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

Voici les trois articles que nous avons retenus (avec les mots-clés “sécurité sur internet” et “comment être en sécurité sur internet” :

● Article 1 = VPNoverview.com - Sécurité en ligne | Un aperçu complet de la protection en ligne

● Article 2 = Assistance aux victimes de cybermalveillance - Les 10 règles de base pour la sécurité numérique

● Article 3 = Avast - Qu’est-ce qu’une arnaque ? | Détecter, signaler et bloquer

2 - Créer des mots de passe forts

Désormais, lorsque je me connecte à mes comptes, je peux enregistrer le mot de passe grâce à LastPass.

3 - Fonctionnalité de sécurité de votre navigateur

1/ Les sites web qui semblent être malveillants sont :

● www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l’univers Marvel

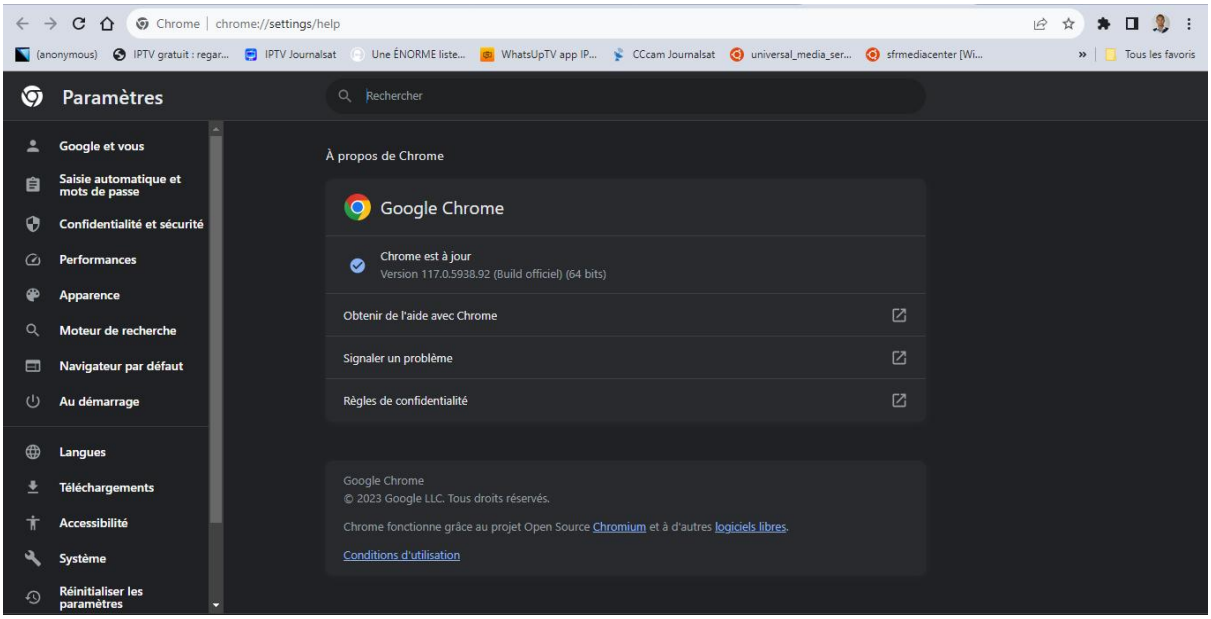
● www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde

