

## 1 - Introduction à la sécurité sur Internet

Objectif : à la découverte de la sécurité sur internet

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

- Article 1 = Boutique box internet - L'importance de la sécurité sur Internet

<https://www.boutique-box-internet.fr/actualites/securite-sur-internet/>

- Article 2 = CNIL - Sécurité : Sécuriser les sites web

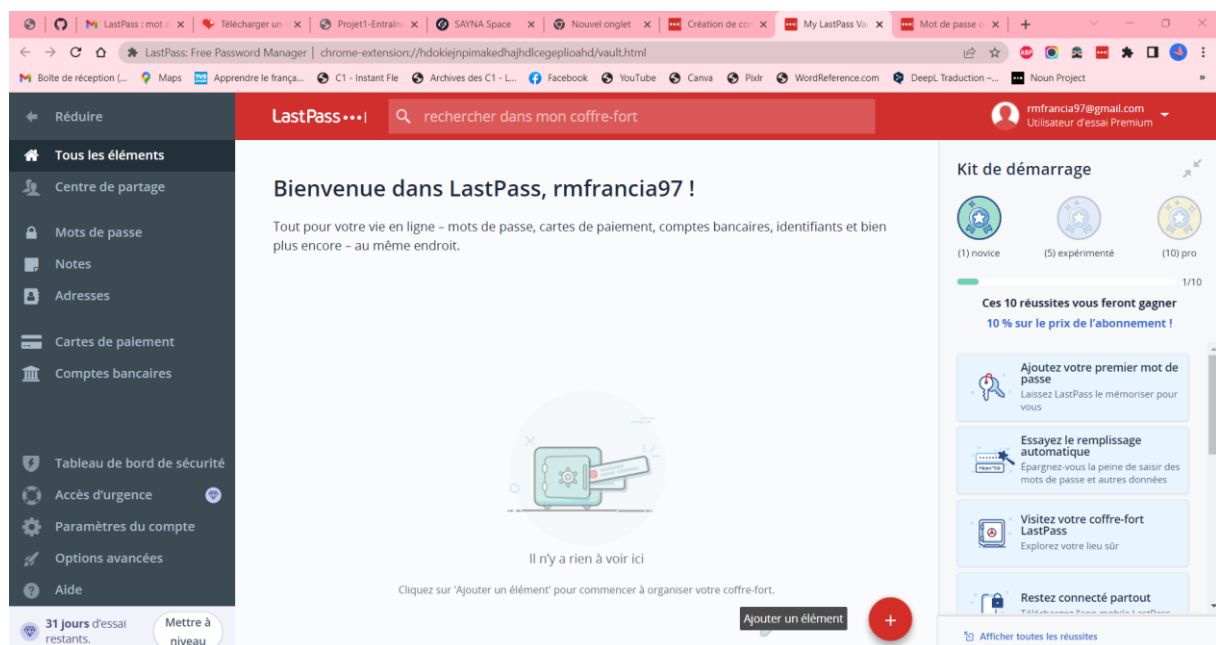
<https://www.cnil.fr/fr/securite-securiser-les-sites-web>

- Article 3 = Le monde informatique - Du code Python compilé utilisé pour du piratage

