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, consultons trois articles qui parlent de sécurité sur internet. Voici les articles que nous avons retenus :**

   - 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

2) Créer des mots de passe forts

1. **Dans cet exercice, nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Ce gestionnaire prend la forme d'une application web, accessible sur tous supports (PC, Mac, mobile). Il est simple à prendre en main et propose un niveau de sécurité optimal. Suis les étapes suivantes…**

   Dans cet exercice, nous voyons comment utiliser le gestionnaire de mot de passe LastPass.

3) Fonctionnalité de sécurité de votre navigateur

1. **Identifions les adresses internet qui semblent provenir de sites web malveillants :**

   - 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.

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…**

   Dans cette partie, nous voyons comment vérifier que les navigateurs Chrome et Firefox sont à jour.

4) Éviter le spam et le phishing

1. **Dans cet exercice, on va exercer ta capacité à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.**

   Pour ce faire, nous avons accédé au lien suivant pour nous exercer : Exercice 4 - Spam et Phishing .

5) Comment éviter les logiciels malveillants

1. Pour chaque site, précisons l'indicateur de sécurité et le rapport d'analyse de l'outil Google :

   ❖ Site 1 : https://vostfree.tv/

   Indicateur de sécurité :

   - HTTPS

   Analyse Google :

   - Aucun contenu suspect détecté

   ❖ Site 2 : https://www.tv5monde.com/

   Indicateur de sécurité :

   - HTTPS

   Analyse Google :

   - Aucun contenu suspect détecté

   ❖ Site 3 : https://www.baidu.com/

   Indicateur de sécurité :

- HTTPS

Analyse Google :

- Vérifier une URL en particulier

6) Achats en ligne sécurisés

1. **Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le bilan de tes dépenses du mois.**

   Cet exercice nous montre comment créer un registre des achats en créant un libellé dans notre boite mail dans lequel on insèrera tous les emails liés à nos achats.

7) Comprendre le suivi du navigateur

Cette section a été traité sur la gestion des cookies et l'utilisation de la navigation privée.

8) Principes de base de la confidentialité des médias sociaux

1. **Plus tôt dans le cours (Internet de base) tu as déjà été amené à utiliser ce réseau social en partageant une publication. Dans cet exercice on va te montrer le réglage des paramètres de confidentialité pour Facebook. Suis les étapes suivantes.**

   Dans cet exercice, nous voyons comment régler nos paramètres de confidentialités sur le réseau social Facebook.

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

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

Voici quelques exercices pour vérifier la sécurité en fonction de l'appareil utilisé :

- Exercice pour les ordinateurs : Vérifiez les mises à jour du système d'exploitation et des logiciels régulièrement. Assurez-vous que les paramètres de sécurité sont bien configurés, comme un pare-feu activé et un antivirus à jour. Effectuez une analyse antivirus pour détecter d'éventuelles menaces.

- Exercice pour les smartphones : Activez un code PIN, un mot de passe ou un schéma de verrouillage sur votre téléphone. Utilisez des applications de confiance provenant de sources officielles uniquement. Vérifiez régulièrement les autorisations des applications installées.

- Exercice pour les tablettes : Chiffrez les données sensibles stockées sur votre tablette. Utilisez des réseaux Wi-Fi sécurisés et évitez de vous connecter à des réseaux publics non sécurisés. Ne téléchargez pas d'applications provenant de sources douteuses.

- Exercice pour les objets connectés : Changez les mots de passe par défaut des objets connectés (caméras, enceintes intelligentes, etc.). Mettez à jour régulièrement le firmware ou le logiciel des appareils. Désactivez les fonctionnalités inutiles qui peuvent représenter des risques potentiels.

- Exercice pour les réseaux domestiques : Changez le mot de passe par défaut de votre routeur Wi-Fi. Activez le chiffrement WPA2 ou WPA3 pour sécuriser votre réseau. Utilisez un pare-feu matériel ou logiciel pour bloquer les tentatives d'accès non autorisées.

Ces exercices peuvent nous aider à vérifier la sécurité de nos appareils, mais il est également essentiel de rester informé des dernières menaces et bonnes pratiques en matière de sécurité pour assurer une protection optimale.

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

Voici un exercice pour installer et utiliser un antivirus et un antimalware en fonction de l'appareil utilisé.

- **Pour un ordinateur Windows :**

1. Recherchez un antivirus réputé tel que Avast, AVG, Avira, ou Bitdefender.

2. Rendez-vous sur le site officiel de l'antivirus choisi et téléchargez le programme d'installation.
3. Une fois le téléchargement terminé, ouvrez le fichier d'installation et suivez les instructions à l'écran pour installer l'antivirus.
4. Une fois installé, lancez l'antivirus et effectuez une mise à jour complète de sa base de données.
5. Après la mise à jour, effectuez une analyse complète de votre ordinateur pour détecter et supprimer les éventuelles infections.
6. Assurez-vous de régulièrement mettre à jour votre antivirus et d'activer les fonctions de protection en temps réel pour une sécurité continue.

- **Pour un Mac :**

1. Ouvrez l'App Store sur votre Mac.
2. Recherchez un antivirus approuvé comme Norton, Bitdefender ou Sophos.
3. Sélectionnez l'antivirus de votre choix, puis cliquez sur le bouton "Obtenir" pour télécharger et installer l'application.
4. Une fois l'installation terminée, lancez l'antivirus et suivez les instructions pour effectuer une analyse complète de votre Mac.
5. Supprimez les éventuels logiciels malveillants détectés et configurez l'antivirus pour effectuer des analyses régulières.

- **Pour un appareil Android :**

1. Ouvrez le Google Play Store sur votre appareil Android.
2. Recherchez un antivirus populaire comme Avast, AVG, McAfee ou Bitdefender.
3. Sélectionnez l'antivirus de votre choix, puis appuyez sur le bouton "Installer" pour télécharger et installer l'application.
4. Une fois l'installation terminée, lancez l'antivirus et suivez les instructions pour effectuer une analyse complète de votre appareil.
5. Supprimez les éventuels logiciels malveillants détectés et configurez l'antivirus pour effectuer des analyses régulières.

N'oublions pas de mettre à jour régulièrement notre antivirus et d'effectuer des scans fréquents pour protéger notre appareil.