# SOMMAIRE

# I. Introduction à la sécurité internet

Article 1: cyber.gouv.fr-Dix règle d'or preventives

Article 2: CYBERMALVAILLANCE- LES DIX MESSURES ESSENTIEL POUR ASSURÉ VOTRE SÉCURITÉ

Article 3: OECD-La sécurité Numérique

# II. Crée des mots de passe fort

Désormais je peux enregistrer mes mot de passe lorsque je me connecte à mes comptes grâce à mon compte LastPass

# III. Fonctionnalité de sécurité de votre Navigateur

Réponse 1

Les sites web qui semblent être malveillants sont :

- www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel
- www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social Du monde
- www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très Utilisé

Les seuls sites qui semblaient être cohérents sont donc :

- www.dccomics.com, le site officiel de l'univers DC Comics
- www.ironman.com, le site officiel d'une compétition internationale de triathlon (et non Du super-héros issu de l'univers Marvel)

Réponse 2

## IV. Eviter le spam el le pushing

Réponse 1


Pour aller plus loin:

● Site du gouvernement cybermalveillance.gouv.fr

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconn

## V. comment éviter les logiciels malveillant

Réponse 1

● Site n°1

○ Indicateur de sécurité

■ HTTPS

○ Analyse Google

■ Aucun contenu suspect

● Site n°2

○ Indicateur de sécurité

■ Not secure

○ Analyse Google

■ Aucun contenu suspect

● Site n°3

○ Indicateur de sécurité

■ Not secure

○ Analyse Google

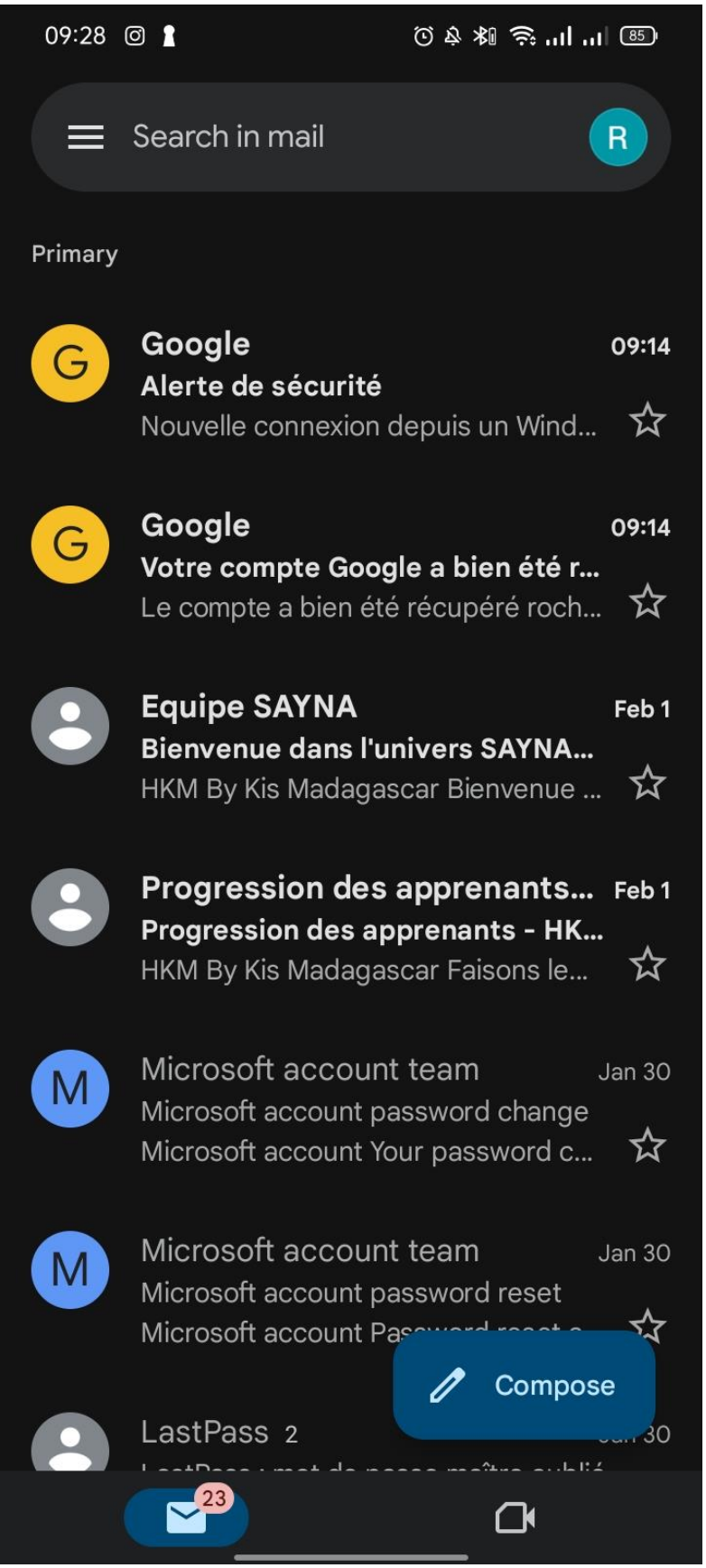
■ Vérifier un-URL en particulier (analyse trop générale)

