

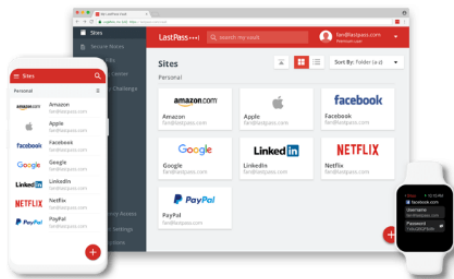
1- Introduction à la sécurité sur internet

- Site : Wired, Article : " The state of Cybersecurity in 2023"
- Site : TechCrunch, Article : "Latest Trends in Online Security : A comprehensive overview"
- Site : Cent, Article : "Top 10 Tips for staying Safe Online in 2023"

2- Créer des mots de passe forts

**Un mot de passe.
Zéro souci.**

| LastPass s'occupe du reste.



Fonctionnalités Free

- ✓ Coffre-fort de mots de passe sécurisé ⓘ
- ✓ Accès sur un type d'appareils ⓘ
- ✓ Partage d'une personne à une autre ⓘ

⚠ Il semble que quelque chose ne va pas. Vérifiez que vous avez tout saisi correctement.

Créer un compte

[ou Connexion](#)

Adresse e-mail

baelhadjisamba40@gmail.com

Mot de passe maître

••••••••••

Force

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

Mes conseils :

J'ai accédé à la plateforme lastpass et y créer un compte

✓ Votre compte a été créé avec succès !

FÉLICITATIONS

Bienvenue à LastPass !


Installez l'extension de navigateur, puis
connectez-vous avec le compte que vous
venez de créer.

Installer LastPass ↓

Super !! Le compte a été bien créé

chrome web store

Découvrir Extensions Thèmes

 **LastPass: Free P**

Sélection 4,3 ★ (27,7 k avis)

Extension Workflows/planification 10 000 000 utilisateurs

Installer "LastPass: Free Password Manager" ?

Cette extension Chrome peut :

- Lire et modifier toutes vos données sur tous les sites Web
- Afficher les notifications

Ajouter l'extension Annuler

Over 25 million people worldwide securely
save & fill passwords with LastPass

Instantly autofill pas
to all your save

For your eyes only. That's our

Maintenant on ajoute l'extension de générateur de mot de passe au niveau de notre navigateur à partir du chrome web store.

3- Fonctionnalité de sécurité de votre navigateur

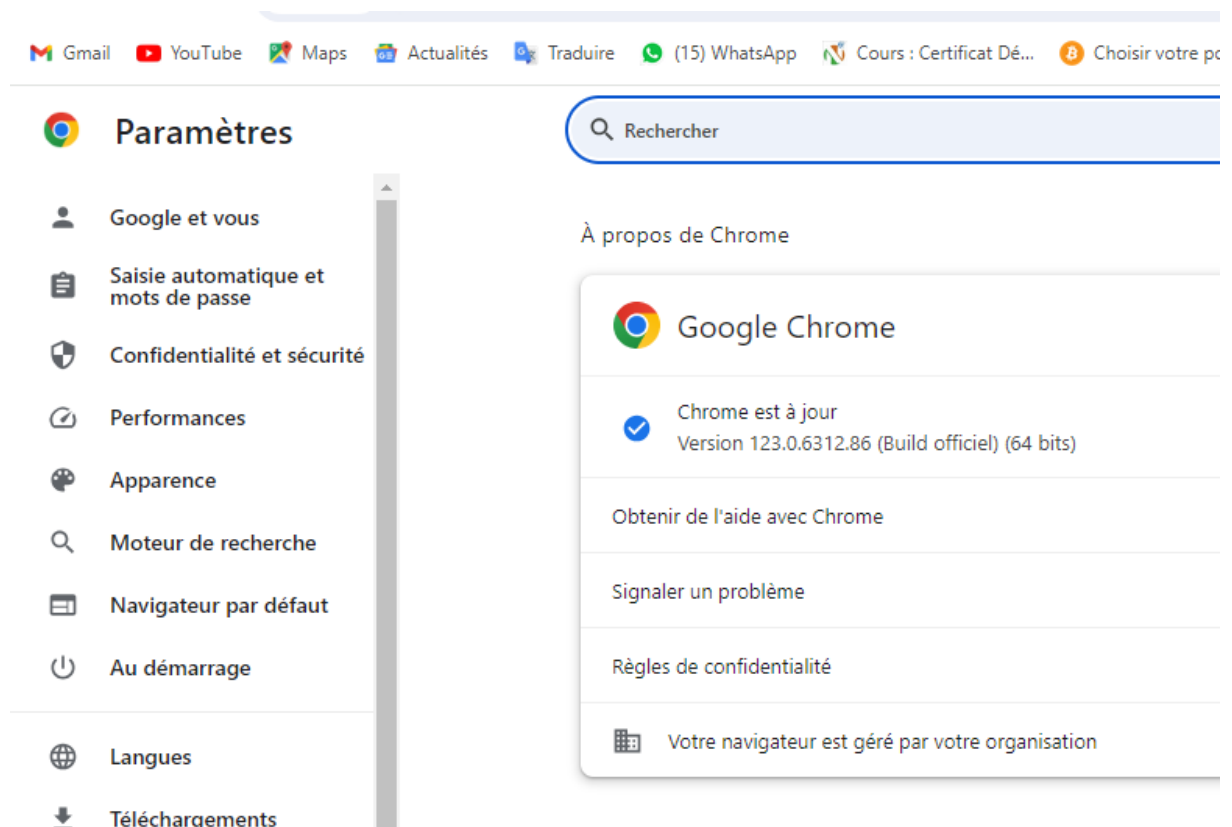
1. Identifions les adresses de site web qui nous semblent malveillantes :

