

Parcours : DISCOVERY

Module : Naviguer en toute sécurité

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

Tokinirina RATSITOMANDIMBY

1- Introduction à la sécurité internet

Objectif : à la découverte de la sécurité sur internet

1/ Trois articles qui parlent de la sécurité sur internet

Article 1 = Kapersky - Sécurité Internet : Qu'est-ce que c'est et comment vous protéger en ligne ?

Article 2= Laposte - 5 conseils pour être en sécurité sur Internet

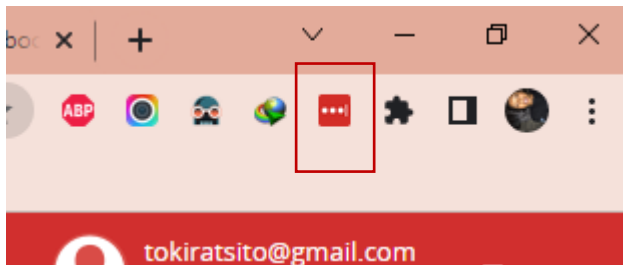
Article 3= Boutique Box internet - L'importance de la sécurité sur Internet

2- Création des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass

1/ Utilisation de gestionnaire de mot de passe nommé LastPass

- Création d'un compte LastPass
- Ajout de l'extension LastPass
- Ajout des sites dans LastPass



3- Fonctionnalité de sécurité de votre navigateur

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

1/ Identification des adresses internet qui me semblent provenir de sites web malveillants. (Case à cocher)

- ☐ www.morvel.com
- www.dccomics.com
- www.ironman.com
- ☐ www.fessebook.com
- ☐ www.instagam.com

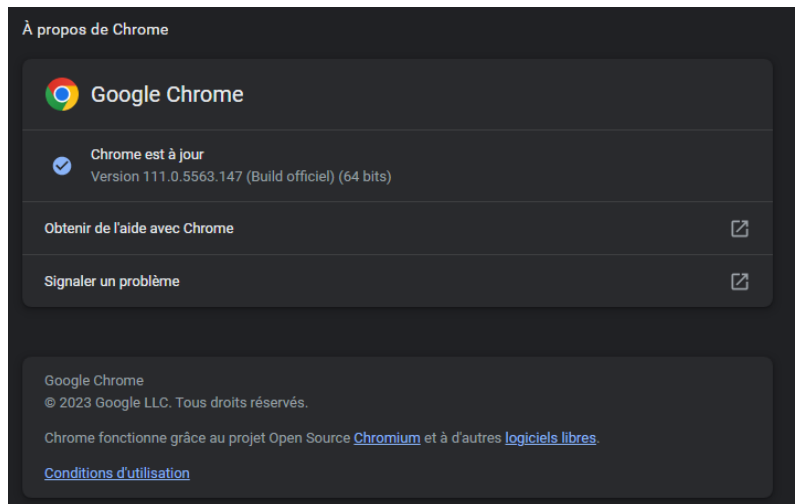
Ceux qui me semblent provenir de sites web malveillants sont : les trois sites avec un rond plein

- www.morvel.com on dirait que c'est le site de Marvel, utilise un mot dérivé et qui ça sonne pareil à Marvel

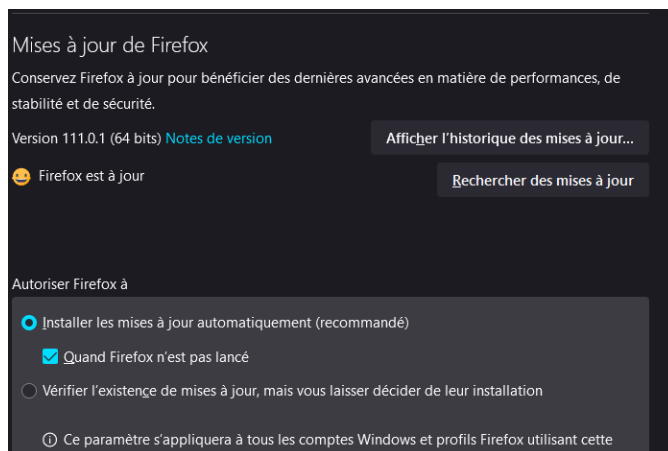
- www.fessebook.com= un dérivé du réseau social www.facebook.com
- www.instagram.com= un dérivé du réseau social www.instagram.com

2/Vérification de la version de Chrome et Firefox si elles sont à jour. Pour ce faire, suis les étapes suivantes.

