

1- Introduction à la sécurité sur internet

1/Trois articles qui parlent de sécurité sur internet.

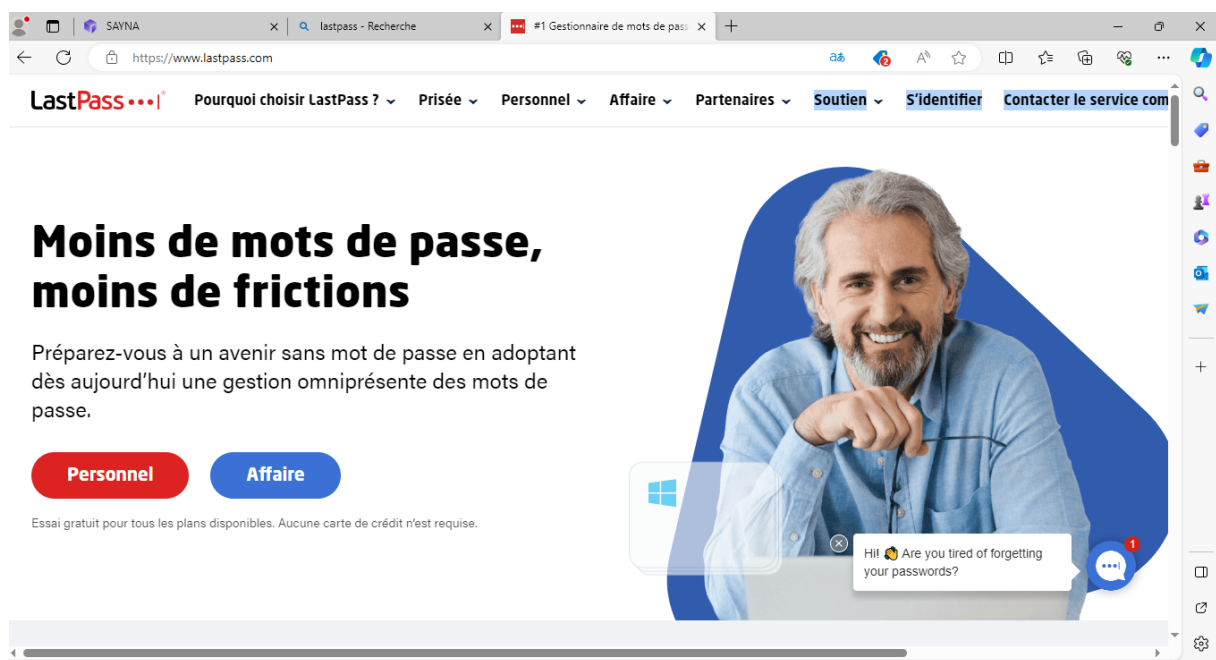
Voici les articles qu'on a retenu.

- Article 1= Le Monde Informatique-sécurité informatique : les tendances à suivre en 2024
- Article 2= 01net-Les meilleurs antivirus de 2024
- Article 3= Journal du Net-Cybersécurité : les défis de demain

2- 1-Créer des mots de passe forts

1/Gestionnaire de mot de passe

- Accéder au site de LastPass



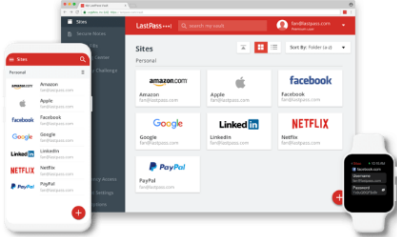
- Créer un compte en remplissant le formulaire

https://lastpass.com/families/trial

LastPass

Démarrez un essai gratuit de 30 jours de LastPass Families.

Obtenez le gestionnaire de mots de passe le plus fiable et essayez LastPass Families pendant 30 jours.



Créer un compte

ou [Connexion](#)

Adresse e-mail
tolotraramahenina@gmail.com

Mot de passe maître
.....