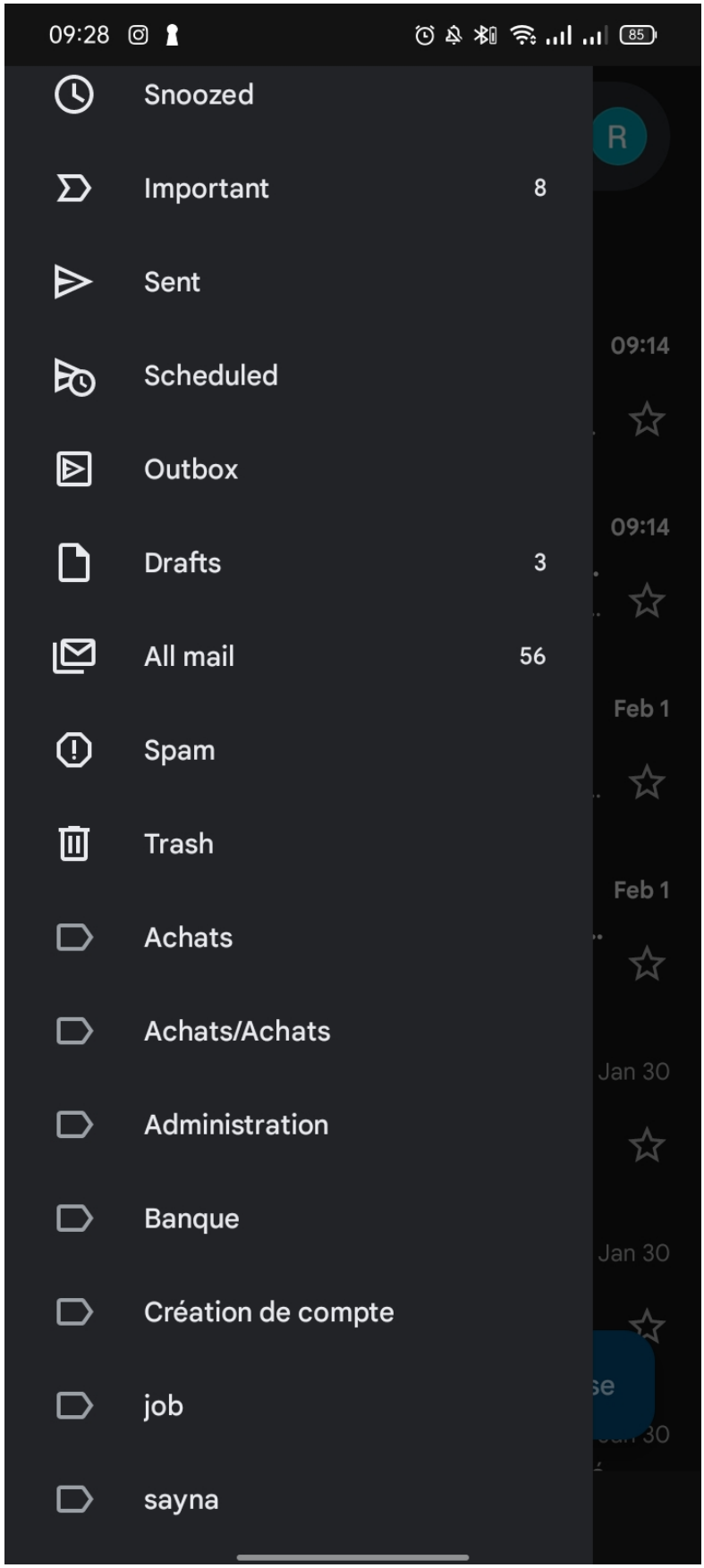
Tu peux tester la sécurité d'autres sites à partir de ce lien. Ce site référence et explique les Défauts de sécurité des sites dans le monde.