- Pour Chrome



- Pour Firefox



4- Éviter le spam et le phishing

Objectif : Reconnaître plus facilement les messages frauduleux



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



5- Comment éviter les logiciels malveillants

Objectif : sécuriser votre ordinateur et identifier les liens suspects

3/ Vérification de la sécurité et de la protection d'un site internet

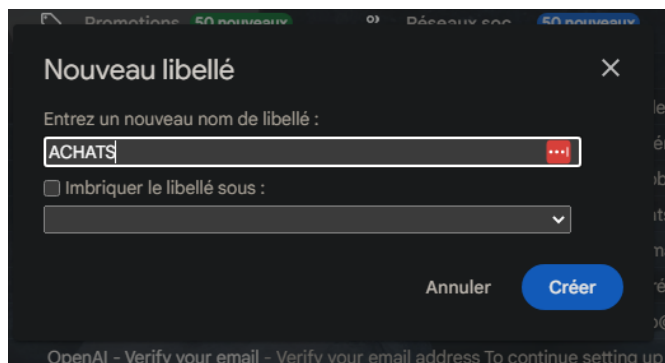
Site	Indicateur de sécurité	Analyse Google
Site 1	HTTPS 	Aucun contenu suspect détecté
Site 2	HTTPS 	Aucun contenu suspect détecté
Site 3	Non sécurisé	Vérifier une URL en particulier

6- Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

1/ Création d'un registre d'achat avec la messagerie de Google

- Accès à ma messagerie électronique
- Sur la page d'accueil de ta messagerie, je trouve sur la gauche les libellés initialement prévus (boîte de réception, messages envoyés, etc.)
- Création d'une rubrique « ACHATS »



- Gestion de l'affichage des libellés

- Un libellé « ACHATS » pour stocker tous tes messages électroniques relatifs aux achats effectués sur internet : confirmation de l'achat, détail de la commande, modalités de livraison

7- Comprendre le suivi du navigateur

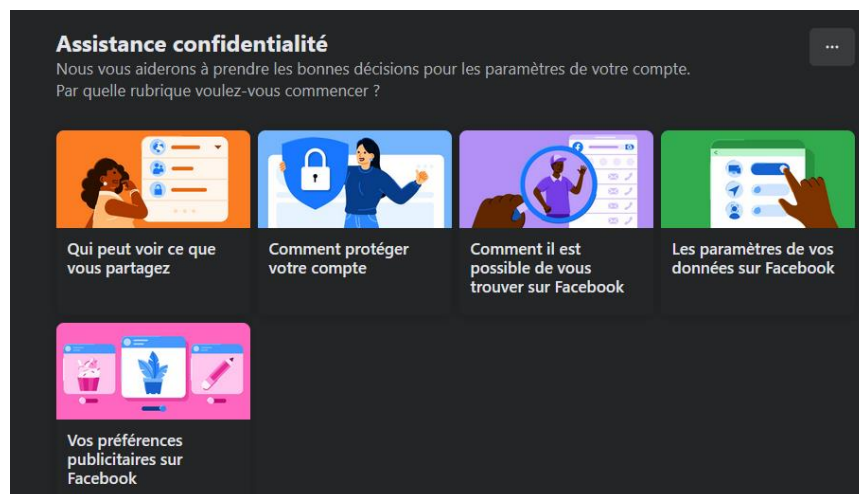
Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée

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

- Connection au compte Facebook
- Aller dans « Paramètres et confidentialité »
- Aller dans l'onglet « Confidentialité » et « Publications publiques »
- Arriver sur les grandes lignes de la confidentialité sur Facebook



- Gérer les filtres et outils des publications publiques

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

Proposition d'exercice

Objectif : Connaître les étapes d'analyse et de suppression des virus sur un ordinateur

- Installer un logiciel antivirus

Voici des exemples d'antivirus

- Bitdefender: <https://shop.journaldugeek.com/antivirus/2/bitdefender>
 - Norton: <https://shop.journaldugeek.com/antivirus/6/norton>
 - Intego: <https://shop.journaldugeek.com/antivirus/3/intego>
 - Avast: <https://shop.journaldugeek.com/go/10383/>
- Lancer une première analyse complète
 - Examiner les menaces découvertes et les actions recommandées
 - Détecter les logiciels malveillants par des logiciels anti-malware