

Parcours : DISCOVERY Module

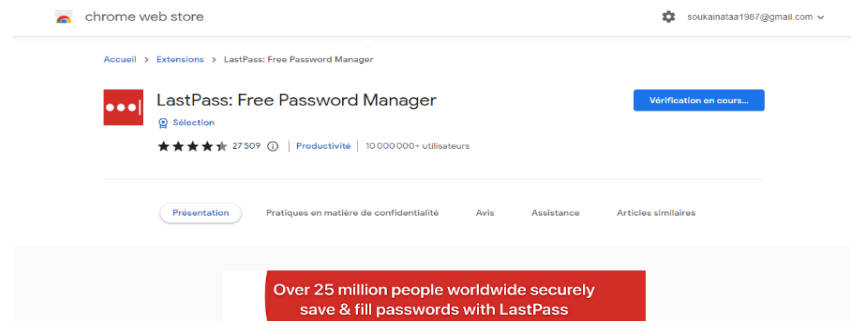
Module : Naviguer en toute sécurité

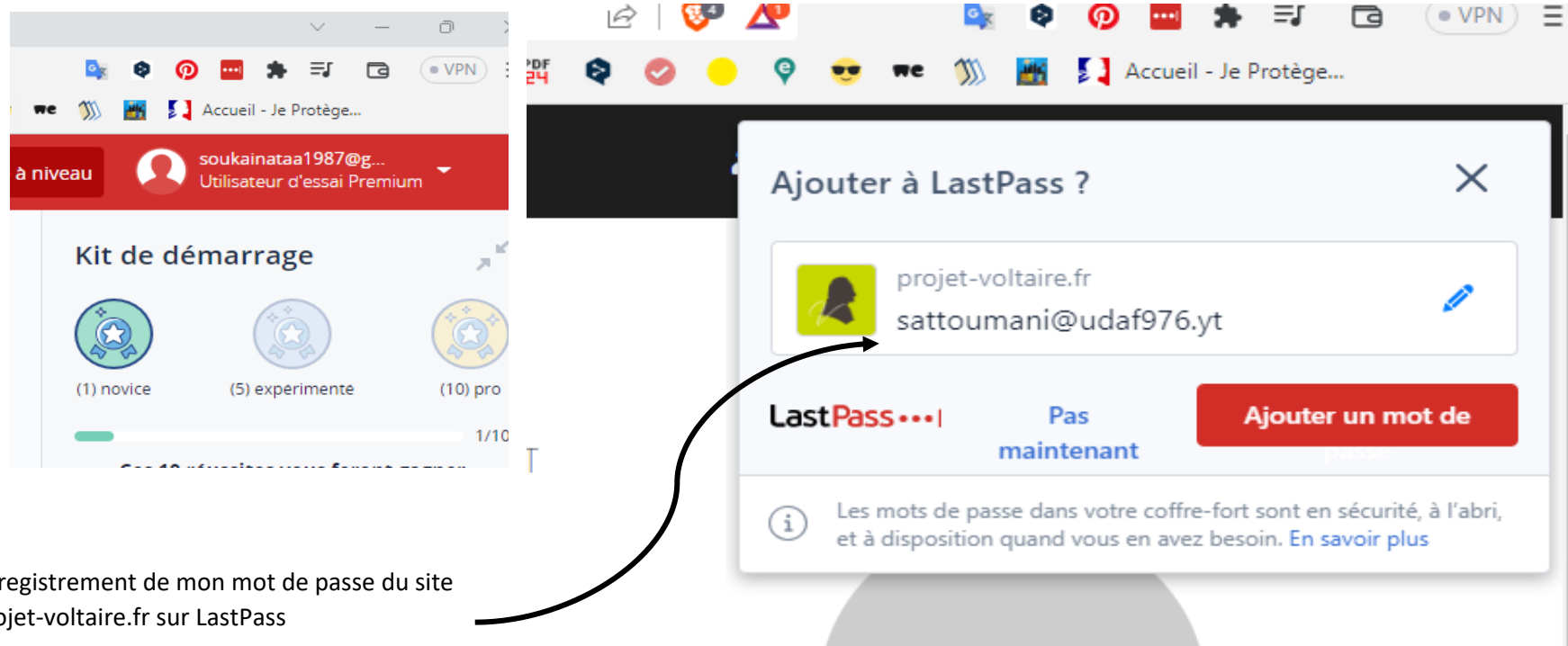
Projet 1 - Un peu plus de sécurité, on n'en a jamais assez !

1 - Introduction à la sécurité sur Internet

Article 1	www.futura-sciences.com	Ivacy VPN : sécurisez intégralement votre connexion à Internet pour moins de 1 euro par mois
Article 2	www.francetvinfo.fr	Sécurité sur internet : un plan anti arnaque efficace, mais pas infaillible
Article 3	www.cybermalveillance.gouv.fr	Comment sécuriser ses achats sur Internet ?

