Sommaire

1 - Introduction à la sécurité sur Internet

2 - Créer des mots de passe forts

3 - Fonctionnalité de sécurité de votre navigateur

4 - Éviter 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

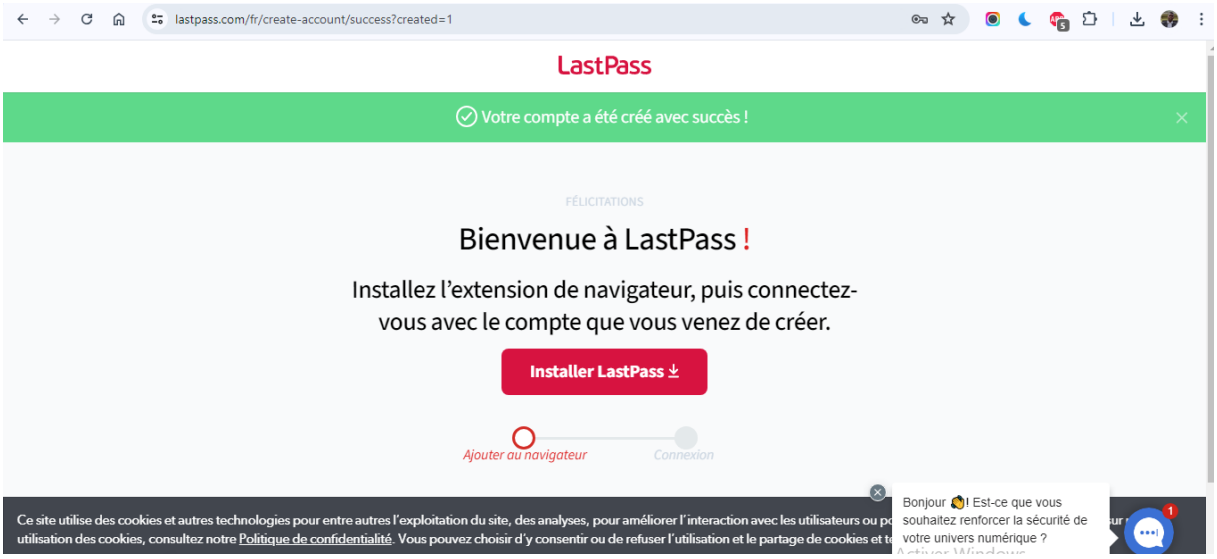
9 - Que faire si votre ordinateur est infecté par un virus

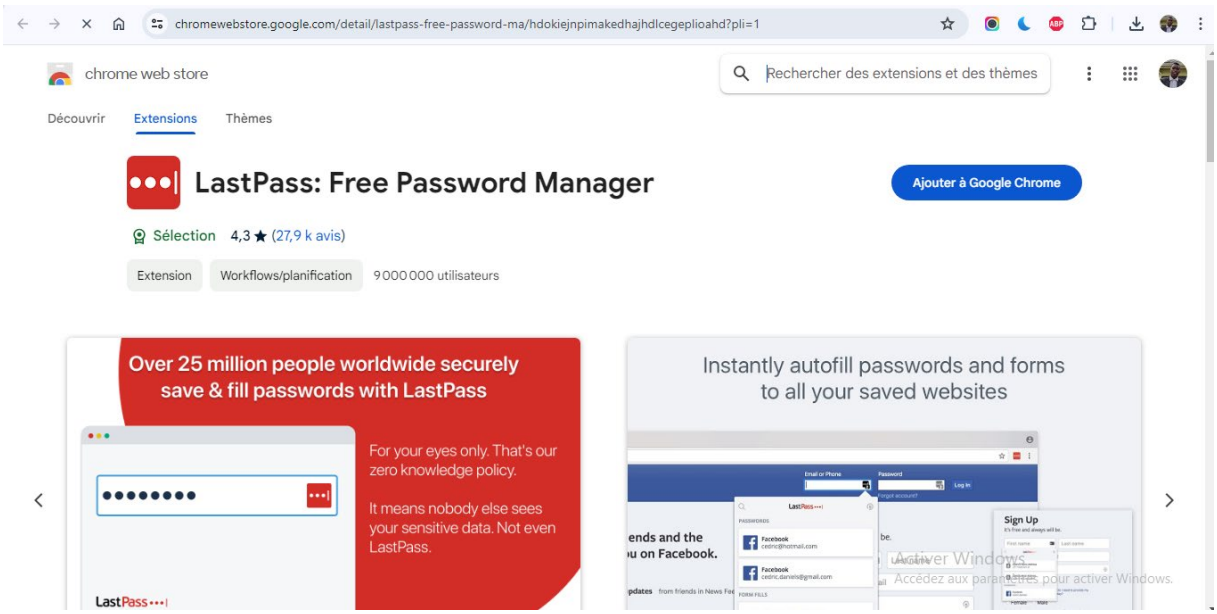
1 – Introduction à la sécurité sur Internet

