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

Objectif : à la découverte de la sécurité sur internet

1/ Trois (3) articles qui parlent de sécurité sur internet

● Article 1 = ISAGRI – 11 règles pour naviguer sur Internet en sécurité

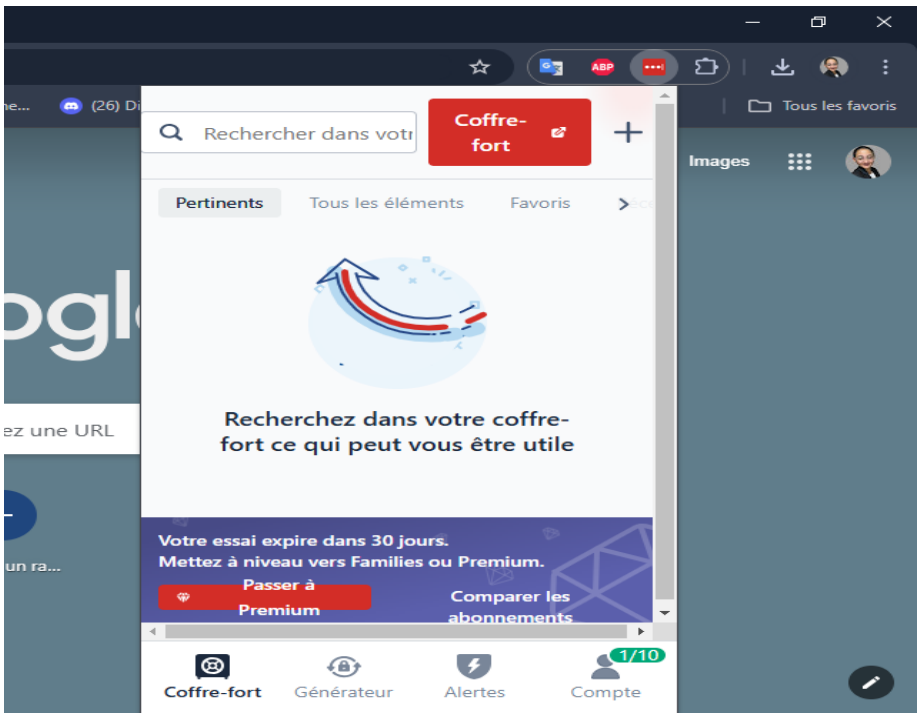
● Article 2 = KASPERSKY – Les 15 principaux règles de sécurité sur Internet et ce qu'il ne faut pas faire en ligne

● Article 3 = SAFETY CULTURE – Un guide complet de la sécurité sur Internet

2 - Créer des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass

1/ Gestionnaire de mot de passe LastPass



3 - Fonctionnalité de sécurité de votre navigateur

Objectif : identifier les éléments à observer pour naviguer sur le web en toute sécurité

1/ Identification de sites web malveillants

Les sites web qui semblent être malveillants sont :

- www.morvel.com : Cette adresse semble suspecte, car elle ressemble à une tentative de fraude en imitant un site légitime (Marvel).

- www.fessebook.com: Cela ressemble à une tentative de phishing visant à imiter Facebook mais avec une orthographe délibérément incorrecte.

- www.instagam.com : C'est également une tentative de phishing visant à imiter Instagram, mais avec une faute de frappe dans le nom.

