Parcours : DISCOVERY

Module :Naviguer en toute sécurité

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

Réalisée par : RAJANEVASON Zarainarivo Marie Floriat URL du projet 1 :
https://github.com/Zarajosiane/SAYNA-CULTUREG-PROJET

0.1 Introduction à la sécurité sur Internet

Dans ce projet, on demande de déposé tout mes travaux sur mon compte Github. Ensuite, de s'entrainer dans sur les bases de l'Internet. L'objectif de cet projet est de découvrir la sécurité sur internet.

1. En naviguant sur le web, je consulte ces trois articles qui parlent de sécurité sur internet, avec la vérification de la sources des informations et je vais essayer de consulter des articles récents pour que les informations soient à jour :

   - Article1 : avast-malware
   - kaspersky-mac-security
   - wired-nsa-rob-joyce-chatgpt-security

0.2 Créer des mots de passe forts

L'objectif est utiliser un gestionnaire de mot de passe LastPass

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.

0.3 Fonctionnalité de sécurité de votre navigateur

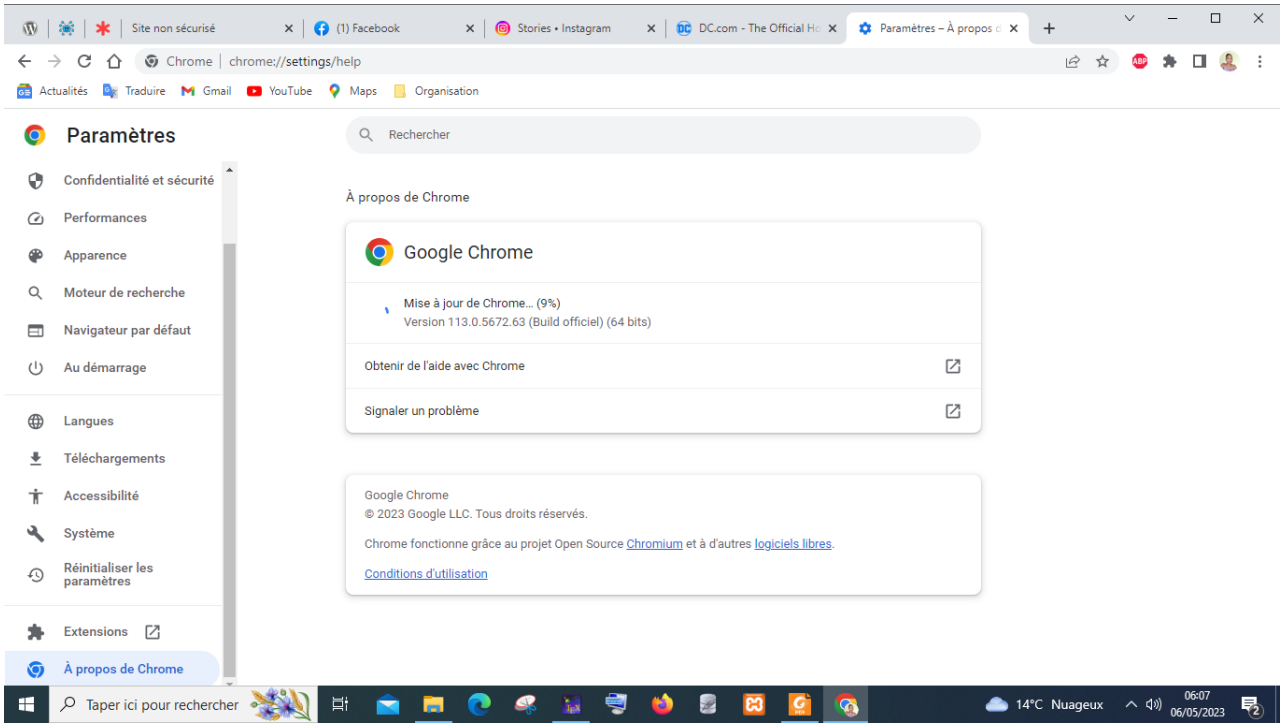
Objectif est d'identifier les éléments à observer pour naviguer sur le web en toute sécurité.