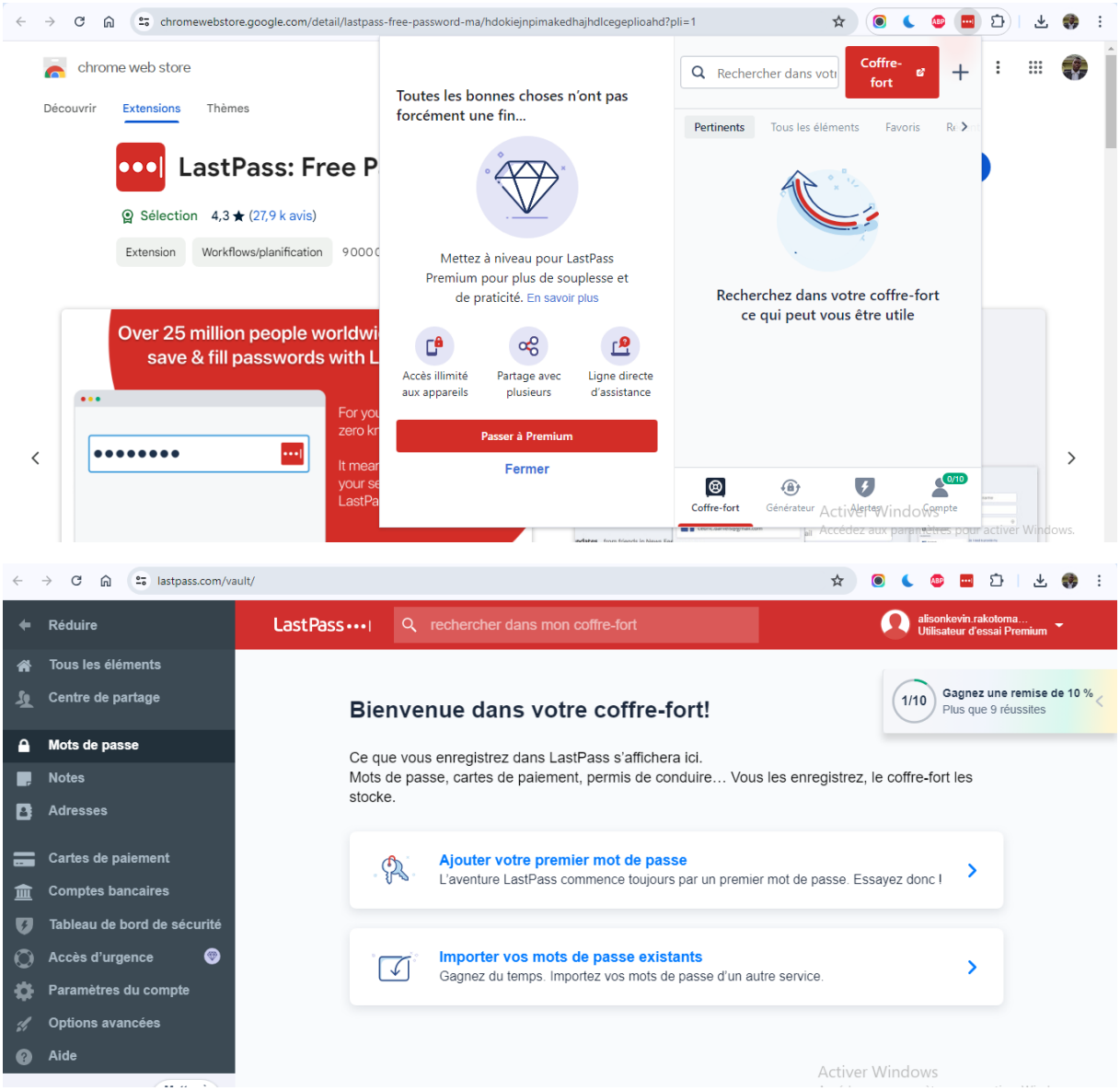
1/Les articles qui parlent de sécurité sur internet.

- Article 1 = cybermalveillance.gouv.fr-Comment se protéger sur Internet.
- Article 2 = European Youth Portal-La sécurité sur internet.
- Article 3 = F -Secure-Articles et conseils utiles sur la sécurité en ligne.