www.morvel.com c'est peut-être un site web malveillant car ce site ressemble à peut près du site officiel des Marvels qui est : www.marvel.com

www.fessbook.com est un site qui peut être malveillant car il est dérivé du site officiel de Facebook qui est www.facebook.com

www.instagram.com est aussi peut-être un site malveillant pour essayer de duper les utilisateurs quand ils se trompent d'URL

2- vérifions si les navigateurs utilisés sont à jour



Ici on peut voir que notre navigateur chrome est à jour

Mises à jour de Firefox

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

Version 124.0.1 (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.

Pareil aussi pour firefox

4- Eviter le spam et le phishing

C'est exact ! Il s'agit d'un e-mail d'hameçonnage.

Vous avez sans doute remarqué que l'URL ressemble à la véritable adresse. Prenez garde aux liens hypertextes et pièces jointes que vous ouvrez à partir des e-mails, car ils peuvent rediriger vers des sites Web frauduleux qui vous invitent à saisir des informations sensibles.

MONTREZ-MOI

Luke Johnson <luke.json8000@gmail.com>
à moi ▾

Luke Johnson a partagé un lien vers le document suivant :

 [Budget département 2024.docx](#)



Bonjour. Voici le document demandé. N'hésitez pas à me contacter si vous avez besoin d'autre chose !

C'est exact ! Il s'agit d'un e-mail
d'hameçonnage.

en vu ! Comme vous l'avez remarqué, le domaine de messagerie de l'expéditeur est mal orthographié ("efacks"
en redirige vers le site "mailru382.co". L'hameçonnage consiste généralement à vous induire en erreur avec de
ressemblant à celle du site officiel.

MONTREZ-MOI

NoReply [admin] <noreply@efacks.com>

à moi

Vous avez reçu un fax d'une page le 02/04/2024 19:21

[Cliquez ici pour afficher ce fax en ligne](#)



C'est exact ! Il s'agit d'un e-mail
d'hameçonnage.

Vous avez correctement identifié l'URL trompeuse. Le véritable domaine est "sytez.net", que l'on a camouflé pour le faire
passer pour un lien Google Drive. Soyez particulièrement vigilant si vous n'êtes pas sûr de connaître l'expéditeur.

MONTREZ-MOI



TK <tk867530@gmail.com>

à moi

Salut, tu te souviens de [CETTE PHOTO](#) !

C'est exact ! Il s'agit d'un e-mail d'hameçonnage.

Cette tentative d'hameçonnage était difficile à repérer ! Les documents PDF peuvent contenir des logiciels malveillants ou des virus. Vérifiez toujours que l'expéditeur est digne de confiance, et utilisez votre navigateur ou un service comme Google Drive pour les ouvrir en toute sécurité.

MONTREZ-MOI



Sharon Mosley <sharon.mosley@westmountdayschool.org>
à moi

Bonjour El hadji samba Ba,

Veuillez trouver ci-joint le rapport d'activité financière de 2024, à lire attentivement.

Cordialement,

Mme Sharon Mosley
Westmount Day School

C'est exact ! Il s'agit d'un e-mail d'hameçonnage.

Cette tentative d'hameçonnage était difficile à repérer ! Les documents PDF peuvent contenir des logiciels malveillants ou des virus. Vérifiez toujours que l'expéditeur est digne de confiance, et utilisez votre navigateur ou un service comme Google Drive pour les ouvrir en toute sécurité.

