Projet 3: Naviguer en toute Sécurité

1. Introduction à la sécurité

Réponse 1: Les 3articles qui parlent de sécurité sur Internet :

Article 1 : Economie.gouv/ Comment assurer votre sécurité sur Internet ? (https://www.economie.gouv.fr/particuliers/comment-assurer-securite-numerique) Article publié le 09 Octobre 2023

Article 2 : Avast.com/Qu'est-ce que la sécurité sur Internet ? (https://www.avast.com/fr-fr/c-internet-safety-tips) Article publié le 09 Avril 2023

Article 3 : mesquestionsdargent.fr/ Comment utiliser Internet en toute sécurité ? (https://www.mesquestionsdargent.fr/budget/comment-utiliser-internet-en-toute-securite) Article Publié le 31 Janvier 2024

2. Créer des mots de passe forts

Réponse 1 : L'utilisation d'un gestionnaire de mot de passe : Case à cocher

☒Accès au site Lastpass

☒Création d'un compte

☒Téléchargement de l'extension

☒Ajout à Chrome

☒Accéder à l'extension

3. Fonctionnalité de sécurité du Navigateur

Réponse 1 : Identification des adresses Internet qui semblent provenir de sites malveillant (case à cocher) :

☒www.morvel.com

On remarque déjà que c'est un site qui a pour but malveillant. C'est le dérivé de Marvel.com, ils ont leur propre logo, quand on est sur le site, on voit des images, des menus quant à l'autre site morvel il demande directement nos informations personnelles.

☒www.fessebook.com

Site malveillant, dérivé de Facebook

☒www.instagm.com

Dérivé de Instagram,le navigateur nous montre directement que le site n'est pas sécurisé dans la barre de navigation.

www.dccomics.com et www.ironman.com sont des sites officiels qui ne représentent aucun risque malveillant.

Réponse 2 : Vérification de mise à jour des navigateurs.

☒Pour Chrome :

☒Accès au paramètre

☒Clic sur la rubrique « A propos de chrome »

☒Je constate que Chrome est à Jour

Pour Firefox :

☒Accès au paramètre

☒Dans la rubrique « général » et dans la section mise à jour de Firefox

☒Le Firefox est à jour

Le mise à jour de ces 2 navigateur est automatique.

4. Éviter le spam et le phishing

Réponse 1 :

Il est important de bien vérifier les adresses mail, URL de l'expéditeur, car c'est vraiment difficile de faire la différence entre la légitime et l'hameçonnage.

5. Comment éviter les logiciels malveillants ?

☒**Site 1 :**

Indicateur de sécurité :

☒ Https

Analyse Google :

☒Aucun contenu suspect

Site 2 :

Indicateur de sécurité :

☒Https

Analyse Google :

☒Aucun contenu suspect

Site 3 :

Indicateur de sécurité :

☒Not sécure

Analyse Google :

☒Vérifier un URL en particulier

6. Achat en ligne sécurisé

Réponse 1 : Organisation d'un registre d'achat en ligne

☒Création d'un dossier sur mon messagerie électronique :

☒Accès à la messagerie électronique
☒Création d'un dossier libellé « Achat » et Créer
☒Gestion des libellés, affichage des libellés initiaux, gestion des libellés pesonnels

L'utilisation des libellés est vraiment pratique pour le classement et l'organisation des messages. On gagne du temps, c'est très facile aussi de retrouver les mails et d'être plus productif.

7. Comprendre le suivi du navigateur

Réponse 1 :

Il ne faut pas s'inquiéter sur les cookies, mais si on veut limiter la collecte des informations, on peut l'interdire, on peut aussi utiliser le navigateur privé.

8. Principes de base de la confidentialité des médias sociaux

Réponse 1 : Réglage de paramètre pour Facebook

☒Connexion à mon compte Facebook

☒Accès au paramètre et confidentialité de Facebook

☒Accès à Confidentialité

☒Résumé des grandes lignes de la confidentialité de Facebook

☒Rubrique Orange : régler la visibilité de mes informations personnelles

☒Rubrique Bleu : Changement de mot de passe

☒Rubrique Violet : gestion de la visibilité de mon profil

☒Rubrique vert : qui permet de gérer la connexion simplifiée sur des applications ou des sites utilisés qui permettent cela.

☒Rubrique rose : qui permet de gérer les informations récoltées par Facebook utiles pour les annonceurs

☒Personnalisation de mes paramètres

Il est nécessaire de bien réfléchir avant de partager quelques choses, et aussi de bien vérifier les paramètres de confidentialité.

9. Que faire si mon Ordinateur est infecté par un virus ?

Réponse 1. Les exercices pour vérifier la sécurité de Windows :

C’est qu’il faut faire :

Il faut avoir un logiciel d’antivirus et antimalware pour protéger l’ordinateur contre les logiciels malveillants.

Pour Windows 10 et 11, la sécurité Windows met en disposition un antivirus « Windows defender), l’appareil sera activement protégé au moment où on fait le démarrage de Windows. Des analyses sont effectuées en permanence par Sécurité Windows pour détecter des programmes malveillants, des virus et des menaces liées à la sécurité.

En plus de cette protection en temps réel, on reçoit automatiquement des mises à jour pour garantir la sécurité de notre appareil et le protéger contre les menaces.

Pour vérifier rapidement la sécurité Windows :

Sélectionnez le menu **Démarrer** de Windows /Paramètre / Mise à jour et sécurité/Sécurité Windows/Protection contre les virus et menaces.

Réponse 2 : Un exercice pour installer et utiliser un logiciel antivirus+antimalware :

Comme nous venons d’aborder en haut, pour Windows, il dispose déjà un logiciel antivirus et antimalware intégré « Windows defender »

Pour l’installation :

Windows Defender est déjà intégré aux versions modernes de Windows, comme Windows 10 et Windows 11. Il est activé par défaut.

Utilisation :

Ouverture de Windows :

Defender Recherchez "Windows Defender" dans le menu Démarrer et ouvrez l'application

Analyse de l’Ordinateur:

Cliquez sur "Analyser maintenant" pour rechercher les virus et logiciels malveillants

Protection en temps réel :

Assurez-vous que la protection en temps réel est activée pour une sécurité continue.

Mise à jour automatique :

Gardez Windows à jour pour obtenir les dernières définitions de virus et mises à jour de sécurité.

Paramètres personnalisés :

Personnalisez les fonctionnalités de sécurité selon vos besoins.

Navigation sécurisée :

Utilisez la fonctionnalité de navigation sécurisée dans Microsoft Edge pour une expérience web plus sûre.

Suppression des menaces :

Suivez les instructions pour supprimer les menaces détectées.

Pour aller plus loin :

- https://support.microsoft.com/fr-fr/windows/rester-prot%C3%A9g%C3%A9-avec-s%C3%A9curit%C3%A9-windows-2ae0363d-0ada-c064-8b56-6a39afb6a963