La sécurité sur Internet

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 = Economie.gouv - Comment assurer votre sécurité numérique
- Article 3 = Site W - Naviguez en toute sécurité sur Internet
- Article bonus = wiki How - Comment surfez en sécurité sur internet

2 - Créer des mots de passe forts

utiliser un gestionnaire de mot de passe LastPass pour enregistrer les t de passe de votre réseaux sociaux.
LastPass est une extension de chrome ou firefox

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

2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes. (case à cocher)

- Pour Chrome
  - Ouvre le menu du navigateur et accède aux "Paramètres"
  - Clic sur la rubrique "A propose de Chrome"
  - Si tu constates le message "Chrome est à jour", c'est Ok

- Pour Firefox
    - Ouvre le menu du navigateur et accède aux “Paramètres”
    - Dans la rubrique “Général”, fais défiler jusqu’à voir la section “Mise à jour de Firefox (astuce : tu peux également saisir dans la barre de recherche (2) “mises à jour” pour tomber directement dessus)
    - Vérifie que les paramètres sélectionnés sont identiques que sur la photo

4 - Éviter le spam et le phishing

Objectif : *Reconnaître plus facilement les messages frauduleux*

Pour ce faire accède au lien suivant et suis les étapes qui y sont décrites : Exercice 4 - Spam et Phishing

7 - Comprendre le suivi du navigateur

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

1- Qu'est-ce qu'un cookie et à quoi sert-il ?

Un cookie est un petit fichier texte stocké sur votre ordinateur par un site web que vous visitez. Les cookies permettent aux sites web de stocker des informations sur votre visite, telles que vos préférences, vos paramètres de connexion et votre historique de navigation. Les cookies peuvent également être utilisés pour suivre votre activité en ligne et diffuser des publicités ciblées.

2- Comment pouvez-vous gérer les cookies dans votre navigateur ?

Un cookie est un petit fichier texte stocké sur votre ordinateur par un site web que vous visitez. Les cookies permettent aux sites web de stocker des informations sur votre visite, telles que vos préférences, vos paramètres de connexion et votre historique de navigation. Les cookies peuvent également être utilisés pour suivre votre activité en ligne et diffuser des publicités ciblées.

3- Qu'est-ce que la navigation privée et comment fonctionne-t-elle ?

La navigation privée est une fonctionnalité proposée par la plupart des navigateurs qui vous permet de naviguer sur le Web sans que votre historique de navigation, vos cookies ou vos informations de formulaire ne soient enregistrés sur votre ordinateur. Les navigateurs utilisent généralement des fenêtres privées distinctes pour la navigation privée.

4 - Pourquoi utiliser la navigation privée peut-il être utile pour protéger votre vie privée en ligne ?

L'utilisation de la navigation privée peut être utile pour protéger votre vie privée en ligne, car elle empêche les sites web de stocker des cookies ou des informations sur votre activité en ligne. Cela peut être particulièrement utile si vous partagez un ordinateur ou si vous naviguez sur des sites web sensibles, tels que des sites bancaires ou de commerce électronique, où la sécurité est importante. Cependant, il est important de noter que la navigation privée ne garantit pas une confidentialité totale, car votre fournisseur de services Internet et d'autres tiers peuvent toujours suivre votre activité en ligne..

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

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

Ordinateur : - Effectuez une analyse de vulnérabilités à l'aide d'un logiciel dédié, comme Nessus ou OpenVAS, pour détecter les failles potentielles dans le système.
-Vérifiez les paramètres de sécurité du pare-feu de votre ordinateur pour vous assurer qu'il est correctement configuré pour bloquer les connexions non autorisées.

Smartphone : - Vérifiez les paramètres de sécurité du smartphone, comme les autorisations d'application et les options de sécurité du système d'exploitation.
-Vérifiez les paramètres de sécurité du pare-feu de votre ordinateur pour vous assurer qu'il est correctement configuré pour bloquer les connexions non autorisées.

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

Ordinateur :

-Recherchez un logiciel antivirus et antimalware réputé, comme Avast, Kaspersky, Bitdefender, ou Malwarebytes.

- Téléchargez le logiciel d'installation à partir du site Web officiel du fournisseur de logiciel.
- Exécutez le programme d'installation et suivez les instructions à l'écran pour installer le logiciel sur votre ordinateur
- Une fois l'installation terminée, lancez le logiciel antivirus et antimalware et effectuez une analyse complète du système pour détecter les virus et les logiciels malveillants.
- Si des menaces sont détectées, suivez les instructions du logiciel pour les supprimer.
- Assurez-vous de mettre à jour régulièrement le logiciel antivirus et antimalware pour rester protégé contre les nouvelles menaces.