Introduction à la sécurité sur Internet

Réponse 1

● Article 1 = ANSSI - Dix règles de base

● Article 2 = Economie.gouv - Comment assurer votre sécurité numérique

● Article 3 = Site W - Naviguez en toute sécurité sur Internet

● Article bonus = wikiHow - Comment surfez en sécurité sur internet

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

Les paramètres par défaut de Chrome et Firefox sont réglés pour réaliser les mises à jour automatiquement. Comme d'habitude, Firefox affiche une personnalisation des paramètres un peu plus poussée.

Comment éviter les logiciels malveillants

Réponse

● 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)

Achats en ligne sécurisés

Réponse

Voici un exemple d’organisation de libellé pour gérer sa messagerie électronique :

● Achats : historique, facture, conversations liés 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

Proposition deux exercices pour vérifier la sécurité en fonction de l’appareil

Exercice 1 : Vérification des mots de passe et de leur gestion

Étapes :

- Vérifiez si les mots de passe sont longs, complexes (utilisation de majuscules, minuscules, chiffres et caractères spéciaux) et différents pour chaque service.
- Testez l’utilisation d’un gestionnaire de mots de passe et vérifiez si toutes les informations sont correctement stockées et chiffrées.
- Si le téléphone ou l'ordinateur utilise une fonction de "connexion automatique" ou "souvenir du mot de passe", assurez-vous qu'elle est sécurisée (p.ex. verrouillage par empreinte digitale, code PIN).

Exercice 2 : Vérification des mises à jour de sécurité

Étapes :

- Vérifiez si le système d’exploitation de l’appareil (Windows, macOS, Android, iOS, etc.) est bien à jour avec les derniers patches de sécurité.
- Vérifiez les applications installées pour voir si elles sont à jour, en particulier les applications sensibles (banque, messagerie, etc.).
- Assurez-vous que les mises à jour automatiques sont activées pour l'ensemble du système et des applications.

Proposition d’un exercice pour installer et utiliser un antivirus + antimalware en fonction de l’appareil utilisé

Exercice : Installer et utiliser un antivirus et un antimalware

1. Sur un ordinateur (Windows ou macOS)

Étapes à suivre :

a. Choisir un antivirus et un antimalware

Pour cet exercice, nous allons choisir un antivirus populaire et un logiciel antimalware :

- **Antivirus** : **Windows Defender** (préinstallé sur Windows) ou **Avast** (gratuit pour Windows/macOS)
- **Antimalware** : **Malwarebytes** (disponible en version gratuite et premium)

b. Installer un antivirus (si nécessaire)

- **Pour Windows** : Windows Defender est déjà intégré dans le système, il suffit de vérifier s'il est activé.
  - Allez dans **Paramètres > Mise à jour et sécurité > Sécurité Windows**.
  - Vérifiez que la protection antivirus est activée. Si ce n'est pas le cas, activez-la.
- **Pour macOS** : Téléchargez et installez **Avast** (ou un autre antivirus de votre choix).
  - Allez sur le site d'Avast et téléchargez la version gratuite pour Mac.
  - Suivez les instructions d'installation.

c. Installer un antimalware

- Téléchargez et installez **Malwarebytes** depuis leur site officiel.
  - Choisissez la version gratuite pour commencer.
  - Une fois installé, ouvrez Malwarebytes.

d. Effectuer un scan complet

- **Antivirus** : Si vous utilisez Avast (ou un autre antivirus), ouvrez-le et effectuez un scan complet de votre ordinateur.
  - Cela peut prendre plusieurs minutes en fonction de la taille de votre disque dur.
- **Antimalware** : Ouvrez **Malwarebytes** et lancez un scan complet de votre système.
  - Malwarebytes va analyser les fichiers, les programmes et les applications à la recherche de malwares, de ransomwares, de virus et autres menaces.
  - Si des menaces sont détectées, suivez les recommandations pour les supprimer.

e. Vérification et nettoyage

- Après le scan, Malwarebytes ou l'antivirus vous fourniront un rapport avec les menaces détectées. Si des menaces sont trouvées, suivez les instructions pour les éliminer.
- **Windows Defender** vous fournira également un rapport de nettoyage une fois le scan terminé.

2. Sur un smartphone (Android ou iOS)

Étapes à suivre :

a. Choisir un antivirus et un antimalware
Pour cet exercice, nous allons utiliser un antivirus et un antimalware gratuits disponibles sur les deux plateformes :

- **Antivirus** : **Avast Mobile Security** (disponible sur Android et iOS)
- **Antimalware** : **Malwarebytes pour Android/iOS**

b. Installer l'antivirus et l'antimalware

- **Pour Android** :
  - Allez sur le **Google Play Store** et recherchez **Avast Mobile Security**.
  - Téléchargez et installez l'application.
  - Ensuite, recherchez **Malwarebytes** dans le Play Store et installez-le également.
- **Pour iOS** :
  - Allez sur l'**App Store** et recherchez **Avast Mobile Security**.
  - Téléchargez et installez l'application.
  - Ensuite, recherchez **Malwarebytes** et installez-le également.

c. Effectuer un scan antivirus et antimalware

- **Avast** : Ouvrez l'application et effectuez un scan rapide de votre appareil pour détecter toute menace.
  - Avast vérifiera les applications installées, les fichiers téléchargés et la sécurité de votre réseau Wi-Fi.
- **Malwarebytes** : Ouvrez l'application et lancez un scan complet de votre téléphone.
  - L'application vérifiera les applications, les fichiers et les données à la recherche de logiciels malveillants ou de comportements suspects.

d. Vérification et nettoyage

- Après le scan, les applications vous indiqueront si des menaces ont été détectées.
  - Si des menaces sont trouvées, suivez les instructions pour les supprimer ou les mettre en quarantaine.

e. Prévention

- Configurez des **alertes en temps réel** dans les paramètres des applications pour être informé immédiatement si une menace potentielle est détectée sur votre appareil.