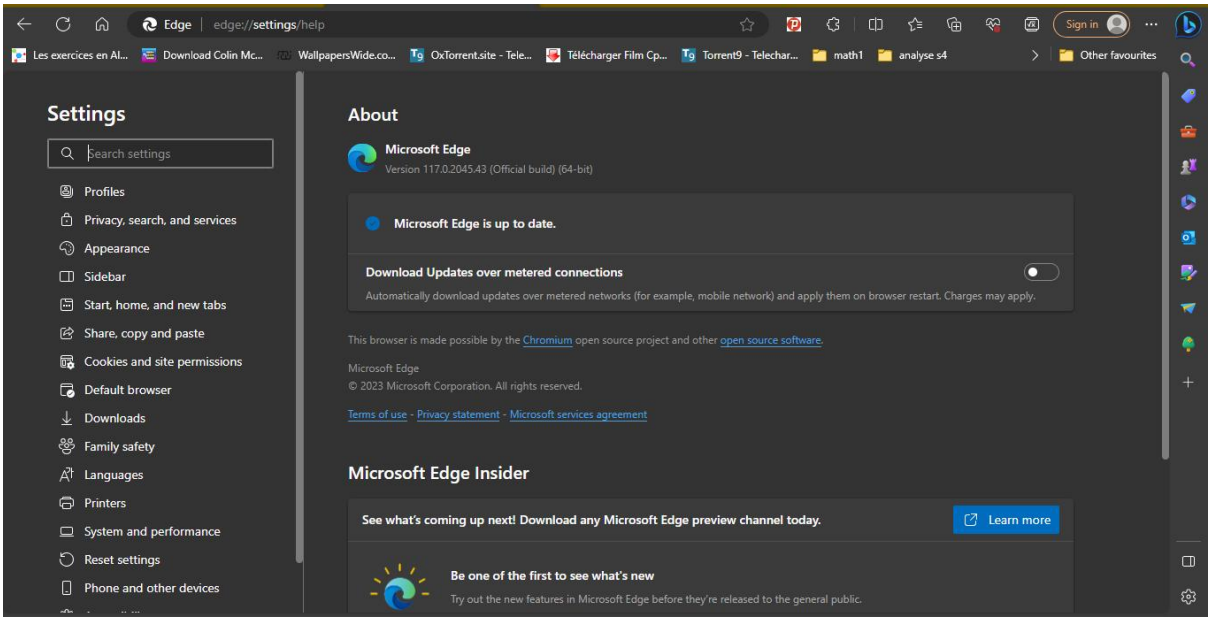
● www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très utilisé. Les seuls sites qui semblaient être cohérents sont donc :

● www.dccomics.com, le site officiel de l'univers DC Comics

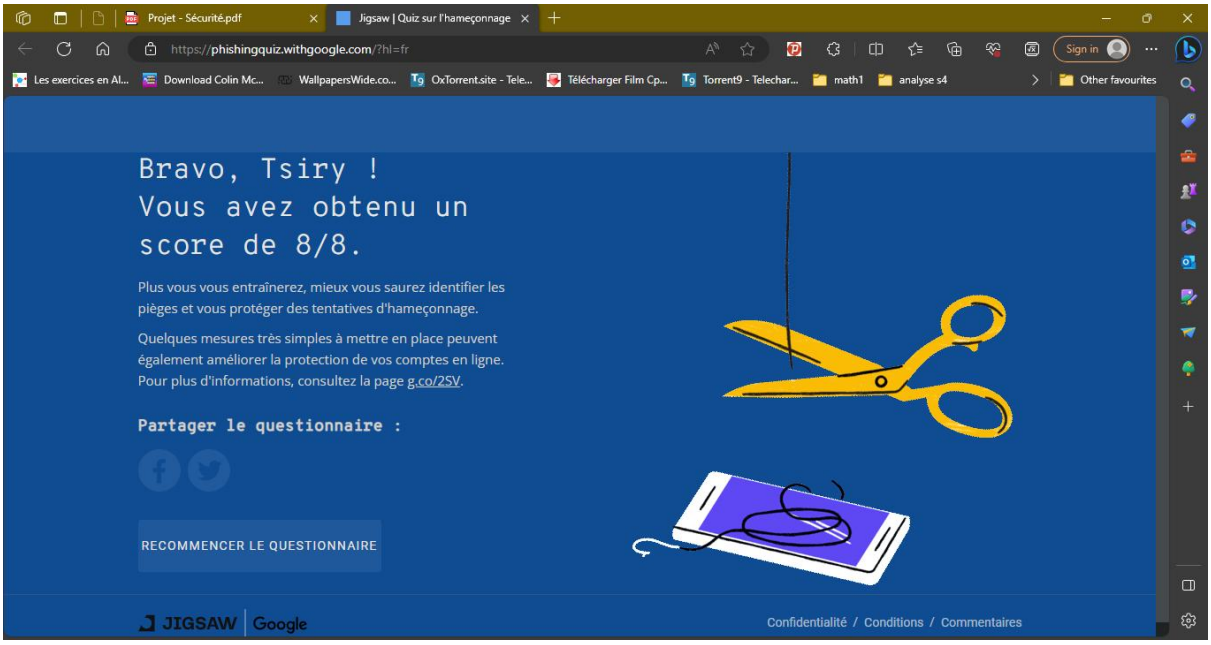
● www.ironman.com, le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox sont à jour :





4 - Éviter le spam et le phishing



5 - Comment éviter les logiciels malveillants

3/

- Site n°1 (vostfree.tv - Ce site web est à vendre ! - Ressources et information concernant vostfree Resources and Information.)

