Parcours : DISCOVERY

Module : Naviguer en toute sécurité

Projet 1 – Un peu plus de sécurité, on n'en a jamais assez !

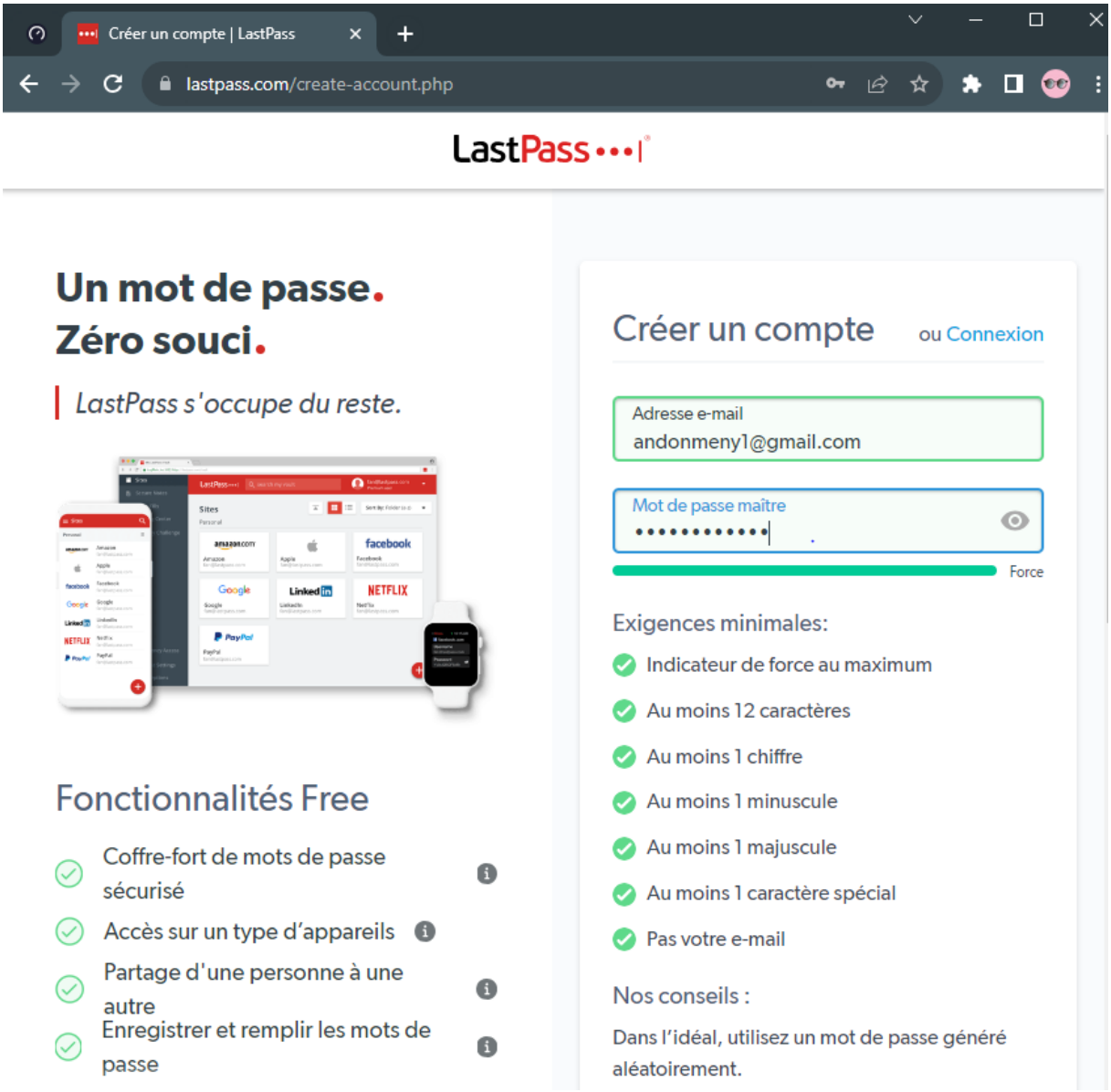
1 – Introduction à la sécurité sur Internet

