SAYNA-SECURITE-PROJET1

Parcours : DISCOVERY

Module : Naviguer en toute sécurité

Projet 1 : Un peu plus de sécurité on en a jamais assez !

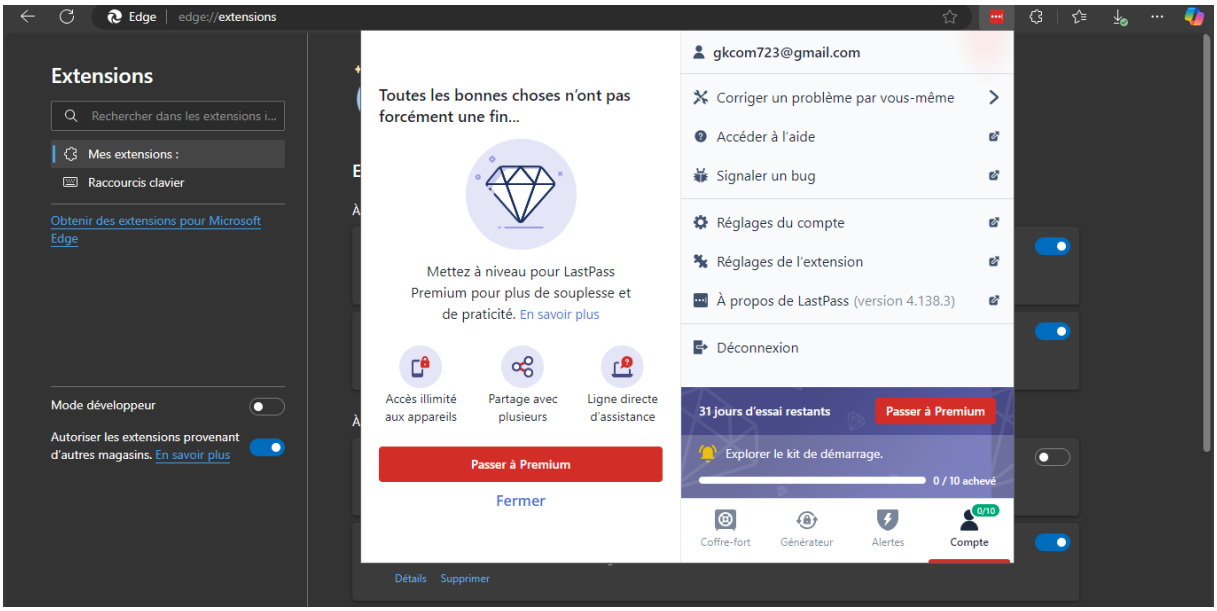
1. Introduction à la sécurité sur Internet

Réponse :
Voici les articles :

- Article 1 = passion-net.fr - 10 conseils simples pour naviguer
- *Publié le 8 janvier 2025*
- Article 2 = bhmag.fr – Antivirus et VPN : deux outils indispensables pour surfer sur Internet en toute sécurité
  Publié le 9 janvier 2025
- Article 3 = phongnhaexplorer.com - Comment protéger sa vie privée sur internet ?
  Publié le 9 janvier 2025

2. Créer des mots de passe forts

Voici une capture d'écran de mon activité avec le gestionnaire de mot de passe LastPass :



3 - Fonctionnalité de sécurité de votre navigateur

1/ Identifions les adresses internet qui te semblent provenir de sites web malveillants.

Réponse :
Les sites web qui semblent être malveillants sont :