Exigences minimales:

- ✓ Indicateur de force au maximum
- ✓ Au moins 12 caractères
- ✓ Au moins 1 chiffre
- ✓ Au moins 1 minuscule
- ✓ Au moins 1 majuscule
- ✓ Au moins 1 caractère spécial
- ✓ Pas votre e-mail

- Une fois le compte créé, tu arrives sur une page de validation qui propose le téléchargement

https://www.lastpass.com/fr/install-lastpass-families

LastPass

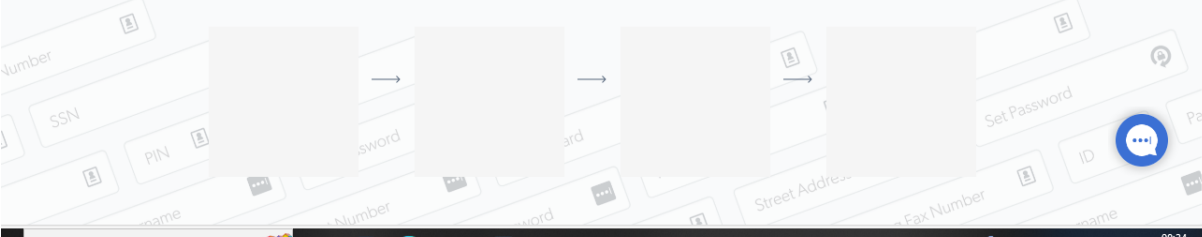
✓ Votre compte a été créé avec succès !

Remarque :

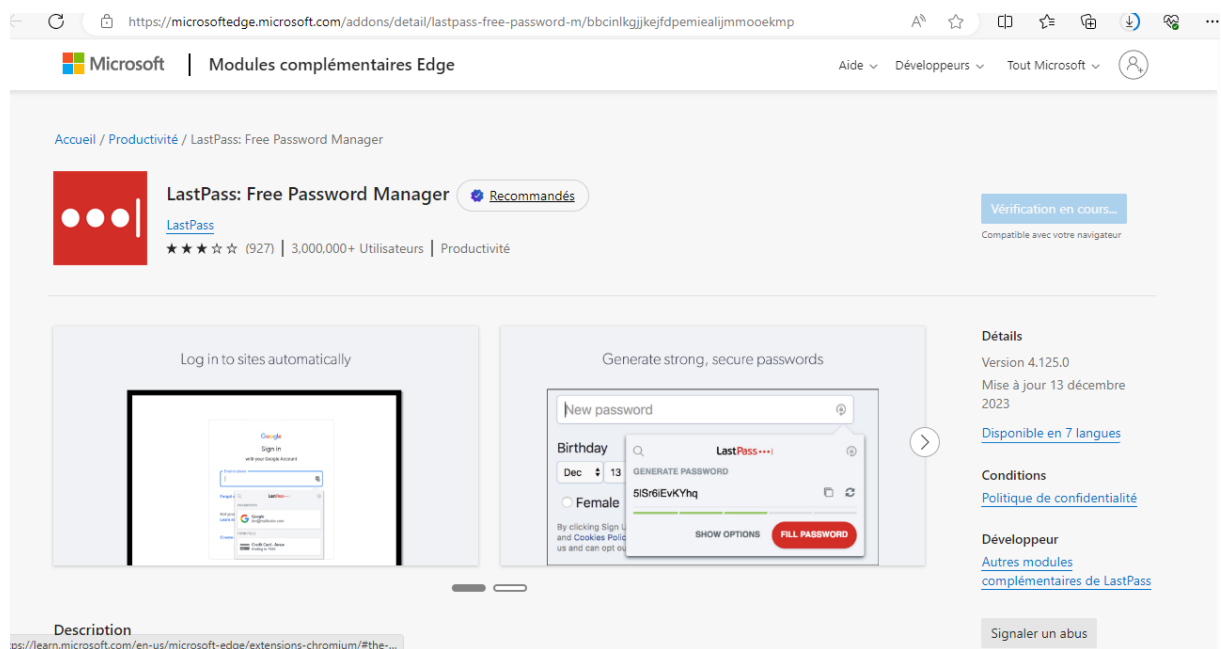
redirection dans 0

Installez l'extension de navigateur pour enregistrer et remplir les mots de passe et plus encore.