0.3.1 Identification des adresses internet qui me semblent provenir de sites web malveillants

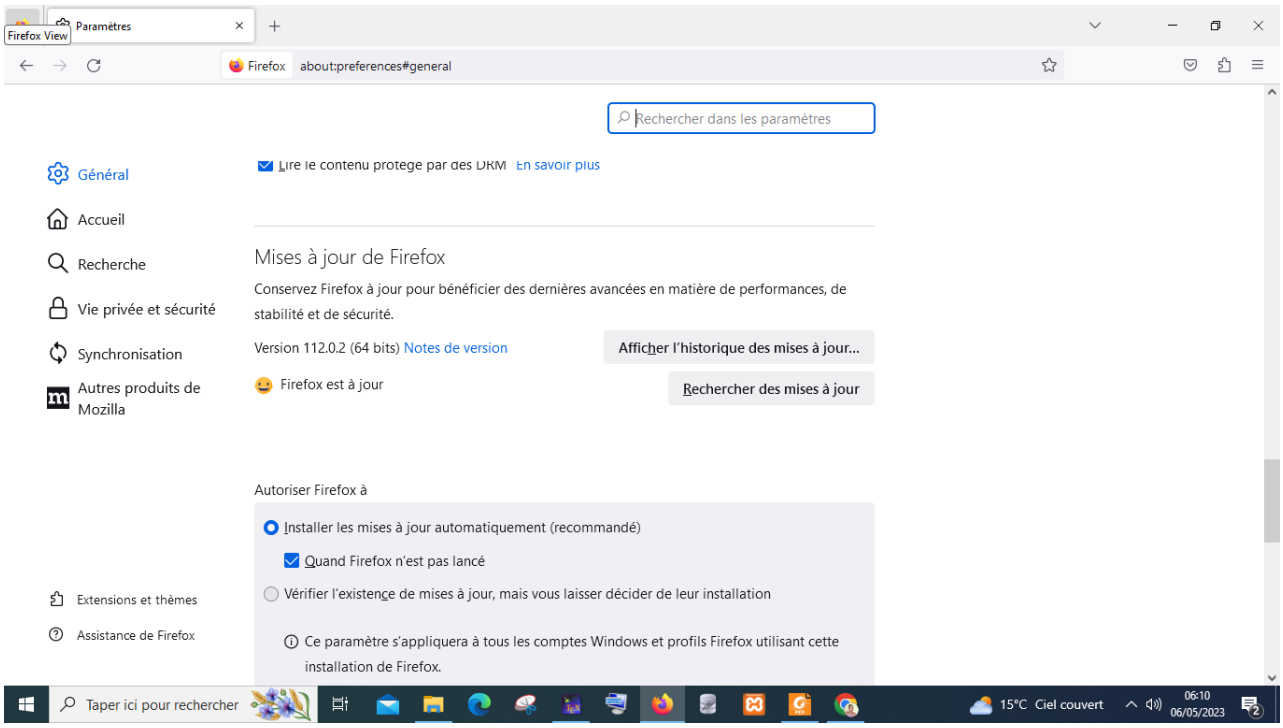
Les seuls sites en sécurité sont des `www.morvel.com`, `www.facebook.com`, `www.instagram.com` , et les autres `www.dccomics.com`, `www.ironman.com`.

0.3.2 Vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes.

Pour Chrome



Pour Firefox



0.4 Éviter le spam et le phishing

L'objectif pour éviter spam et pushing est reconnaître plus facilement les messages frauduleux.

