Projet 3 Naviguer en toute sécurité

1 – Introduction à la sécurité sur internet

1/ Consulte 3 articles qui parlent de sécurité sur internet. Pense à vérifier la source des informations et essaie de consulter des articles récents pour que les informations soient à jours. Saisis le nom du site et de l'article :

- **Article 1** = https://www.avast.com/fr-fr/c-internet-safety-tips - qu'est-ce que la sécurité sur internet ? (Publication : 9 avril.2023/ Auteur : Deepan Ghimiray)

- **Article 2** = https://www.mesquestionsdargent.fr/budget/comment-utiliser-internet-en-toute-securite – comment utiliser internet en toute sécurité ? (Publication : 7 fev.2023)

- **Article 3** = https://heyme.care/fr/blog/comment-proteger-sa-vie-privee-sur-internet - comment protéger sa vie privée sur internet ? (Publication: 9 Nov.2022 / Mise à jour: 23 Août.2023)

2 – Créer des mots de passe forts

1/ Dans cet exercice nous allons voir comment utiliser la première fois un gestionnaire de mot de passe nommée LastPass. Suis les étapes suivantes :

- Accède au site de LastPass Création de compte réussie (lastpass.com) ☒

- Créer un compte en remplissant le formulaire. ☒

- Une fois la création du compte effectuer, 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 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, 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 de mot de passe

3 – Fonctionnalité de sécurité de votre navigateur

1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants. ☒

- www.morvel.com : site qui semble être malveillant car dérivé de www.marvel.com, site officiel de l'univers Marvel. ☒

- www.dccomics.com: site officiel de l'univers DC Commics.
- www.ironman.com: site officiel de la compétition internationale de triathlon. ☒

- www.fessebook.com: site qui semble être malveillant car dérivé de www.facebook.com, le plus grand réseau social du monde. ☒

- www.instagam.com: site qui semble être malveillant car dérivé de www.instagram.com, un réseau social très utilisé. ☒

2/ Dans cet exercice nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Suis les étapes suivantes : ☒

- Pour chrome :
    - Ouvre le menu du navigateur et accède aux « Paramètres » ☒
    - Clic sur la rubrique « à propos 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 « General », fais défiler jusqu'à voir la section « Mise à jour de Firefox » ☒
    - Vérifie que les paramètre sélectionner sont sur la photo ☒

4 – Éviter le spam et phishing

1/ Dans cet exercice, on va exercer ta capacite 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 : Jigsaw | Quiz sur l'hameçonnage (phishingquiz.withgoogle.com) ☒

5 – Comment éviter les logiciels malveillants

1/ 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 :

- https://vostfree.tv/ :
    - Indicateur de sécurité :
        - HTTPS ☒
        - HTTPS Not sécure ☐
        - Not sécure ☐
    - Analyse Google :
        - Aucun contenu suspect ☒
        - Vérifier un URL en particulier ☐

- https://www.tv5monde.com/ :
    - Indicateur de sécurité :
        - HTTPS ☐
        - HTTPS Not sécure ☐
        - Not sécure ☒

- Analyse Google :
  - Aucun contenu suspect ☒
  - Vérifier un URL en particulier ☐

➢ https://www.baidu.com/ :

- Indicateur de sécurité :
  - HTTPS ☐
  - HTTPS Not sécure ☐
  - Not sécure ☒
- Analyse Google :
  - Aucun contenu suspect ☐
  - Vérifier un URL en particulier ☒

6 – Achat en ligne sécurisés

1/ Dans cet exercice, on va t'aider à créer un registre des achats. Suis les étapes suivantes :

➢ Pour commencer, accède à ta messagerie électronique. Pour rappel, tu peux y accéder rapidement en ouvrant u nouvel onglet. ☒

➢ 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 » ☒

➢ Effectue un clic sur le bouton « Créer » pour valider l'opération ☒

➢ Tu peux également gérer les libellés en effectuant un clic sur « Gérer les libellés »(1). Sur cette page, tu peux gérer l'affichage des libellés initiaux (2) et gérer les libellés personnels (3). ☒

- Tu as maintenant un libellé pour stocker tous tes messages électroniques relatifs aux achats effectués sur internet : confirmation de l'achat, détail de la demande ; modalités de Livraison. ☒

7 – Comprendre le suivi du navigateur

8 – Principes de bases de la confidentialité des médias sociaux

1/ Dans cet exercice on va te montrer le réglage des paramètres de confidentialité pour Facebook. Suis les étapes suivantes :

- 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 » ☒

- 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 (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 haut gauche. Voici quelques conseils :

- Si tu utilises ton compte Facebook pour communiquer uniquement avec tes amis, règles les paramètres en conséquence en choisissant une visibilité « Amis » ou « Amis de leurs amis ». ☒
- Tu peux utiliser Facebook pour ton réseau personnel et LinkedIn pour ton réseau professionnel. ☒
- Pour limiter les hâteurs 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 ». choisir tout en étant conscient ce que tu souhaites partager. ☒

9 – Que faire si votre ordinateur est infecté par un virus

1/ Proposez un ou plusieurs exercices pour vérifier la sécurité en fonction de l'appareil utilisé ?????? Comment faire ??????

