# Projet 1 – Un peu plus de sécurité, on n'en a jamais assez !

## 1- Introduction à la sécurité sur Internet

1/ voici trois articles récents sur la sécurité sur internet :

- Article 1 = Le Monde – Article : « Piratage informatique : les entreprises ont du mal à se protéger des attaques »
- Article 2 = Forbes – Article : « 5 Cybersecurity Threats to Watch For in 2023 »
- Article 3 = TechRadar – Article : « Why VPN is important for online privacy and data security in 2023 »

## 2- Créer des mots de passe forts

1/☑

## 3- Fonctionnalité de sécurité de votre navigateur

1/

- www.morverl.com ☑
- www.dccomics.com
- www.ironman.com
- www.fessebook.com ☑
- www.instagam.com ☑

2/

- Pour Chrome ☑
- Pour Firefox ☑

## 4- Éviter le spam et le phising

1/☑

## 5- Comment éviter les logiciels malveillants

3/

- Site n°1 :
  - Indicateur de sécurité :
    - ¤ HTTPS
  - Analyse Google
    - ¤ Aucun contenu suspect
- Site n°2 :
  - Indicateur de sécurité :
    - ¤ HTTPS
  - Analyse Google
    - ¤ Aucun contenu suspect
- Site n°3 :
  - Indicateur de sécurité :
    - ¤ Not secure
  - Analyse Google
    - ¤ Vérifier une URL en particulier
- Site n°4 :
  - Indicateur de sécurité :
    - ¤ Not secure
  - Analyse Google
    - ¤ Aucun contenu suspect

## 6- Achats en ligne sécurisés ☑

## 7- Comprendre le suivi du navigateur ☑
## 8- Principe de base de la confidentialité des médias sociaux☑
## 9- Que faire si mon ordinateur est infecté par un virus

1/ Voici quelques idées d'exercices pour vérifier la sécurité en fonction de l'appareil utilisé :

1. Ordinateur :

- Utilisez un logiciel antivirus pour scanner votre ordinateur et détecter les éventuelles menaces.
- Effectuez une mise à jour de tous vos logiciels pour vous assurer qu'ils sont à jour et protégés contre les vulnérabilités connues.
- Testez votre pare-feu en vérifiant que les ports non nécessaires sont fermés et que les connexions entrantes et sortantes sont contrôlées.

2. Smartphone :

- Utilisez un logiciel antivirus pour scanner votre smartphone et détecter les éventuelles menaces.
- Vérifiez les autorisations de toutes vos applications et désactivez celles qui ne sont pas nécessaires.
- Activez le chiffrement des données pour protéger vos informations sensibles.

3. Routeur :

- Modifiez les paramètres de connexion par défaut de votre routeur (nom et mot de passe).
- Vérifiez que le firmware de votre routeur est à jour pour éviter les vulnérabilités connues.
- Vérifiez les paramètres de sécurité de votre routeur pour vous assurer que les connexions entrantes et sortantes sont contrôlées et que les ports non nécessaires sont fermés.

4. Disque dur externe :

- Utilisez un logiciel antivirus pour scanner votre disque dur externe et détecter les éventuelles menaces.
- Cryptez vos fichiers sensibles pour les protéger contre les accès non autorisés.
- Vérifiez régulièrement l'intégrité de vos fichiers pour éviter les pertes de données.

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

1. Ordinateur :

a. Téléchargez un logiciel antivirus gratuit tel que Avast, AVG, ou Bitdefender. b. Installez le logiciel antivirus en suivant les instructions fournies. c. Une fois l'installation terminée, mettez à jour la base de données de virus pour vous assurer que le logiciel est à jour. d. Exécutez une analyse complète de votre système pour détecter les éventuelles menaces et virus. e. Si le logiciel antivirus détecte une menace, suivez les instructions pour la supprimer.