## VI. 6 – Achats en ligne sécurisés

Réponse 1

Registre des Achats – Janvier 2024


09:28
Search in mail
R
Primary
Google
09:14
Alerte de sécurité
Nouvelle connexion depuis un Wind...
Google
09:14
Votre compte Google a bien été r...
Le compte a bien été récupéré roch...
Equipe SAYNA
Feb 1
Bienvenue dans l'univers SAYNA...
HKM By Kis Madagascar Bienvenue ...
Progression des apprenants...
Feb 1
Progression des apprenants - HK...
HKM By Kis Madagascar Faisons le...
Microsoft account team
Jan 30
Microsoft account password change
Microsoft account Your password c...
Microsoft account team
Jan 30
Microsoft account password reset
Compose
LastPass 2
23


09:28
Snoozed
Important 8
Sent
Scheduled
Outbox
Drafts 3
All mail 56
Spam
Trash
Achats
Achats/Achats
Administration
Banque
Création de compte
job
sayna

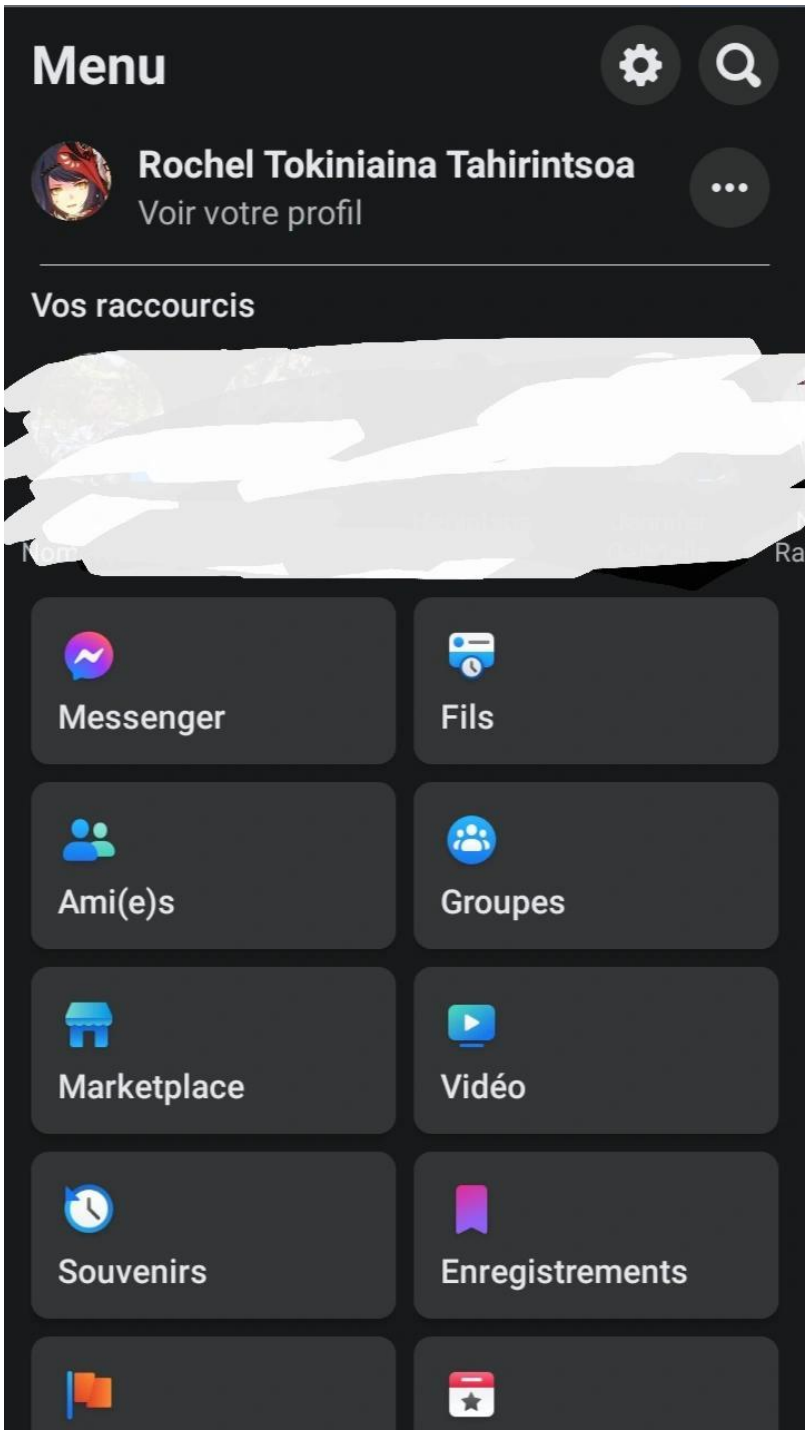
## VII. Comprendre le suivi du navigateur