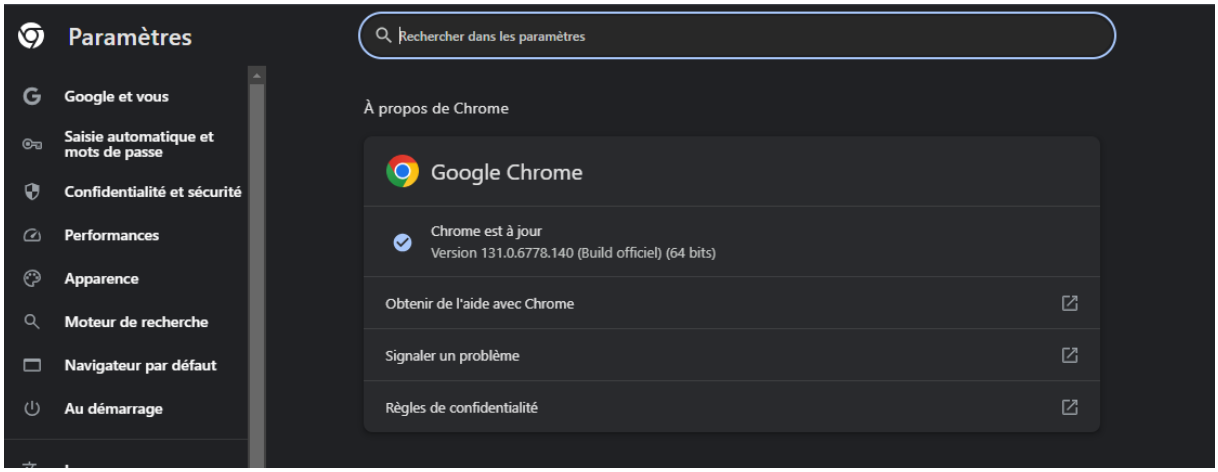
Les seuls sites qui semblaient être cohérents sont donc :

- www.dccomics.com : Il s'agit du site officiel de DC Comics, un site légitime.

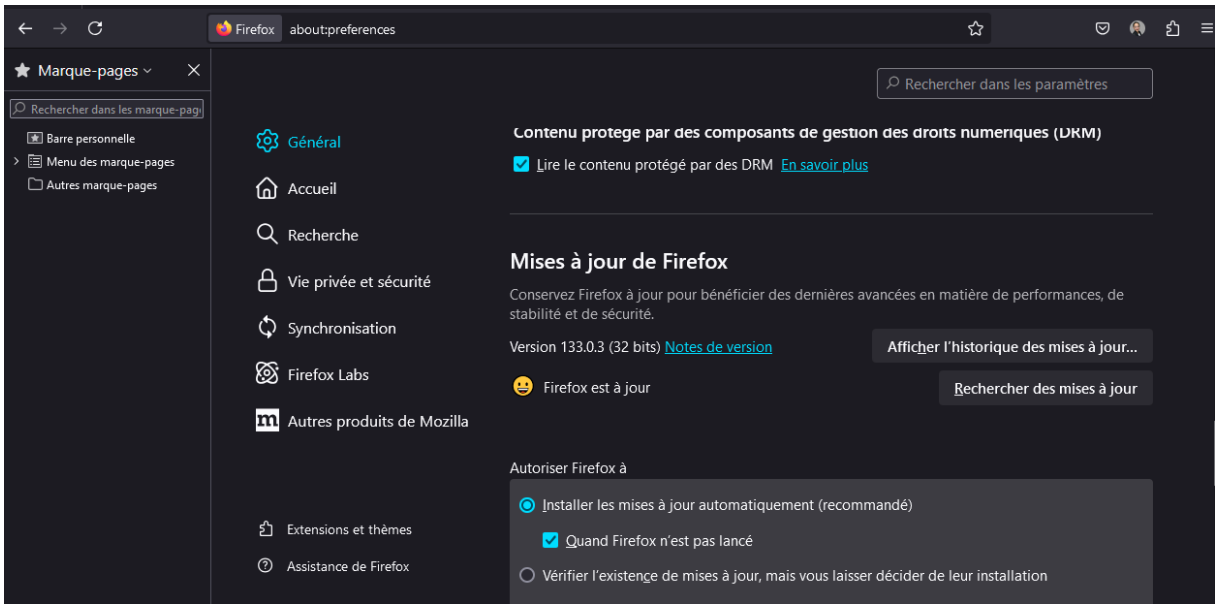
- www.ironman.com : Il s'agit d'un site officiel, mais il n'est pas directement lié à Iron Man en tant que personnage de Marvel. Cela pourrait être lié à des événements Ironman (course), mais il ne semble pas malveillant en soi.

