PROJET1 – un peu plus de sécurité, on n’en a jamais assez

1- Introduction à la sécurité sur Internet

Réponse1

1- Article 1 = ANSSI – Découvrir la cybersécurité
2- Article2 = économie gouv = comment assurer votre sécurité numérique
3- Article3 = site W – Naviguez en toute sécurité sur internet

2 – sur mon ordinateur

3 – Fonctionnalité de sécurité de votre navigateur

REPONSE1

1°

Les sites web qui semblent être malveillants sont :

1- www.morvel.com , un dérivé de WWW.MARVEL.COM le site web officiel de l'univers Marvel
2- www.fesseboook.com, un dérivé de www.facebook.com , le plus grand réseau social du monde
3- www.instagam.com, un dérivé de www.instagram.com, un autre réseau très utilisé

les seuls sites web qui semblent 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/

Sur mon PC

4- EVITER LE SPAM ET LE PHISHING

9- QUE FAIRE SI VOTRE ORDINATEUR EST INFECTE PAR UN VIRUS

1. **Analyse antivirus** :
   - Téléchargez et installez un logiciel antivirus fiable si vous n'en avez pas déjà un.
   - Effectuez une analyse complète de votre système pour détecter les éventuelles infections virales.
   - Notez les résultats de l'analyse pour référence ultérieure.
2. **Mises à jour du système et des logiciels** :
   - Assurez-vous que votre système d'exploitation (comme Windows, macOS, Linux) ainsi que tous les logiciels installés sont à jour.
   - Activez les mises à jour automatiques si ce n'est pas déjà fait.

3. **Scan anti-malware spécifique** :
   - Utilisez un logiciel anti-malware réputé pour effectuer un scan spécifique à la recherche de logiciels malveillants autres que des virus, comme les logiciels espions et les chevaux de Troie.
4. **Analyse des comportements suspects** :
   - Examinez les comportements inhabituels de votre ordinateur, tels que des ralentissements soudains, des fenêtres pop-up non sollicitées, des modifications inexpliquées des paramètres, etc.
5. **Contrôle des extensions de navigateur et des programmes au démarrage** :
   - Vérifiez les extensions installées dans votre navigateur web. Supprimez celles

que vous n'avez pas ajoutées intentionnellement.
   - Examinez la liste des programmes démarrant automatiquement avec votre système d'exploitation et désactivez ceux qui semblent suspects ou inutiles.
6. **Sauvegarde des données importantes** :
   - Assurez-vous que vos données importantes sont sauvegardées régulièrement sur un support externe ou dans le cloud.
7. **Nettoyage du système** :
   - Utilisez des outils de nettoyage du système pour supprimer les fichiers temporaires, les cookies et autres éléments inutiles qui pourraient potentiellement être exploités par des logiciels malveillants.
8. **Renforcement de la sécurité** :

- Renforcez les mesures de sécurité de votre ordinateur en activant le pare-feu intégré, en installant des extensions de sécurité du navigateur, en utilisant des mots de passe forts et en activant la double authentification lorsque cela est possible.

9. **Rapport et suivi** :
   - Si des infections sont détectées, suivez les instructions fournies par votre logiciel antivirus/anti-malware pour les supprimer.
   - Faites un rapport de l'exercice en notant les actions entreprises, les problèmes rencontrés et les mesures correctives prises.