1-Introduction à la sécurité sur Internet

1/ voici trois articles qui parlent de sécurité sur internet :

- Article 1 = Swisscom community - 10 conseils pour plus de sécurité sur Internet
- Article 2 = O'communication - Sécurité Internet
- Article 3 = Letecode - Tout ce que vous devez savoir sur la sécurité sur internet

2-Créer des mots de passes forts

- ☑ 1/ utilisation d'un gestionnaire de mot de passe

3-Fonctionnalité de sécurité de votre navigateur

1/ Les adresses internet qui me semblent provenir de sites Web malveillants sont :

- www.morvel.com
- www.fessebook.com
- www.instagam.com

- ☑ 2/Voyons si Chrome et Firefox sont à jour.

4-Éviter le spam et le phishing

- ☑ 1/ Exercice de capacité à déceler les erreurs dans les messages cachant une action malveillant

5-Comment éviter les logiciels malveillants

1/ Vérification d'une site

- Site n° 1
  - **Indicateur de sécurité**
    - HTTPS
  - **Analyse Google**
    - Aucun contenue suspect
- Site n° 2
  - **Indicateur de sécurité**
    - Not secure
  - **Analyse Google**
    - Aucun contenue suspect

- Site n° 3
    - **Indicateur de sécurité**
        - Not secure
    - **Analyse Google**
        - Vérifier l'URL en particulier

6-Achats en ligne sécurisés

1/ Registre des achats
1-1/ création d'un dossier sur ma messagerie électronique

7-Comprendre le suivi du navigateur

- ☑ gestion des cookies et l'utilisation de la navigation privée

8-Principes de base de la confidentialité des médias sociaux

- ☑ 1/ Réglage des paramètres de confidentialité pour facebook

9-Que faire si votr ordinateur est infecté par un virus

1/ Pour vérifier la sécurité de son ordinateur :

- Mettez à jour votre logiciel antivirus : s'assurer que l'antivirus est activé et mis à jour
- Effectuez une analyse complète du système : lancez une analyse complète du système à l'aide du logiciel antivirus pour détecter et supprimer tout malware potentiel.
- Vérifiez les mises à jour du système d'exploitation : Assurez-vous que votre système d'exploitation (Windows, macOS, Linux, etc.) est entièrement mis à jour avec les derniers correctifs de sécurité.
- Vérifiez les autorisations des applications : Passez en revue les autorisations accordées aux applications installées sur votre ordinateur. Révoquez toute autorisation qui semble excessive ou non nécessaire.
- Effectuez une sauvegarde régulière des données : Assurez-vous que vos données sont sauvegardées régulièrement afin de pouvoir les récupérer en cas d'attaque de malware ou de perte de données.

2/Installation et utilisation d’un antivirus + antimalware sur un ordinateur :

Premièrement il faut choisir un logiciel et le télécharger sur l’ordinateur. Pour faire l’installation, on doit accéder au site officiel du logiciel choisi, trouver la page de téléchargement et télécharger la version appropriée selon votre système d’exploitation puis lancer le fichier d’installation.

Une fois le logiciel installé, il faut suivre ces quelques étape pour l’utilisation :

4. **Configuration de l'antivirus** :

- Après l'installation, ouvrez le logiciel antivirus.
- Configurez les paramètres selon vos préférences. Assurez-vous d'activer les fonctions de protection en temps réel et de planification des analyses.

5. **Mise à jour des définitions de virus** :

- Vérifiez les mises à jour des définitions de virus. Cette étape est cruciale pour garantir une protection maximale.

6. **Analyse du système** :

- Lancez une analyse complète de votre système à la recherche de virus et de malwares. Observez le processus et notez s'il détecte des menaces.

7. **Installation de l'antimalware :**

- Répétez les étapes 2 à 5 pour installer et configurer le logiciel antimalware choisi.

8. **Analyse complémentaire avec l'antimalware** :

- Utilisez le logiciel antimalware pour effectuer une analyse complète de votre système. Comparer les résultats avec ceux de l'antivirus.

9. **Planification des analyses automatique**s :

- Configurez des analyses automatiques régulières pour garantir une protection continue.

10. **Observation des notifications** :

- Familiarisez-vous avec les notifications de votre logiciel antivirus et antimalware. Comprenez comment réagir en cas de menace détectée.

11. **Rapport de santé du système** :

- Explorez les fonctionnalités du logiciel qui vous permettent de consulter un rapport de santé du système. Comprenez les informations fournies.