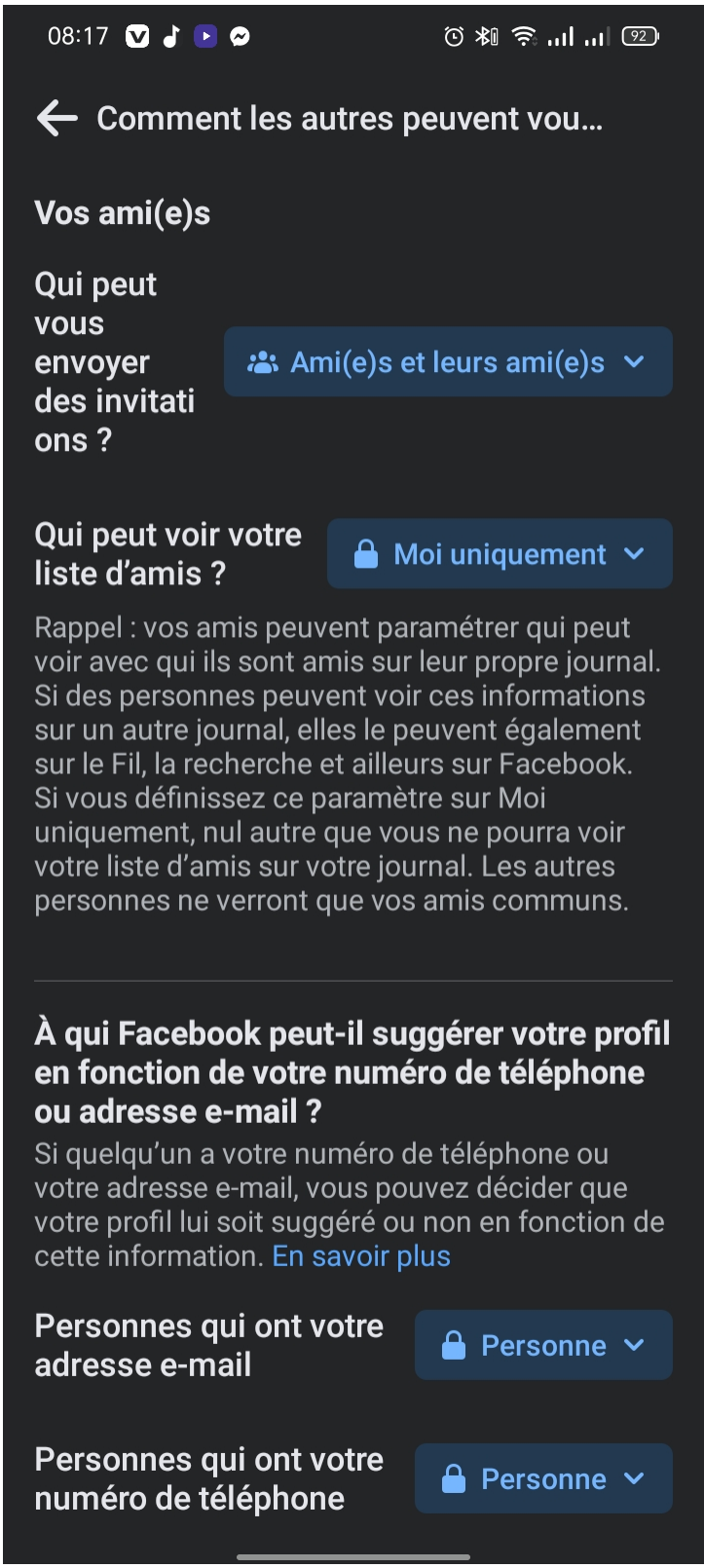
Voici quelques principes clés pour bien comprendre et suivre la navigation d'un navigateur web:

