

Mon hygiène numérique

Ou

Ma routine au quotidien

Tutoriel pour rencontre CIVBDL sur Zoom du 03 mai 2023

Première partie : requête à Bing AI :

Je vous recommande de consulter le tutoriel "Conseils d'hygiène numérique" d'Anne Pédron-Moinard sur YouTube.

Il contient des conseils pratiques pour protéger votre vie privée et votre sécurité en ligne. Vous pouvez également consulter le guide d'hygiène informatique de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui présente les 42 mesures essentielles pour assurer la sécurité de votre système d'information.

Source : Conversation avec Bing, Tutoriel: Conseils d'hygiène numérique (Anne Pédron-Moinard). <https://www.youtube.com/watch?v=MN1L9an6FBE>

(2) Hygiène numérique: 7 conseils à appliquer | Banque Nationale.

<https://www.bnc.ca/particuliers/conseils/securite/conseils-hygiene-numerique.html>

(3) Guide d'hygiène informatique | Agence nationale de la ... - ANSSI.

<https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/>

(4) Comment avoir une bonne hygiène numérique ? | Les Sherpas.

<https://sherpas.com/blog/hygiene-numerique/>

(5) 5 conseils pour créer une formation efficace d'hygiène numérique en

<https://www.zdnet.fr/pratique/comment-creeer-une-formation-efficace-d-hygiene-numerique-en-entreprise-39848824.htm>

Deuxième partie : requête à ChatGPT :

Bonjour Michel,

Bien sûr, je peux vous aider à créer un tutoriel sur "Mon hygiène numérique". Voici quelques conseils pour vous aider à rester en sécurité en ligne :

1. Utilisez des mots de passe forts : Les mots de passe sont la première ligne de défense pour protéger vos informations en ligne. Assurez-vous d'utiliser des mots de passe forts, avec une combinaison de lettres, de chiffres et de caractères spéciaux. Ne partagez jamais vos mots de passe avec qui que ce soit.
2. Mettez à jour votre système d'exploitation : Les mises à jour du système d'exploitation sont souvent publiées pour corriger des failles de sécurité. Assurez-vous de mettre régulièrement à jour votre système d'exploitation pour vous protéger contre les nouvelles menaces.
3. Utilisez des logiciels antivirus : Les logiciels antivirus peuvent aider à protéger votre ordinateur contre les logiciels malveillants et les virus. Assurez-vous d'en avoir un installé sur votre ordinateur et de le mettre à jour régulièrement.
4. Faites attention aux courriels de phishing : Les courriels de phishing sont des courriels frauduleux qui tentent de vous faire cliquer sur des liens malveillants ou de vous inciter à partager des informations sensibles. Assurez-vous de ne jamais cliquer sur des liens dans les courriels que vous ne connaissez pas ou que vous ne faites pas confiance.
5. Utilisez des réseaux Wi-Fi sécurisés : Évitez d'utiliser des réseaux Wi-Fi publics non sécurisés, car ils peuvent être vulnérables aux attaques de hackers. Utilisez plutôt votre propre réseau ou un réseau Wi-Fi sécurisé.
6. Sauvegardez régulièrement vos données : Les sauvegardes régulières de vos données sont essentielles pour vous protéger contre les pertes de données, les piratages et les accidents. Assurez-vous de sauvegarder régulièrement vos fichiers importants sur un disque dur externe ou dans le cloud.

7. Limitez vos informations personnelles en ligne : Limitez les informations personnelles que vous partagez en ligne, telles que votre adresse ou votre numéro de téléphone. Évitez de partager des informations sensibles sur les réseaux sociaux ou les forums en ligne.

En suivant ces conseils, vous pouvez rester en sécurité en ligne et protéger vos informations personnelles. N'oubliez pas que la sécurité en ligne est une responsabilité partagée, alors assurez-vous de sensibiliser vos amis et votre famille à ces pratiques de sécurité en ligne.

Merci, cela me convient. Michel

Je suis ravi d'avoir pu vous aider.

N'hésitez pas à me contacter si vous avez besoin d'autres conseils ou informations.
Bonne journée !

Étapes quotidiennes avec ordinateur* :

Nom du produit : HP modèle Omen

*Qui est presque toujours « mis en veille » (7/24)

**Système opération : Windows 11 Pro

***Microsoft 365 (Suite Office intégrée)

- Vérifier les mises à jour avec Windows Update
 - Paramètres
- Nettoyer l'espace de stockage des Fichiers temporaires
 - Paramètres > Système > Stockage > Fichiers temporaires > Supprimer les fichiers
- Vérifier les mises à jour de l'antivirus Bitdefender
- Vérifier Malwarebytes
- Vérifier Ashampoo WinOptimizer : mises à jour de l'optimisateur Windows
- Vérifier Ashampoo Driver Updater : mises jour des pilotes

- Vérifier Microsoft 365 et Office : mises à jour
 - Vérifier PC Manager : Boost your PC's performance
 - Vérifier Sécurité Windows: mises à jour de la protection
 - Vérifier les menaces actuelles : analyse rapide
 - Vérifier Google Chrome : mise à jour de la version
 - >Nettoyer l'historique
 - >Paramètres
 - >Confidentialité et sécurité
 - >Contrôle de sécurité
 - >Effacer les données de navigation
 - Vérifier Microsoft Edge : mise à jour de la version
 - Nettoyer l'historique
 - Vider corbeille
 - Vérifier Gestionnaire des tâches : redémarrer Explorateur Windows
 - Vérifier applications de démarrage
 - Vérifier Panneau de configuration
 - >Programmes
 - >Désinstaller un programme
-

Étapes quotidiennes avec cellulaire et tablette* :

*Produits Samsung

*Système d'exploitation : Version Android : 13

- Gérer les applications et l'appareil :
 - Lancer Applications mettre à jour
 - Lancer Analyse Play Protect
- Chrome : effacer les données avec données avancées
- Paramètres et mises à jour :
 - >Pile et entretien de l'appareil
 - >Optimiser >Pile
 - >Optimiser >Mémoire

- >Optimiser >Protection de l'appareil >Analyse
 - Vérifier antivirus Bitdefender :
 - Lancer l'analyse
 - Vérifier antimalware Malwarebytes :
 - Lancer l'analyse
 - Vérifier Nettoyeur Droid Optimizer :
 - Lancer l'analyse
 - Vérifier CCleaner et lancer l'analyse de nettoyage rapide
-

Recherche et mise en page:

Michel Cloutier

CIVBDL

20230503

"C'est ensemble qu'on avance"+