Parcours : DISCOVERY

Module : Naviguer en toute sécurité

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

Sommaire

1 - Introduction à la sécurité sur Internet

1/ En naviguant sur le web, voici trois articles qui parlent de sécurité sur internet. Voici le nom du site et de l'article.

● Article 1 = LA JAUNE & LA ROUGE – Sécurité et liberté sur l'internet

● Article 2 = kapersky - Sécurité Internet : Qu'est-ce que c'est et comment vous protéger en ligne ?

● Article 3 = CAIRN - L'informatique et sa sécurité

2 - Créer des mots de passe forts

1/ Dans cet exercice, nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Ce gestionnaire prend la forme d'une application web, accessible sur tous supports (PC, Mac, mobile). Il est simple à prendre en main et propose un niveau de sécurité optimal. Suis les étapes suivantes.
Crée un compte en remplissant le formulaire. Un conseil, on te demande de choisir un mot de passe maître. Pour rappel, ce mot de passe sera unique et te permettrad'accéder à tous tes comptes. Choisis donc un mot de passe avec un niveau de sécurité élevé et assure-toi de pouvoir le retrouver

○ Tu peux également générer un mot de passe maître, mais pense à l'écrire dans un endroit sûr pour pouvoir l'utiliser lorsque tu en as besoin

● Une fois la création du compte effectuée, tu arrives sur une page de validation qui propose le téléchargement de l'extension sur ton navigateur. Lance l'installation en effectuant un clic sur le bouton prévu à cet effet

3 - Fonctionnalité de sécurité de votre navigateur

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

● www.morvel.com

● www.fessebook.com

● www.instagam.com

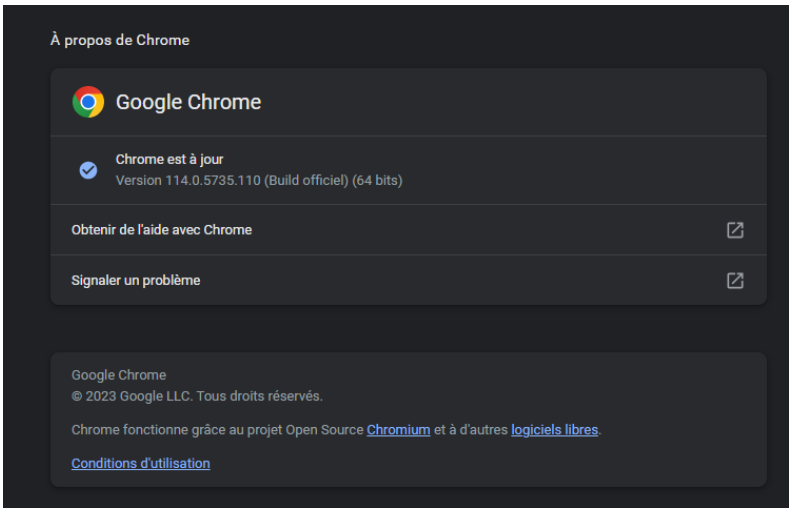
2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour.

● Pour Chrome

○ Ouvre le menu du navigateur et accède aux "Paramètres"

○ Clic sur la rubrique "A propose de Chrome"

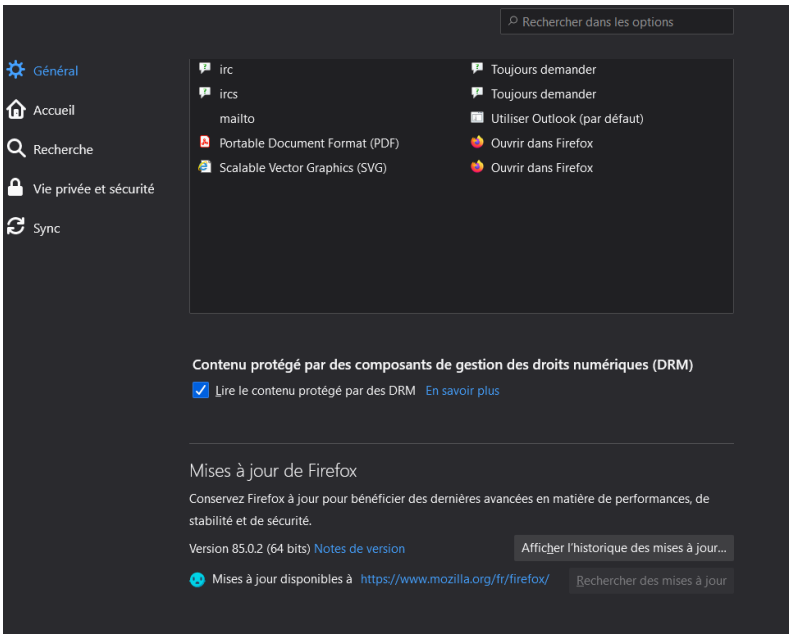
○ Si tu constates le message "Chrome est à jour", c'est Ok



