NAVIGUER EN TOUTE SÉCURITÉ

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 = 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

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

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 deChrome" ○ 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

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

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

○ 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. (case à cocher)

● Pour commencer, accède à ta messagerie électronique. Pour rappel, tu peux y accéder rapidement en ouvrant un nouvel onglet (dans la barre des favoris ou via le raccourci)

● Sur la page d'accueil de ta messagerie, tu trouveras sur la gauche les libellés initialement prévus (boite de réception, messages envoyés, etc.)

● C'est dans cette partie que tu vas créer ta rubrique des achats. Pour ce faire, clic sur "Plus" et va tout en bas des libellés. Pour créer un libellé rapidement il te suffit d'effectuer un clic sur "Créer un libellé" et de le nommer "ACHATS" (pour notre exercice)

● Effectuer un clic sur le bouton "Créer" pour valider l'opération

● Tu peux également gérer les libellés en effectuant un clic sur "Gérer les libellés")

● Tu as maintenant un libellé pour stocker tous tes messages électroniques relatifs aux achats effectués sur internet : confirmation de l'achat, détail de la commande, modalités de livraison

7 - Comprendre le suivi du navigateur

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

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.

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 ????????

Exercice 1 : Analyse de vulnérabilités des smartphones

Objectif : Évaluer la sécurité d'un smartphone en utilisant un outil d'analyse de vulnérabilités.

Instructions :

- Sélectionnez un smartphone à évaluer. Assurez-vous que le smartphone est mis à jour avec la dernière version du système d'exploitation et des applications.
- Installez un outil d'analyse de vulnérabilités sur un ordinateur, tel que Nessus, OpenVAS ou Qualys.
- Connectez le smartphone à l'ordinateur à l'aide d'un câble USB.
- Lancez l'outil d'analyse de vulnérabilités et scannez le smartphone pour détecter les vulnérabilités connues.
- Analysez les résultats du scan et identifiez les vulnérabilités potentielles. Classez-les en fonction de leur impact sur la sécurité du smartphone.
- Proposez des mesures pour corriger les vulnérabilités identifiées. Par exemple, mettez à jour le système d'exploitation ou désinstallez les applications vulnérables.
- Réalisez une nouvelle analyse de vulnérabilités après avoir appliqué les mesures de sécurité.

- Évaluez les résultats de l'analyse de vulnérabilités après les mesures de sécurité. Assurez-vous que les vulnérabilités potentielles ont été corrigées et que la sécurité globale du smartphone a été améliorée.

Notez que cet exercice nécessite des compétences techniques en sécurité informatique et peut nécessiter l'aide d'un professionnel de la sécurité pour les débutants.

Il est également important de noter que l'utilisation d'outils d'analyse de vulnérabilités peut être soumise à des restrictions légales et éthiques. Assurez-vous de respecter les lois et réglementations applicables avant d'utiliser ces outils.

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

Exercice 2 : Installation et utilisation d'un antivirus et antimalware

Objectif : Installer et utiliser un logiciel antivirus et antimalware pour protéger un ordinateur.

Instructions :

- Sélectionnez un logiciel antivirus et antimalware fiable et réputé, tel que Norton, Kaspersky ou McAfee.
- Téléchargez le logiciel sur le site officiel du fournisseur.
- Installez le logiciel sur l'ordinateur en suivant les instructions d'installation.
- Mettez à jour le logiciel avec les dernières définitions de virus et de malware.
- Configurez les paramètres de l'antivirus et de l'antimalware en fonction de vos besoins.
- Planifiez des analyses régulières du système pour détecter les virus et les malwares.
- Analysez le système avec le logiciel pour détecter les menaces potentielles.
- Supprimez les menaces détectées en suivant les instructions du logiciel.
- Vérifiez régulièrement l'état de l'antivirus et de l'antimalware pour vous assurer qu'ils sont à jour et fonctionnent correctement.

Notez que l'utilisation d'un logiciel antivirus et antimalware ne garantit pas une protection totale contre les menaces en ligne. Il est important de compléter l'installation d'un logiciel de sécurité par des pratiques de sécurité informatique, telles que l'utilisation de mots de passe forts et la mise à jour régulière des logiciels et du système d'exploitation.