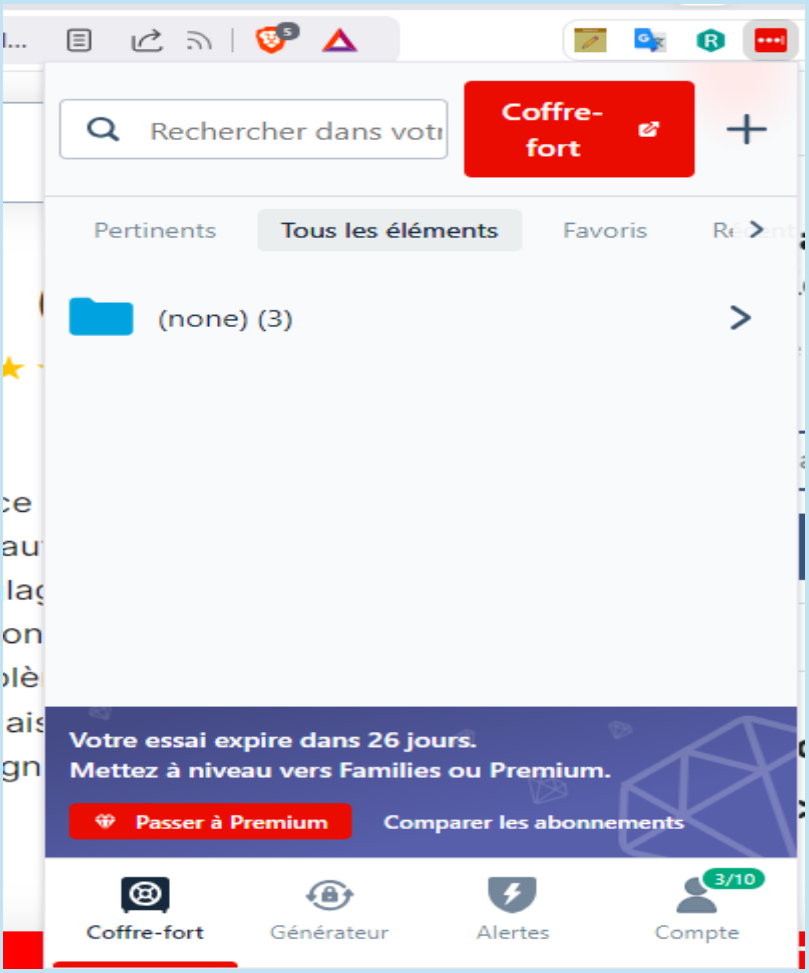
Projet 1 - Un peu plus de sécurité, on n'en a jamais assez !

1 - Introduction à la sécurité sur Internet

- **Article 1** = **Panda Security** - Comment accélérer votre ordinateur avec un antivirus
- **Article 2** = **MAIF** - Comment naviguer sur internet en toute sécurité
- **Article 3** = **L'Informatique pour les Néophytes** - La Sécurité Informatique pour Débutants et Néophytes
- **Article bonus = France Num** - Sécurité dans le cloud : quelles sont les bonnes pratiques à adopter

Ces articles présentent des conseils essentiels pour sécuriser votre navigation sur Internet, optimiser votre ordinateur et protéger vos données dans le cloud. Adoptez ces bonnes pratiques pour naviguer en toute confiance.

2 - Créer des mots de passe forts



Grâce à LastPass, j'ai appris à sécuriser mes comptes avec des mots de passe forts et uniques, tout en simplifiant leur gestion. Je m'engage à structurer mes accès sur toutes les plateformes, à mettre à jour mes mots de passe régulièrement et à activer des mesures de sécurité.

3 - Fonctionnalité de sécurité de votre navigateur

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

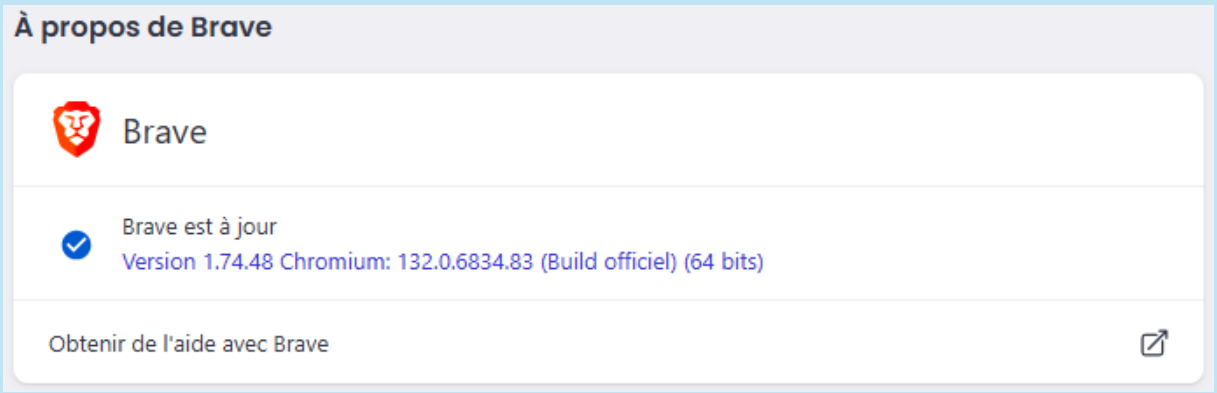
Après avoir soigneusement analysé les adresses et mené des recherches approfondies, voici les sites qui se révèlent être potentiellement malveillants.