2 – Créer des mots de passe forts





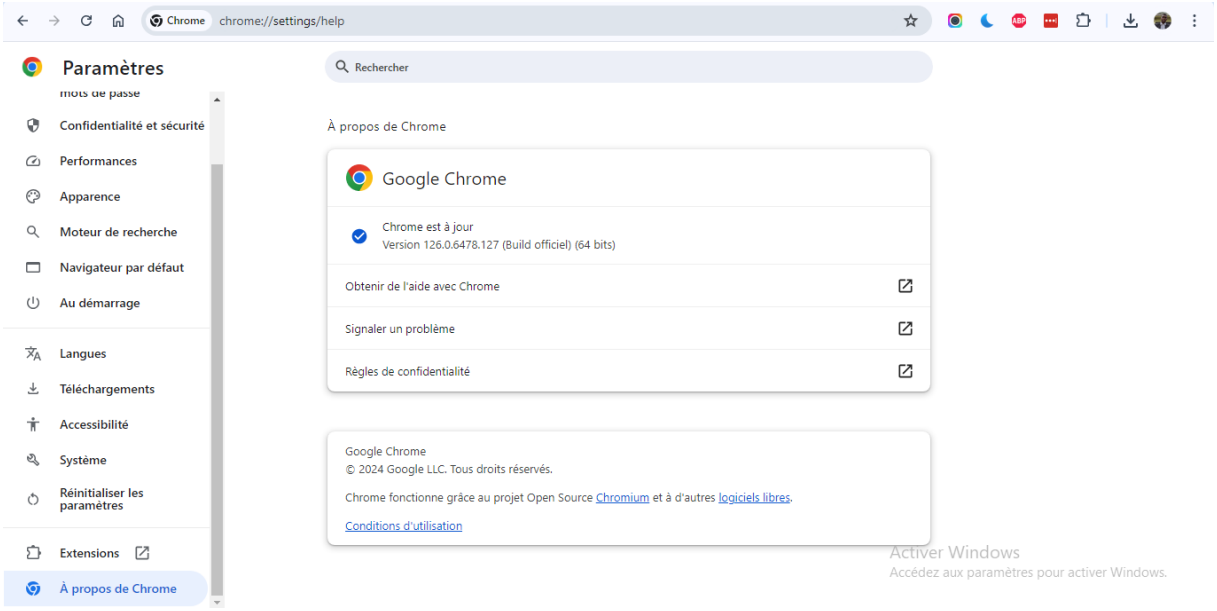


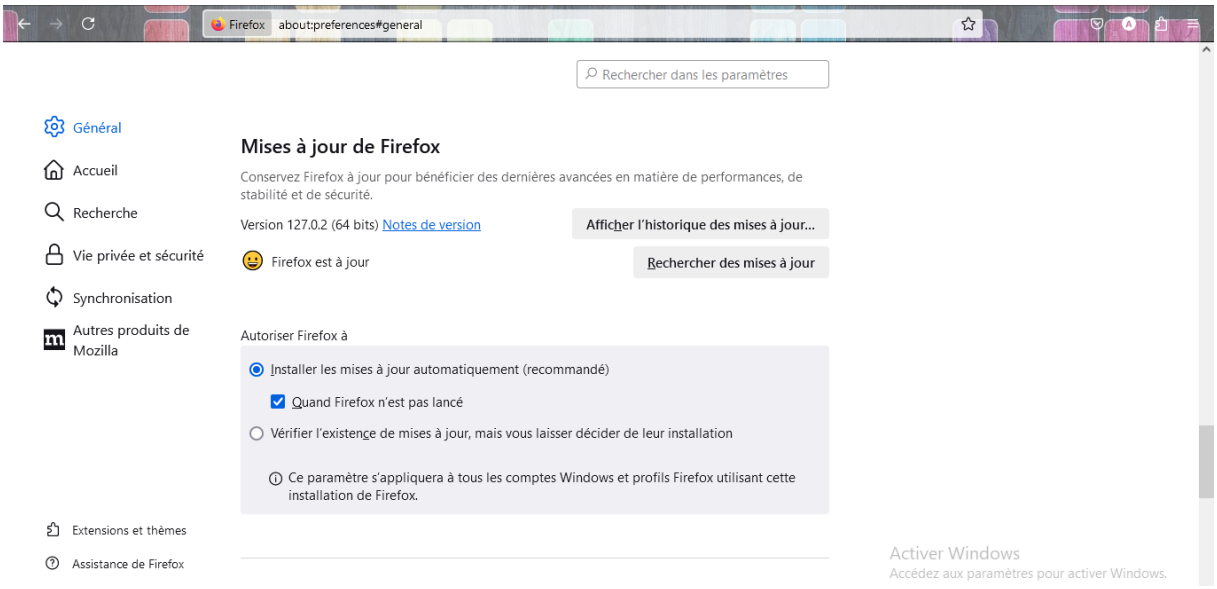
3 – Fonctionnalité de sécurité de votre navigateur

