Parcours : DISCOVERY

Module : Naviguer en toute sécurité

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

Tous vos travaux devront être déposés sur votre compte Github

Sommaire

1 - INTRODUCTION A LA SECURITE SUR INTERNET

Objectif : *à la découverte de la sécurité sur internet*

1/ En naviguant sur le web, je consulte trois articles qui parlent de sécurité sur internet.

Voici les articles que vous m'avez suggéré (avec les mots-clés "sécurité sur internet" et "comment être en sécurité sur internet" :

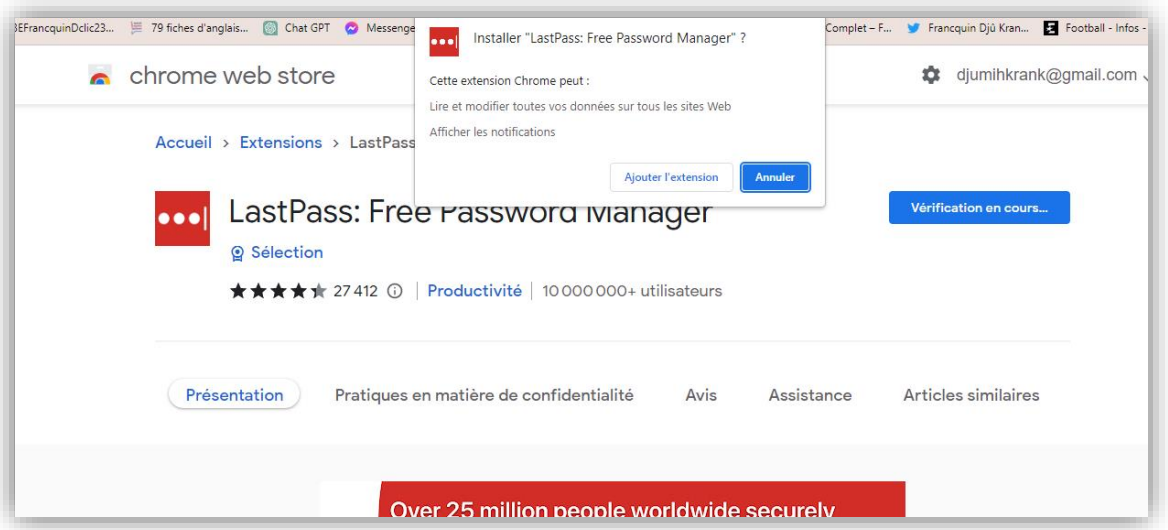
- Article 1 = ANSSI - Dix règles de base
- Article 2 = Economie.gouv - Comment assurer votre sécurité numérique
- Article 3 = Site W - Naviguez en toute sécurité sur Internet
- Article bonus = wikiHow - Comment surfez en sécurité sur internet

