

PROJET : Un peu plus de sécurité, on n'en a jamais assez !

1/INTRODUCTION A LA SECURITE SUR INTERNET :

article1: <https://www.kaspersky.fr/>- Sécurité Internet : Qu'est-ce que c'est et comment vous protéger en ligne ?

article2: <https://www.francetvinfo.fr/-Cyberattaque> contre plusieurs ministères : le parquet de Paris ouvre une enquête

article3: <https://www.cybermalveillance.gouv.fr/> -Comment se protéger sur Internet ?

2-CRÉER DES MOT DE PASS DE FORT :

Pour utiliser LastPass :

Installation : Téléchargez l'application LastPass et créez un compte.

Stockage des mots de passe : Enregistrez vos identifiants de connexion lorsqu'on vous le propose.

Utilisation : LastPass remplira automatiquement les champs de connexion lorsque vous visiterez des sites web.

Génération de mots de passe : utilisez l'outil intégré pour créer des mots de passe sécurisés.

Partage (optionnel) : Vous pouvez partager en toute sécurité des mots de passe avec d'autres utilisateurs LastPass.

Synchronisation : Assurez-vous que la synchronisation est activée pour accéder à vos mots de passe sur tous vos appareils.

3-FONCTIONNALITÉS DE SÉCURITÉ DU NAVIGATEUR

Identifions les adresses internet suspectes parmi celles-ci :

www.morvel.com
www.dccomics.com
www.ironman.com
www.fessebook.com
www.instagam.com

Les sites web potentiellement malveillants sont :

www.morvel.com : une variante de www.marvel.com, le site officiel de l'univers Marvel.

www.fessebook.com : une variante de www.facebook.com, le plus grand réseau social au monde.

www.instagam.com : une variante de www.instagram.com, un autre réseau social populaire.


Les sites web considérés comme sûrs sont :

www.dccomics.com
www.ironman.com


2-VÉRIFIONS SI NOS NAVIGATEURS SONT À JOUR:


CHROME:

À propos de Chrome

 **Google Chrome**

Une erreur s'est produite pendant la vérification des mises à jour : Échec du téléchargement (code d'erreur : 7: [0x80070005](#) – system level)..
[En savoir plus](#)
Version 108.0.5359.125 (Build officiel) (64 bits)

[Obtenir de l'aide avec Chrome](#) 


[Signaler un problème](#) 


Google Chrome
© 2024 Google LLC. Tous droits réservés.


Chrome fonctionne grâce au projet Open Source [Chromium](#) et à d'autres [logiciels libres](#).


[Conditions d'utilisation](#)


Mozilla :


 **Général**


 Accueil


 Recherche

 Vie privée et sécurité

 Synchronisation

 Autres produits de Mozilla

 Extensions et thèmes

 Assistance de Firefox

Mises à jour de Firefox

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

Version 122.0 (64 bits) [Notes de version](#)

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

[Redémarrer pour mettre à jour Firefox](#)

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 SPAM ET PHISHING

Bon travail, ELHADJI
CHEIKH DIOP !
Vous avez obtenu un
score de 4/8.

Plus vous vous entraînez, mieux vous saurez identifier les
pièges et vous protégerez 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

5/COMMENT ÉVITER LES LOGICIELS MALVEILLANTS

Réponse 1:

Réponse 1

Site n°1: <https://www.fifa.com/fifaplus/fr/>

Indicateur de sécurité :

HTTPS

Analyse Google:

Aucun contenu suspect

Site n°2: <https://learn.sayna.io/parcours>

Indicateur de sécurité :

HTTPS

• Analyse Google

Aucun contenu suspect

Site n°3: <https://www.lefigaro.fr/>

Indicateur de sécurité :