1/Les adresses internet 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

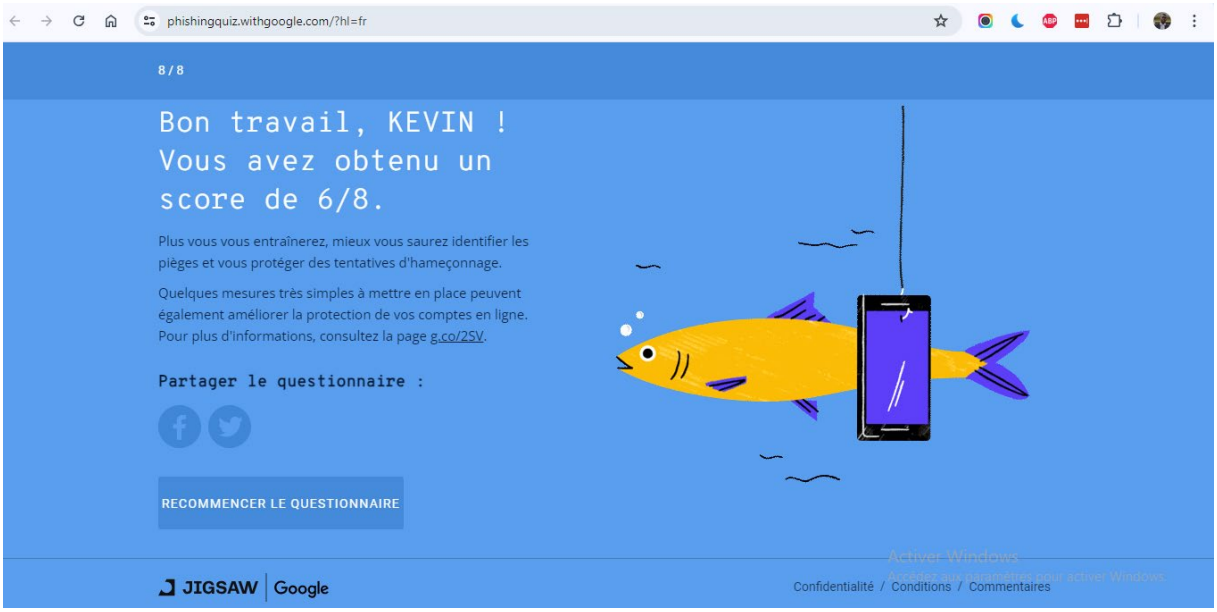
2/





4 – Eviter le spam et le phishing

1/



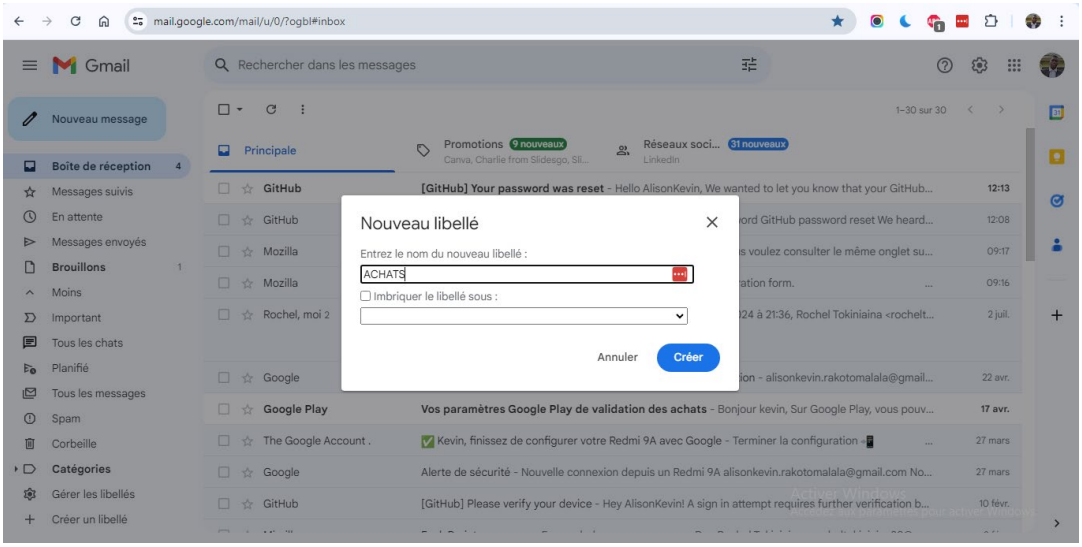
5 – Comment éviter les logiciels malveillants