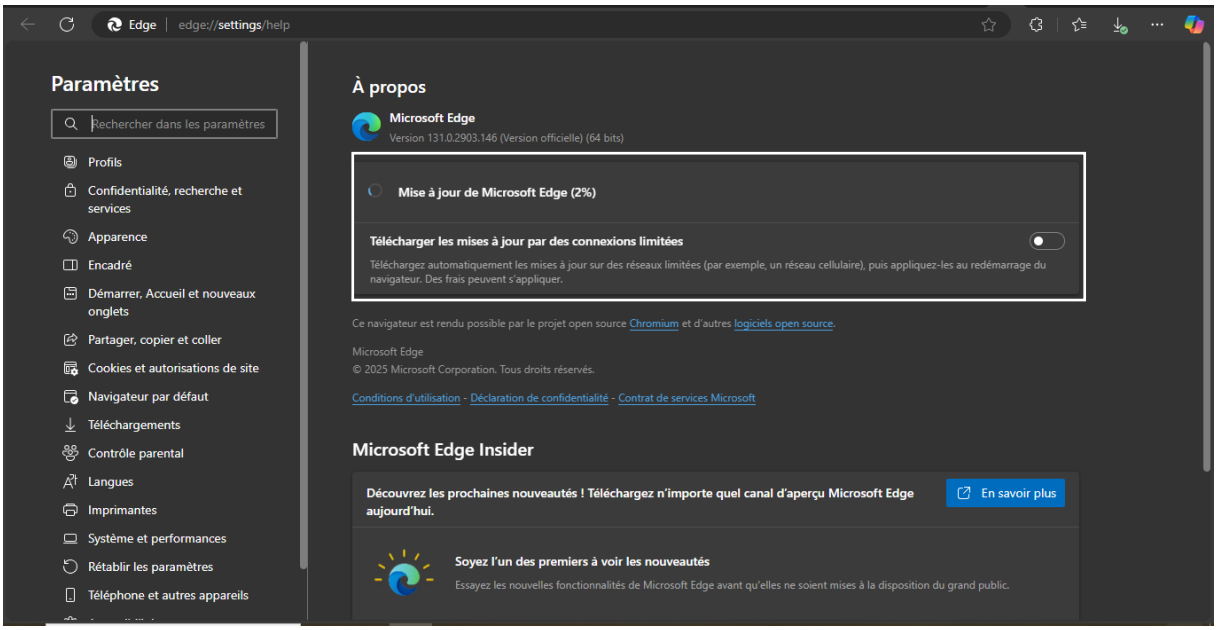
- www.morvel.com
- www.fessebook.com
- www.instagam.com

Les seuls sites qui semblaient être cohérents sont donc :

- www.dccomics.com
- www.ironman.com

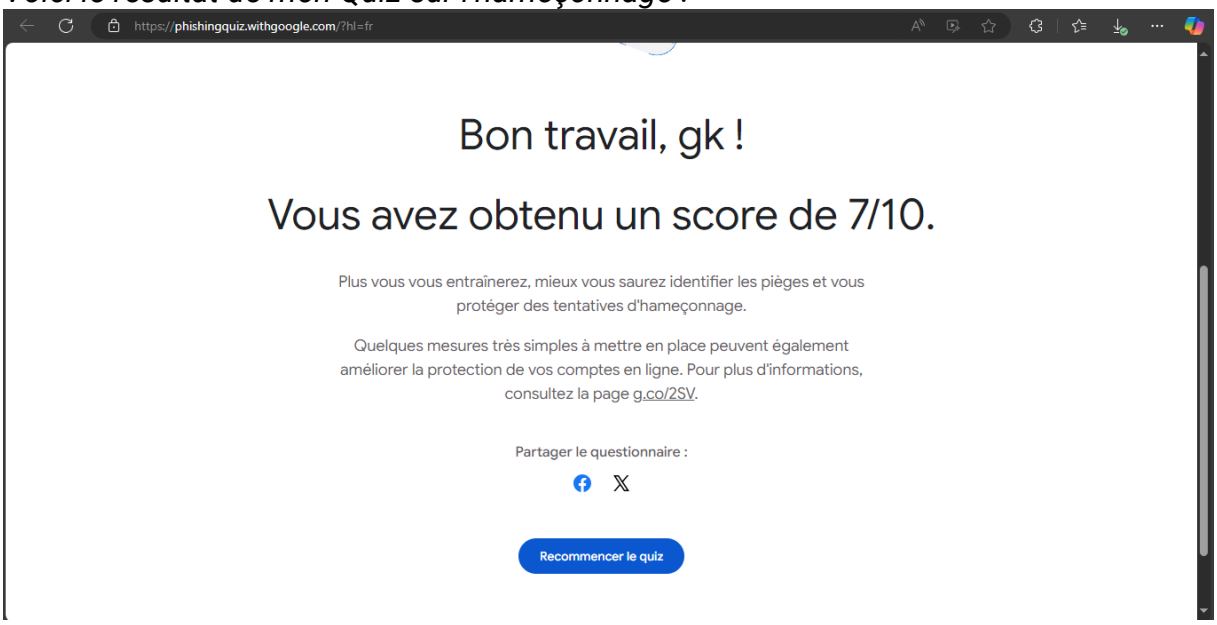
2/ Vérifions si les navigateurs utilisés, sont à jour

Après la vérification j'ai constaté que mon navigateur (Microsoft Edge) n'est pas à jour.



