SAYNA Naviguer en toute sécurité

1. Introduction à la sécurité sur Internet
   a) Voici les articles que nous avons retenus pour toi (avec les mots-clés “sécurité sur internet” et “comment être en sécurité sur internet” :
      - 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
2. Créer des mots de passe forts
   Fait
3. Fonctionnalité de sécurité de votre navigateur
   a) 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

      Les seuls sites qui semblaient être cohérents sont donc :

      - www.dccomics.com, le site officiel de l’univers DC Comics
      - www.ironman.com, le site officiel d’une compétition internationale de triathlon (et non du super-héros issu de l’univers Marvel)
   b) Fait
4. Éviter le spam et le phishing : Fait
5. Comment éviter les logiciels malveillants
   Site 1 : Indicateur de sécurité : HTTPS
   Analyse Google : Aucun contenu suspect
   Site 2 : Indicateur de sécurité : Not secure
   Analyse Google : Aucun contenu suspect
   Site 3 : Indicateur de sécurité : Not secure
   Analyse Google : Vérifier un URL en particulier (analyse trop générale)
6. Achats en ligne sécurisés : Fait
7. Comprendre le suivi du navigateur : Fait
8. Principes de base de la confidentialité des médias sociaux : Fait
9. **Exercice pour vérifier la sécurité en fonction de l’appareil utilisé**
   Exercice pour vérifier la sécurité de votre appareil : • Objectif : Identifier les éventuelles failles de sécurité de l’appareil. • Étapes : 1. Vérification des mises à jour : ♣ Accédez aux paramètres de votre système d'exploitation. ♣ Recherchez la rubrique "Mise à jour" ou "Update". ♣ Assurez-vous que le système est à jour avec les derniers correctifs de sécurité. 2. Examen des logiciels installés : ♣ Listez tous les logiciels installés. ♣ Identifiez les logiciels que vous n'avez pas installés intentionnellement ou qui semblent suspects. 3. Analyse des autorisations : ♣ Pour les appareils mobiles, vérifiez les autorisations accordées aux applications installées (caméra, microphone, localisation, etc.). 4. Test des indicateurs de sécurité du réseau : ♣ Connectez-vous à un réseau Wi-Fi sécurisé. ♣ Vérifiez la configuration réseau en vous assurant de la présence d’un chiffrement WPA2 ou WPA3.
   Exercice pour installer et utiliser un antivirus + antimalware en fonction de l’appareil utilisé
   Exercice : Installer et configurer un antivirus/antimalware • Objectif : Sécuriser l’appareil en

le protégeant contre les menaces. • Étapes : 1. Choisir un antivirus fiable : ♣ Exemples recommandés : Avast, Bitdefender, Kaspersky, Malwarebytes. ♣ Téléchargez le logiciel à partir du site officiel. 2. Installation : ♣ Téléchargez l'exécutable (PC/Mac) ou l'application (Android/iOS) depuis la boutique officielle. ♣ Lancez l'installation et suivez les instructions à l'écran. 3. Configuration : ♣ Activez les mises à jour automatiques pour les bases de données des virus. ♣ Planifiez des analyses régulières (quotidiennes ou hebdomadaires). 4. Première analyse : ♣ Lancez une analyse complète de l'appareil pour détecter et supprimer les éventuelles menaces. 5. Test de l'antivirus : ♣ Téléchargez un fichier de test de virus sécurisé (par exemple, le fichier EICAR) pour vérifier la détection en temps réel. 6. Antimalware complémentaire : ♣ Installez un antimalware comme Malwarebytes pour détecter les logiciels malveillants non détectés par l'antivirus.