Adresse internet	Malveillant ?	
www.morvel.com	☒	Ressemble à www.marvel.com sauf qu'à la place de « a », on a « o »
www.dccomics.com	☐	Ce site existe réellement
www.ironman.com	☐	Ce site existe réellement
www.fessebook.com	☒	Ressemble à www.facebook.com sauf qu'à la place de « face », on a « fesse ».
www.instagam.com	☒	Ressemble à www.instagram.com sauf que le « r » est omis.

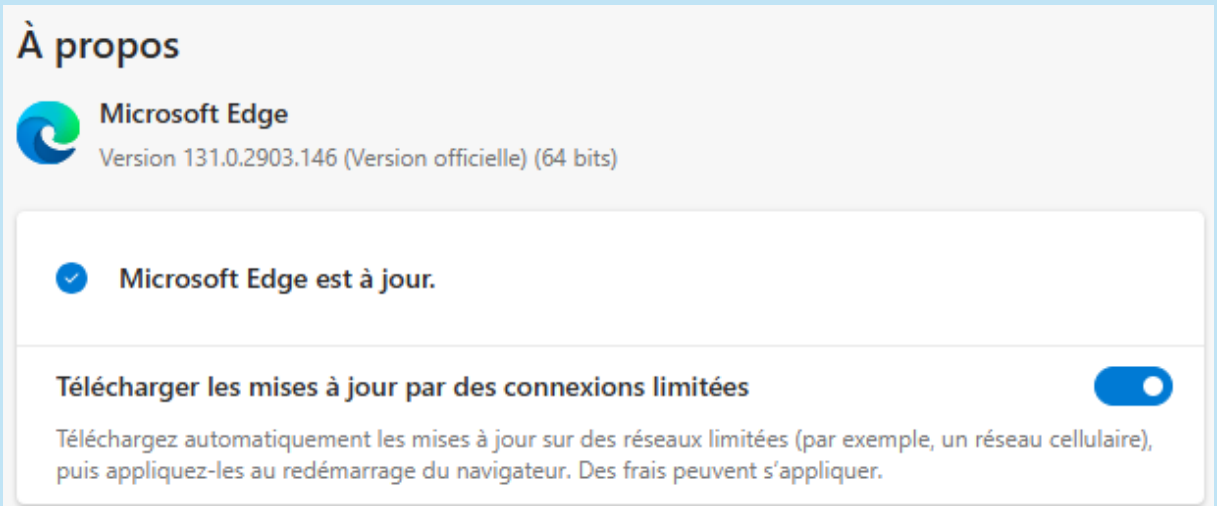
2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes. (case à cocher)

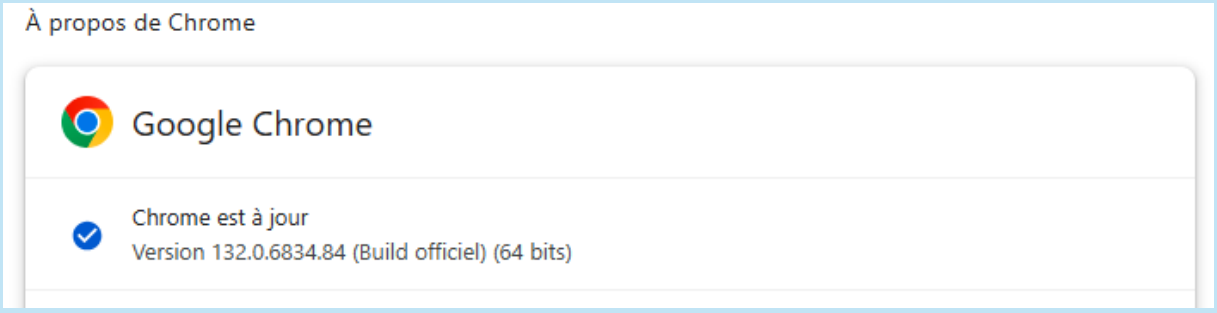
Brave est mon navigateur principal pour sa rapidité, son blocage natif des publicités et son respect de la vie privée, en limitant le suivi en ligne. Je l'ai choisi pour une navigation plus sécurisée et sans distractions.