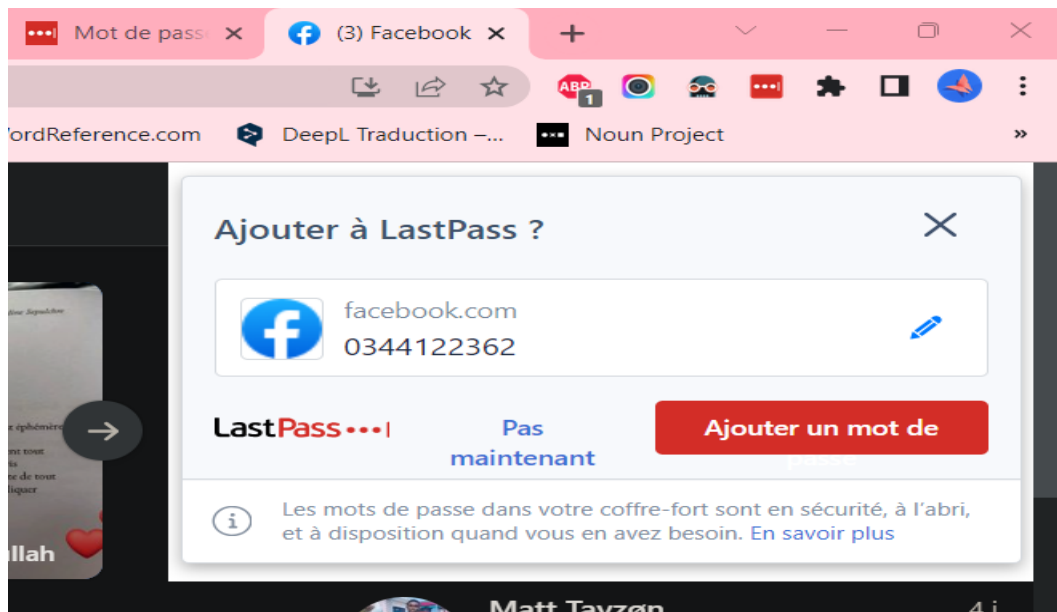
<https://www.lemondeinformatique.fr/actualites/lire-du-code-python-compile-utilise-pour-du-piratage-90612.html>

## 2- Créer des mots de passe forts

1/ Utilisation des gestionnaires de mot de passe LastPass



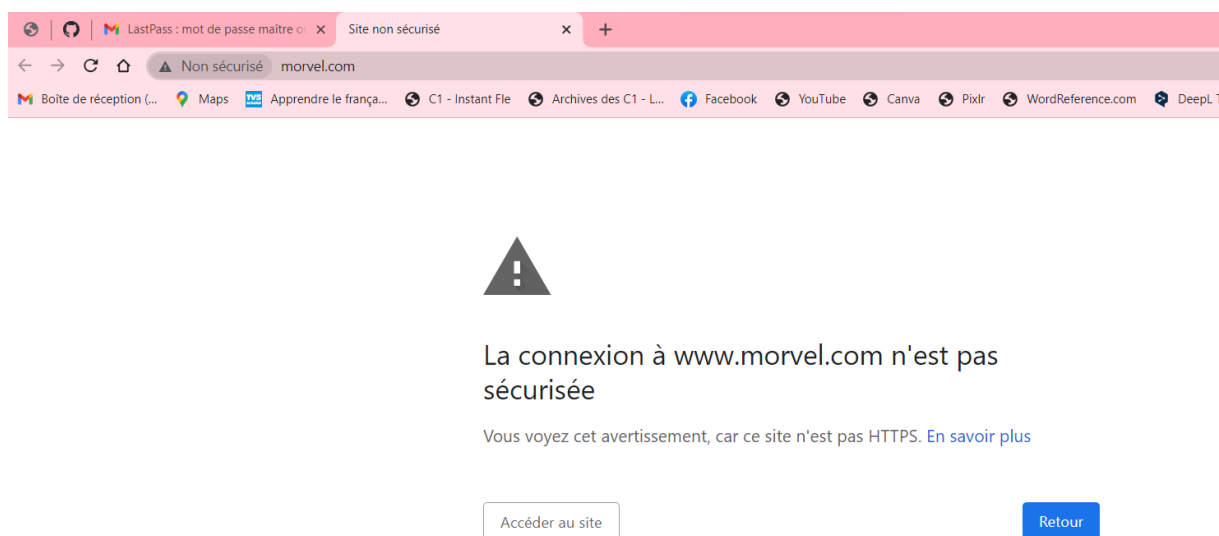
J'ai essayé de se connecter avec mon compte Facebook



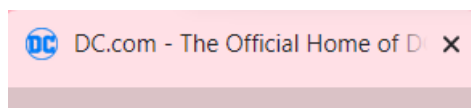
### 3- Fonctionnalité de sécurité de votre navigateur

