

UN PEU DE SECURITE, ON N'EN A JAMAIS ASSEZ !

1- Introduction à la sécurité sur internet

1/

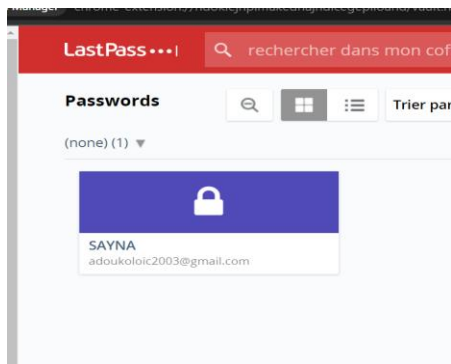
Article 1 = <https://www.kaspersky.fr/resource-center/definitions/what-is-internet-security>

Article 2 = <https://www.checkpoint.com/fr/cyber-hub/cyber-security/what-is-internet-security/>

Article 3 = <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-se-proteger-sur-internet>

2- Créer des mots de passe forts

1/



3- Fonctionnalité de sécurité de votre navigateur

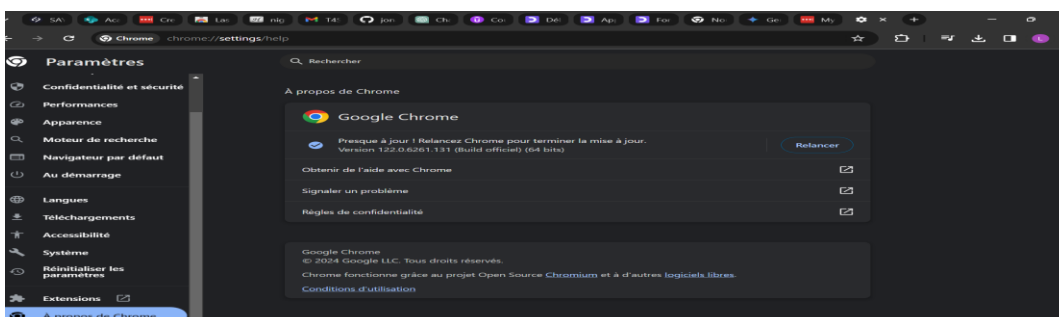
1/

- www.marvel.com

- www.facebook.com

- www.instagram.com

2/(Je l'ai redemarré après)



4- Eviter le spam et le phishing



5- Comment éviter les logiciels malveillants

6- Achats en ligne sécurisés



7- Comprendre le suivi du navigateur

8- Principes de base de la confidentialité des médias sociaux

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

1/

Pour un ordinateur (Windows, macOS, Linux)

- Vérifiez que votre système d'exploitation est à jour en installant les dernières mises à jour de sécurité.
- Effectuez une analyse antivirus pour détecter et supprimer les éventuels logiciels malveillants.
- Activez un pare-feu pour bloquer les connexions non autorisées à votre ordinateur.
- Utilisez un gestionnaire de mots de passe pour stocker vos mots de passe de manière sécurisée.
- Vérifiez que les paramètres de confidentialité de votre navigateur sont configurés pour protéger votre vie privée en ligne.

Pour un smartphone (iOS, Android)

- Mettez à jour votre système d'exploitation et toutes vos applications pour bénéficier des dernières corrections de sécurité.
- Activez le verrouillage de l'écran avec un code PIN, un mot de passe, un schéma ou une empreinte digitale.
- Utilisez des applications de sécurité mobile pour détecter et supprimer les logiciels malveillants et protéger votre vie privée.
- Configurez des sauvegardes automatiques de vos données pour éviter de perdre des informations importantes en cas de perte ou de vol de votre téléphone.
- Examinez les autorisations accordées à chaque application et révoquez celles qui semblent excessives ou suspectes.

Pour un routeur Wi-Fi

- Changez le mot de passe par défaut de votre routeur pour un mot de passe fort et unique.
- Activez le chiffrement Wi-Fi (WPA2 ou WPA3) pour sécuriser votre réseau sans fil.
- Désactivez le WPS (Wi-Fi Protected Setup) si vous ne l'utilisez pas, car il peut présenter des vulnérabilités de sécurité.
- Activez la détection des intrusions sur votre routeur pour détecter les activités suspectes sur votre réseau.
- Mettez à jour le firmware de votre routeur régulièrement pour bénéficier des dernières corrections de sécurité.

2/

Ordinateur (Windows)

- Téléchargez et installez un logiciel antivirus + antimalware fiable comme Malwarebytes, Avast, Bitdefender, ou utilisez Windows Defender pour Windows 10.
- Lancez le logiciel et mettez à jour les définitions de virus.

- Configurez les paramètres selon vos préférences.
- Effectuez une analyse complète de votre système.
- Supprimez ou mettez en quarantaine les menaces détectées.
- Assurez-vous de maintenir le logiciel à jour.