2 - Créer des mots de passe forts





Enregistrement de mon mot de passe du site projet-voltaire.fr sur LastPass

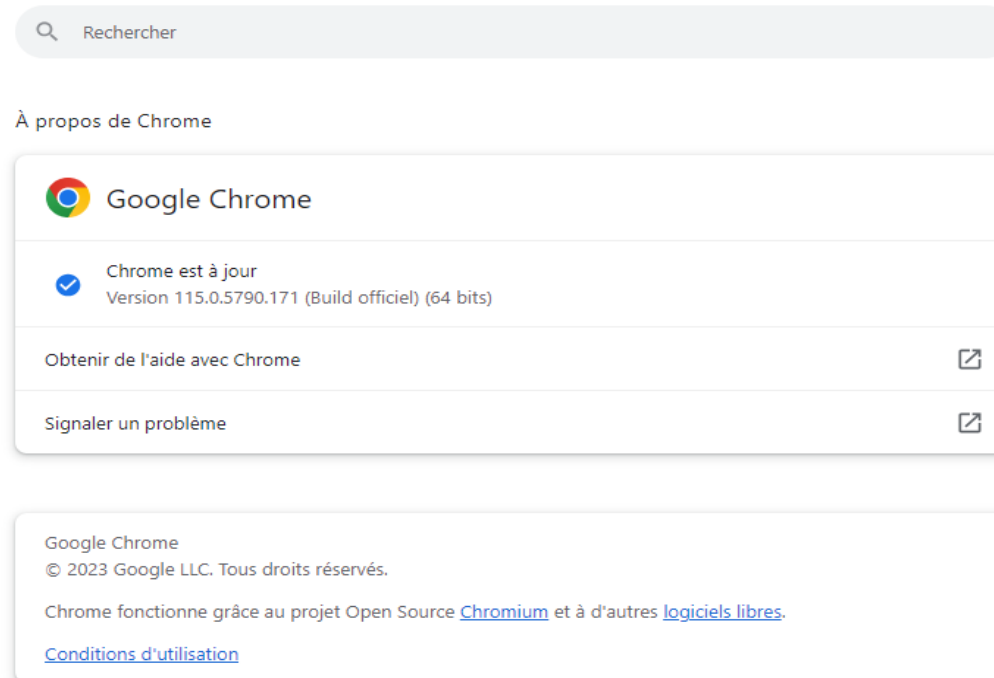
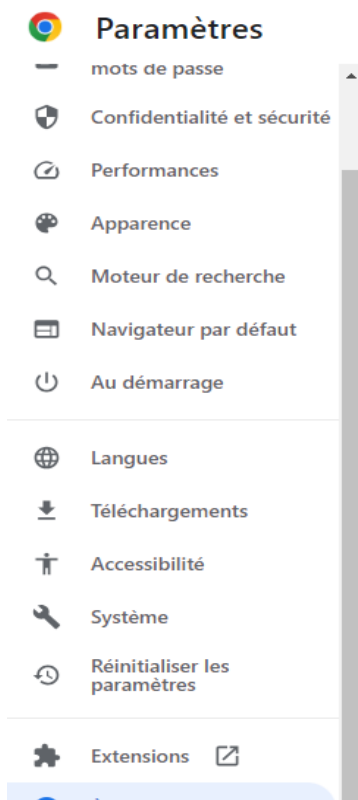
3 - Fonctionnalité de sécurité de votre navigateur

a) Les sites web qui semblent être malveillants sont :

Zone-telechargement	Site de téléchargements illégaux. Confronté à des ennuis judiciaires, le site a été forcé de changer d'adresse. Mais Zone téléchargement fait aussi face à une véritable guerre des clones qui augmente encore le risque pour les internautes mal informés.
lebonstream.info	Site de streaming demandant de se connecter et de mettre ses coordonnées bancaires afin de pouvoir visualiser les vidéos. Il n'est pas le seul site web du genre.
Steam	Plateforme de distribution de contenu en ligne, de gestion des droits et de communication. Ce site web est pourtant bien sécurisé mais parfois il peut y avoir des failles, j'ai failli être victime d'un vol de données bancaires qui m'a poussé à faire opposition, depuis, je n'ai plus confiance en ce site.

b) Mise à jour du navigateur :


Chrome



Firefox

Rechercher dans les paramètres


 Général


 Accueil


 Recherche

 Vie privée et sécurité

 Synchronisation


 Autres produits de Mozilla

 Extensions et thèmes

 Assistance de Firefox

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

Version 116.0.2 (64 bits) [Notes de version](#)

 Firefox est à jour

Afficher l'historique des mises 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

① 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 - Éviter le spam et le phishing

Bravo, Soukainata !
Vous avez obtenu un score de 8/8.