#### 1/ Identification des sites web malveillants :

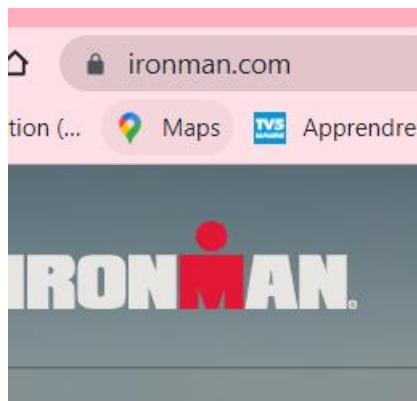
- [www.morvel.com](http://www.morvel.com) : Malveillant car cela ressemble à un dérivé de morvel



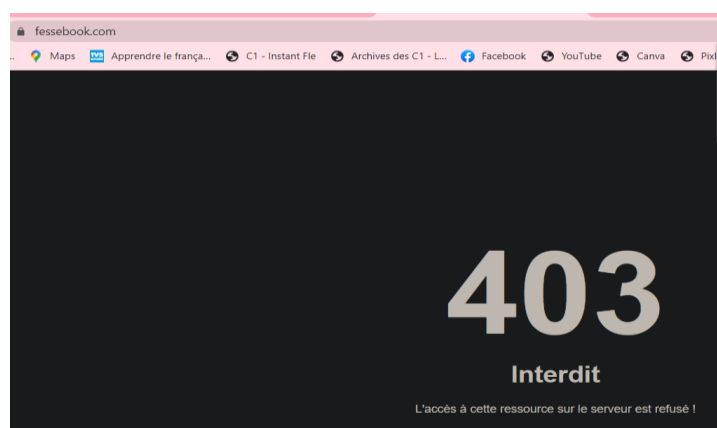
- [www.dccomics.com](http://www.dccomics.com) : semble en sécurité car le nom du domaine a une liaison avec le site généré



- [www.ironman.com](http://www.ironman.com) : le nom de domaine est cohérent aussi avec le contenu du site



- [www.fessebook.com](http://www.fessebook.com) : A la première vue, cet URL semble suspect car cela ressemble à un dérivé de site Facebook

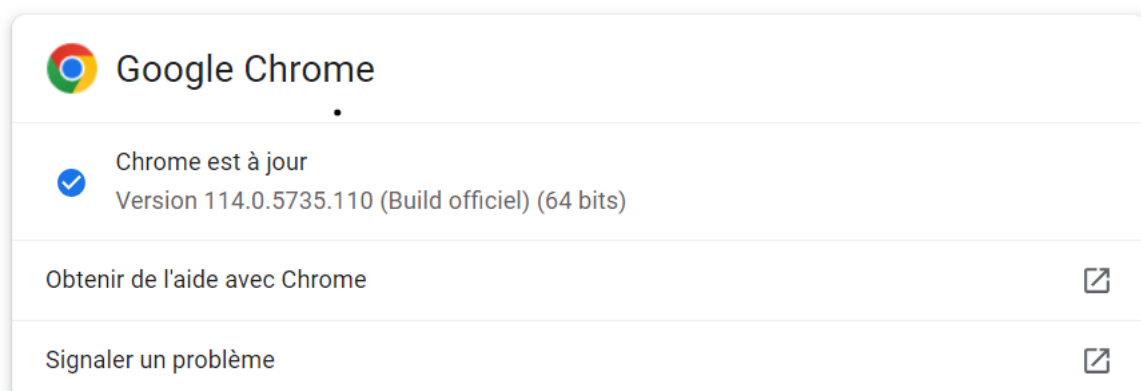


- [www.instagram.com](http://www.instagram.com) : Pareil cas, il s'agit d'un dérivé du site d'Instagram qui est comme Facebook, est un réseau social très populaire.

## 2/ Vérification des mises à jour des navigateurs web :

- Chrome :

À propos de Chrome



- Mozilla

## Mises à jour de Firefox

Conservez Firefox à jour pour bénéficier des dernières avancées en matière de performances, de stabilité et de sécurité.

