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.

Réponse 1

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

● 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

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)

● Accède au site de LastPass avec ce lien

● Crée un compte en remplissant le formulaire. Un conseil, on te demande de choisir un mot de passe maître. Pour rappel, ce mot de passe sera unique et te permettra d'accéder à tous tes comptes. Choisis donc un mot de passe avec un niveau de sécurité élevé et assure-toi de pouvoir le retrouver ○ Exemple de mot de passe maître : c3c!3s!l3M0!2P@SS3 (Ceci est le mot de passe, en remplaçant le "e" par "3" le "i", "t" par "!", "a" par "@" et les premières lettres en minuscules puis majuscules à partir de "mot") ○ Tu peux également générer un mot

de passe maître, mais pense à l'écrire dans un endroit sûr pour pouvoir l'utiliser lorsque tu en as besoin

● Une fois la création du compte effectuée, tu arrives sur une page de validation qui propose le téléchargement de l'extension sur ton navigateur. Lance l'installation en effectuant un clic sur le bouton prévu à cet effet

● Il te suffit de valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome"

● Une fois installé, il te suffit d'accéder à cette extension et de t'y connecter

○ (1) En haut à droite du navigateur, clic sur le logo "Extensions"

○ (2) Épingle l'extension de LastPass avec l'icône

○ Il ne te reste plus qu'à te connecter en effectuant un clic sur l'icône de l'extension et en saisissant ton identifiant et mot de passe

Réponse 1

Désormais, lorsqu'on connectes à tes comptes, je peux enregistrer le mot de passe grâce à LastPass. je peux également ajouter des comptes manuellement en accédant au coffre-fort, espace de stockage de tous tes mots de passe. Pour y accéder, clic sur l'icône de l'extension puis sur "Ouvrir mon coffre-fort".

J'arrives alors sur une page de gestion de ton compte LastPass. Pour ajouter un site et une connexion associée (identifiant + mot de passe), accède à la rubrique "Mot de passe" (2) et (3) puis clic sur "Ajouter un élément" (1).

Une fenêtre s'ouvre pour y insérer toutes les informations à retenir pour automatiser la prochaine connexion. LastPass demande l'URL du site en question ; on conseille de mettre l'URL de la page de connexion du site. Ensuite préciser l'id et le mot de passe. On peut personnaliser le nom, un commentaire associé ou encore un dossier si besoin.

Je connais maintenant les grandes lignes de l'utilisation du gestionnaire de mot de passe LastPass.

Pour aller plus loin : L'abonnement gratuit (freemium) te permet de faire les tâches principales. Si tu trouves cet outil incontournable, tu peux passer au compte premium. Il te permettra notamment de synchroniser ton compte LastPass sur tous les supports utilisés.

● Comparatif des gestionnaires de mot de passe : https://www.clubic.com/application-web/article-854952-1-gestionnaires-mots-meilleur-logiciel -gratuit-windows.html

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)

● 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. 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

Réponse 2

Comme tu as pu le constater, les paramètres par défaut de ces deux navigateurs sont réglés pour réaliser les mises à jour automatiquement. Comme d’habitude, Firefox affiche une personnalisation des paramètres un peu plus poussée.

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-reconn aitre-un-mail-de-phishing-ou-dhameconnage

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)

● 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) Tu peux tester la sécurité d'autres sites à partir de ce lien. Ce site référence et explique les défauts de sécurité des sites dans le monde.

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