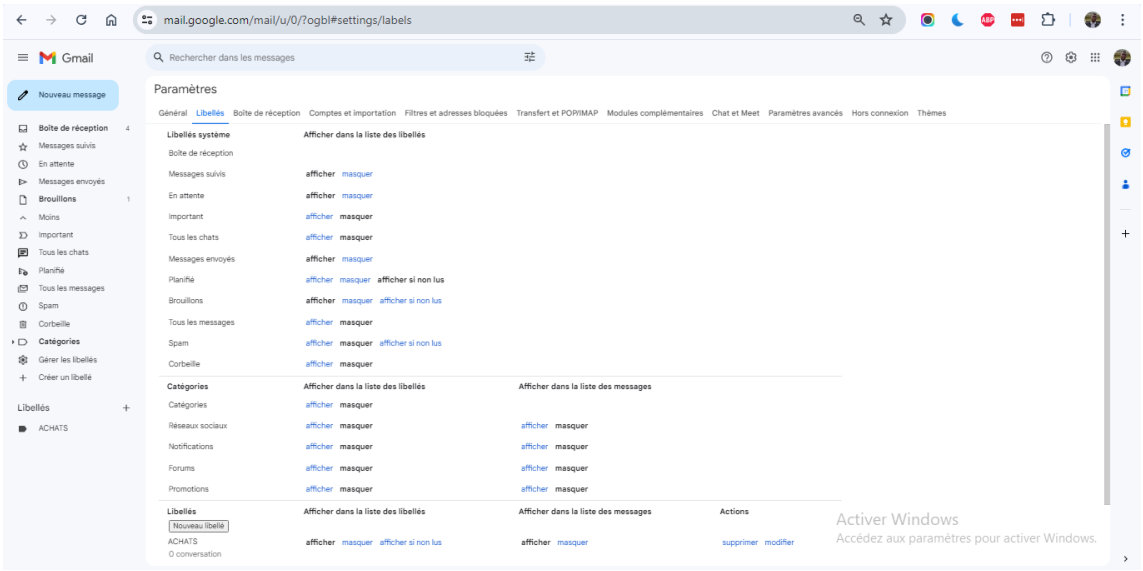
1/

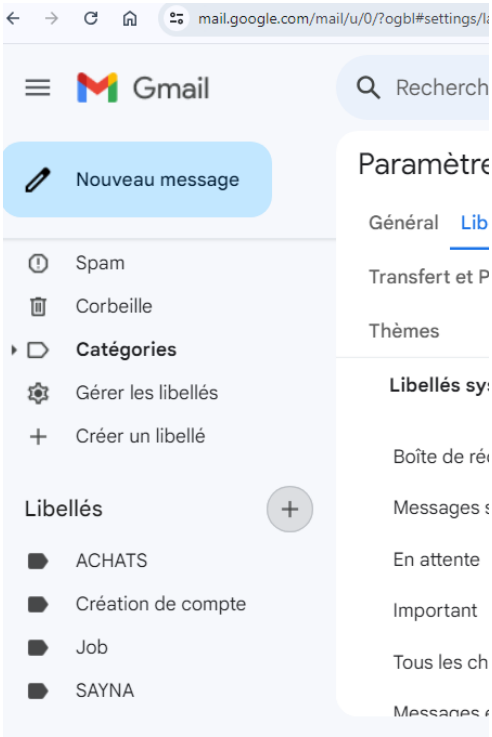
- Site n°1
  - Indicateur de sécurité
    -HTTPS
  - Analyse Google
    -Aucun contenu suspect
- Site n°2
  - Indicateur de sécurité
    -Not secure
  - Analyse Google
    -Aucun contenu suspect
- Site n°3
  - Indicateur de sécurité
    -Not secure
  - Analyse Google
    -Vérifier un URL en particulier (analyse trop générale)