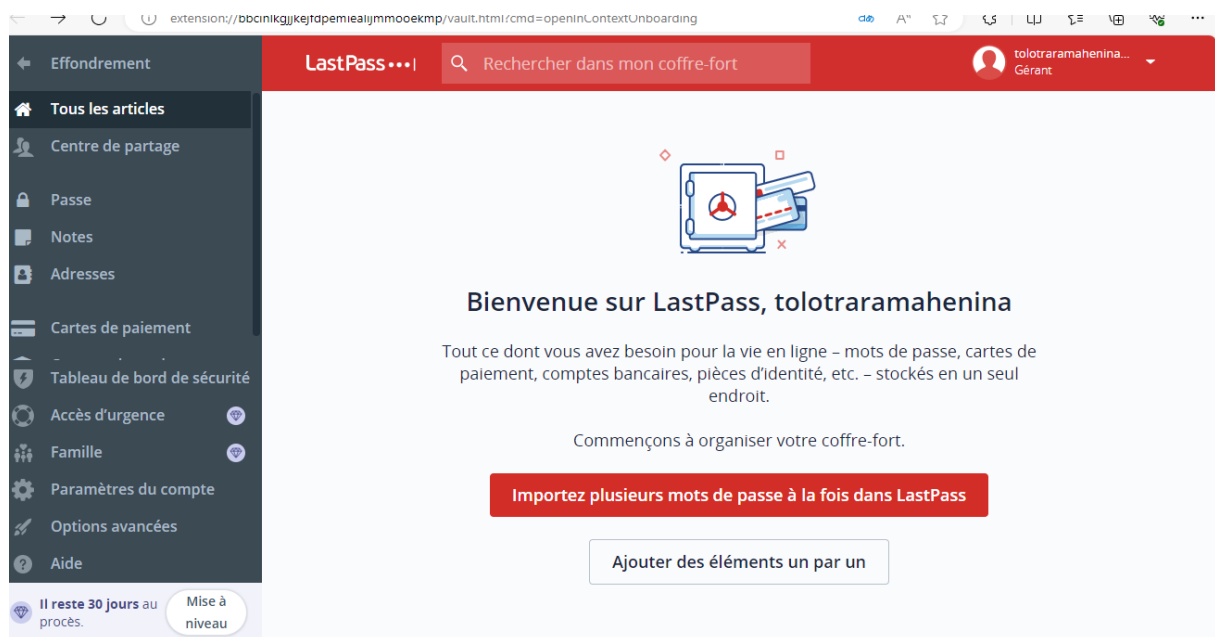
[Installer LastPass](#)



- Il te suffit de valider l'opération sur le chrome Web Store en effectuant un clic sur le bouton « Ajouter à Chrome »



- L'installation fini, il te suffit d'accéder à cette extension et de t'y connecter
Appuyer sur « importez plusieurs mots de passe à la fois dans LastPass »



Et il suffit de suivre les démarches

3- Fonctionnalité de sécurité de votre navigateur

1/On identifie les adresses internet internet qui nous semblent provenir de sites web malveillants.

Les sites web qui semblent être malveillants sont :

- www.morvel.com, c'est un dérivé de « Marvel » une marque bien connue, ce qui pourrait indiquer une redirection vers une site malveillant.
- www.fessebook.com, qui semble un site n'est pas loin de www.facebook.com, qui est le réseau le plus utilisé au monde

- www.instagram.com, un site qui ressemble à www.instagram.com, qui lui un site utilisé par beaucoup de monde.

Les sites qui semblent être cohérent sont :

- www.ironman.com, est le site officiel de la société Ironman, qui organise des courses d'endurance renommées dans le monde entier.
- www.dccomics.com, est un extrait du site www.Dc.Comics qui est une société de bandes dessinée américaine bien connue.

2/Vérification des navigateurs utilisés, Chrome et Firefox dans notre, exemple, sont à jour.

- Pour Chrome.
 - On ouvre le menu du navigateur et accéder aux « paramètre »
 - Clic sur la rubrique « A propos de Chrome »
 - On constate le message « Chrome est à jour » c'est Ok
- Pour Firefox
 - Ouvre le menu navigateur et accéder aux « paramètre »
 - Dans la rubrique « Général », fais défiler jusqu'à voir la section « Mise à jour de Firefox »

Les paramètres de ces deux navigateurs réalisent des mises à jour automatique.

4- -Eviter le spam et le phishing

1/on va déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.

Exercice 4-spam et Phishing

On peut aussi consulter des ressources annexes pour s'exercer.