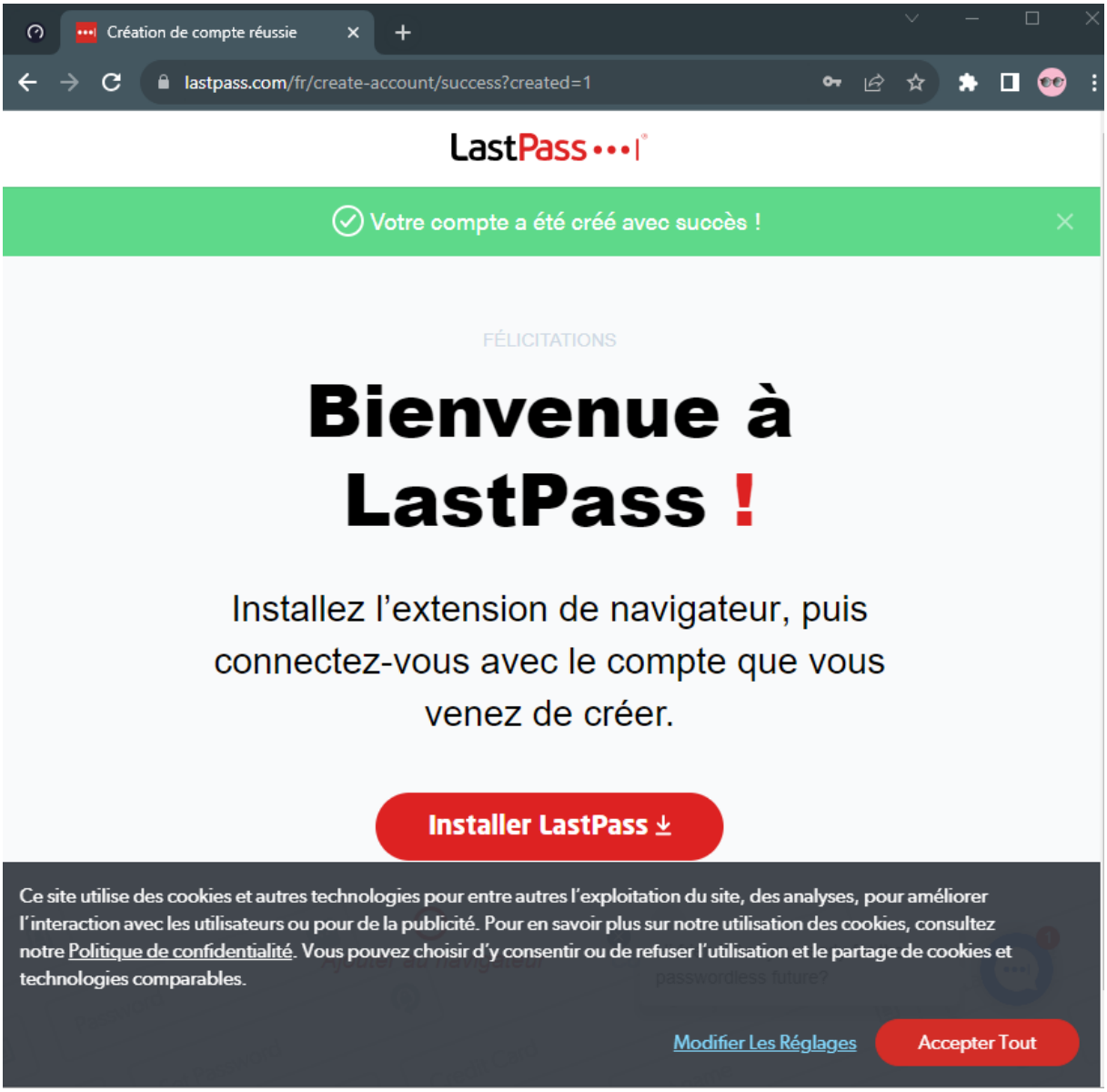
Réponse 1

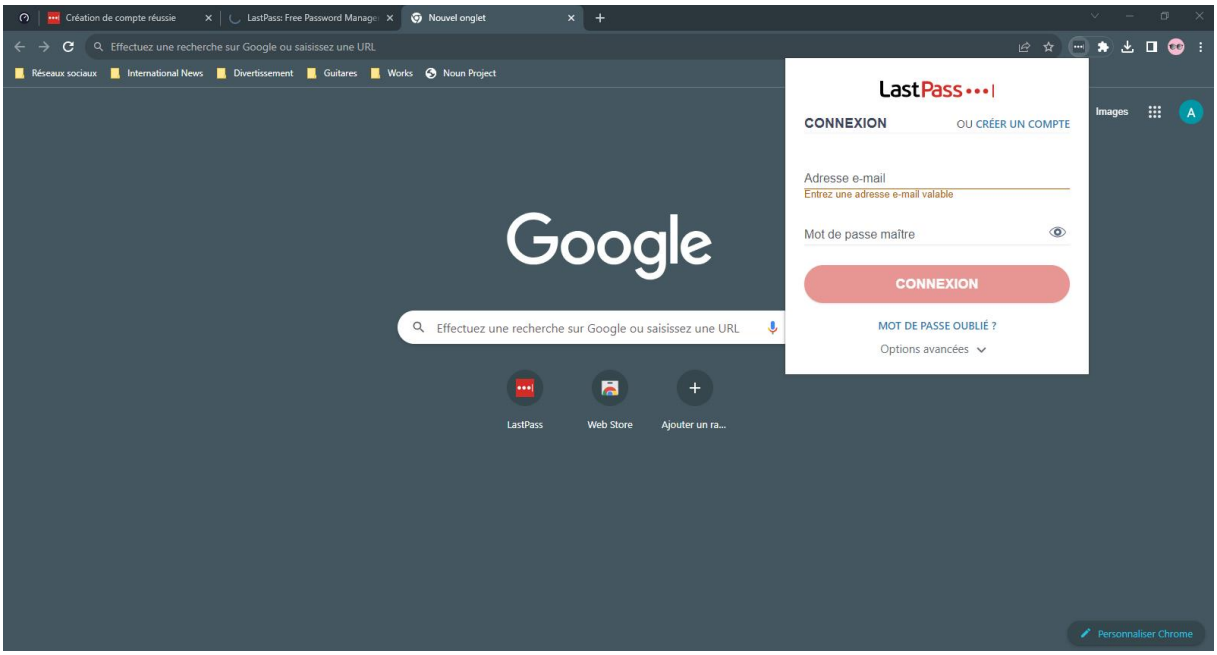
- Article 1 = Lesjeudis - Comment sécuriser votre navigation sur Internet ?
- Article 2 = Digitiz.fr – Comment sécuriser sa navigation sur le web ?
- Article 3 = vpnoverview – Navigation sécurisée

2 – Créer des mots de passe forts

Réponse 1




Création de compte réussie
lastpass.com/fr/create-account/success?created=1
LastPass
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
Ce site utilise des cookies et autres technologies pour entre autres l'exploitation du site, des analyses, pour améliorer l'interaction avec les utilisateurs ou pour de la publicité. Pour en savoir plus sur notre utilisation des cookies, consultez notre Politique de confidentialité. Vous pouvez choisir d'y consentir ou de refuser l'utilisation et le partage de cookies et technologies comparables.
Modifier Les Réglages
Accepter Tout