6 – Achats en ligne sécurisés

1/Un exemple d'organisation de libellé pour gérer sa messagerie électronique :
-Achats : historique, facture, conversations liées aux achats
-Administratif : toutes les démarches administratives
-Banque : tous les documents et les conversations liés à la banque personnelle
-Création de compte : tous les messages liés à la création d'un compte (message de bienvenue, résumé du profil, etc.)
-Job : tous les messages liés à mon projet professionnel
-SAYNA : tous les messages liés mon activité avec SAYNA


mail.google.com/mail/u/0/?ogbl#inbox
Gmail
Rechercher dans les messages
Nouveau message
Boîte de réception
Messages suivis
En attente
Messages envoyés
Brouillons
Moins
Important
Tous les chats
Planifié
Tous les messages
Spam
Corbeille
Catégories
Gérer les libellés
Créer un libellé
Principale
Promotions
Réseaux soci...
Nouveau libellé
Entrez le nom du nouveau libellé :
ACHATS
Imbriquer le libellé sous :
Annuler
Créer


mail.google.com/mail/u/0/?ogbl#settings/labels
Gmail
Paramètres
Général
Libellés
Boîte de réception
Comptes et importation
Filtres et adresses bloquées
Transfert et POP/IMAP
Modules complémentaires
Chat et Meet
Paramètres avancés
Hors connexion
Thèmes
Libellés système
Afficher dans la liste des libellés
Catégories
Afficher dans la liste des messages
Actions
Nouveau libellé
ACHATS
Activer Windows


Gmail
Nouveau message
Spam
Corbeille
Catégories
Gérer les libellés
Créer un libellé
Libellés
ACHATS
Création de compte
Job
SAYNA
Général
Thèmes
En attente
Important

7 – Comprendre le suivi du navigateur

Vous pouvez autoriser ou bloquer les cookies tiers pour n'importe quel site :

1. Sur votre appareil Android, ouvrez Chrome.
2. En haut à droite, appuyez sur Plus. Paramètres.
3. Appuyez sur Paramètres du site. **Cookies** tiers. ...
4. Sélectionnez une option : Autoriser les **cookies** tiers.

Limites de la navigation privée :

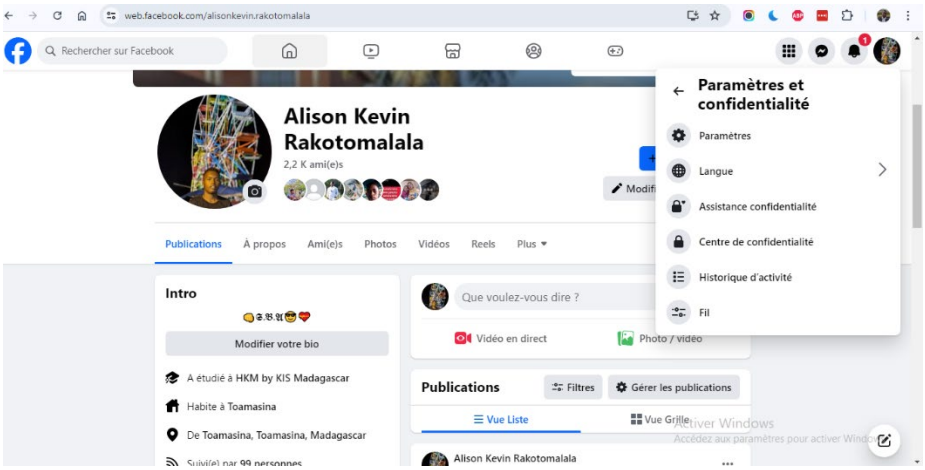
-Discutez des limites de la navigation privée :

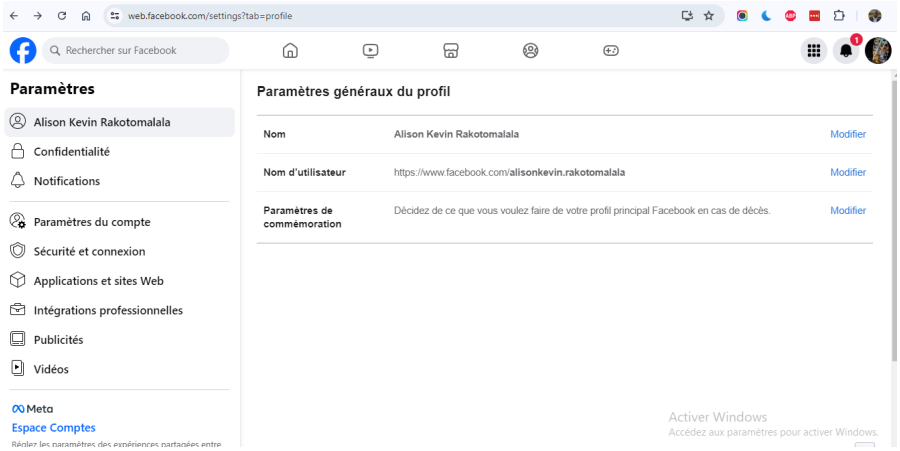
-Bien que les cookies temporaires soient supprimés à la fin de la session, d'autres types de suivi (comme l'adresse IP) peuvent toujours être visibles.