MONTREZ-MOI



Sharon Mosley <sharon.mosley@westmountdayschool.org>
à moi

Bonjour El hadji samba Ba,

Veuillez trouver ci-joint le rapport d'activité financière de 2024, à lire attentivement.

Cordialement,

Mme Sharon Mosley
Westmount Day School

5- Comment éviter les logiciels malveillants

Vérifier l'état du site

www.sayna.io

État actuel



Aucun contenu suspect détecté

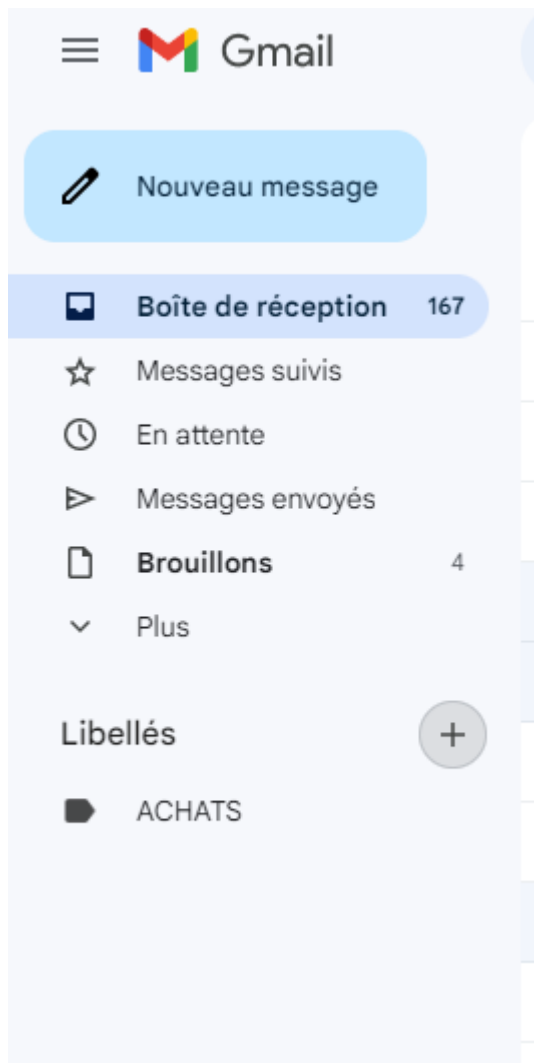
Informations sur le site

Ces informations ont été mises à jour pour la dernière fois le 2 avr. 2024.

La sécurité d'un site peut évoluer. Vérifiez régulièrement s'il y a des changements.

Par exemple ici on peut être rassuré que au niveau du site de sayna cote sécurité