2/ Vérification mis à jour Chrome et Firefox

Google Chrome à jour



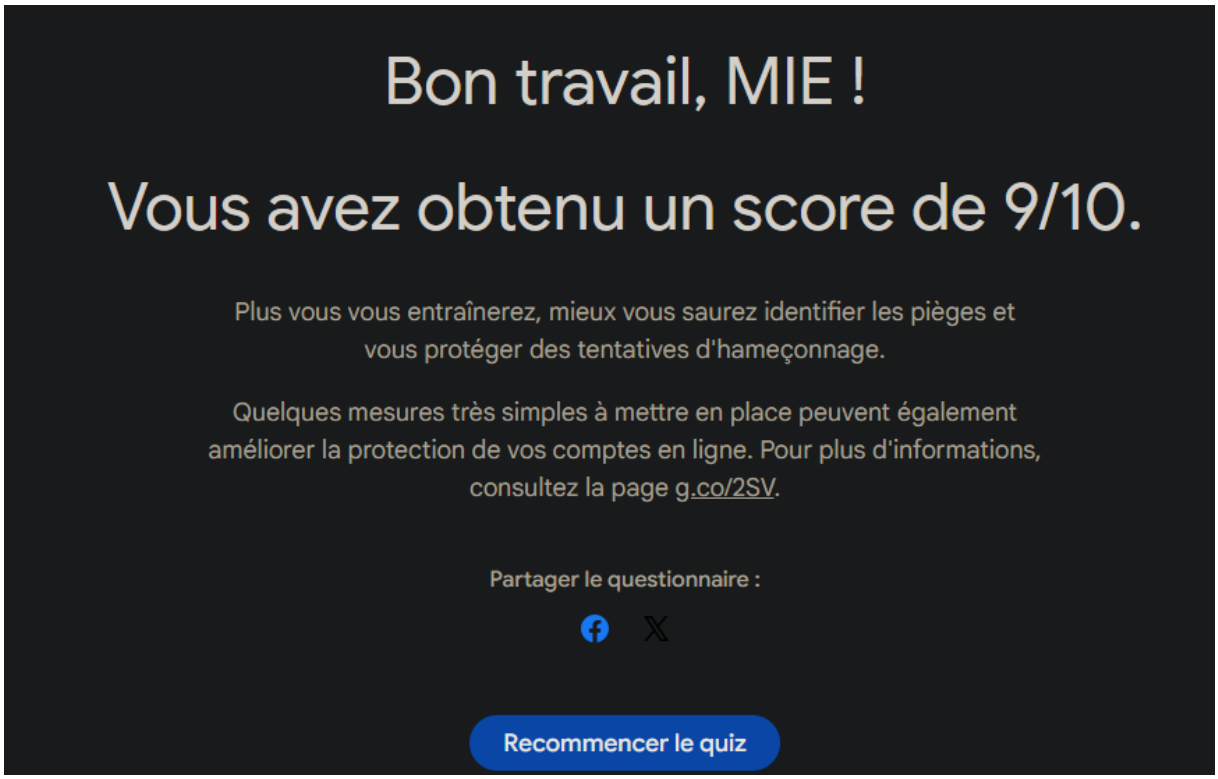
Mozilla Firefox à jour



4 - Éviter le spam et le phishing

Objectif : Reconnaître plus facilement les messages frauduleux

1/ Quizz Spam et Phishing



5 - Comment éviter les logiciels malveillants

Objectif : sécuriser votre ordinateur et identifier les liens suspects

3/ Indicateur de sécurité et le rapport d'analyse de l'outil Google Transparency Report ou Google Transparence des Informations