3 – Fonctionnalité de sécurité de votre navigateur

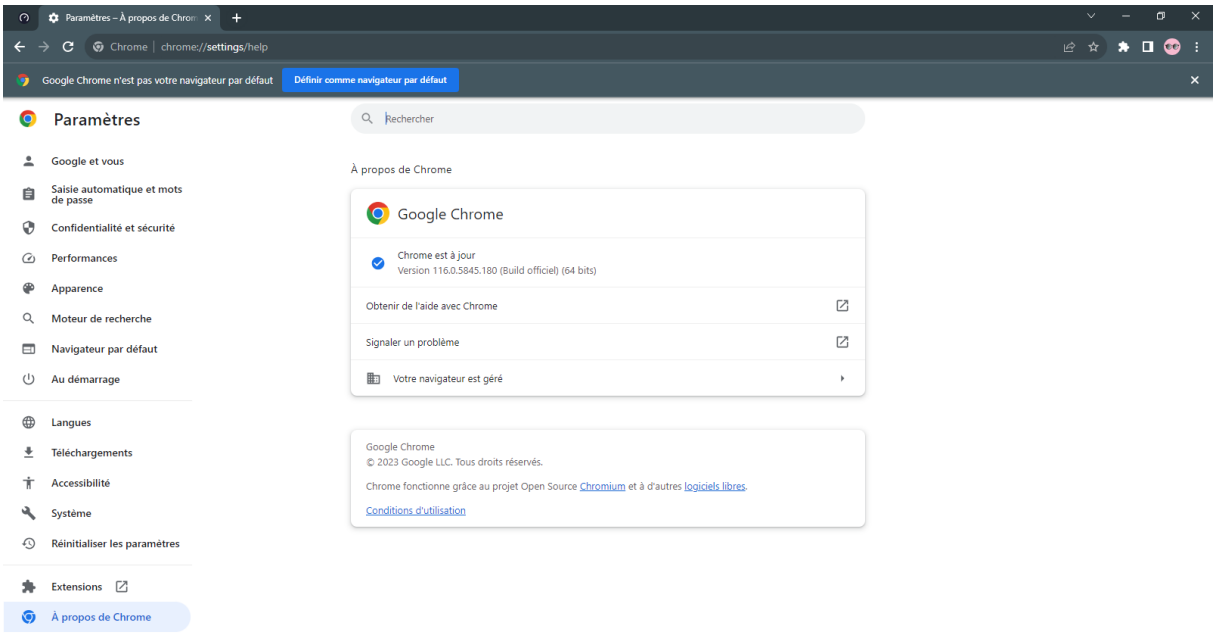
Réponse 1

Les sites web qui semblent être malveillants sont :