○ Indicateur de sécurité

☐ HTTPS

○ Analyse Google

☐ Aucun contenu suspect

● Site n°2 (TV5MONDE : TV internationale francophone : Info, Jeux, Programmes TV, Météo, Dictionnaire)

○ Indicateur de sécurité

☐ HTTPS

○ Analyse Google

☐ Aucun contenu suspect

● Site n°3 (百度一下，你就知道 (baidu.com))

○ Indicateur de sécurité

☐ Not secure

○ Analyse Google

☐ Vérifier un URL en particulier

6 - Achats en ligne sécurisés

1/

1. Créer un dossier sur ta messagerie électronique

Voici un exemple d'organisation de libellé pour gérer sa messagerie électronique :

● Achats : historique, facture, conversations liés aux achats

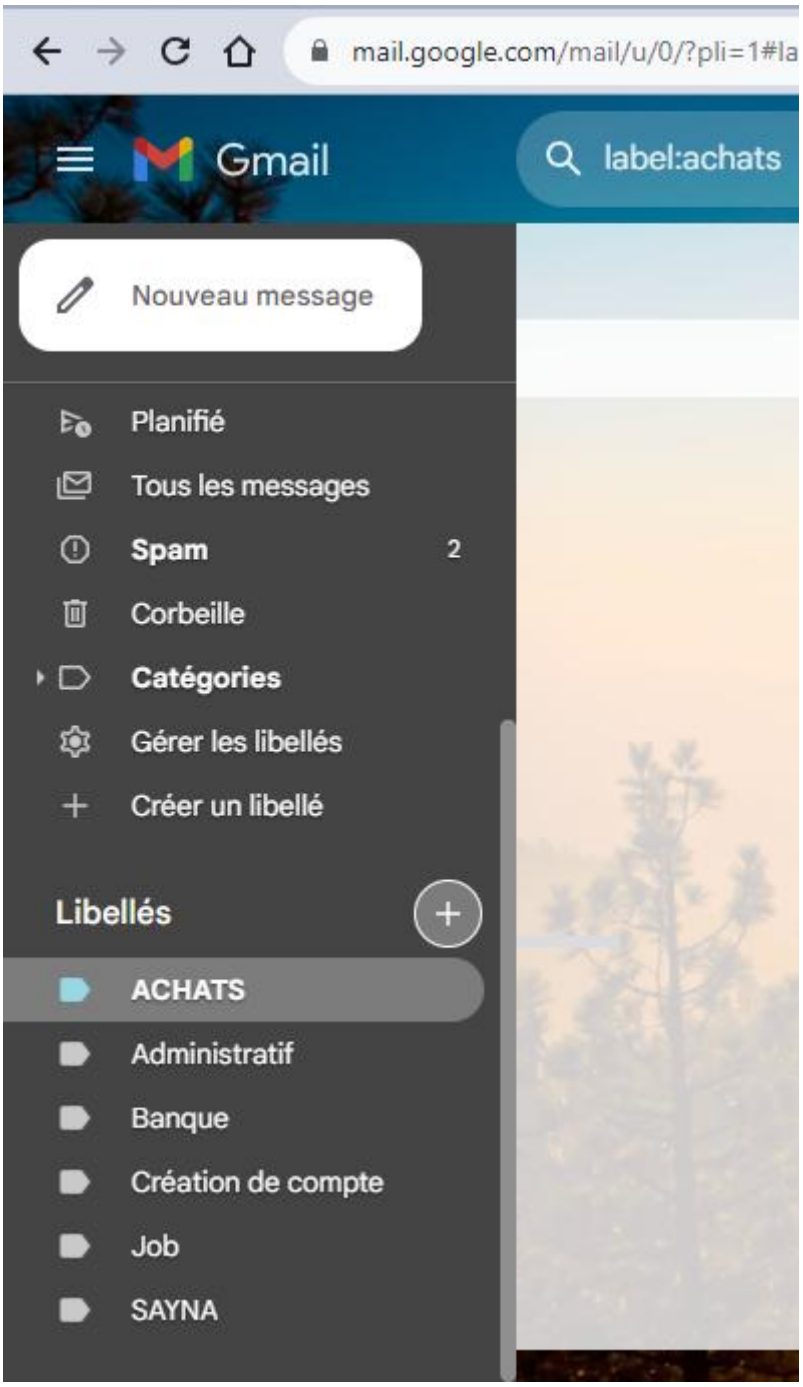
● Administratif : toutes les démarches administratives