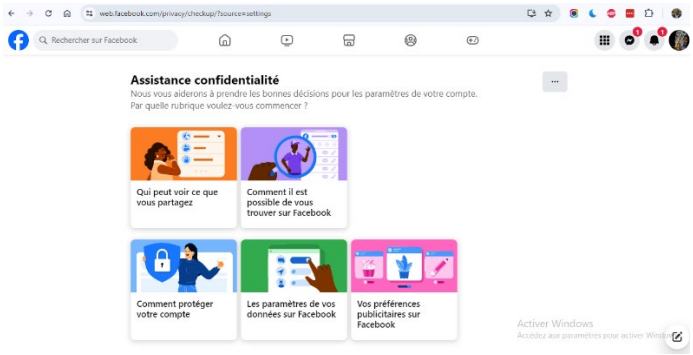
-Les activités effectuées dans la navigation privée peuvent être visibles pour l'employeur, l'école ou le fournisseur de services Internet.

8 – Principes de base de la confidentialité des médias sociaux

1/

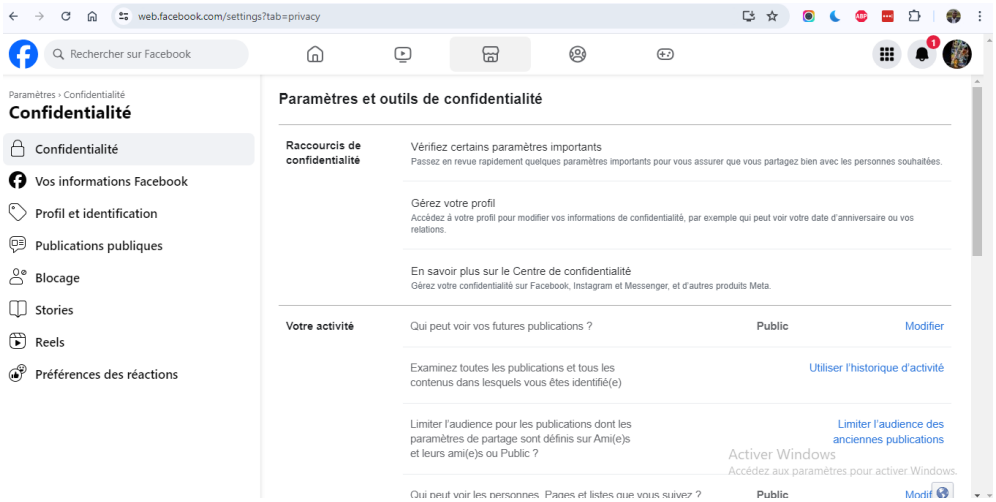




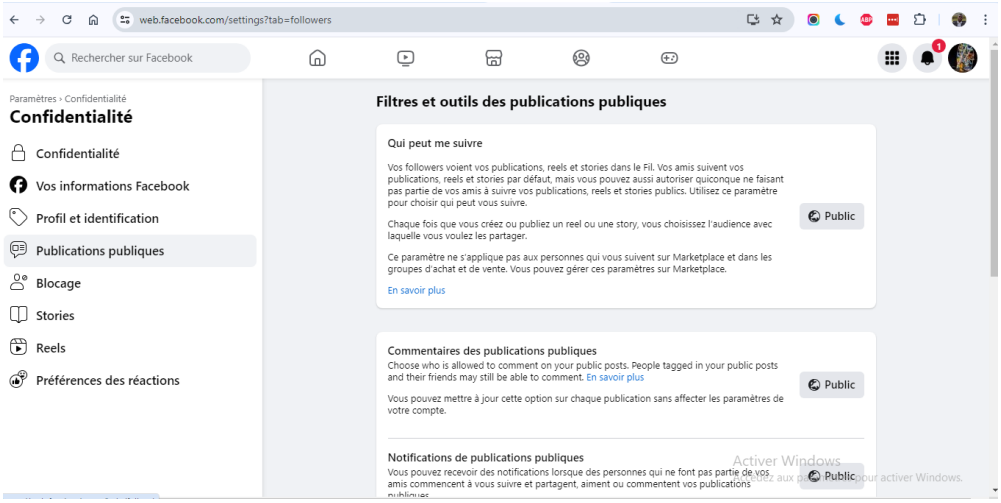


Voici un exemple de paramétrage de compte Facebook pour une utilisation privilégiant les échanges avec les amis, mais autorisant le contact avec des inconnus (limite de leurs actions) :

- Confidentialité



- Publications publiques



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

1/**Exercice 1 : Évaluation de la sécurité d'un appareil**

Objectif : Évaluer et améliorer la sécurité d'un appareil en identifiant les vulnérabilités potentielles et en appliquant les bonnes pratiques de sécurité.