Version 113.0.2 (32 bits) [Notes de version](#)

[Afficher l'historique des mises à jour...](#)

😊 Firefox est à jour

[Rechercher des mises à jour](#)

### Autoriser Firefox à

- ☒ Installer les mises à jour automatiquement (recommandé)
  - ☒ Quand Firefox n'est pas lancé
  - ☐ Vérifier l'existence de mises à jour, mais vous laisser décider de leur installation
- ☐ Ce paramètre s'appliquera à tous les comptes Windows et profils Firefox utilisant cette installation de Firefox.

☒ Utiliser un service en arrière-plan pour installer les mises à jour

## 4- Eviter le Spam et le phishing

### 1/Entrainement sur détection des erreurs dans des messages :

Bon travail, RAVO !  
Vous avez obtenu un score de 6/8.

Plus vous vous entraînez, mieux vous saurez identifier les pièges et vous protéger des tentatives d'hameçonnage.

Quelques mesures très simples à mettre en place peuvent également améliorer la protection de vos comptes en ligne. Pour plus d'informations, consultez la page [g.co/25V](https://www.google.com/25V).

Partager le questionnaire :

[f](#) [t](#)

RECOMMENCER LE QUESTIONNAIRE



JIGSAW | Google

Confidentialité / Conditions / Commentaires

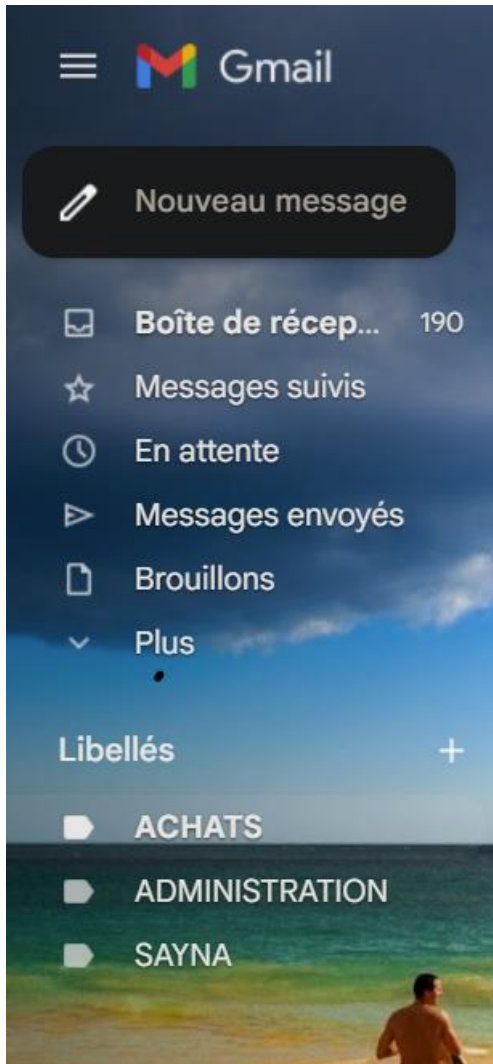
## 5- Comment éviter les logiciels malveillants

### 3/ Comparaison entre Indicateur de sécurité et Analyse google :

	Indicateur de sécurité	Analyse google
Site 1	HTTPS	Aucun contenu suspect
Site 2	HTTPS Not secure	Aucun contenu suspect
Site 3	HTTPS	Vérifier un URL en particulier