5- Comment éviter les logiciels malveillants

3/pour chaque site on devra préciser l'indicateur de sécurité et le rapport d'analyse de l'outil Google

- Site n°1
 - Indicateur de sécurité
HTTPS
 - Analyse Google
Aucun contenu suspect
- Site n°2
 - Indicateur de sécurité
Not sécurée
 - Analyse Google
Aucun contenu suspect
- Site n°3
 - Indicateur de sécurité
Not secure
 - Analyse Google
Vérifier un URL en particulier

6- Achats en ligne sécurisés

1/Création d'un registre des achats pour que les informations relatives aux achats en ligne

Deux possibilités qui sont offertes pour organiser le registre :

1. On va créer un dossier sur la messagerie électronique
2. On va créer un dossier sur l'espace de stockage personnel

Pour choisir la plus simple, c'est le premier qui est facile à manipuler

- Il faut accéder à ta messagerie électronique
- Sur la page de messagerie, sur la gauche les libellés initialement prévus
- Créer ta propre rubrique des achats. Pour créer un libellé rapidement, juste un clic sur « créer un libellé » et nommer « ACHATS »
- On effectue un clic sur le bouton « créer » pour valider l'opération
- En effectuant un clic sur « Gérer les libellés »

7- Comprendre le suivi du navigateur

Le suivi sur internet désigne la pratique où les sites web enregistrent nos activités en ligne pour personnaliser les publicités et améliorer l'expérience utilisateur, soulevant des préoccupations en matière de vie privée et de sécurité des données.

8- Principes de base de la confidentialité des médias sociaux

1/le réglage des paramètres de confidentialité pour Facebook

- Se connecter à ton compte Facebook
- Une fois sur la page d'accueil, ouvre le menu Facebook, puis effectuer un clic sur « paramètres et confidentialité », et enfin sur « paramètre »
- Ce sont les onglets « confidentialité » et « Publications publiques » qui nous intéressent
- Dans les paramètres Facebook on a aussi un onglet « cookies »

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

1/Voici un exercice pour vérifier la sécurité en fonction de l'appareil utilisé :

Exercice : Test de sécurité des appareils

- Objectif : Vérifier la sécurité des différents appareils (ordinateur, smartphone, tablette) utilisés pour accéder à internet.
- Étapes :
 - a. Identifiez les différents appareils que vous utilisez pour accéder à internet (ordinateur, smartphone, tablette).

b. Pour chaque appareil, effectuez les actions suivantes :

- Vérifiez si les mises à jour système et des applications sont activées et à jour.
- Vérifiez si un antivirus/antimalware est installé et à jour (le cas échéant).
- Vérifiez les paramètres de sécurité et de confidentialité du système d'exploitation et des applications installées.
- Vérifiez si le pare-feu est activé (le cas échéant).
- Vérifiez la présence de logiciels malveillants en effectuant une analyse complète du système (le cas échéant).
- Vérifiez si le réseau Wi-Fi utilisé est sécurisé et si vous utilisez une connexion VPN (le cas échéant).
- Vérifiez les autorisations accordées aux applications installées et désinstallez celles qui ne sont pas nécessaires ou suspectes.
- Vérifiez si des correctifs de sécurité sont disponibles pour les vulnérabilités connues.

c. Prenez des mesures correctives pour renforcer la sécurité de chaque appareil, le cas échéant.

- Résultats : Évaluez la sécurité de chaque appareil en fonction des mesures prises lors de l'exercice. Identifiez les éventuelles lacunes en matière de sécurité et prenez les mesures nécessaires pour les corriger.

2/Voici un exercice pour installer et utiliser un antivirus + Antimalware en fonction de l'appareil utilisé :

Exercice : Installation et utilisation d'un antivirus + Antimalware

- Objectif : Installer et configurer un logiciel antivirus + antimalware sur l'appareil utilisé pour accéder à internet (ordinateur, smartphone, tablette) afin de renforcer sa sécurité.
- Étapes :
 - a. Sélectionnez un logiciel antivirus + antimalware réputé et adapté à votre appareil. Assurez-vous qu'il est compatible avec votre système d'exploitation.
 - b. Téléchargez et installez le logiciel antivirus + antimalware sur votre appareil en suivant les instructions fournies par le fournisseur.
 - c. Effectuez une analyse complète de votre appareil pour détecter et éliminer les éventuelles menaces existantes.
 - d. Activez les fonctionnalités de protection en temps réel pour surveiller et bloquer les activités suspectes en temps réel.
 - e. Configurez les paramètres de l'antivirus + antimalware en fonction de vos préférences et de votre niveau de sécurité souhaité.
 - f. Planifiez des analyses régulières de votre appareil pour maintenir sa sécurité à jour.
 - g. Assurez-vous que la base de données de signatures de virus est constamment mise à jour pour détecter les nouvelles menaces.

Résultats : Évaluez l'efficacité de l'antivirus + antimalware en fonction de sa capacité à détecter et à éliminer les menaces sur votre appareil. Surveillez les performances de votre appareil après l'installation et l'utilisation du logiciel pour détecter tout impact sur ses performances ou son utilisation.