0.4.1 On va exercer ma capacité à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan

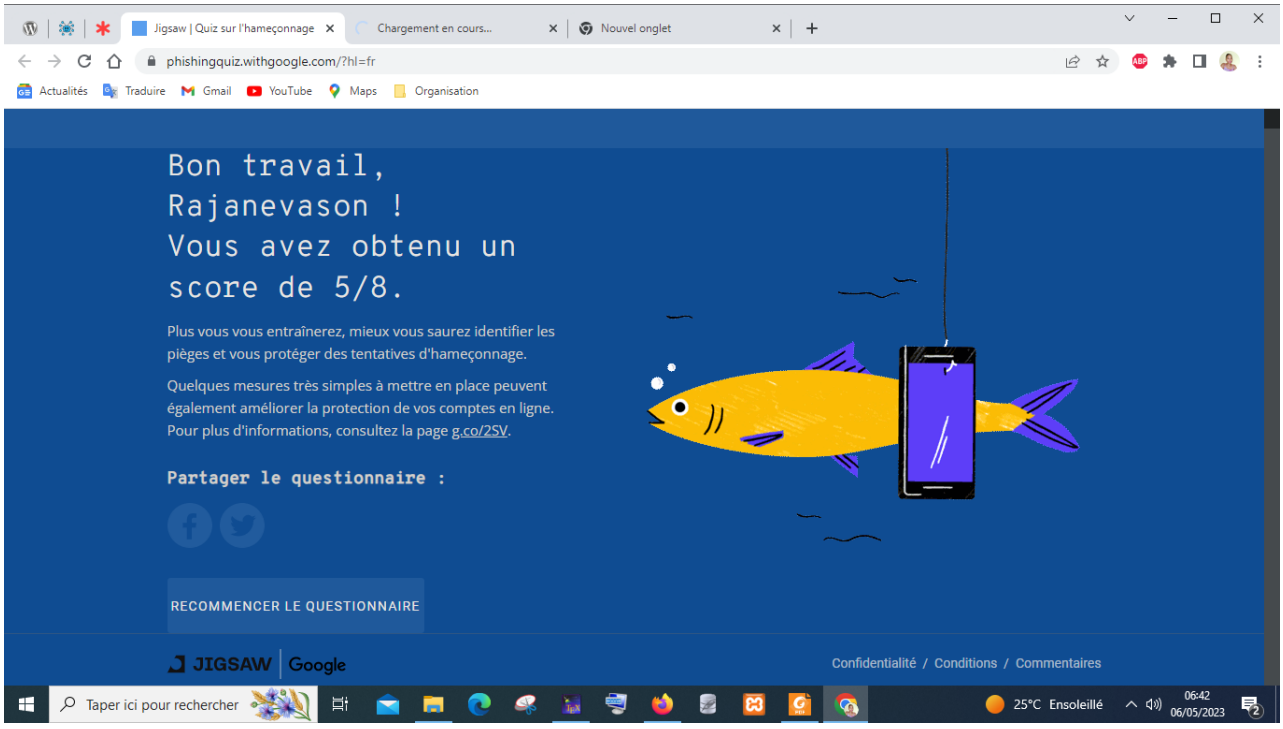
Pour ce faire accède au lien suivant et suis les étapes qui y sont décrites : Spam et Phishing. Commençons par cet e-mail Google Docs.

- **Étape 1 :** vérifiez bien les URL des liens en passant la souris ou en appuyant de manière prolongée dessus, et examinez les adresses e-mail. Ne vous inquiétez pas, aucun des liens ne fonctionne... Nous ne voudrions pas vous rediriger vers des pages louches !

  Rrésultat : C'est exact ! Il s'agit d'un e-mail d'hameçonnage.

  Vous avez sans doute remarqué que l'URL ressemble à la véritable adresse. Prenez garde aux liens hypertextes et aux pièces jointes que vous ouvrez à partir des e-mails, car ils peuvent rediriger vers des sites Web frauduleux qui vous invitent à saisir des informations sensibles.

  Résultat : Voici le résultat de mon exercice :



0.5 Comment éviter les logiciels malveillants

Objectif : sécuriser votre ordinateur et identifier les liens suspects

0.5.1 Indicateur de sécurité

Lors de la navigation sur le web, il arrive d'avoir des doutes sur la sécurité de certains sites. Comme j'ai a pu le voir précédemment, le premier de niveau de vigilance à avoir se trouve dans la barre d'adresse des navigateurs web. La plupart affichent des indicateurs de sécurité pour donner une information sur la protection d'un site internet.