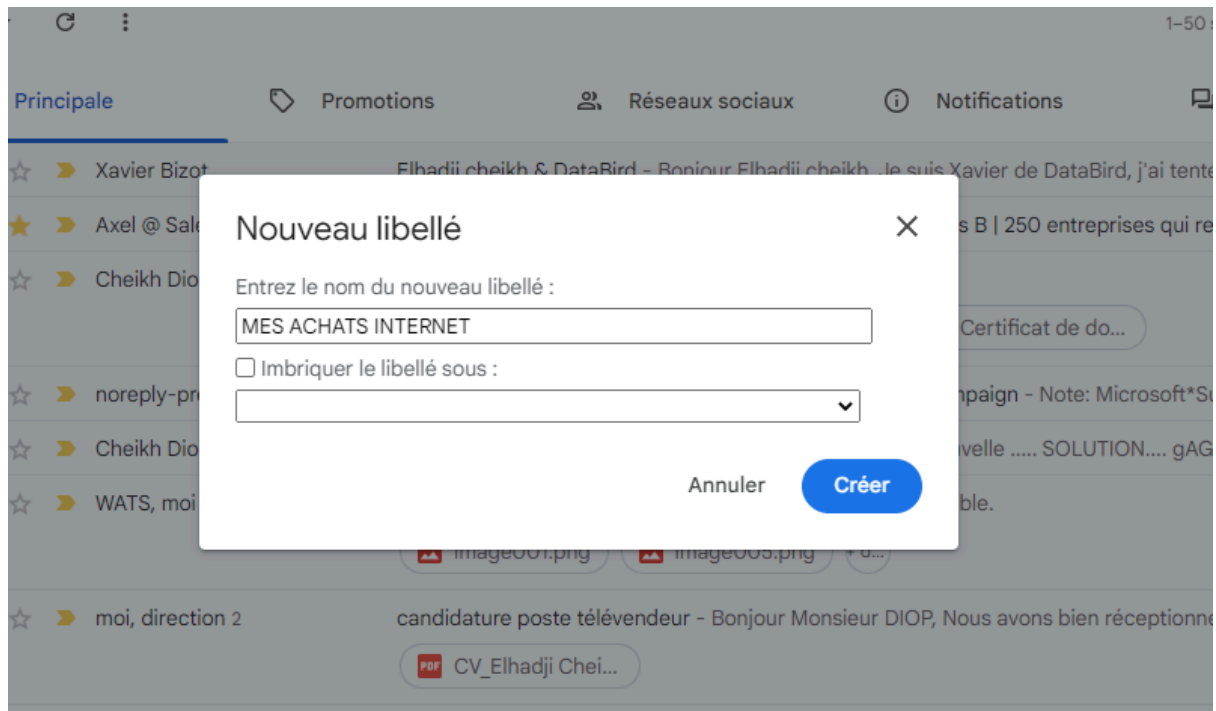
HTTPS

Analyse Google:

Vérifier une URL en particulier

6-ACHAT SÉCURISÉ EN LIGNE:

1 Registre D'achat:



Paramètres

| | | | | | | |
|----------------------------|--|-------------------------|--|------------------------------|-------------------------|---------------------|
| Général | Libellés | Boîte de réception | Comptes et importation | Filtres et adresses bloquées | Transfert et POP/IMAP | Module |
| Chat et Meet | Paramètres avancés | Hors connexion | Thèmes | | | |
| Réseaux sociaux | afficher | masquer | afficher | masquer | | |
| Notifications | afficher | masquer | afficher | masquer | | |
| Forums | afficher | masquer | afficher | masquer | | |
| Promotions | afficher | masquer | afficher | masquer | | |
| Libellés | Afficher dans la liste des libellés | | Afficher dans la liste des messages | | Acti | |
| <div>Nouveau libellé</div> | | | | | | |
| MES ACHATS INTERNET | afficher | masquer | afficher si non lus | afficher | masquer | sup |
| 0 conversation | | | | | | |
| Newsletter | afficher | masquer | afficher si non lus | afficher | masquer | sup |
| 4010 conversations | | | | | | |

7-COMPREDRE LE SUIVI DU NAVIGATEUR :

8-PRINCIPES DE BASES DE LA CONFIDENTIALITÉ DES MÉDIAS SOCIAUX:

Les paramètres de confidentialité sur Facebook comprennent plusieurs rubriques principales :

Confidentialité : Contrôle qui peut voir vos publications et qui peut vous contacter.

Sécurité : Gère les options de sécurité telles que la vérification en deux étapes et les connexions actives.

Paramètres du compte : Comprend des options pour modifier votre nom, votre mot de passe et d'autres informations de compte.

Blocage : Permet de bloquer des utilisateurs et des applications.

Notifications : Personnaliser les notifications que vous recevez de Facebook.

Localisation : Gère vos paramètres de localisation et d'identification.

Chronologie et marquage : Contrôle qui peut publier sur votre chronologie et qui peut vous identifier dans des publications.

Publicité : Gère les préférences publicitaires et les données utilisées pour vous cibler.

Accès au compte : Gère les applications et les sites Web tiers qui ont accès à votre compte Facebook.

Informations de votre compte : Contrôle les informations que vous partagez avec d'autres applications et sites Web.

Supposons que vous vouliez contrôler qui peut voir vos publications. Vous pouvez suivre ces étapes simples :

Allez dans les paramètres de confidentialité de votre compte Facebook.

Trouvez la rubrique "Confidentialité des publications" ou similaire.

Choisissez l'option qui vous convient le mieux : par exemple, "Amis" pour limiter la visibilité à vos amis seulement.

Enregistrez vos modifications.

9-QUE FAIRE SI VOTRE ORDINATEUR EST INFECTÉ PAR UN VIRUS

REPONSE 1:

Mises à jour et antivirus : Vérifiez que votre système d'exploitation et vos logiciels sont à jour. Exécutez une analyse antivirus pour détecter tout logiciel malveillant.

Contrôle du pare-feu : Assurez-vous que votre pare-feu est activé et configuré pour bloquer les connexions non autorisées.

Test de phishing : Exécutez un test de phishing en visitant un site Web de test réputé pour vérifier si votre navigateur ou antivirus détecte les tentatives de phishing.

REPONSE 2:

Téléchargement et installation :

Choisissez un antivirus et un anti-malware fiables et réputés.
Rendez-vous sur le site officiel du logiciel pour télécharger la dernière version.

Suivez les instructions d'installation fournies par le programme d'installation.

Mise à jour et analyse initiale :

Une fois l'installation terminée, assurez-vous que le logiciel est mis à jour avec les dernières définitions de virus et de malware.

Lancez une analyse complète de votre ordinateur pour détecter toute menace potentielle.

Planification des analyses régulières :

Configurez l'antivirus et l'anti-malware pour qu'ils effectuent des analyses régulières de votre système, par exemple une fois par semaine.

Surveillance en temps réel :

Activez la protection en temps réel de l'antivirus pour qu'il surveille activement les activités suspectes et bloque les menaces en temps réel.

Quarantaine et suppression :

Si des logiciels malveillants sont détectés, suivez les instructions de l'antivirus pour les mettre en quarantaine ou les supprimer complètement.

Notifications et alertes :

Configurez l'antivirus pour recevoir des notifications en cas de détection de menaces ou de mises à jour importantes.

Maintenance et suivi :