SAYNA-SECURITE-PROJET1

Sommaire

1 - Introduction à la sécurité sur Internet Objectif : *à la découverte de 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 = Redhat - Comprendre la sécurité informatique
- Article 2 = ANSSI - Dix règles de base
- Article 3 = Economie.gouv - Comment assurer votre sécurité numérique

Consultation des trois articles qui parlent de sécurité sur internet effectués

2 - Créer des mots de passe forts

Objectif : *utiliser un gestionnaire de mot de passe LastPass*

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. (case à cocher)

J'utilise maintenant un gestionnaire de mot de passe avec LastPass

3 - Fonctionnalité de sécurité de votre navigateur

Objectif : *identifier les éléments à observer pour naviguer sur le web en toute sécurité*

1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants. (case à cocher)

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. Pour ce faire, suis les étapes suivantes. (case à cocher)

Vérification bien terminés

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.

Exercice terminés.

5 - Comment éviter les logiciels malveillants

Objectif : *sécuriser votre ordinateur et identifier les liens suspects*

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)

C'est fait

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. (case à cocher)

Exemple d'organisation de libellé pour gérer sa messagerie électronique :

- Achats : historique, facture, conversations liées aux achats
- Administratif : toutes les démarches administratives
- Banque : tous les documents et les conversations liés à la banque personnelle
- Création de compte : tous les messages liés à la création d'un compte (message de bienvenue, résumé du profil, etc.)
- Job : tous les messages liés à mon projet professionnel
- SAYNA : tous les messages liés mon activité avec SAYNA

La création d'un registre des achats effectués

7 - Comprendre le suivi du navigateur

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

C'est fait

8 - Principes de base de la confidentialité des médias sociaux

Objectif : *Régler les paramètres de confidentialité de Facebook*

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. (case à cocher)

- Connecte-toi à ton compte Facebook
- Une fois sur la page d'accueil, ouvre le menu Facebook , puis effectue un clic sur "Paramètres et confidentialité". Pour finir, clic sur "Paramètres"
- Ce sont les onglets "Confidentialité" et "Publications publiques" qui nous intéressent. Accède à "Confidentialité" pour commencer et clic sur la première rubrique
- Cette rubrique résume les grandes lignes de la confidentialité sur Facebook
    - La première rubrique (orange) te permettra de régler la visibilité de tes informations personnelles
    - La deuxième rubrique (bleu) te permet de changer ton mot de passe ○ La troisième rubrique (violet) te permet de gérer la visibilité de ton profil pour la gestion des invitations
    - La quatrième rubrique (vert) permet de gérer la connexion simplifiée sur des applications ou des sites utilisés qui permettent cela
    - La dernière rubrique (rose) permet de gérer les informations récoltées par Facebook utiles pour les annonceurs
- Retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à gauche. Tu peux continuer à explorer les rubriques pour personnaliser tes paramètres. On ne peut pas te dire ce que tu dois faire. C'est à toi de choisir les informations que tu souhaites partager et celles que tu veux garder privées. Voici tout de même quelques conseils :
    - Si tu utilises ton compte Facebook uniquement pour communiquer avec tes amis, règles les paramètres en conséquence en choisissant une visibilité "Amis" ou "Amis de leurs amis".
    - Beaucoup de personnes utilisent Facebook en mêlant réseau professionnel et réseau personnel. Il n'y a pas vraiment de contre-indication, mais on te conseille tout de même de ne pas trop mélanger les deux. Il existe LinkedIn pour utiliser un média social pour le réseau professionnel
    - Pour limiter les haters et les commentaires malveillants, tu peux restreindre les commentaires de tes publications. Ça se passe dans l'onglet "Publications publiques"
- Dans les paramètres de Facebook tu as également un onglet "Cookies". On t'en a parlé dans le cours précédent (Comprendre le suivi du navigateur). Maintenant que tu sais

comment sont utilisées tes données, tu es capable de choisir en pleine conscience ce que tu souhaites partager.

Réponse 1
Voici un exemple de paramétrage de compte Facebook pour une utilisation privilégiant les échanges avec les amis, mais autorisant le contact avec des inconnus (limite de leurs actions) :

- Confidentialité
- Publications publiques

Sur les autres médias sociaux, tu retrouveras sensiblement le même type de paramétrage. Maîtrise ton utilisation de ces outils en paramétrant selon tes souhaits.

C’est fait

Pour aller plus loin :

- Les conseils pour utiliser en toute sécurité les médias sociaux

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 ????????

Déconnecter l'ordinateur d'Internet pour éviter la propagation du virus. Exécuter un logiciel antivirus pour scanner le système à la recherche de virus. Suiver les instructions de l'antivirus pour supprimer le virus. Si l'antivirus ne parvient pas à supprimer complètement le virus, essayer de le supprimer manuellement en recherchant des fichiers suspects et en les supprimant. Une fois le virus supprimé, il faut mettre à jour l'antivirus et faire des scans réguliers pour éviter de nouvelles infections.

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

Téléchargez et installez l'antivirus et l'antimalware de choix en les téléchargez les versions compatibles avec votre système d'exploitation Windows.
Ouvrez l'antivirus et l'antimalware et mettez à jour les bases de données de virus et de malwares.
Planifiez une analyse complète de l'ordinateur.
Configurez les paramètres de l'antivirus et l'antimalware en fonction du besoin.
Utilisez l'antivirus et l'antimalware régulièrement pour scanner l'ordinateur et détecter tout virus ou malware.
Si l'antivirus détecte un virus, suivez les instructions pour supprimer le virus ou mettre en quarantaine les fichiers infectés.