Lorsque le doute persiste je peux m'appuyer sur un outil proposé par Google : Google-Transparency Report (en anglais) ou Google Transparence des Informations (en français). Afin d'améliorer ma lecture de la sécurité sur internet, je vais devoir analyser les informations de plusieurs sites. Pour chaque site je devrais préciser l'indicateur de sécurité et le rapport d'analyse de l'outil Google. Il te suffit d'accéder aux liens proposés ci-dessous pour observer l'indicateur de sécurité et de copier-coller l'URL du site dans l'outil Google.

1. Site 1 :

   Indicateur de sécurité :HTTPS

   Analyse Google : Aucun contenu suspect

2. Site 2 :

   Indicateur de sécurité : Not secure

   Analyse Google :Aucun contenu suspect

3. Site 2 :

   Indicateur de sécurité :Not secure

   Analyse Google :Vérifier un URL en particulier.

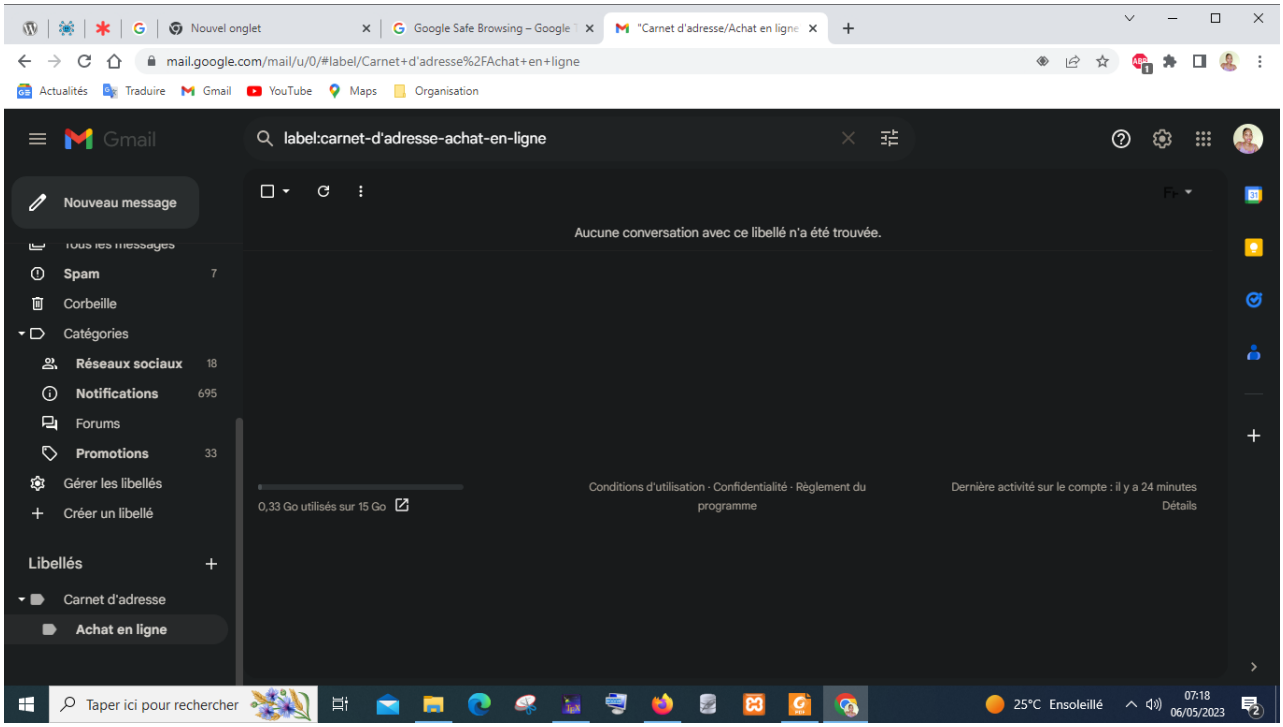
0.6 Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

0.6.1 Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le bilan de tes dépenses du mois.Deux possibilités s'offrent à toi pour organiser ce registre :

Créer un dossier sur ta messagerie électronique

Créer un dossier sur ton espace de stockage personnel (en local ou sur le cloud)



0.7 Comprendre le suivi du navigateur

Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée.