NAVIGATEUR	A JOUR
Google Chrome	☒
Firefox	☒
Microsoft Edge	☒
Brave	☒


À propos de Brave
Brave
Brave est à jour
Version 1.74.48 Chromium: 132.0.6834.83 (Build officiel) (64 bits)
Obtenir de l'aide avec Brave


À propos de Mozilla Firefox
Firefox Browser
Firefox est à jour
134.0.1 (64 bits) Notes de version
Aide de Firefox Donner votre avis
Firefox est conçu par Mozilla, une communauté mondiale de contri
travaillent ensemble pour garder le Web ouvert, public et accessible
Vous souhaitez aider ? Vous pouvez faire un don ou bien participer
Informations de licence
Droits de l'utilisateur
Politique de confidentialit
Firefox et les logos Firefox sont des marques déposées de la Mozilla Foundation.


À propos
Microsoft Edge
Version 131.0.2903.146 (Version officielle) (64 bits)
Microsoft Edge est à jour.
Télécharger les mises à jour par des connexions limitées
Téléchargez automatiquement les mises à jour sur des réseaux limitées (par exemple, un réseau cellulaire), puis appliquez-les au redémarrage du navigateur. Des frais peuvent s'appliquer.



4 - Éviter le spam et le phishing

Après avoir étudié plusieurs articles sur l'hameçonnage, j'ai mieux compris les techniques des cybercriminels, comme les erreurs de syntaxe, liens suspects ou demandes d'informations urgentes. Ces connaissances m'ont aidé à réussir le quiz "Exercice 4 - Spam et Phishing" avec un score parfait de 10/10. Cet entraînement renforce ma capacité à reconnaître les tentatives malveillantes et à protéger mes comptes en ligne.

5 - Comment éviter les logiciels malveillants

- Site n°1

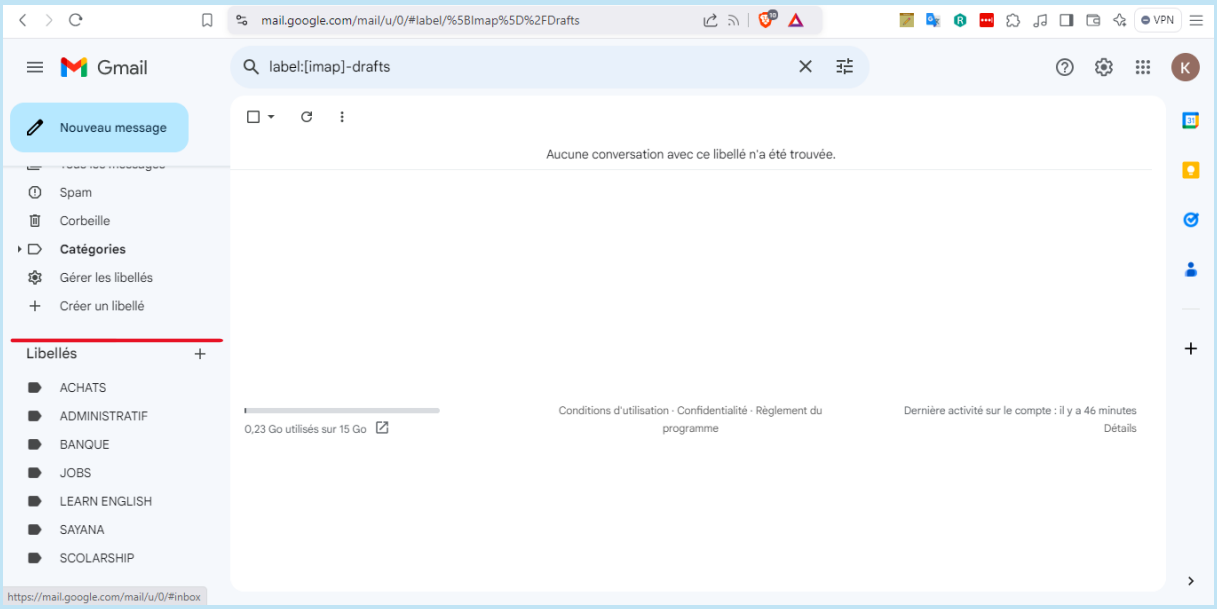
- Indicateur de sécurité
    - Not secure
- Analyse Google
    - Aucun contenu suspect

- Site n°2
    - Indicateur de sécurité
        - HTTPS
    - 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

En réorganisant ma messagerie électronique et en créant de nouveaux libellés comme "Achats", "Administratif" et plein d’ autres, j’ai pu structurer mes messages de manière claire et efficace. Cette organisation simplifie mon quotidien en me permettant de retrouver rapidement les informations importantes. Je suis ravi de cette méthode, qui me fait gagner du temps tout en apportant plus de sérénité dans la gestion de mes données.