❖ **Vérifiez les performances et l'intégrité de votre appareil**: Sécurité Windows surveille votre appareil à la recherche de problèmes de sécurité et fournit un rapport d'intégrité, qui s'affiche dans la page Performances & d'intégrité de l'appareil. Le rapport d'intégrité vous avertit des problèmes courants dans quatre domaines clés et propose des recommandations pour y remédier. Pour plus d'informations sur Sécurité Windows, consultez Rester protégé avec Sécurité Windows

(1) Dans la zone de recherche de la barre des tâches, saisissez **Sécurité Windows**, puis sélectionnez-le dans les résultats.
(2) Sélectionnez **Performances et intégrité de l'appareil** pour afficher le rapport d'intégrité.

Remarque : Si votre appareil est géré par votre organization, votre administrateur ne vous a peut-être pas accordé l'autorisation d'afficher les **performances & l'intégrité de l'appareil**.

Le Rapport d'intégrité commence en vous affichant la dernière fois qu'une analyse d'intégrité de l'appareil a été exécutée. L'heure affichée doit en principe être l'heure actuelle, car Sécurité Windows tente d'exécuter une

analyse d’intégrité de l’appareil lorsque vous ouvrez la page **Performances et intégrité de l’appareil**.

Au-delà de la dernière analyse, vous pouvez voir l’état des principales zones que l’intégrité de l’appareil surveille :

- **Capacité de stockage** : votre système manque-t-il d'espace disque ?
- **Applications et logiciels** : l'un de vos logiciels est-il défaillant ou a-t-il besoin d'une mise à jour ?
- **Autonomie de la batterie** : la batterie de votre PC est-elle soumise à une tension supplémentaire ? *Il se peut que vous ne voyiez pas cela sur un PC de bureau toujours branché.*
- **Service Windows Time** : Il est important que votre système soit réglé à la bonne heure pour un grand nombre de processus système. Le service Windows Time synchronise automatiquement votre horloge système avec un service de temps basé sur Internet afin que votre heure système soit toujours correcte. Si ce service est hors service, ou s'il est défaillant, la performance et l'intégrité de l'appareil vous le fera savoir afin que vous puissiez le réparer.

❖ **Utilisez un logiciel antivirus**: Les logiciels antivirus peuvent aider à détecter et à supprimer les virus et les logiciels malveillants de votre appareil.

(1) **Téléchargez et installez un logiciel antivirus**: Il existe de nombreux logiciels antivirus disponibles sur le marché(pour tout type d’appareil), tels que Norton, McAfee, Avast, etc. Téléchargez et installez le logiciel antivirus de votre choix sur votre appareil.

(2) **Exécutez une analyse complète de votre appareil**: Une fois que vous avez installé le logiciel antivirus, exécutez une analyse complète de votre appareil. L’analyse complète vérifiera tous les fichiers et dossiers de votre appareil pour détecter les virus et les logiciels malveillants.

(3) **Supprimez les virus et les logiciels malveillants détectés**: Si le logiciel antivirus détecte des virus ou des logiciels malveillants sur votre appareil, suivez les instructions du logiciel pour les supprimer.

(4) **Planifiez des analyses régulières**: Pour maintenir la sécurité de votre appareil, planifiez des analyses régulières à l'aide du logiciel antivirus. Les analyses régulières aideront à détecter et à supprimer les virus et les logiciels malveillants avant qu'ils ne causent des dommages à votre appareil.

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

❖ Ordinateur:

(1) **Téléchargez et installez un logiciel antivirus**: Il existe de nombreux logiciels antivirus disponibles sur le marché, tels que Norton, McAfee, Avast, etc. Téléchargez et installez le logiciel antivirus de votre choix sur votre ordinateur.

(2) **Exécutez une analyse complète de votre ordinateur**: Une fois que vous avez installé le logiciel antivirus, exécutez une analyse complète de votre ordinateur. L'analyse complète vérifiera tous les fichiers et dossiers de votre ordinateur pour détecter les virus et les logiciels malveillants.

(3) **Supprimez les virus et les logiciels malveillants détectés**: Si le logiciel antivirus détecte des virus ou des logiciels malveillants sur votre ordinateur, suivez les instructions du logiciel pour les supprimer.

(4) **Planifiez des analyses régulières**: Pour maintenir la sécurité de votre ordinateur, planifiez des analyses régulières à l'aide du logiciel antivirus. Les analyses régulières aideront à détecter et à supprimer les virus et les logiciels malveillants avant qu'ils ne causent des dommages à votre ordinateur.

❖ Téléphone portable:

(1) **Téléchargez et installez un logiciel antivirus**: Il existe de nombreux logiciels antivirus disponibles sur le marché, tels que AVG AntiVirus pour Android . Téléchargez et installez le logiciel antivirus de votre choix sur votre téléphone portable.

(2) **Exécutez une analyse complète de votre téléphone portable**: Une fois que vous avez installé le logiciel antivirus, exécutez une analyse complète de votre

téléphone portable. L'analyse complète vérifiera tous les fichiers et dossiers de votre téléphone portable pour détecter les virus et les logiciels malveillants.

(3) **Supprimez les virus et les logiciels malveillants détectés**: Si le logiciel antivirus détecte des virus ou des logiciels malveillants sur votre téléphone portable, suivez les instructions du logiciel pour les supprimer.

(4) **Planifiez des analyses régulières**: Pour maintenir la sécurité de votre téléphone portable, planifiez des analyses régulières à l'aide du logiciel antivirus. Les analyses régulières aideront à détecter et à supprimer les virus et les logiciels malveillants avant qu'ils ne causent des dommages à votre téléphone portable.