4 - Éviter le spam et le phishing

Voici le résultat de mon Quiz sur l'hameçonnage :



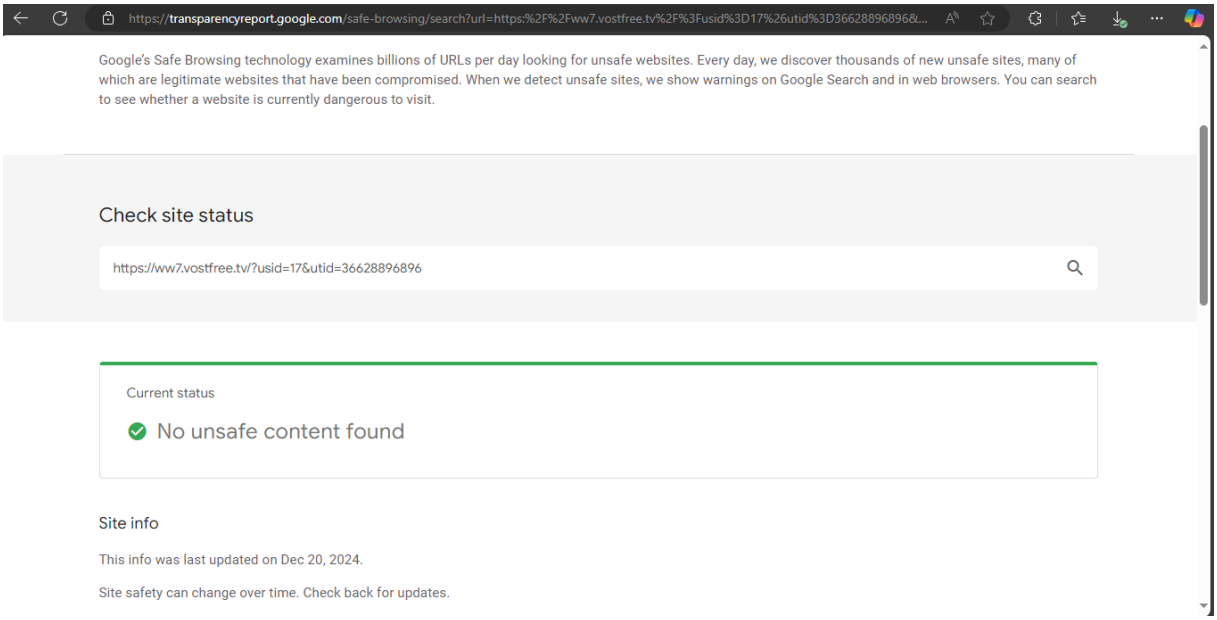
5 - Comment éviter les logiciels malveillants

Réponse :