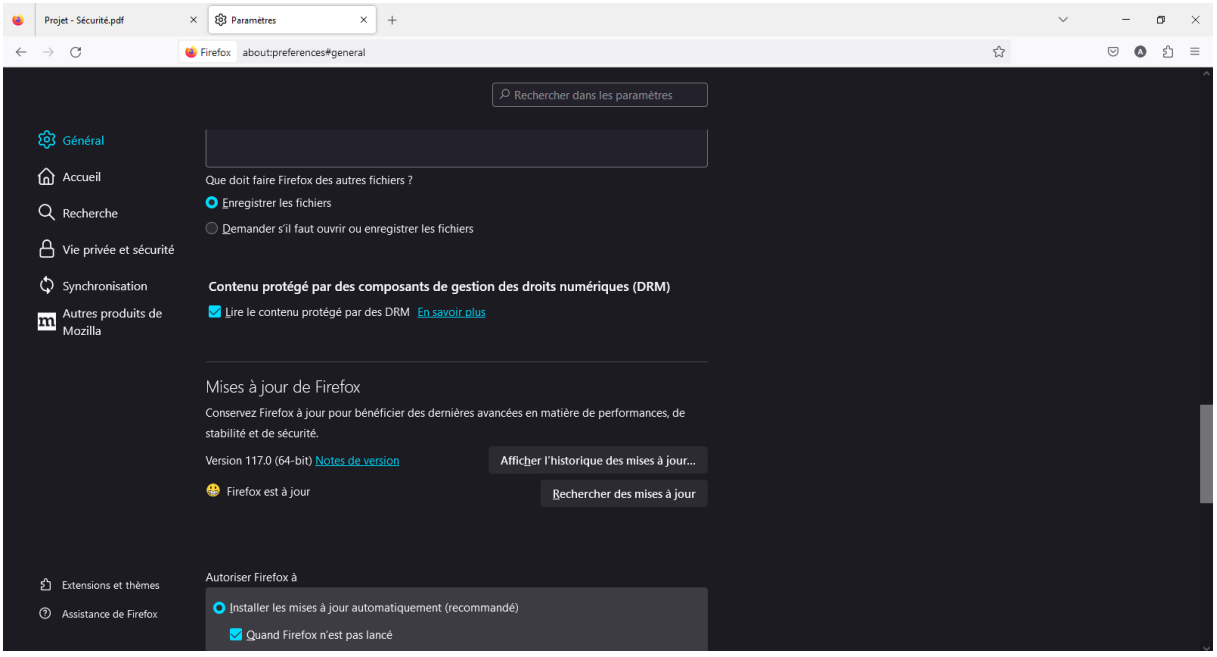
- www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel
- www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde
- www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très utilisé

Réponse 2

- **Pour Chrome**



- **Pour Firefox**



4 – Eviter les spam et phishing

Réponse 1

5 – comment éviter les logiciels malveillants

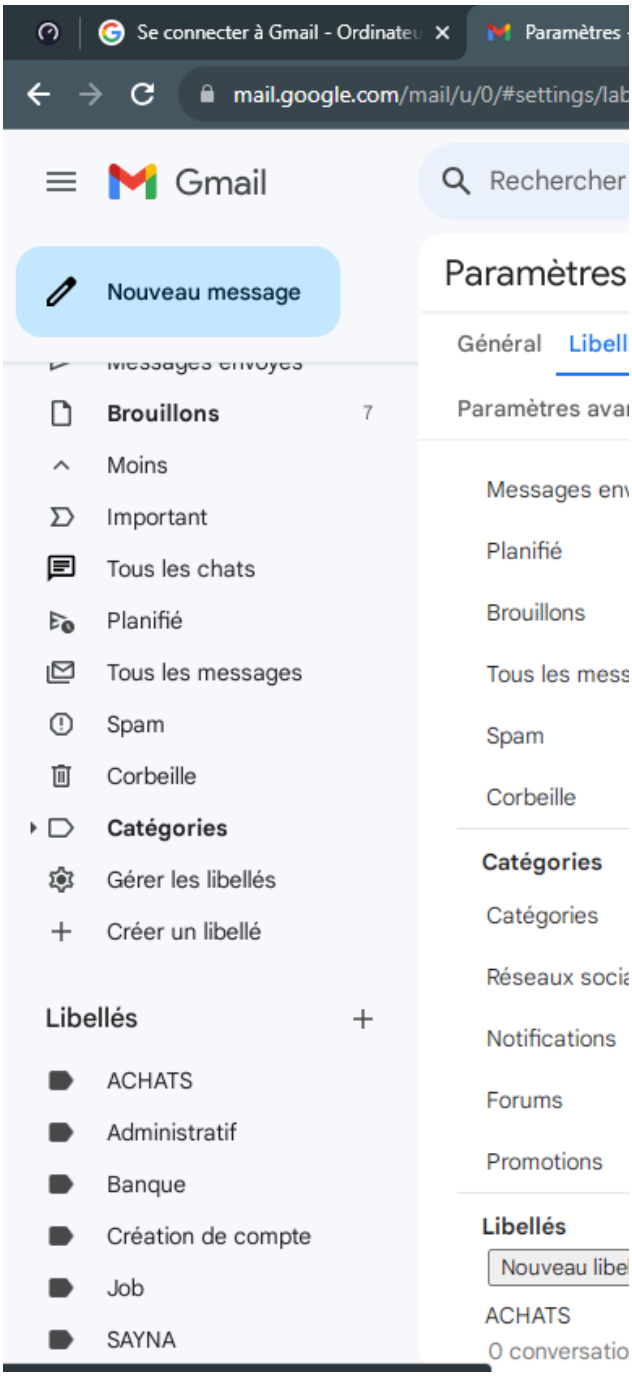
- Site n°1
  - **Indicateur de sécurité**
    - HTTPS
  - **Analyse de Google**
    - Aucun contenu suspect détecté
- Site n°2
  - **Indicateur de sécurité**
    - HTTPS
  - **Analyse de Google**
    - Aucun contenu suspect détecté