● Banque : tous les documents et les conversations liés à la banque personnelle

● Création de compte : tous les messages liés à la création d’un compte (message de bienvenue, résumé du profil, etc.)

● Job : tous les messages liés à mon projet professionnel

● SAYNA : tous les messages liés mon activité avec SAYNA



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

Objectif : Régler les paramètres de confidentialité de Facebook

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

1/

Si un ordinateur est infecté par un virus, voici quelques étapes à suivre :

1. **Installer un logiciel antivirus**
2. **Se déconnecter d'Internet** : Pour empêcher le virus de causer plus de dégâts ou de se propager à d'autres systèmes, déconnecter l'ordinateur d'Internet.
3. **Redémarrer en mode sans échec** : Redémarrer l'ordinateur en mode sans échec pour limiter les processus et services qui s'exécutent au démarrage. Cela peut empêcher le virus de se lancer automatiquement.
4. **Exécuter une analyse antivirus** : Utiliser un logiciel antivirus pour analyser l'ordinateur et supprimer tous les fichiers infectés.

Pour vérifier la sécurité de l'appareil, on peut effectuer les exercices suivants :

- **Mettre à jour régulièrement les logiciels** : Assurer que tous vos logiciels, y compris le système d'exploitation et les applications sont à jour. Les mises à jour contiennent souvent des correctifs de sécurité qui peuvent protéger l'appareil contre les menaces récentes.
- **Utiliser un pare-feu** : Un pare-feu peut aider à bloquer les menaces avant qu'elles n'atteignent un appareil. Assurer que le pare-feu est activé et correctement configuré.
- **Faire attention aux e-mails et aux pièces jointes suspectes** : Beaucoup de virus se propagent par e-mail. Ne pas cliquer sur les liens ou ne pas ouvrir les pièces jointes dans les e-mails non sollicités ou suspects.

2/

Voici un exercice pour installer et utiliser un antivirus et un antimalware sur un appareil :

Étape 1 : Choisir un logiciel antivirus et antimalware : Il existe de nombreux logiciels antivirus et antimalware disponibles. Certains sont gratuits, tandis que d'autres sont payants. Faites des recherches pour trouver celui qui convient le mieux à vos besoins.

Étape 2 : Télécharger le logiciel : Une fois que vous avez choisi un logiciel, rendez-vous sur le site officiel du logiciel pour le télécharger. Assurez-vous de télécharger le logiciel à partir d'une source fiable pour éviter les logiciels malveillants.

Étape 3 : Installer le logiciel : Suivez les instructions fournies par le logiciel pour l'installer sur votre appareil. Cela peut impliquer de cliquer sur le fichier que vous avez téléchargé, puis de suivre les instructions à l'écran.

Étape 4 : Exécuter une analyse : Une fois le logiciel installé, ouvrez-le et exécutez une analyse de votre appareil. Cela permettra au logiciel de rechercher et d'identifier tout logiciel malveillant potentiel.

Étape 5 : Supprimer ou mettre en quarantaine les menaces détectées : Si le logiciel détecte des menaces, il vous donnera généralement l'option de les supprimer ou de les mettre en quarantaine. Suivez les recommandations du logiciel pour traiter ces menaces.

Étape 6 : Planifier des analyses régulières : Pour maintenir la sécurité de votre appareil, planifiez des analyses régulières avec votre logiciel antivirus et antimalware. Cela peut généralement être fait dans les paramètres du logiciel.