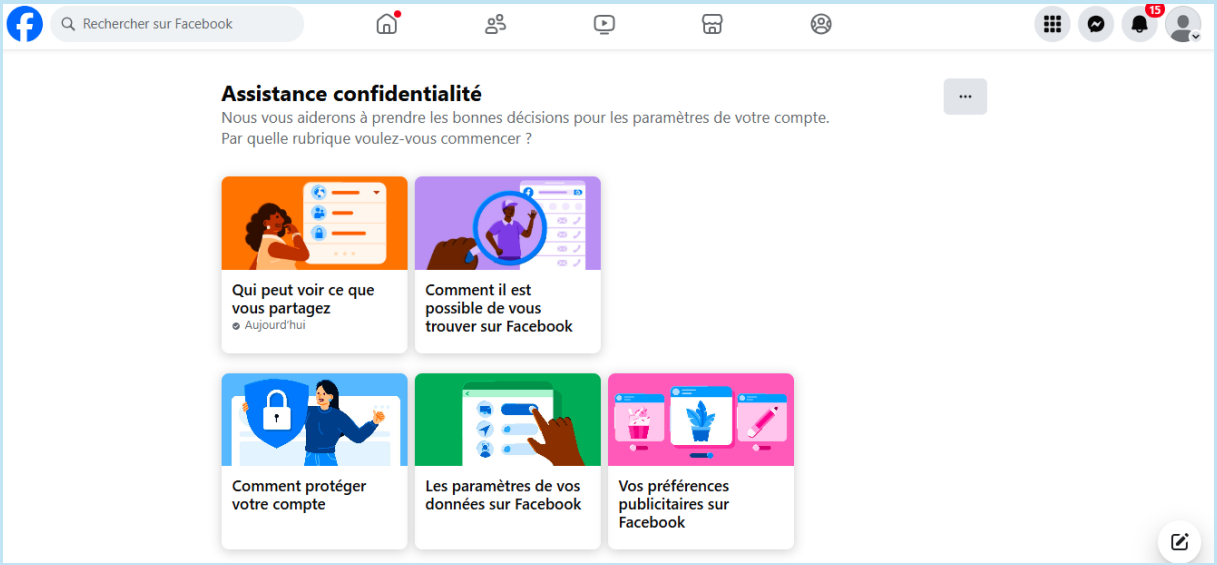


7 - Comprendre le suivi du navigateur

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

En suivant ces consignes, j'ai compris l'importance de gérer les paramètres de confidentialité pour protéger mes informations personnelles sur Facebook. J'ai ajusté la visibilité de mes données, limité l'accès à mes publications et restreint les commentaires pour éviter les interactions malveillantes. Cela m'apporte une plus grande maîtrise de mon compte et une utilisation plus sereine des réseaux sociaux. Je m'engage désormais à appliquer ces bonnes pratiques sur mes autres comptes, comme LinkedIn ou Instagram, pour garantir une présence en ligne sécurisée et adaptée à mes besoins, tout en restant conscient des données partagées avec ces plateformes.



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

Exercice : Test de la sécurité de votre appareil

1. Vérifiez la sécurité de votre appareil en quelques étapes simples

Commencez par évaluer si votre appareil est bien protégé :

- **Pour votre ordinateur (Windows ou macOS)** :
    1. Assurez-vous que votre système est à jour en vérifiant les mises à jour dans les paramètres.
    2. Utilisez les outils de sécurité intégrés comme "Sécurité Windows" ou "XProtect" pour effectuer un scan rapide.
    3. Testez les vulnérabilités en utilisant des outils comme Belarc Advisor (Windows) ou DetectX Swift (macOS).
- **Pour votre smartphone (Android ou iOS)** :
    1. Vérifiez les autorisations des applications installées pour détecter les accès inutiles à vos données.
    2. Installez une application de sécurité mobile comme Avast Mobile ou Panda Dome pour effectuer un scan antivirus rapide.

2. Installer et utiliser un antivirus adapté

Un antivirus est indispensable pour protéger vos données et maintenir les performances de votre appareil :

1. Téléchargez un antivirus fiable comme Panda Security, Bitdefender ou Avast depuis leur site officiel ou la boutique d'applications de votre appareil.
2. Installez-le en suivant les instructions à l'écran.
3. Une fois configuré :
    - Effectuez une analyse complète pour repérer et supprimer les menaces.
    - Activez la protection en temps réel pour empêcher les infections futures.
    - Planifiez des analyses automatiques pour une protection continue.

➡ Pour en savoir plus sur l'impact des antivirus et des astuces pour accélérer votre ordinateur, consultez cet article : Comment accélérer votre ordinateur avec un antivirus.