- Site n°3
  - **Indicateur de sécurité**
    - HTTPS
  - **Analyse de Google**

    Vérifie un URL en particulier

6 – Achats en ligne sécurisés

Réponse 1

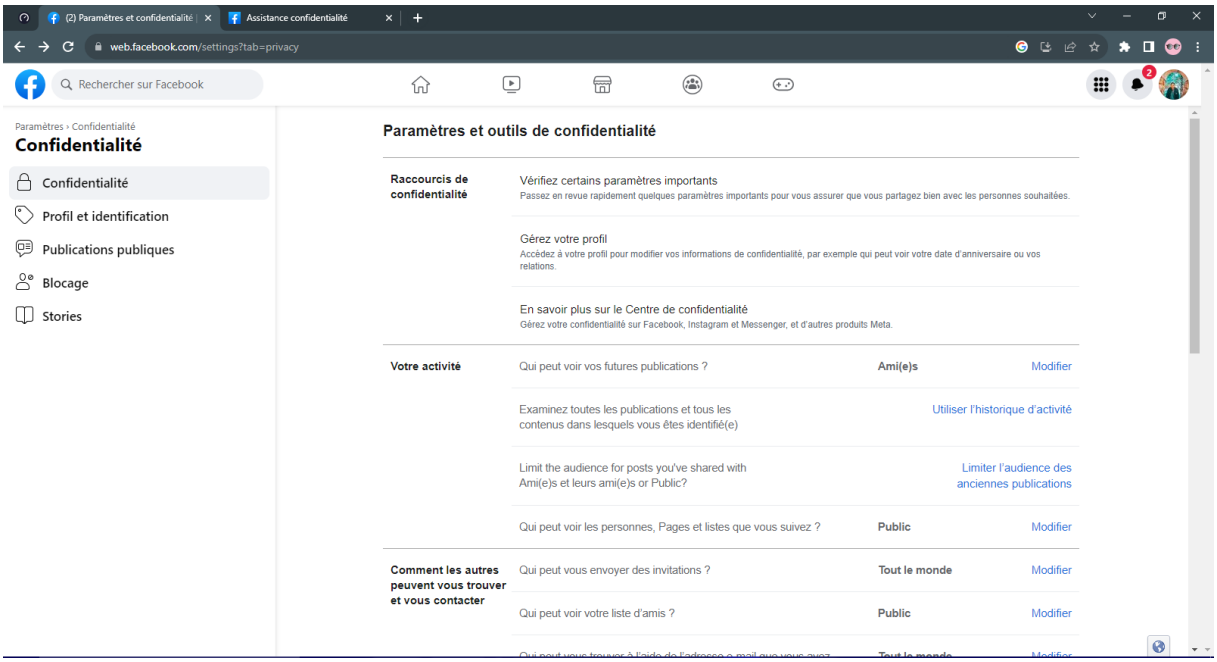


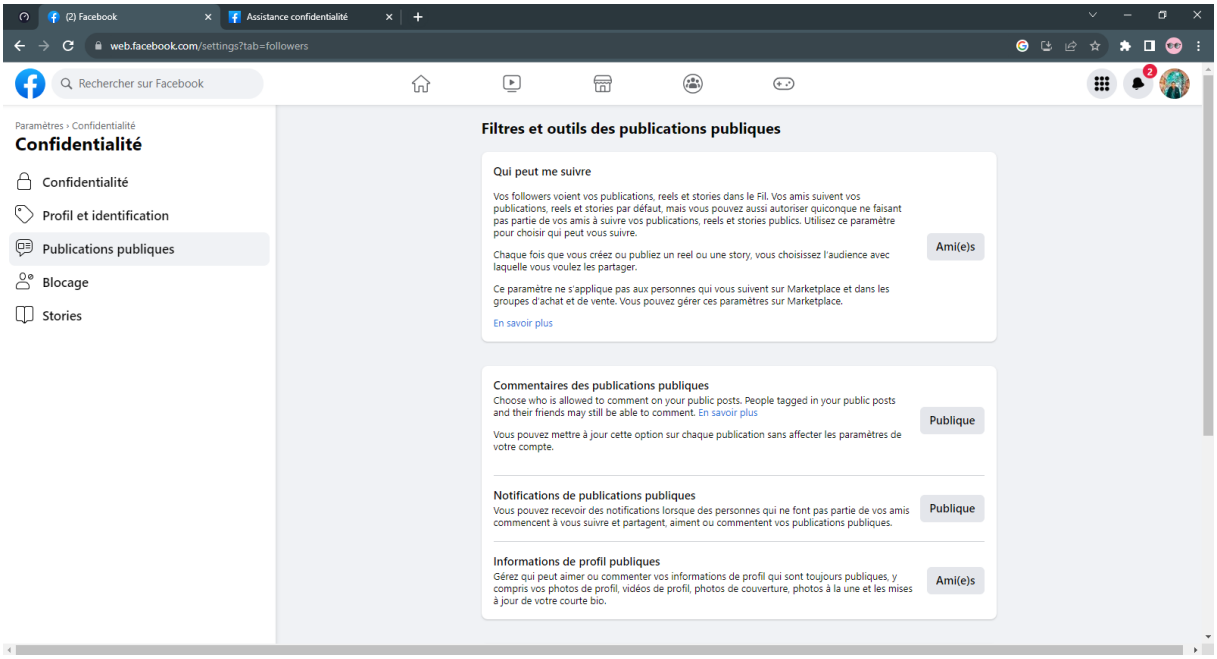
7 – Comprendre le suivi du navigateur

Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée.

8 – Principes de base de la confidentialité des médias sociaux

Réponse 1





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

Réponse 1

1. Mettez à jour votre système d'exploitation :
   Assurez-vous que votre système d'exploitation (comme Windows, macOS, Linux) est à jour avec les dernières mises à jour de sécurité. Les mises à jour régulières aident à corriger les vulnérabilités connues et à renforcer la sécurité de votre ordinateur.
2. Installez un logiciel antivirus et antispyware :
   Utilisez un logiciel antivirus réputé et maintenez-le à jour pour détecter et supprimer les logiciels malveillants (virus, chevaux de Troie, spywares, etc.) qui pourraient compromettre la sécurité de votre ordinateur.
3. Activez le pare-feu :
   Assurez-vous que le pare-feu de votre système d'exploitation est activé. Le pare-feu aide à bloquer les connexions non autorisées et à protéger votre ordinateur contre les attaques réseau.
4. Utilisez des mots de passe forts :
   Utilisez des mots de passe uniques et complexes pour vos comptes d'utilisateur et vos services en ligne. Utilisez une combinaison de lettres, de chiffres et de caractères spéciaux, et évitez d'utiliser des mots courants ou faciles à deviner.
5. Naviguez en toute sécurité sur Internet :
   Utilisez un navigateur sécurisé et assurez-vous que vous visitez des sites Web fiables. Vérifiez toujours l'URL du site avant de fournir des informations sensibles et évitez de cliquer sur des liens ou des pièces jointes provenant de sources non fiables.
6. Faites des sauvegardes régulières :
   Sauvegardez régulièrement vos fichiers importants sur des supports externes ou dans le cloud. En cas de problème de sécurité ou de perte de données, vous pourrez restaurer vos fichiers à partir des sauvegardes.
7. Soyez vigilant face aux emails et aux téléchargements suspects :
   Évitez de cliquer sur des liens ou de télécharger des fichiers provenant d'e-mails non sollicités ou de sources douteuses. Ces e-mails peuvent contenir des logiciels malveillants.