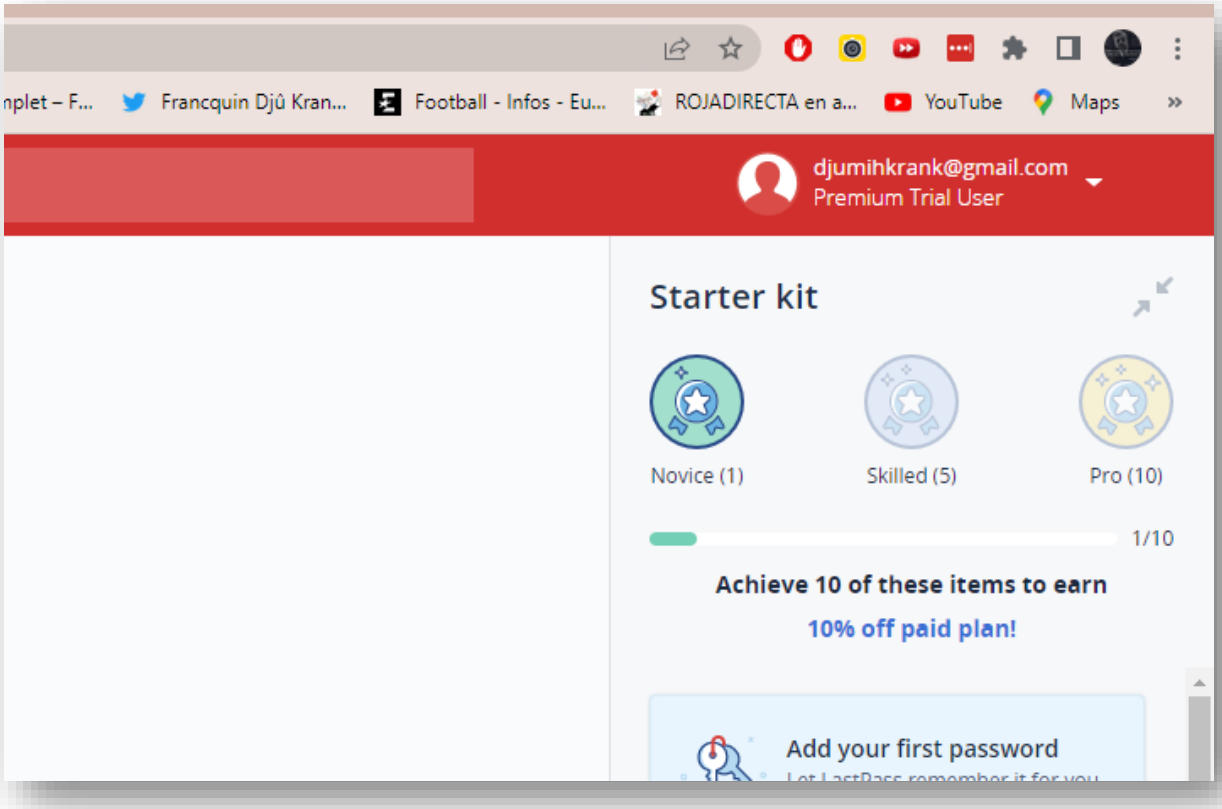
2 - CREER DES MOTS DE PASSE FORTS

Objectif : *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.

- J'accède au site de LastPass et je crée un compte en remplissant le formulaire.
- Une fois la création du compte effectuée, j'arrives sur une page de validation qui propose le téléchargement de l'extension sur mon navigateur. Je lance l'installation en effectuant un clic sur le bouton prévu à cet effet.
- Il me suffit de valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome".





3 - FONCTIONNALITE DE SECURITE DE VOTRE NAVIGATEUR

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

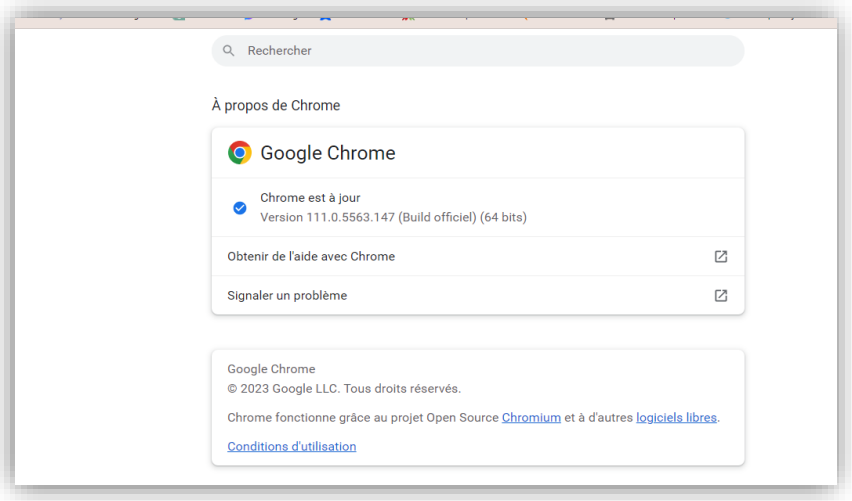
1/ J'identifie les adresses internet qui me semblent provenir de sites web malveillants.

Les sites web qui semblent être malveillants sont :