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/2SV.

Partager le questionnaire :

RECOMMENCER LE QUESTIONNAIRE



 **JIGSAW** | Google

Confidentialité / Conditions / Commentaires

5 - Comment éviter les logiciels malveillants

	Indicateur de sécurité	Analyse Google
Site 1	HTTPS	Aucune donnée disponible
Site 2	HTTPS	Aucun contenu suspect détecté

Site 3	HTTPS	Vérifier une URL en particulier
--------	-------	---------------------------------

6 - Achats en ligne sécurisés

Gmail

Rechercher dans les messages

Nouveau message

Planifié

Tous les messages

Spam 2

Corbeille

Gérer les libellés

Créer un libellé

Libellés

+

Achats

Administratif

Banque

Création de compte

Job

SAYNA

Paramètres

Général

Libellés

Boîte de réception

Comptes et importation

Filtres et adresses bloquées

Chat et Meet

Paramètres avancés

Hors connexion

Thèmes

Libellés système

Afficher dans la liste des libellés

Boîte de réception

afficher masquer

Messages suivis

afficher masquer

En attente

afficher masquer

Important

afficher masquer

Tous les chats

afficher masquer

Messages envoyés

afficher masquer

Planifié

afficher masquer

afficher si non lus

Brouillons

afficher masquer

afficher si non lus

Tous les messages

afficher masquer

Spam

afficher masquer

afficher si non lus

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

Exercice 1 : Vérification des processus en cours d'exécution

- a) Ouvrez le gestionnaire des tâches de votre système d'exploitation (Ctrl + Maj + Échap sur Windows, Activité sur Linux, Commande + Espace puis "Monitor" sur macOS).
- b) Passez en revue les processus en cours d'exécution pour détecter tout processus suspect ou inconnu. Recherchez des noms de processus étranges ou qui consomment anormalement des ressources.

Exercice 2 : Analyse des autorisations et des paramètres de sécurité

- a) Passez en revue les autorisations des applications et des logiciels installés sur votre ordinateur. Assurez-vous qu'ils n'ont pas d'autorisations excessives qui pourraient compromettre votre sécurité.
- b) Vérifiez les paramètres de pare-feu et de sécurité de votre système d'exploitation. Assurez-vous qu'ils sont correctement configurés pour bloquer tout trafic suspect.

Installation et utilisation d'un antivirus et d'un anti-malware

Recherche et sélection du logiciel :

- a) Effectuez une recherche en ligne pour trouver un logiciel antivirus et un logiciel anti-malware fiables et bien notés.
- b) Choisissez des solutions provenant de sources réputées et évitez les téléchargements à partir de sources non officielles.

Téléchargement et installation :

- a) Rendez-vous sur le site officiel du logiciel choisi et téléchargez la version appropriée pour votre système d'exploitation (Windows, macOS, Linux, etc.).
- b) Suivez les instructions d'installation pour installer les deux logiciels sur votre appareil.

Configuration de l'antivirus :

- a) Une fois installé, ouvrez l'antivirus et suivez les étapes de configuration initiale.
- b) Activez les fonctionnalités de protection en temps réel, de pare-feu si disponible, et de mises à jour automatiques des définitions de virus.

Configuration de l'anti-malware :

- a) Procédez de la même manière pour l'anti-malware en suivant les étapes de configuration.
- b) Vérifiez également les options de planification de scan régulier.

Mise à jour des bases de données :

Après l'installation, assurez-vous que les bases de données de virus et de malwares sont à jour en lançant manuellement une mise à jour.

Scans complets et rapides :

- a) Planifiez des scans complets réguliers de votre système (au moins une fois par semaine) avec l'antivirus et l'anti-malware.
- b) Effectuez également des scans rapides lorsque vous téléchargez des fichiers ou installez de nouveaux logiciels.

Quarantaine et nettoyage :

Si l'antivirus ou l'anti-malware détecte des fichiers suspects, suivez les instructions pour les mettre en quarantaine ou les supprimer en toute sécurité.

Rapports de sécurité :

Vérifiez régulièrement les rapports de sécurité générés par les logiciels pour vous assurer qu'aucune menace n'a été détectée.

Éducation sur la sécurité :

Profitez de l'occasion pour rappeler les bonnes pratiques de sécurité en ligne, telles que l'évitement des téléchargements depuis des sources non fiables et la prudence lors de l'ouverture de pièces jointes.

Maintenance continue :

Assurez-vous de maintenir vos logiciels antivirus et anti-malware à jour en installant les mises à jour recommandées par les fournisseurs.

