Réponses au Projet - Sécurité sur Internet

1. Introduction à la sécurité sur Internet

Question : Consulte trois articles récents qui parlent de sécurité sur Internet et note le nom du site ainsi que le titre de l'article.

Réponse :

1. Article 1 :

- Nom du site : ANSSI
- Titre de l'article : Dix règles de base pour la sécurité informatique

2. Article 2 :

- Nom du site : Economie.gouv
- Titre de l'article : Comment assurer votre sécurité numérique

3. Article 3 :

- Nom du site : Site W
- Titre de l'article : Naviguez en toute sécurité sur Internet

2. Créer des mots de passe forts avec LastPass

Objectif : Utiliser un gestionnaire de mots de passe.

Étapes :

1. Accédez au site LastPass via le lien indiqué (ou lastpass.com).

2. Créez un compte en remplissant le formulaire. Choisissez un mot de passe maître fort, par exemple :

Exemple de mot de passe maître : c3c!3sI3M0l2@P@SS3 (utilisant des substitutions pour renforcer la sécurité).

3. Installez l'extension sur votre navigateur via le Chrome Web Store en cliquant sur 'Ajouter à Chrome'.

4. Finalisez l'installation et connectez-vous avec votre compte.

1/ 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) Verification de la mise à jour des 2 navigateurs (Chrome et Firefox)
Chrome et Firefox sont à jour.

3) Comment détecter les erreurs dans les messages cachant une action malveillante en arrière-plan.

1. Une notification de la messagerie ou de l'antivirus

Votre messagerie ou votre antivirus peuvent vous signaler la réception d'un mail frauduleux. N'ignorez pas leur avertissement et **assurez-vous régulièrement que votre antivirus est activé et à jour**.

2. Un email d'un service ou d'une société dont vous n'êtes pas client

Les cybercriminels n'ont généralement pas accès aux bases de données d'utilisateurs des entreprises dont ils usurpent l'identité et envoient parfois leur mail de phishing au hasard. **Si vous recevez un email d'un service ou d'une société dont vous n'êtes pas client, méfiez-vous. Attention cependant,**

un cybercriminel peut également s'en prendre aux vrais clients d'un service ou d'une société, soit parce que le hasard voudra que dans leur envoi de masse leur message de phishing soit adressé à des clients du service usurpé, soit parce qu'ils ont réussi à récupérer une base d'adresses des clients du service concerné.

4. Une adresse d'expédition fantaisiste

La plupart des phishings par email utilisent des adresses de messagerie qui ne ressemblent pas à des adresses officielles. **Pour vérifier qu'il s'agit bien d'un message officiel, pensez à vérifier l'adresse email de l'expéditeur.** Si cette dernière ne comporte pas le nom de l'entité, qu'elle présente des fautes d'orthographe ou que le nom vous paraît suspect, n'ouvrez pas le message. Il s'agit sûrement d'un mail frauduleux.

4- Comment détecter les logiciels malveillants ?

Réponse 1

● Site n°1

○ Indicateur de sécurité

■ HTTPS

○ Analyse Google

■ Aucun contenu suspect

● Site n°2

○ Indicateur de sécurité

■ Not sécure

○ Analyse Google

■ Aucun contenu suspect

● Site n°3

○ Indicateur de sécurité

■ Not secure

○ Analyse Google

■ Vérifier un URL en particulier (analyse trop générale

7)

Voici un 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.

9) Propositions pour vérifier la Sécurité de l'appareil utilisé

1. Vérification de la sécurité en fonction de l'appareil utilisé :

Exercice 1 : Analyse de vulnérabilités

- Utiliser un outil d'analyse de vulnérabilités comme Nessus, Burp Suite ou Metasploit pour scanner l'appareil et identifier les failles de sécurité potentielles.
- Examiner les résultats et classez les vulnérabilités par ordre de priorité en fonction de leur gravité.
- Proposer des solutions pour corriger les vulnérabilités identifiées, comme l'application de correctifs, la configuration de paramètres de sécurité ou l'utilisation d'outils de protection supplémentaires.

Exercice 2 : Test d'intrusion

- Effectuer des tests d'intrusion simulés sur l'appareil en utilisant des outils comme Kali Linux ou Metasploit.
- Évaluer la capacité de l'appareil à détecter et à se défendre contre les attaques.
- Identifiez les points faibles et proposez des améliorations pour renforcer la sécurité.

Exercice 3 : Analyse des journaux de sécurité

- Examiner les journaux de sécurité de l'appareil (par exemple, les journaux système, les journaux d'événements, les journaux d'audit) pour détecter les activités suspectes ou les tentatives d'intrusion.
- Analyser les informations collectées et proposez des mesures pour améliorer la surveillance et la détection des menaces.

2. Installation et utilisation d'un antivirus et d'un anti-malware en fonction de l'appareil utilisé :

Exercice 1 : Installation et configuration d'un antivirus

- Choisissez un antivirus adapté à votre système d'exploitation (par exemple, Windows Defender pour Windows, ClamAV pour Linux, Malwarebytes pour macOS).
- Installez l'antivirus en suivant les instructions du fournisseur.
- Configurez les paramètres de l'antivirus pour qu'il effectue des analyses régulières et mette à jour automatiquement ses définitions de virus.
- Testez l'antivirus en effectuant une analyse complète de l'appareil.

Exercice 2 : Installation et configuration d'un anti-malware

- Choisir un anti-malware adapté à votre système d'exploitation (par exemple, Malwarebytes pour Windows, ClamXav pour macOS, Clamav pour Linux).

- Installer l'anti-malware en suivant les instructions du fournisseur.
- Configurer les paramètres de l'anti-malware pour qu'il effectue des analyses régulières et mette à jour automatiquement ses définitions de malware.
- Tester l'anti-malware en effectuant une analyse complète de l'appareil.

Gestion des mises à jour et des paramètres de sécurité

- Vérifier régulièrement que l'antivirus et l'anti-malware sont à jour.
- Ajuster les paramètres de sécurité en fonction des recommandations du fournisseur ou des meilleures pratiques de sécurité.
- Surveiller les journaux de sécurité pour détecter toute activité suspecte et prenez les mesures nécessaires.