Projet 1 - SECURITE

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 source 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.

Voici les articles (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
● Article bonus = wikiHow - Comment surfez en sécurité sur internet
Beaucoup de notions traitées dans les articles sont également traitées dans le cours et des exercices y sont associés.

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.

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

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
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)

2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour **(c'est fait pratiquer !)**

4 - Éviter le spam et le phishing
Objectif : *Reconnaître plus facilement les messages frauduleux*
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 accède au lien suivant et suis les étapes qui y sont décrites : Exercice 4 - Spam et Phishing

Réponse 1
Tu veux réessayer pour continuer à t'exercer, c'est possible ! Tu peux également consulter des ressources annexes pour t'exercer.
Pour aller plus loin :
● Site du gouvernement cybermalveillance.gouv.fr
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage

5 - Comment éviter les logiciels malveillants
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. (choix multiples)
● Site n°1
○ Indicateur de sécurité
■ HTTPS
■ HTTPS Not secure
■ Not secure
○ **Analyse Google**
■ Aucun contenu suspect
■ Vérifier un URL en particulier
● Site n°2
○ **Indicateur de sécurité**
■ HTTPS
■ HTTPS Not secure
■ Not secure
○ **Analyse Google**
■ Aucun contenu suspect
■ Vérifier un URL en particulier
● Site n°3

○ **Indicateur de sécurité**
■ HTTPS
■ HTTPS Not secure
■ Not secure
○ **Analyse Google**
■ Aucun contenu suspect
■ Vérifier un URL en particulier
● Site n°4 (site non sécurisé)
Réponse 1
● 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)

6 - Achats en ligne sécurisés
Objectif : *créer un registre des achats effectués sur internet*
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.
Deux possibilités s'offrent à toi pour organiser ce registre :
1. Créer un dossier sur ta messagerie électronique
2. Créer un dossier sur ton espace de stockage personnel (en local ou sur le cloud)
La première est la plus pratique à utiliser et la plus facile à mettre en place. Nous prendrons pour exemple la messagerie de Google (les autres messageries fonctionnent sensiblement de la même manière). Suis les étapes suivantes pour créer un registre des achats sur ta messagerie électronique. **(C'est fait pratiquer !)**

7 - Comprendre le suivi du navigateur

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. **(C'est fait pratiquer !)**

9 - Que faire si votre ordinateur est infecté par un virus
Objectif :
1/ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé ??????? Comment faire ????????

Si l'ordinateur est infecté par un virus, il est important de prendre des mesures immédiates pour protéger les données et empêcher la propagation du virus. Voici deux propositions d'exercices pour vérifier la sécurité en fonction de l'appareil utilisé :

Pour un ordinateur de bureau :
Exercice 1 : Utiliser un logiciel antivirus pour scanner le système à la recherche de virus. Si un virus est détecté, le logiciel doit être en mesure de le supprimer ou de le mettre en quarantaine pour empêcher sa propagation.
Exercice 2 : Vérifier les mises à jour de sécurité pour le système d'exploitation et les applications installées. Les mises à jour de sécurité peuvent corriger les vulnérabilités connues et empêcher les attaques malveillantes. Il est important de s'assurer que les mises à jour sont installées régulièrement.

Pour un appareil mobile :
Exercice 1 : Utiliser un logiciel antivirus pour scanner le système à la recherche de virus. Les appareils mobiles peuvent également être infectés par des virus, donc l'utilisation d'un logiciel antivirus est importante.
Exercice 2 : Vérifier les autorisations des applications installées sur l'appareil. Certaines applications peuvent demander des autorisations excessives qui peuvent compromettre la sécurité de l'appareil. Il est important de s'assurer que les applications n'ont pas accès à des données sensibles ou à des fonctions critiques de l'appareil sans raison valable.
En résumé, pour vérifier la sécurité en fonction de l'appareil utilisé, il est important de prendre des mesures spécifiques pour protéger l'appareil contre les menaces potentielles. Cela peut inclure l'utilisation d'un logiciel antivirus, la vérification des mises à jour de sécurité et la gestion des autorisations des applications installées

2/ Proposer 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 : Recherchez un logiciel antivirus et antimalware fiable, tel que Windows Defender, Avast, AVG ou Malwarebytes. Téléchargez et installez le logiciel sur votre ordinateur. Suivez les instructions d'installation pour configurer les paramètres et les options de scan. Lancez une analyse complète de votre ordinateur pour détecter les virus, les logiciels malveillants et les autres menaces potentielles. Si des menaces sont détectées, suivez les instructions du logiciel pour les supprimer ou les mettre en quarantaine. Configurez le logiciel pour effectuer des scans réguliers afin de maintenir la sécurité de votre ordinateur à long terme. Pour un appareil mobile Android : Recherchez un logiciel antivirus et antimalware fiable, tel que Avast, AVG ou Norton Mobile Security. Téléchargez et installez le logiciel depuis le Google Play Store. Suivez les instructions d'installation pour configurer les paramètres et les options de scan. Lancez une analyse complète de votre appareil pour détecter les virus, les logiciels malveillants et les autres menaces potentielles. Si

des menaces sont détectées, suivez les instructions du logiciel pour les supprimer ou les mettre en quarantaine. Configurez le logiciel pour effectuer des scans réguliers afin de maintenir la sécurité de votre appareil à long terme. En résumé, pour installer et utiliser un antivirus et un antimalware en fonction de l'appareil utilisé, il est important de rechercher un logiciel fiable, de le télécharger et de l'installer, de lancer des analyses régulières et de suivre les instructions pour supprimer les menaces détectées.