Site n°1

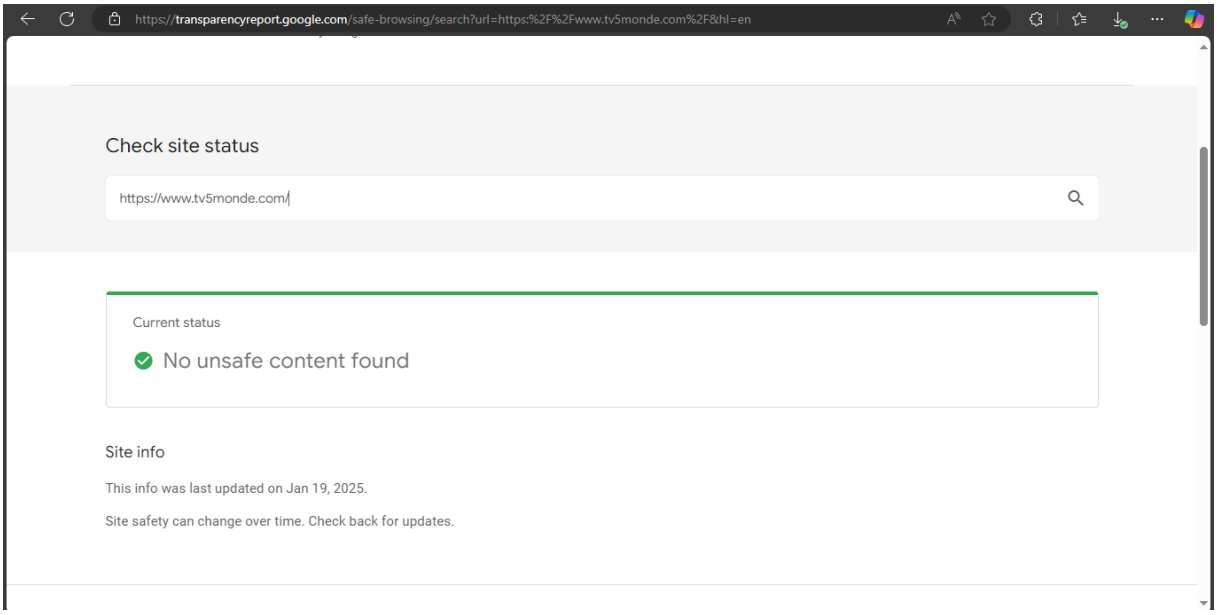
- Indicateur de sécurité
  - HTTPS

- Analyse Google
    - Aucun contenu suspect



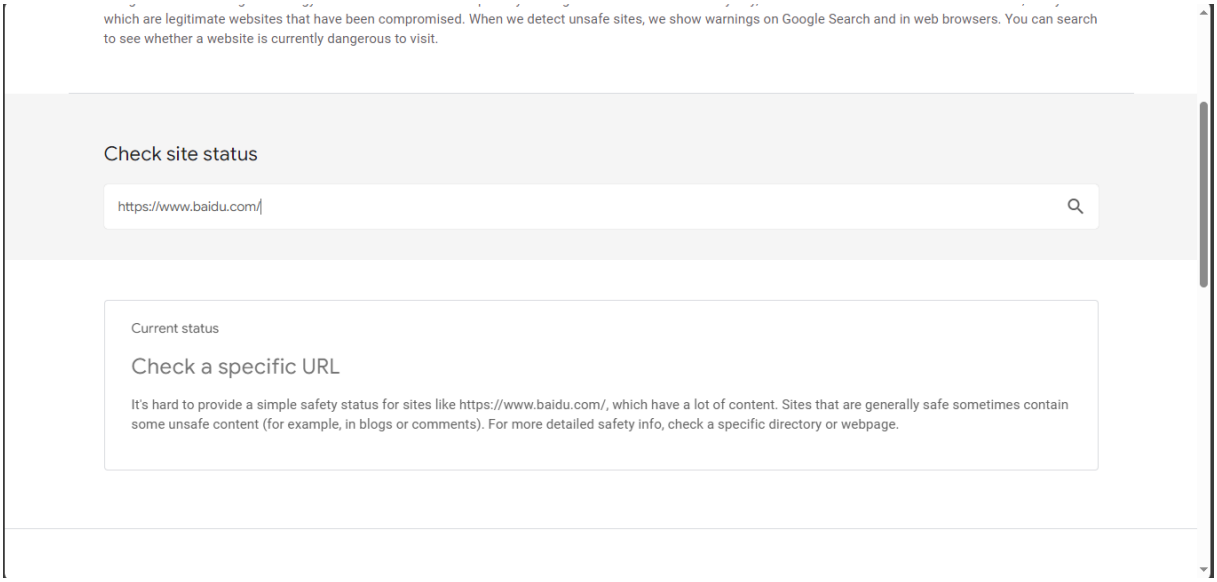
Site n°2

- Indicateur de sécurité
    - HTTPS
- Analyse Google
    - Aucun contenu suspect