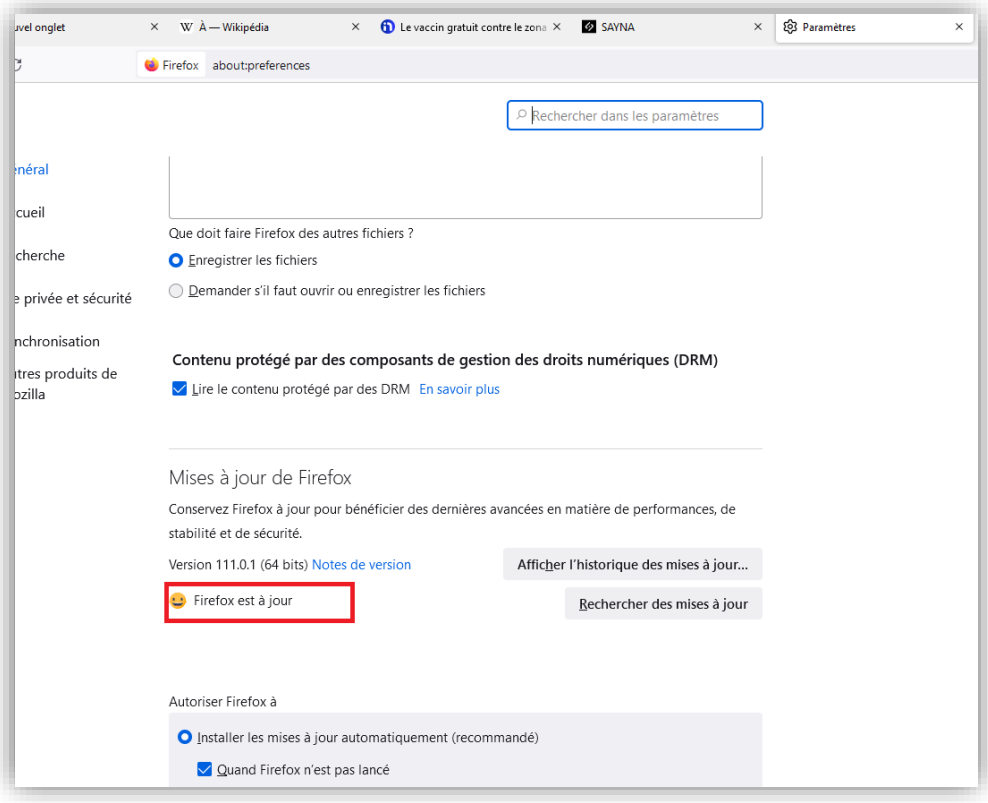
- www.morvel.com , un dérivé de www.marvel.com, le site web officiel de l'univers Marvel.
- www.fessebook.com , un dérivé de www.facebook.com, le plus grand réseau social du monde.
- www.instagam.com , un dérivé de www.instagram.com, un autre réseau social très utilisé.

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 dans notre exemple, sont à jour.
● Pour Chrome, il est à jour.



● Pour Firefox, il est à jour.

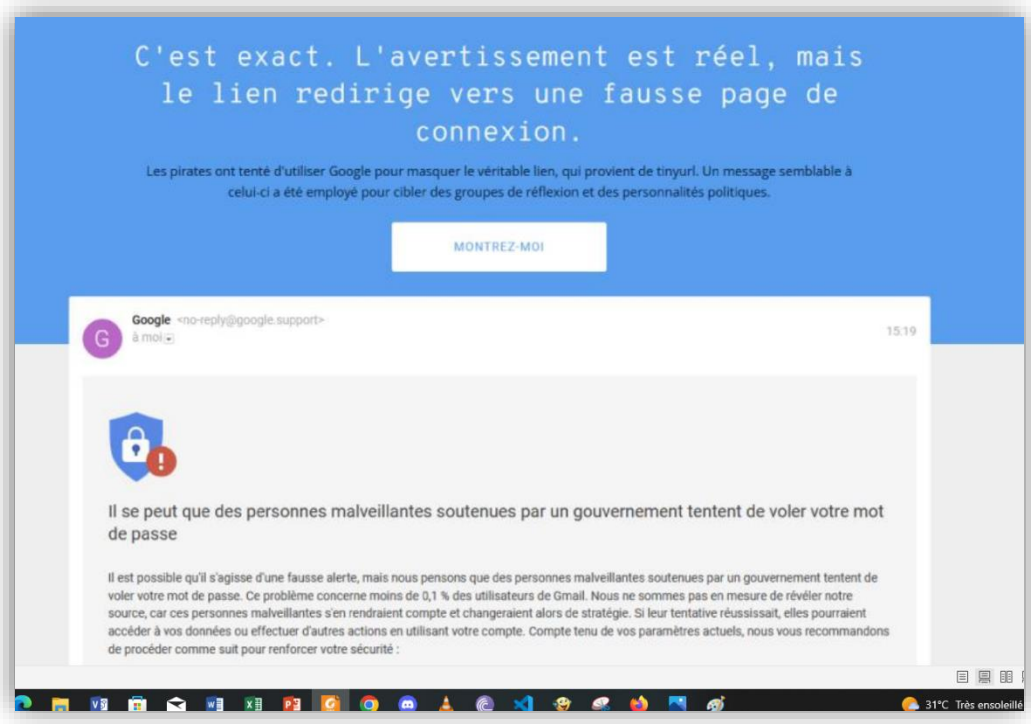


4 - ÉVITER LE SPAM ET LE PHISHING

Objectif : *Reconnaître plus facilement les messages frauduleux*

1/ Dans cet exercice, on va exercer ma capacité à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.