- Comprendre comment fonctionnent les requêtes HTTP et les réponses du serveur. Le navigateur envoie des requêtes HTTP (GET, POST, etc) au serveur et reçoit des réponses avec le code HTML/CSS/JS pour afficher la page.
- Savoir comment le navigateur traverse et construit le DOM (Document Object Model) à partir du code HTML reçu. Le DOM représente la structure de la page et permet de la manipuler avec JavaScript.
- Connaître le rendu CSS, comment les styles sont appliqués aux éléments du DOM pour obtenir le rendu visuel final.
- Comprendre le modèle d'événements et comment JavaScript peut réagir aux actions de l'utilisateur et mettre à jour dynamiquement le DOM et le CSS.
- Savoir comment les ressources (images, fichiers CSS/JS) sont récupérées et mises en cache pour optimiser les performances.
- Comprendre le fonctionnement du moteur JavaScript (V8 pour Chrome, SpiderMonkey pour Firefox etc) et l'exécution du code.
- Avoir des notions sur le sandbox de sécurité du navigateur et la même-origin policy pour isoler les contenus de différents sites.
- Connaître les outils de développement du navigateur pour debugger le JavaScript, inspecter le DOM, analyser les requêtes réseau, etc.

Ce sont quelques uns des concepts clés pour maîtriser ce qu'il se passe sous le capot d'un navigateur web. La compréhension de ces mécanismes est essentielle pour bien développer et debugger des sites et applications web.

## VIII. Principe de base de la confidentialité des medias sociaux



# IX. Que faire si votre ordinateur est infecté par un virus

1) Exercice pour verifier la sécurité en fonction de l'appareil utilisé? Comment faire?

Voici quelques suggestions d'exercices pour vérifier la sécurité d'un PC:

- Faites un scan antivirus complet et vérifiez que la définition des virus est à jour. Installez un antivirus réputé si vous n'en avez pas déjà un.

- Vérifiez que le pare-feu Windows est activé et correctement configuré. Assurez-vous qu'il filtre les connexions entrantes et sortantes.

- Exécutez un scan anti-logiciels malveillants pour détecter d'éventuels programmes indésirables. Utilisez Malwarebytes par exemple.

- Vérifiez que toutes les mises à jour Windows sont installées, en particulier les mises à jour de sécurité.

- Changez les mots de passe par défaut de votre routeur WiFi et désactivez la diffusion SSID. Sécurisez votre réseau.

- Vérifiez que des ports non nécessaires ne sont pas ouverts et exposés sur internet. Utilisez un scan de ports comme ShieldsUP.

- Activez le pare-feu de Windows et désactivez le partage de fichiers/imprimantes.

- Sauvegardez vos données importantes sur un support externe ou le cloud au cas où.

Faites ces vérifications régulièrement pour assurer une bonne hygiène de sécurité de votre ordinateur. N'hésitez pas à me recontacter si vous avez d'autres questions!

2) Exercice pour installer et utilisé un antivirus + antimalware en function de l'appareil utilsé

Voici les étapes pour installer et utiliser un antivirus et un anti-malware sur un PC

Téléchargez et installez un antivirus réputé comme Bitdefender, Kaspersky ou Avast. Assurez-vous de télécharger la version complète avec protection en temps réel.

Lancez une analyse complète avec l'antivirus pour vérifier que votre système est propre. Analysez tous les lecteurs et dossiers.

Téléchargez et installez un anti-malware comme Malwarebytes. Ce logiciel va détecter les programmes malveillants que l'antivirus peut manquer.

Faites une analyse complète avec Malwarebytes pour détecter les logiciels malveillants.

Dans les paramètres de l'antivirus, activez la protection en temps réel pour analyser automatiquement les fichiers au lancement ou téléchargement.

Planifiez des analyses complètes et mises à jour régulières (au moins une fois par semaine) pour vos logiciels de sécurité.

Lorsqu'une menace est détectée, mettez le fichier en quarantaine ou supprimez-le si l'antivirus ou l'anti-malware vous le recommande.

Surveillez les alertes et avertissements des logiciels. Ne désactivez pas la protection sans raison valable.

Maintenez vos logiciels de sécurité à jour pour qu'ils puissent détecter les nouvelles menaces