Réponse 2

1. Ordinateurs de bureau et portables (Windows ou macOS) :

- Recherchez des antivirus et antimalwares réputés tels que Avast, Norton, McAfee, Bitdefender, Malwarebytes, etc.

- Rendez-vous sur le site Web du fournisseur de l'antivirus et téléchargez le programme d'installation correspondant à votre système d'exploitation.

- Exécutez le programme d'installation et suivez les instructions à l'écran pour installer le logiciel.

- Une fois installé, mettez à jour l'antivirus et effectuez une analyse complète de votre ordinateur.

- Configurez les paramètres de l'antivirus selon vos préférences, tels que les scans planifiés, les mises à jour automatiques, etc.

- Gardez l'antivirus et l'antimalware à jour en installant les mises à jour régulières fournies par le fournisseur.

2. Téléphones et tablettes Android :

- Accédez au Google Play Store et recherchez des applications antivirus et antimalwares populaires telles que Avast, McAfee, Bitdefender, Malwarebytes, etc.

- Sélectionnez l'application souhaitée, appuyez sur "Installer" et suivez les instructions pour l'installation.

- Une fois installée, ouvrez l'application, acceptez les autorisations nécessaires et effectuez une analyse complète de votre appareil.

- Configurez les paramètres de l'application selon vos préférences, tels que les analyses automatiques, les blocages d'applications suspectes, etc.

- Mettez régulièrement à jour l'application antivirus en installant les mises à jour disponibles sur le Google Play Store.

3.Pour les iPhone et iPad (iOS),

Il convient de noter que le système d'exploitation iOS est conçu de manière à être sécurisé par défaut, et il est généralement moins vulnérable aux logiciels malveillants par rapport à d'autres plateformes. Cela est dû à des mesures de sécurité intégrées telles que la validation stricte des applications via l'App Store et le bac à sable (sandboxing) qui limite l'accès des applications à d'autres parties du système.

En raison de ces mesures de sécurité, il n'est pas aussi courant ni aussi nécessaire d'installer un antivirus ou un antimalware sur un iPhone ou un iPad par rapport aux ordinateurs et aux appareils Android. Apple a mis en place des contrôles stricts sur les applications disponibles sur l'App Store pour s'assurer qu'elles sont sûres avant de les rendre accessibles aux utilisateurs. Cependant, si vous souhaitez ajouter une couche de protection supplémentaire, vous pouvez toujours trouver des applications antivirus et antimalwares sur l'App Store, telles que Avira Mobile Security, McAfee Mobile Security, etc. Ces applications peuvent offrir des fonctionnalités telles que la protection contre le phishing, le blocage des sites Web malveillants et la localisation à distance de votre appareil en cas de perte.

Il est important de noter que lors de l'installation d'applications antivirus ou antimalwares sur iOS, elles fonctionnent généralement en tant qu'outils de sécurité supplémentaires et ne sont pas capables de scanner l'ensemble du système iOS ou d'analyser les applications tierces installées. Elles se concentrent principalement sur la protection contre les menaces en ligne telles que les sites Web malveillants et les liens dangereux.