Pour ce faire, j'accède au lien suivant et je suis les étapes qui y sont décrites : Exercice 4 - Spam et Phishing



5 - COMMENT EVITER LES LOGICIELS MALVEILLANTS

Objectif : *sécuriser votre ordinateur et identifier les liens suspects*

3/ Lors de la navigation sur le web, il arrive d'avoir des doutes sur la sécurité de certains sites. Comme j'ai pu le voir précédemment, le premier 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.

L'indicateur de sécurité et le rapport d'analyse de l'outil Google pour chaque site est :

- Site n°1
  - **Indicateur de sécurité**
    - HTTPS

○ **Analyse Google**
■ Aucun contenu suspect

● Site n°2
○ **Indicateur de sécurité**
■ Not secure
○ **Analyse Google**
■ Aucun contenu suspect

● Site n°3
○ **Indicateur de sécurité**
■ Not secure
○ **Analyse Google**

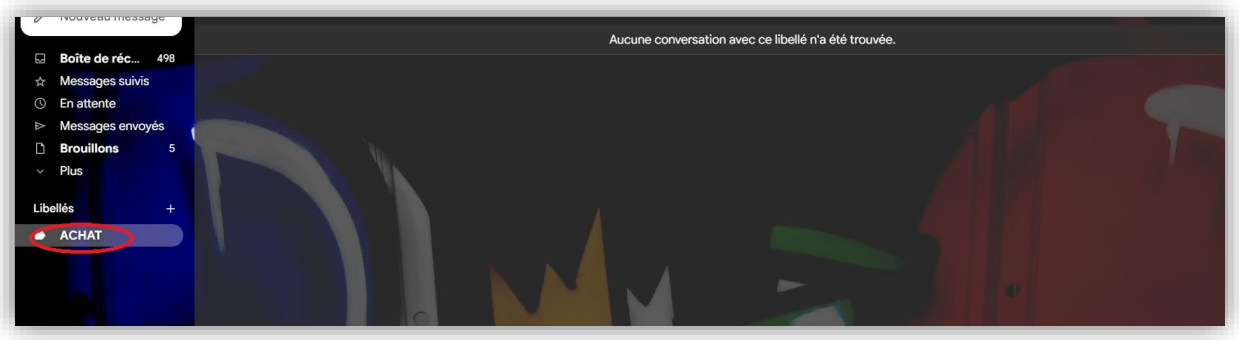
6 - ACHATS EN LIGNE SECURISES
Objectif : *créer un registre des achats effectués sur internet*

1/ Comme j'ai pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à mes achats en ligne. Très pratique lorsqu'on fait face à un litige, un problème sur la commande ou tout simplement pour faire le bilan de nos dépenses du mois.

Deux possibilités pour organiser ce registre :
1. Je crée un dossier sur ma messagerie électronique
2. Je crée un dossier sur mon espace de stockage personnel (en local ou sur le cloud)

La première est la plus pratique à utiliser et la plus facile à mettre en place. Nous prendrons pour exemple la messagerie de Google (les autres messageries fonctionnent sensiblement de la même manière).

Je crée un registre des achats sur ma messagerie électronique.

