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

1/ En naviguant sur le web, consulte trois articles qui parlent de sécurité sur internet.

Pense à vérifier la sources des informations et essaie de consulter des articles

récents pour que les informations soient à jour. Saisis le nom du site et de l'article.

- Article 1 = ANSSI - Dix règles de base
- Article 2 = wikiHow - Comment surfez en sécurité sur internet
- Article 3 = Le site de la CNIL (Commission nationale de l'informatique et des libertés

3 - Fonctionnalité de sécurité de votre navigateur

1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants.

(case à cocher)

- www.morvel.com
- www.dccomics.com
- www.ironman.com
- www.fessebook.com
- www.instagam.com

3/ Lors de la navigation sur le web, il arrive d'avoir des doutes sur la sécurité de certains sites. Comme tu as pu le voir précédemment, le premier de niveau de vigilance à avoir se trouve dans la barre d'adresse des navigateurs web. La plupart affichent des indicateurs de sécurité pour donner une information sur la protection d'un site internet. Lorsque le doute persiste tu peux t'appuyer sur un outil proposé par Google : Google Transparency Report (en anglais) ou Google Transparence des Informations (en français). Afin d'améliorer ta lecture de la sécurité sur internet, tu vas devoir analyser les informations de plusieurs sites. Pour chaque site tu devras préciser l'indicateur de sécurité et le rapport d'analyse de l'outil Google. Il te suffit d'accéder aux liens proposés ci-dessous pour observer l'indicateur de sécurité et de copier-coller l'URL du site dans l'outil Google.

- 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)

1/ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé ??????? Comment faire ????????

1. Identifiez l'appareil que vous utilisez (ordinateur, smartphone, tablette, etc.).
2. Vérifiez que l'appareil est équipé d'un logiciel antivirus et d'un pare-feu.
3. Assurez-vous que votre système d'exploitation et vos applications sont à jour avec les dernières mises à jour de sécurité.
4. Effectuez un test de vulnérabilité en utilisant un outil de test de vulnérabilité en ligne pour votre appareil spécifique. Vous pouvez trouver des outils de test de vulnérabilité gratuits en ligne en effectuant une recherche rapide sur votre moteur de recherche préféré.
5. Si l'outil de test de vulnérabilité identifie des vulnérabilités, suivez les recommandations fournies par l'outil pour résoudre ces vulnérabilités.
6. Vérifiez vos paramètres de sécurité et vos autorisations d'application pour vous assurer que vous ne partagez pas accidentellement des informations privées ou sensibles.
7. Évitez de visiter des sites web douteux ou de télécharger des fichiers provenant de sources inconnues.

Répétez cet exercice régulièrement pour vous assurer que vous êtes toujours protégé contre les menaces de sécurité en ligne.

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

1. Identifiez l'appareil que vous utilisez (ordinateur, smartphone, tablette, etc.).
2. Recherchez un antivirus et antimalware approprié pour votre appareil. Pour cela, vous pouvez utiliser des sites de référence comme AV-TEST ou AV Comparatives qui proposent des comparatifs d'antivirus.
3. Téléchargez et installez l'antivirus et antimalware choisi en suivant les instructions fournies par le logiciel.
4. Effectuez une analyse complète de votre appareil en utilisant l'antivirus et antimalware.
5. Si des menaces sont détectées, suivez les recommandations fournies par le logiciel pour les éliminer.
6. Vérifiez les paramètres de votre antivirus et antimalware pour vous assurer que les mises à jour automatiques sont activées et que les paramètres de sécurité sont correctement configurés.
7. Évitez de télécharger des fichiers provenant de sources inconnues et de visiter des sites web douteux.

Répétez cet exercice régulièrement pour vous assurer que vous êtes toujours protégé contre les menaces de sécurité en ligne.