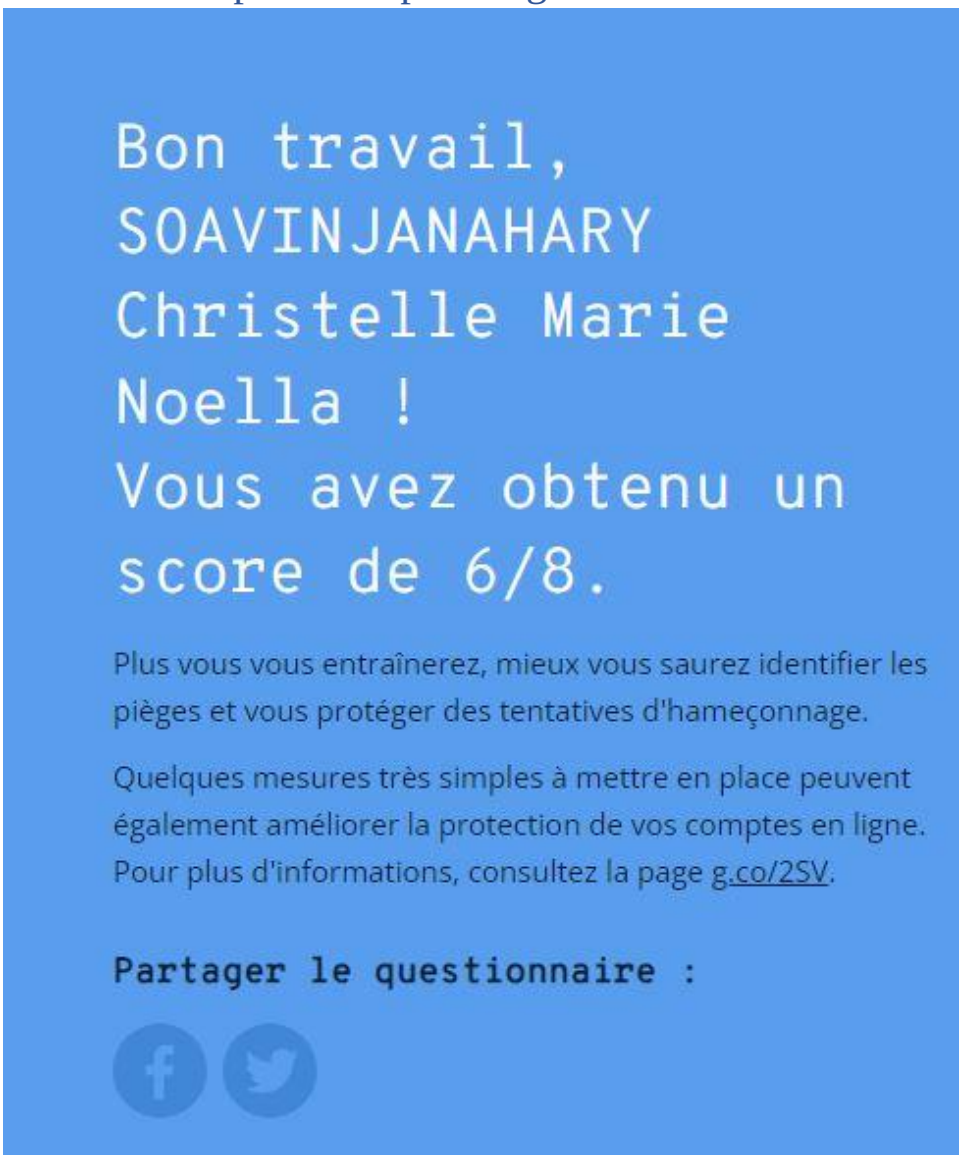
- Pour Firefox

○ Ouvre le menu du navigateur et accède aux “Paramètres”

○ Dans la rubrique “Général”, fais défiler jusqu’à voir la section “Mise à jour de Firefox (astuce : tu peux également saisir dans la barre de recherche “mises à jour” pour tomber directement dessus