Instructions :

1. **Analyse des paramètres de sécurité :**
    - Guidez les participants à travers les paramètres de sécurité de base de leur appareil :

        - Vérification des mises à jour : Assurez-vous que le système d'exploitation et toutes les applications sont à jour avec les derniers correctifs de sécurité.
        - Activation du verrouillage par mot de passe, code PIN ou reconnaissance faciale/empreinte digitale pour protéger l'accès physique à l'appareil.
        - Activation de la fonctionnalité de localisation et de verrouillage à distance (si disponible) pour protéger l'appareil en cas de perte ou de vol.
2. **Sécurité des réseaux :**
    - Faites une vérification des paramètres de sécurité du réseau Wi-Fi auquel l'appareil est connecté :
        - Utilisation d'un réseau Wi-Fi sécurisé et chiffrement des données transmises.
        - Activation du pare-feu sur l'appareil pour bloquer les connexions non autorisées.
3. **Protection contre les logiciels malveillants :**
    - Expliquez l'importance d'avoir une solution antivirus/malware installée et activée sur l'appareil.
    - Si possible, effectuez une analyse antivirus pour détecter et supprimer les éventuelles infections.
4. **Exercice pratique : Test de phishing et de sécurité des applications**
    - Simulez un scénario de phishing en envoyant un e-mail ou en visitant un site web suspect sur l'appareil.
    - Demandez aux participants d'identifier les signes de phishing et de discuter des actions à prendre pour éviter de tomber dans le piège (par exemple, ne pas cliquer sur les liens suspects, signaler le message comme phishing).
    - Faites une vérification de sécurité des applications installées sur l'appareil :
        - Vérification des autorisations accordées à chaque application.
        - Suppression des applications non utilisées ou suspectes.
5. **Sécurité des données et bonnes pratiques :**
    - Discutez des bonnes pratiques de sécurité des données, comme la sauvegarde régulière des données importantes et l'utilisation de solutions de stockage sécurisées.
    - Encouragez les participants à utiliser des mots de passe forts et différents pour chaque compte en ligne.

2/Un exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé.

Objectif : Apprendre à installer et à configurer un logiciel antivirus et antimalware pour protéger un ordinateur Windows contre les menaces en ligne.
Matériel requis : Un ordinateur Windows avec accès à Internet.
Instructions :

1. **Recherche et téléchargement :**

- Expliquez l'importance d'avoir un logiciel antivirus et antimalware pour protéger l'ordinateur contre les virus, les logiciels malveillants et autres menaces.
- Guidez les participants à choisir un logiciel antivirus reconnu et réputé. Exemples : Avast, AVG, Bitdefender, Malwarebytes, etc.
- Montrez comment accéder au site web du fournisseur de logiciel antivirus et antimalware choisi pour télécharger la version compatible avec Windows.

2. **Installation du logiciel :**
   - Fournissez des instructions étape par étape sur l'installation du logiciel antivirus :
     - Double-cliquez sur le fichier téléchargé pour démarrer l'installation.
     - Suivez les instructions à l'écran pour compléter le processus d'installation.
     - Pendant l'installation, assurez-vous que les participants comprennent chaque option de configuration (par exemple, installation par défaut vs personnalisée).
3. **Configuration et mise à jour :**
   - Après l'installation, guidez les participants à travers les étapes de configuration initiale du logiciel :
     - Activation du logiciel avec la clé de licence fournie (le cas échéant).
     - Planification des analyses automatiques du système pour détecter et supprimer les menaces.
     - Activation des mises à jour automatiques pour maintenir la base de données de virus à jour.
4. **Première analyse et gestion des menaces :**
   - Initiez une première analyse complète du système pour détecter les menaces potentielles :
     - Montrez aux participants comment lancer une analyse manuelle à partir de l'interface du logiciel antivirus.
     - Expliquez les actions recommandées pour traiter les fichiers suspects détectés pendant l'analyse (mise en quarantaine, suppression, etc.).
5. **Utilisation quotidienne et bonnes pratiques :**
   - Discutez des bonnes pratiques pour une utilisation quotidienne sécurisée de l'ordinateur :
     - Éviter de télécharger des fichiers à partir de sources non fiables.
     - Ne pas cliquer sur des liens suspects ou des pièces jointes d'e-mails inconnus.
     - Encourager la mise à jour régulière du logiciel antivirus et du système d'exploitation.