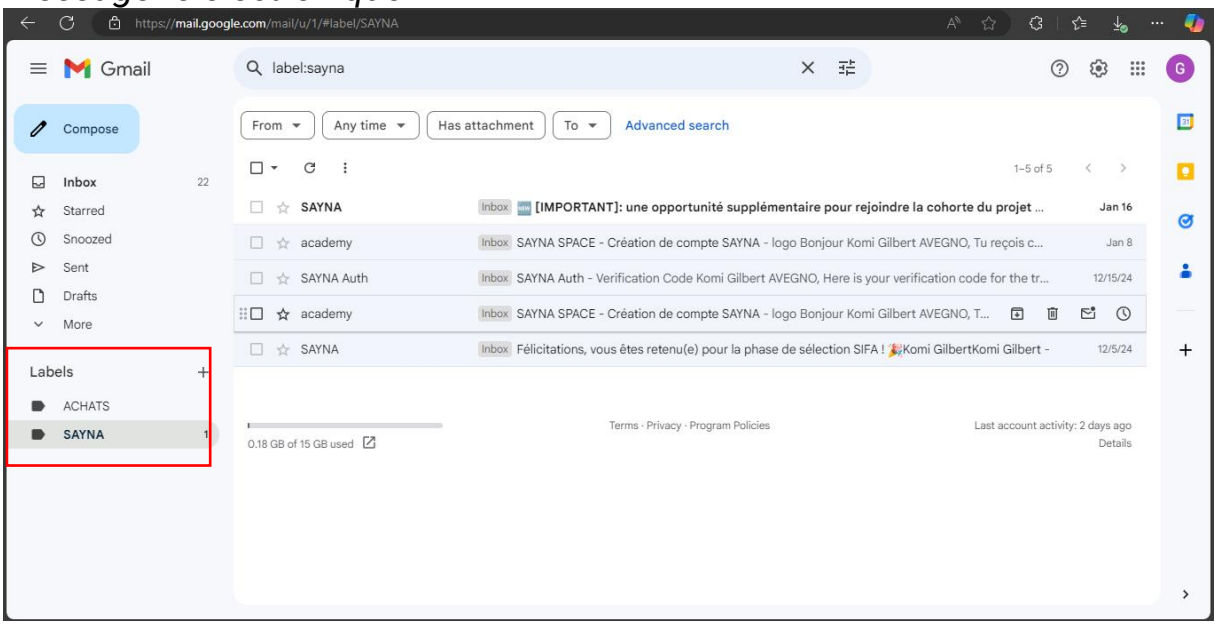
Site n°3

- Indicateur de sécurité
    - HTTPS
- Analyse Google
    - Vérifier un URL en particulier