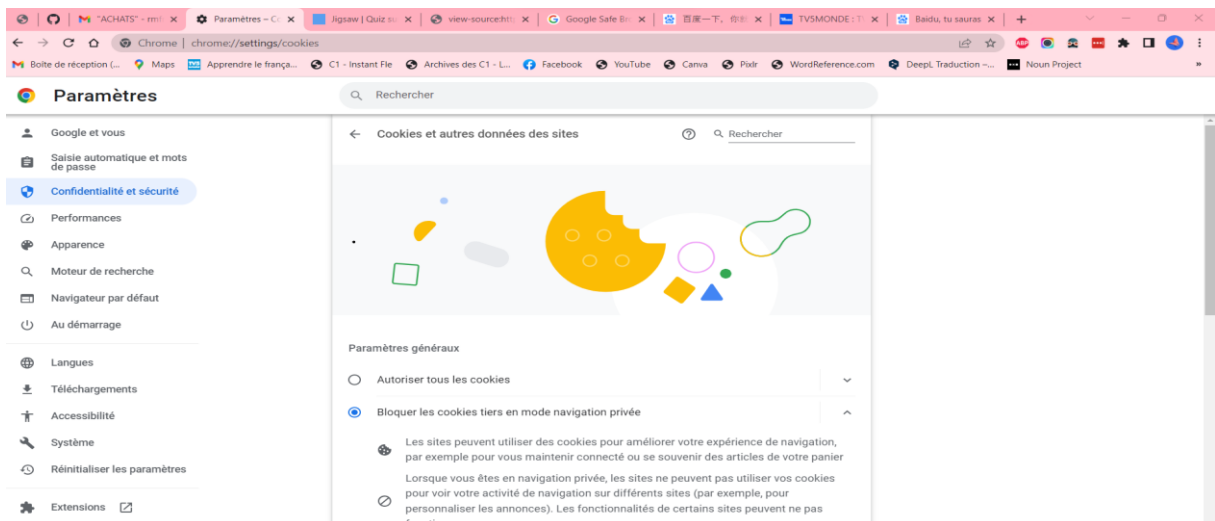
## 6- Achats en ligne sécurisés

### 1/ Création de registre d'achat

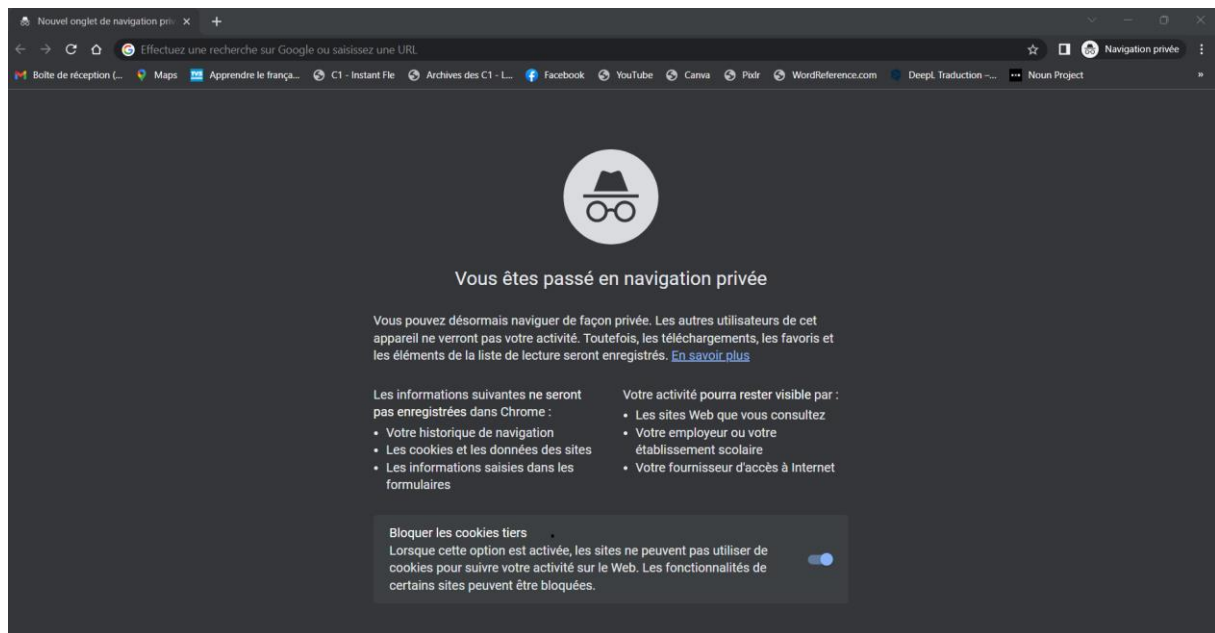


## 7- Comprendre le suivi du navigateur

Lors du cours, j'ai déjà paramétré la gestion des cookies de mon navigateur

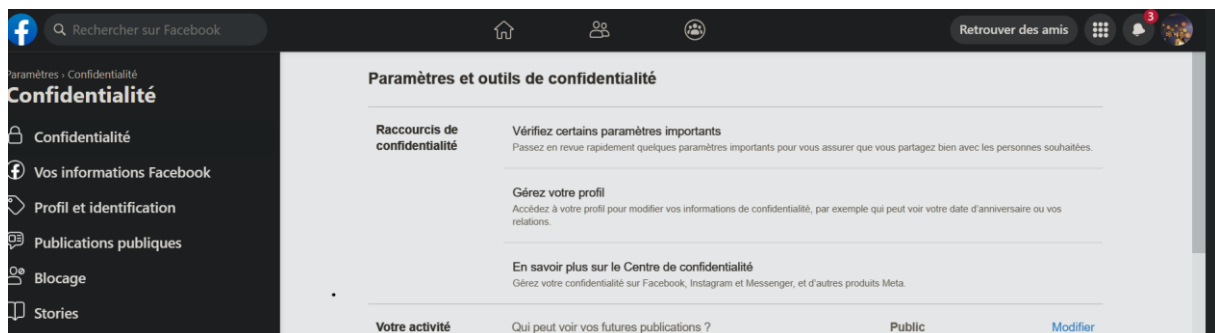


## Les cookies dans la navigation privée sont déjà bloqués



## 8- Principes de base de la confidentialité des médias sociaux

### 1/ réglage des paramètres de confidentialité pour Facebook



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

- Pour un appareil avec le système Windows

Etape 1/ Il faut télécharger et installer d'abord un antivirus si l'appareil n'en possède pas encore :

Par exemple : avast, kaspersky internet security, etc...

Il faut bien faire attention à l'utilisation des plusieurs antivirus dans un seul appareil, puisque cela pourrait avoir des compromis à leurs actions respectives.

Etape 2/ Il faut se déconnecter de l'internet car certains virus utilisent la connexion internet

Etape 3/ Redémarrer l'appareil en mode sans échec en suivant les instructions suivantes :

- Éteignez votre ordinateur et rallumez-le.
- Lorsque l'écran s'allume, appuyez sur F8 pour faire apparaître le menu « Options de démarrage avancées ».
- Cliquez sur « Mode sans échec avec prise en charge réseau ».
- Restez déconnecté d'Internet.

Étape 4/ Il est primordial de supprimer les fichiers temporaires en procédant comme suit :