Site n°1

○ Indicateur de sécurité : HTTPS

○ Analyse Google : Aucun contenu suspect

Site n°2

○ Indicateur de sécurité : Sécurisé

○ Analyse Google : Aucun contenu suspect

Site n°3

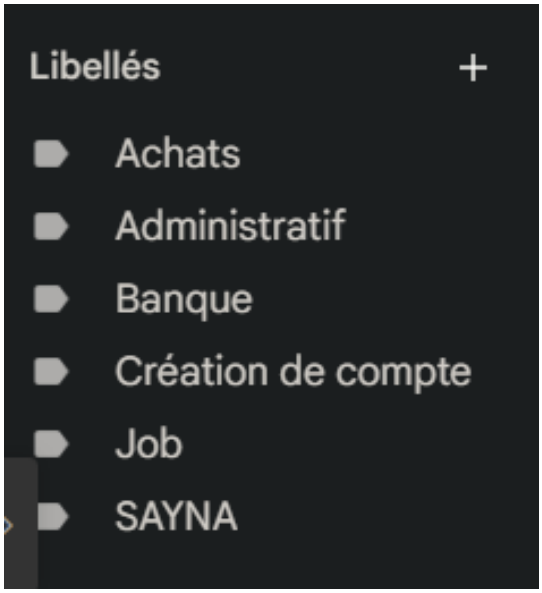
○ Indicateur de sécurité : Sécurisé

○ Analyse Google : analyse trop générale

6 - Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

1/ Création d'un registre des achats



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

1/ Réglage des paramètres de confidentialité pour Facebook

Réglage effectué

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

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

Voici quelques exercices et méthodes pratiques

Vérification sur un PC Windows :

Exercice 1 : Exécuter une analyse antivirus complète

- Étape 1 : Ouvrez votre antivirus (Windows Defender ou un autre antivirus installé).

- Étape 2: Lancez une analyse complète du système.

- Étape 3 : Attendez que l'analyse se termine et suivez les recommandations (quarantaine ou suppression des fichiers infectés).

Cela permet de vérifier si des fichiers malveillants sont présents et les éliminer.

Exercice 2 : Vérification des programmes au démarrage

- Étape 1 : Appuyez sur Ctrl + Shift + Esc pour ouvrir le Gestionnaire des tâches.

- Étape 2 : Allez dans l'onglet Démarrage.

- Étape 3 : Désactivez les programmes suspects ou inconnus.

- Étape 4 : Redémarrez votre ordinateur.

Cela permet d'empêcher les virus de se lancer automatiquement au démarrage.

Vérification sur un Mac :

Exercice 1 : Utilisation de l'antivirus intégré (ou un antivirus tiers)

- Étape 1: Si vous avez un antivirus tiers installé (par exemple, Malwarebytes), ouvrez-le et effectuez une analyse complète.

- Étape 2 : Si vous n'avez pas d'antivirus, vous pouvez installer Malwarebytes (ou un autre) pour analyser les fichiers potentiellement infectés.

Un antivirus fiable peut détecter et éliminer les malwares qui pourraient infecter votre Mac.

Exercice 2 : Vérification des éléments de démarrage

- Étape 1 : Allez dans Préférences Système > Utilisateurs et groupes.

- Étape 2 : Cliquez sur Éléments de connexion.

- Étape 3: Désactivez les éléments qui vous semblent suspects ou inconnus.

Cela empêche les applications malveillantes de se lancer automatiquement.

Vérification sur un appareil Android :

Exercice 1 : Exécuter un scan avec un antivirus mobile

- Étape 1 : Téléchargez une application antivirus fiable depuis Google Play (par exemple, Avast, Bitdefender, ou Malwarebytes).

- Étape 2: Lancez l'application et effectuez une analyse complète de l'appareil.

- Étape 3 : Supprimez les menaces détectées.

Cela permet de détecter et supprimer les malwares sur Android.

Exercice 2 : Vérifier les applications installées

- Étape 1 : Allez dans Paramètres > Applications.

- Étape 2: Parcourez la liste des applications installées et désinstallez celles que vous ne reconnaissez pas ou que vous n'avez pas installées.

Cela permet de retirer les applications suspectes qui pourraient être malveillantes.

Vérification sur un appareil iOS (iPhone/iPad) :

Exercice 1 : Vérifier les applications installées

- Étape 1 : Allez dans Réglages > Général> Stockage iPhone.

- Étape 2 : Parcourez la liste des applications et désinstallez celles qui semblent suspectes.

Les applications malveillantes peuvent parfois se cacher dans cette liste.

Exercice 2 : Vérifier les profils de configuration

- Étape 1 : Allez dans Réglages > Général > Profils.

- Étape 2 : Supprimez tous les profils de configuration que vous ne reconnaissez pas.