0.8 Principes de base de la confidentialité des médias sociaux

Objectif : Régler les paramètres de confidentialité de Facebook.

0.8.1 Plus tôt dans le cours (Internet de base) j'ai déjà été amené à utiliser ce réseau social en partageant une publication. Dans cet exercice on va me montrer le réglage des paramètres de confidentialité pour Facebook. Suis les étapes suivantes.

0.9 Que faire si votre ordinateur est infecté par un virus

0.9.1 Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé ?

Voici un exercice simple pour vérifier la sécurité de votre ordinateur :

1. Ouvrez un navigateur web et rendez-vous sur le site https ://www.grc.com/shieldsup pour tester les ports ouverts de votre ordinateur. Cliquez sur le bouton "Proceed" pour lancer le test.

2. Analysez les résultats du test et vérifiez que tous les ports sont "Stealthed" (cachés) ou "Closed" (fermés). Si vous trouvez un port "Open" (ouvert), cela peut indiquer une faille de sécurité.

3. Téléchargez et installez un logiciel antivirus gratuit comme Avast, AVG ou Bitdefender. Scannez votre ordinateur avec le logiciel pour détecter et supprimer les éventuels virus ou logiciels malveillants.

4. Assurez-vous que votre système d'exploitation et tous les logiciels installés sont à jour avec les dernières mises à jour de sécurité.

5. Vérifiez que votre pare-feu est activé pour empêcher les intrusions non autorisées sur votre ordinateur.

6. Utilisez des mots de passe forts et différents pour chaque compte en ligne que vous possédez. Utilisez un gestionnaire de mots de passe pour faciliter la gestion de vos mots de passe.

7. Évitez de télécharger des fichiers ou des logiciels à partir de sources inconnues ou suspectes. Vérifiez toujours la source avant de télécharger quoi que ce soit.

8. Enfin, utilisez une connexion Internet sécurisée (par exemple, une connexion chiffrée HTTPS) chaque fois que vous utilisez des services en ligne sensibles, tels que la banque en ligne ou le shopping en ligne.

0.9.2 Proposer un exercice pour installer et utiliser un antivirus + antimalware en fonction del'appareil utilisé

Un exercice pour installer et utiliser un antivirus et un antimalware sur votre ordinateur :

1. Tout d'abord, téléchargez un logiciel antivirus et un logiciel antimalware. Il existe de nombreux choix gratuits et payants, tels que Avast, AVG, Malwarebytes, etc.

2. Une fois que vous avez téléchargé les logiciels, installez-les sur votre ordinateur en suivant les instructions fournies.

3. Après l'installation, assurez-vous de mettre à jour les bases de données de virus et de logiciels malveillants pour vous assurer que votre logiciel est à jour et peut détecter les dernières menaces.

4. Planifiez une analyse complète de votre ordinateur. Les logiciels antivirus et antimalware ont des options pour planifier des analyses automatiques à des moments précis. Vous pouvez également effectuer une analyse manuelle à tout moment.

5. Si des menaces sont détectées, suivez les instructions fournies par le logiciel pour les supprimer ou les mettre en quarantaine.

6. Veillez à maintenir votre logiciel antivirus et antimalware à jour et à effectuer régulièrement des analyses pour protéger votre ordinateur des menaces potentielles.

Cet exercice vous permettra de vous familiariser avec l'installation et l'utilisation d'un logiciel antivirus et antimalware pour protéger votre ordinateur contre les menaces de sécurité.