- Cliquez sur « Démarrer ».
- Sélectionnez « Tous les programmes ».
- Cliquez sur « Accessoires ».
- Choisissez « Outils système ».
- Choisissez « Nettoyage du disque ».
- Recherchez « Fichiers temporaires » dans la liste « Fichiers à supprimer ».
- Sélectionnez « Fichiers temporaires » pour les supprimer.

Étape 5/ Lancer une analyse antivirus : Pour ce faire il faut ouvrir le logiciel d'antivirus et scanner l'appareil en appuyant scanner ou analyser. Cela dépend de logiciel utilisé

Étape 6/ Supprimer et mettre en quarantaine des virus

Étape 7 : Redémarrer votre ordinateur

Étape 8 : Modifier tous les mots de passe pour assurer la sécurité

Étape 9 : Mettre à jour le logiciel, le navigateur et le système d'exploitation

- Pour l'appareil Mac by Apple
  - 1- Fermez l'application ou le logiciel qui semble être affecté(e).
  - 2- Accédez au « Moniteur d'activité » et recherchez des virus Mac connus, comme « MacDefender », « MacProtector » et « MacSecurity ».
  - 3- Si vous découvrez l'un de ces virus, cliquez sur « Quitter l'opération » avant de fermer le « Moniteur d'activité ».
  - 4- Ensuite, accédez à votre dossier « Applications » et faites glisser le fichier dans votre corbeille.
  - 5- N'oubliez pas de vider le dossier « Corbeille » par la suite pour supprimer définitivement le virus.
  - 6- À présent, assurez-vous que vos logiciels et applications sont à jour pour bénéficier des derniers correctifs de sécurité.