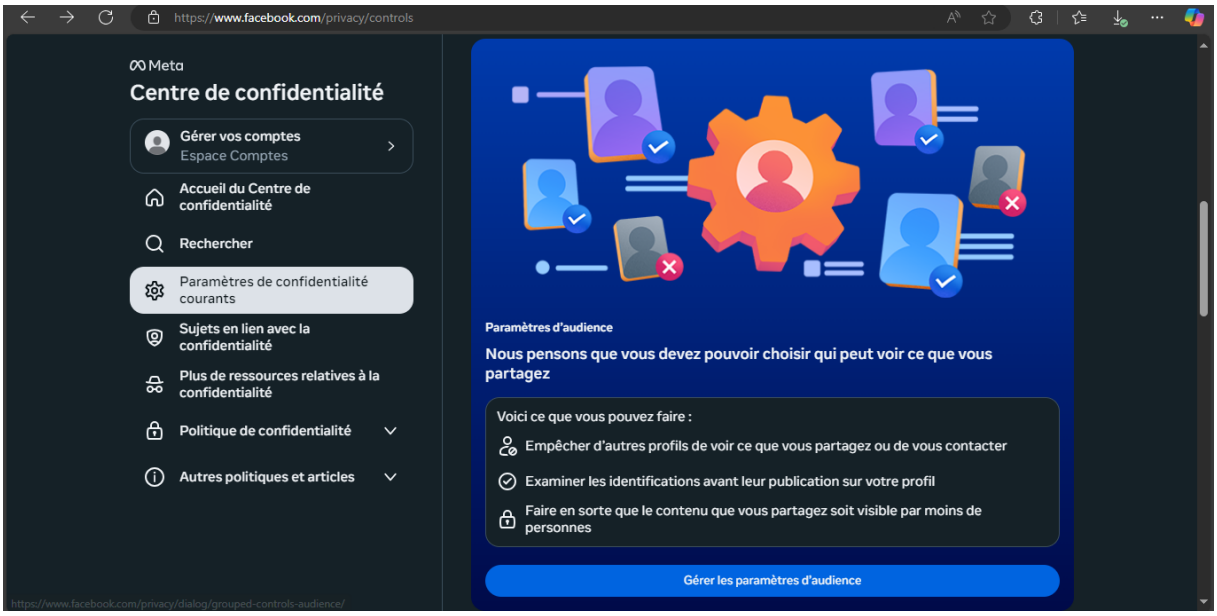
6 - Achats en ligne sécurisés

Voici une capture d'écran de mon organisation de libellé pour gérer ma messagerie électronique :



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

Exercice : Vérifier la sécurité d'un ordinateur (Windows/Mac)

Objectifs :

- Identifier les signes d'infection par un virus.
- Vérifier l'état de sécurité de votre appareil.
- Utiliser les outils intégrés au système pour détecter les menaces.

1- Vérification de la sécurité en fonction de l'appareil utilisé

Étapes pour Windows :

1. **Vérifier les performances du système :**
    - **Exercice :**

1. Ouvrez le **Gestionnaire des tâches**
2. Allez dans l'onglet **Processus**.
3. Recherchez des processus suspects (noms inconnus, utilisation anormale de CPU ou mémoire).

- Avez-vous repéré des processus inhabituels ? Notez leur nom et recherchez-les en ligne pour en savoir plus.

2. **Vérifier les programmes au démarrage :**

- **Exercice :**

  - Toujours dans le Gestionnaire des tâches, allez dans l'onglet **Démarrage**.
  - Désactivez les programmes que vous ne reconnaissez pas ou qui semblent suspects.

- Quels programmes sont activés au démarrage ? Sont-ils tous légitimes ?

3. **Scanner le système avec Windows Defender :**

- **Exercice :**

  - Ouvrez **Sécurité Windows** (via Paramètres > Mise à jour et sécurité).
  - Lancez un scan complet.

- Le scan détecte-t-il des menaces ? Si oui, quelles actions sont recommandées ?

Étapes pour Mac :

1. **Vérifier les applications ouvertes et en arrière-plan :**

- **Exercice :**

  - Ouvrez le **Moniteur d'activité** (via Spotlight : Cmd + Espace > tapez "Moniteur d'activité").
  - Analysez les applications et processus utilisant beaucoup de ressources.
- Voyez-vous des processus inhabituels ? Cherchez leurs noms en ligne.

2. **Contrôler les extensions et programmes :**

- **Exercice :**
    - Allez dans **Préférences système > Utilisateurs et groupes > Ouverture**.
    - Désactivez les éléments suspects qui se lancent au démarrage.
  - Quels éléments se lancent au démarrage ? Sont-ils tous nécessaires ?

3. **Rechercher des logiciels suspects :**
    - **Exercice :**
        - Allez dans **Applications** et cherchez des programmes que vous n'avez pas installés.
      - Avez-vous trouvé des applications inconnues ? Désinstallez-les si nécessaire.

2. Installer et utiliser un antivirus/antimalware

Exercice : Installation et utilisation d'un antivirus

Pour Windows :

- Utilisez des solutions comme **Windows Defender**, **Malwarebytes** ou **Bitdefender**.
- Lancez un scan planifié quotidiennement.

Pour Mac :

- Installez des solutions compatibles comme **Malwarebytes pour Mac**.
- Activez la protection contre les téléchargements suspects dans **Préférences système > Sécurité et confidentialité**.

Pour Android/iOS :

- Téléchargez des applications antivirus reconnues comme **Avast Mobile Security**, **Norton Mobile Security** ou **Bitdefender Mobile Security**.
- Autorisez l'application à scanner les applications installées et les fichiers téléchargés.