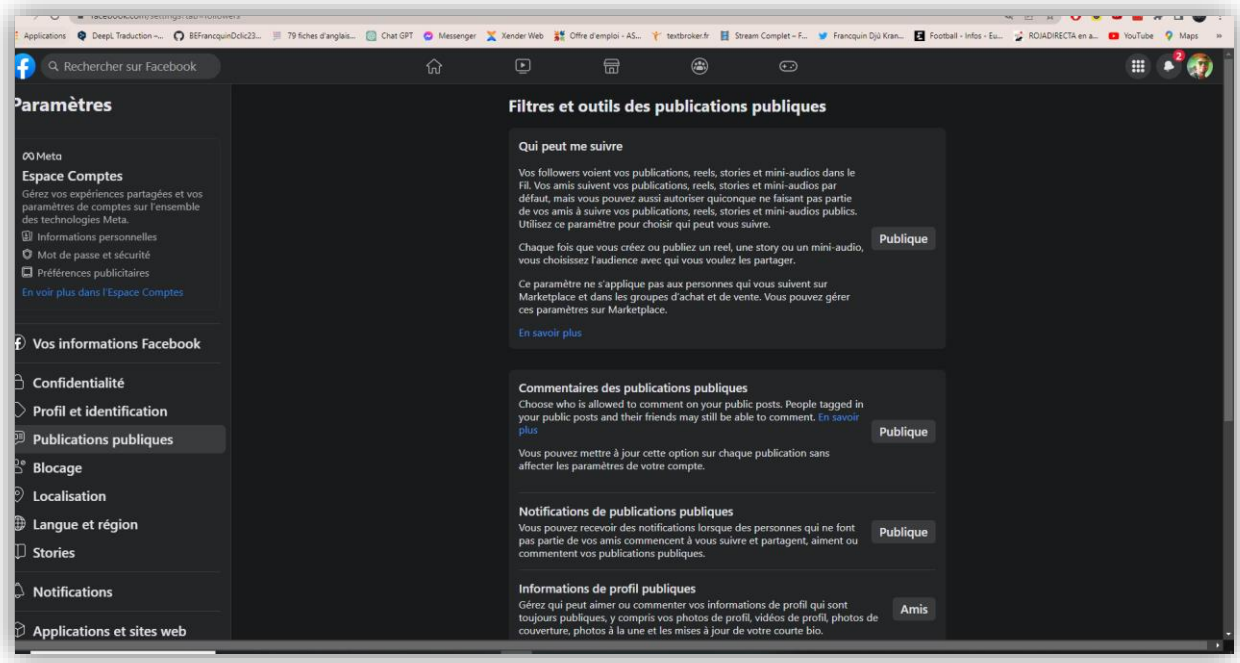


7 - COMPRENDRE LE SUIVI DU NAVIGATEUR
Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée

8 - PRINCIPES DE BASE DE LA CONFIDENTIALITE DES MEDIAS SOCIAUX
Objectif : Régler les paramètres de confidentialité de Facebook

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 te montrer le réglage des paramètres de confidentialité pour Facebook.

● Je me connecte sur mon compte Facebook et je suis les étapes.



Sur les autres médias sociaux, tu retrouveras sensiblement le même type de paramétrage. Maîtrise ton utilisation de ces outils en paramétrant selon tes souhaits.

9 - QUE FAIRE SI VOTRE ORDINATEUR EST INFECTE PAR UN VIRUS

Objectif : **1/ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé ??????? Comment faire ????????**

Pour vérifier la sécurité de votre ordinateur ou de votre appareil, vous pouvez effectuer les exercices suivants :

- Exécutez un scan antivirus régulièrement pour détecter les menaces potentielles.
- Utilisez un mot de passe fort et changez-le régulièrement pour protéger vos comptes en ligne.
- Mettez à jour régulièrement votre navigateur web, et tous vos programmes pour corriger les vulnérabilités de sécurité.
- Évitez de cliquer sur des liens ou des pièces jointes provenant de sources inconnues ou suspectes.
- Sauvegardez régulièrement vos fichiers importants sur un disque dur externe ou sur un service cloud pour éviter de les perdre en cas d'infection par un virus.
- Utilisez un logiciel de cryptage pour protéger vos données sensibles lorsqu'elles sont stockées ou transférées.

Voici quelques étapes que vous pouvez suivre :

- Déconnectez votre ordinateur d'internet pour éviter que le virus ne se propage sur d'autres appareils.
- Exécutez un logiciel antivirus et antimalware pour détecter et éliminer le virus. Veillez à mettre à jour régulièrement votre logiciel antivirus pour protéger votre ordinateur contre les nouvelles menaces.

- Si vous ne pouvez pas éliminer le virus vous-même, demandez l'aide d'un professionnel de la sécurité informatique.

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

Voici un exercice pour installer et utiliser un logiciel antivirus et antimalware :

- Si vous utilisez un PC Windows, téléchargez et installez un logiciel antivirus et antimalware gratuit comme Malwarebytes Anti-Malware ou Avast Antivirus. Si vous utilisez un Mac, vous pouvez utiliser des logiciels comme Malwarebytes pour Mac ou Norton Antivirus.
- Une fois le logiciel installé, exécutez un scan complet de votre système pour détecter les virus et malwares.
- Si des menaces sont détectées, suivez les instructions pour les supprimer.
- Assurez-vous de configurer votre logiciel antivirus pour qu'il se mette à jour automatiquement.
- Utilisez votre logiciel antivirus et antimalware régulièrement pour protéger votre système contre les menaces en ligne.
- Il est important de noter que l'utilisation d'un logiciel antivirus et antimalware ne garantit pas une protection complète contre toutes les menaces en ligne. Il est également important de faire preuve de prudence lors de la navigation sur Internet et de ne pas ouvrir de courriels ou de fichiers suspects.