4 - Éviter le spam et le phishing



5 - Comment éviter les logiciels malveillants

Site n°1

○ Indicateur de sécurité avec un cadenas

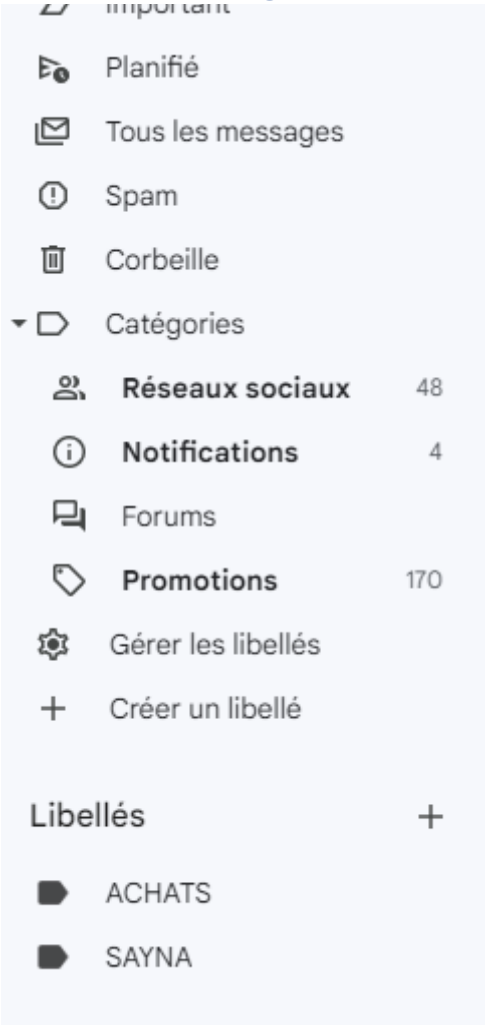
● Site n°2

○ Indicateur de sécurité avec un cadenas

Site n°3

○ site non sécurisé

6 - Achats en ligne sécurisés



7 - Comprendre le suivi du navigateur

Exercice : Gestion des cookies et utilisation de la navigation privée

Commencez par expliquer aux participants ce qu'est un cookie et pourquoi il est important de gérer leur utilisation. Expliquez que les cookies sont de petits fichiers texte stockés sur l'ordinateur par les sites Web visités et qu'ils peuvent être utilisés à des fins de suivi, de personnalisation de contenu, etc.

Demandez aux participants d'ouvrir leur navigateur Internet (par exemple, Google Chrome). Expliquer les différentes options de gestion des cookies disponibles dans leur navigateur. Demander aux participants de passer en revue les différents paramètres de gestion des cookies dans leur navigateur. Expliquez ensuite ce qu'est la navigation privée. Demander aux participants d'ouvrir un nouvel onglet. Encourager les participants à explorer différents sites Web en utilisant la fenêtre de navigation privée. Discutez des cas d'utilisation appropriés pour la navigation privée. Récapitulez les points clés.

8 - Principes de base de la confidentialité des médias sociaux

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

1/Exercice : Analyse comparative de la sécurité des appareils

Objectif : Évaluer la sécurité des différents appareils utilisés.

Instructions :

Sélectionnez quatre appareils couramment utilisés, tels que 2 ordinateur portable, un smartphone et une tablette. assurez-vous que les appareils ont des niveaux de sécurité différents.

Définissez les critères de sécurité pertinents à évaluer, par exemple : a. Niveau de cryptage des données b. Mesures de protection contre les logiciels malveillants c. Possibilité de verrouillage biométrique (empreinte digitale, reconnaissance faciale, etc.) d. Mises à jour régulières du système d'exploitation e. Options de sauvegarde des données f. Politiques de confidentialité et de partage des données

Créez un tableau comparatif avec les critères de sécurité en colonnes et les appareils en lignes.

Recherchez des informations sur chaque appareil et remplissez le tableau avec les détails correspondants à chaque critère de sécurité.

Analysez les résultats et déterminez lesquels des appareils semblent offrir le niveau de sécurité le plus élevé.

2/Exercice pour installer et utiliser un antivirus et antimalware en fonction de l’appareil utilisé :

Instructions :

Avec un ordinateur fonctionnant sous Windows (version de votre choix), rechercher et sélectionner un antivirus avec antimalware de confiance. Il existe de nombreuses options disponibles, telles qu'Avast, AVG, Norton, McAfee, etc. Choisissez celle qui vous convient le mieux.

Rendez-vous sur le site Web officiel de l'antivirus choisi et télécharger

Une fois le téléchargement terminé,

Suivez attentivement les instructions

Ouvrez l'interface de l'antivirus en cliquant sur son icône et recherchez l'option de mise à jour

Une fois les mises à jour effectuées, recherchez une option de scan ou d'analyse

Laissez l'antivirus terminer l'analyse. Cela peut prendre un certain temps, en fonction de la

Une fois l'analyse faite ;

configurez votre antivirus .