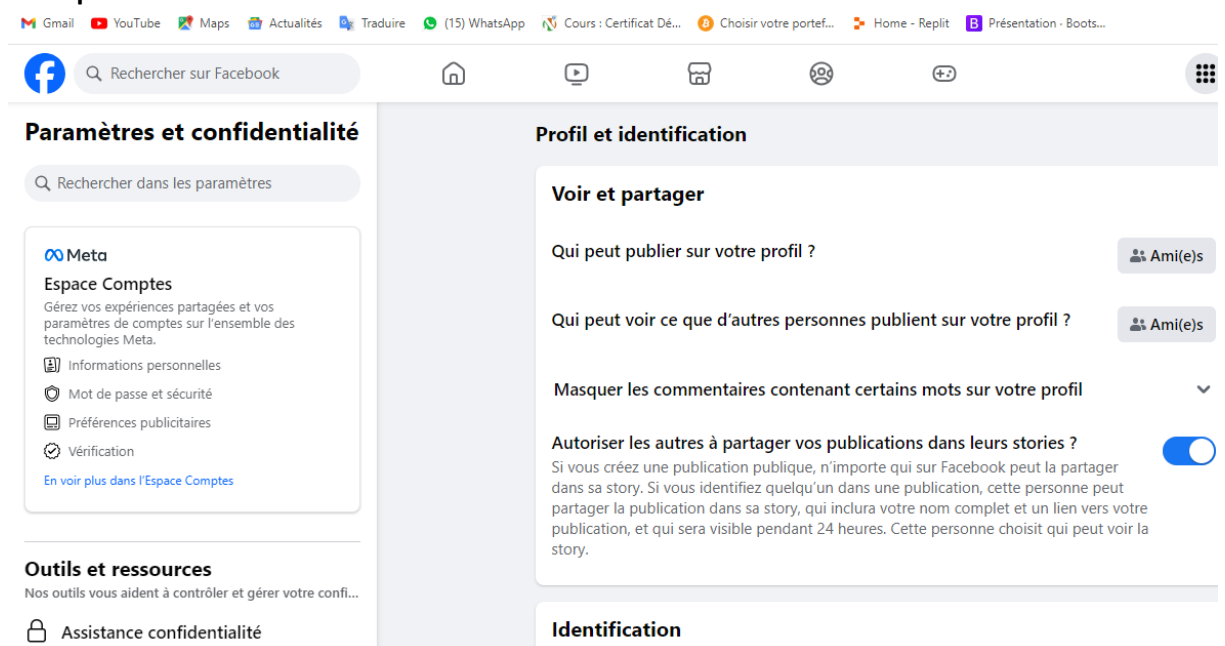
6- Achat en ligne



Ici dans mon messagerie électronique j'ai créé mon libelle ACHATS

7-

8- Principes de base de la confidentialité des medias sociaux



Là je suis au niveau de mon compte Facebook dans paramètre et confidentialité



Rechercher sur Facebook



Assistance confidentialité

Nous vous aiderons à prendre les bonnes décisions pour les paramètres de votre compte.
Par quelle rubrique voulez-vous commencer ?



On est là dans l'assistance de confidentialité

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

Voici quelques exercices pour évaluer la sécurité en fonction de l'appareil utilisé :

Exercice de test de vulnérabilité réseau : Utilisez un outil de test de vulnérabilité réseau tel que Nmap pour scanner les ports ouverts et les services en cours d'exécution sur un appareil. Comparez les résultats avec une liste des services autorisés pour déterminer les éventuelles vulnérabilités.

Exercice d'ingénierie sociale : Créez un scénario d'ingénierie sociale, comme l'envoi d'un e-mail de phishing ou la création d'un faux site Web, et observez la réaction des utilisateurs de différents appareils. Cela peut révéler leur niveau de sensibilisation à la sécurité et leur propension à être trompés.

Exercice de test de sécurité des applications : Téléchargez une application de test de sécurité sur chaque appareil et exécutez des analyses de vulnérabilité sur des applications spécifiques installées sur ces appareils. Cela peut révéler des problèmes de sécurité tels que des autorisations excessives ou des failles de codage.

Exercice de test d'accès physique : Testez la sécurité physique des appareils en les laissant sans surveillance dans des environnements publics pendant une courte période. Voyez combien de temps il faut aux passants pour tenter d'accéder aux données ou aux fonctionnalités sensibles.

Pour chaque exercice, assurez-vous de documenter soigneusement les résultats et de les comparer entre les différents appareils pour évaluer leur niveau de sécurité relatif.

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

Sélection de l'antivirus/antimalware approprié : Avant de commencer l'exercice, effectuez une recherche pour trouver un antivirus + antimalware compatible avec l'appareil utilisé. Assurez-vous de choisir une solution réputée et adaptée au système d'exploitation de l'appareil (par exemple, Windows, macOS, Android, iOS). Téléchargement et installation de

l'antivirus/antimalware : Téléchargez et installez l'antivirus + antimalware sur l'appareil selon les instructions du fournisseur. Assurez-vous de suivre toutes les étapes d'installation correctement. Configuration des paramètres de sécurité : Une fois l'antivirus/antimalware installé, configurez les paramètres de sécurité en fonction des recommandations du fournisseur. Cela peut inclure la planification des analyses régulières, la mise à jour automatique des définitions de virus, et l'activation des pare-feu intégrés. Analyse du système :

Lancez une analyse complète du système pour détecter les éventuelles menaces. Assurez-vous de comprendre les résultats de l'analyse et de prendre des mesures appropriées pour traiter les infections détectées. Surveillance et maintenance régulières : Après l'installation et la configuration initiales, assurez-vous de maintenir l'antivirus/antimalware à jour en installant les mises à jour de sécurité et en effectuant des analyses régulières du système. Évaluation de la performance : Surveillez l'impact de l'antivirus/antimalware sur les performances de l'appareil, notamment en termes de vitesse et d'utilisation des ressources. Si l'antivirus/antimalware ralentit considérablement l'appareil, explorez les options de configuration pour optimiser les performances. Rapport d'exercice : À la fin de l'exercice, rédigez un rapport décrivant les étapes suivies, les résultats des analyses, les performances de l'antivirus/antimalware et toute autre observation pertinente. En fonction de l'appareil utilisé, notez également les différences dans l'expérience d'installation et d'utilisation de l'antivirus/antimalware.