Certains profils peuvent être utilisés pour installer des logiciels malveillants ou pour contourner les règles de sécurité d'iOS.

2/ Exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé.

Sur un PC Windows :

Antivirus à installer : Windows Defender (intégré) ou un antivirus tiers (ex: Avast, Bitdefender, Kaspersky)

Antimalware à installer : Malwarebytes

Étape 1 : Installer un antivirus (ex. Windows Defender ou Avast)

Windows Defender (intégré) :

- Ouvrir les paramètres de Windows : Cliquez sur le menu Démarrer, puis sur l'icône Paramètres.
- Accédez à Mise à jour et sécurité > Sécurité Windows.
- Sous la section Protection contre les virus et menaces, vérifiez que Windows Defender Antivirus est activé. Si ce n'est pas le cas, activez-le.
- Lancez une analyse rapide ou complète en cliquant sur Analyse rapide ou Analyse complète.

Étape 2 : Installer un antimalware (Malwarebytes)

- Allez sur le site officiel de Malwarebytes : www.malwarebytes.com.
- Téléchargez la version gratuite ou payante de Malwarebytes.
- Ouvrez le fichier d'installation et suivez les instructions pour installer l'application.
- Une fois installé, ouvrez Malwarebytes et cliquez sur Analyser.

- Choisissez une analyse complète pour vérifier la présence de malwares sur votre système.

-Si des menaces sont détectées, choisissez de les mettre en quarantaine ou de les supprimer.

Sur un Mac :

Antivirus à installer : Malwarebytes, Bitdefender, Norton

Antimalware à installer : Malwarebytes

Étape 1 : Installer un antivirus (ex. Malwarebytes ou Bitdefender)

- Ouvrez Safari et allez sur le site officiel de Malwarebytes ou Bitdefender.

Malwarebytes : www.malwarebytes.com.

Bitdefender : www.bitdefender.com.

- Téléchargez la version macOS du programme antivirus.
- Ouvrez le fichier .dmg téléchargé et suivez les instructions pour installer l'antivirus.
- Une fois installé, ouvrez l'application et effectuez une analyse complète de votre Mac.
-

Étape 2 : Utiliser l'antimalware (Malwarebytes)

- Téléchargez et installez Malwarebytes depuis le site officiel si vous ne l'avez pas déjà installé.
- Ouvrez l'application Malwarebytes et choisissez l'option d'analyse complète.

- Si des malwares sont détectés, cliquez sur Supprimer ou Mettre en quarantaine les menaces trouvées.

Sur un appareil Android :

Antivirus à installer : Avast Mobile Security, Bitdefender Mobile Security

Antimalware à installer : Malwarebytes for Android

Étape 1 : Installer un antivirus (ex. Avast Mobile Security)

- Ouvrez le Google Play Store.
- Recherchez Avast Mobile Security ou un autre antivirus mobile comme Bitdefender Mobile Security.
- Cliquez sur Installer et attendez que l'installation soit terminée.
- Ouvrez l'application et effectuez une analyse rapide ou complète de votre appareil.

Étape 2 : Installer et utiliser Malwarebytes

- Allez sur le Google Play Store.
- Recherchez Malwarebytes pour Android.
- Installez l'application et ouvrez-la.
- Cliquez sur Analyser pour effectuer un scan complet de votre appareil à la recherche de malwares.

- Si des menaces sont détectées, vous pouvez les supprimer ou les mettre en quarantaine.

Sur un iPhone/iPad (iOS) :

Remarque : iOS est un système très sécurisé, et les antivirus classiques ne sont pas nécessaires. Cependant, des applications de protection comme Malwarebytes ou Lookout peuvent aider à détecter des menaces potentielles, mais leur fonction est limitée par les restrictions d'iOS.

Étape 1 : Installer Malwarebytes ou Lookout

- Ouvrez l'App Store.
- Recherchez Malwarebytes ou Lookout.
- Téléchargez et installez l'application.
- Une fois installée, ouvrez l'application et suivez les instructions pour scanner votre appareil à la recherche de menaces ou de vulnérabilités.

Note : L'analyse d'iOS est souvent limitée à la recherche de comportements suspects ou de vulnérabilités.