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

**1 - Introduction à la sécurité sur Internet**

Article 1 = https://www.lajauneetlarouge.com/securite-et-liberte-sur-linternet/

Article 2 = https://www.boutique-box-internet.fr/actualites/securite-sur-internet/

Article 3 = https://www.cnil.fr/fr/securite-securiser-les-sites-web

**2 - Créer des mots de passe forts**

Utiliser un gestionnaire de mot de passe LastPass.

**3 - Fonctionnalité de sécurité de votre navigateur**

Les navigateurs sécurisés aident à bloquer les outils tiers, tels que les cookies.

Permettre la consultation d'informations disponibles (« ressource » dans la terminologie du Web) sur le World Wide Web.

Identification des adresses internet qui se semble provenir de sites web malveillants.

Vérification si les navigateurs utilisés sont à jour.

**4 - Éviter le spam et le phishing**

Vérifiez le sujet et l'expéditeur de l'email ou SMS

Identifier les messages de phishing et de smishing

Ne cliquez pas sur les liens

Site web sécurisé

Augmenter la sécurité de votre système

**5 - Comment éviter les logiciels malveillants**

Sécurisation de l'ordinateur et identification des liens suspects.

1. Vérifier l'authenticité du site. Eviter de naviguer sur des sites dont l'origine des produits ou services ne pourrait pas être justifiée. ...
2. Contrôler les mises à jour. ...
3. Méfier des pièces jointes.

**6 - Achats en ligne sécurisés**

Création d'un registre des achats effectués sur internet.

**7 - Comprendre le suivi du navigateur**

Permet de préserver la confidentialité de vos préférences personnelles.

**8 - Principes de base de la confidentialité des médias sociaux**

Réglage des paramètres de confidentialité de Facebook

- Confidentialité
- Publications publiques

**9 - Que faire si votre ordinateur est infecté par un virus**

Objectif : Utilisation d'un logiciel antivirus ou antimalware.

1/ Proposition d'un exercice pour vérifier la sécurité en fonction de l'appareil utilisée :

La première chose à faire est de vous assurer que les bases de données de votre antivirus sont à jour pour ensuite réaliser une analyse de votre ordinateur. Si cela n'aide pas, les solutions antivirus d'autres fournisseurs pourraient faire l'affaire. De nombreux fabricants d'antivirus offrent des versions d'essai gratuites de leurs produits : nous vous recommandons d'utiliser un de ces produits sur votre ordinateur. Si un virus ou un cheval de Troie est détecté, assurez-vous d'envoyer une copie du fichier infecté à l'éditeur de la solution antivirus qui n'a pas réussi à le détecter avant. Cela aidera ce dernier à développer une protection contre cette menace plus rapidement et à empêcher les autres utilisateurs qui utilisent également cet antivirus d'être infectés.

Si un autre antivirus ne détecte pas de malware, nous vous recommandons de déconnecter l'ordinateur d'Internet ou du réseau local, de désactiver la connexion Wi-Fi et le modem, avant de rechercher des fichiers infectés. N'utilisez le réseau que si c'est absolument nécessaire. N'utilisez surtout pas les systèmes de paiement en ligne ou les services bancaires en ligne. Évitez d'utiliser des données personnelles ou confidentielles, n'utilisez pas de site Web qui requiert un nom d'utilisateur et un mot de passe.

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

Activer l'antivirus Windows Defender

1. Tapez et cliquez sur Centre de Sécurité Windows Defender dans Cortana.
2. La fenêtre Centre de Sécurité Windows Defender s'ouvre. ...
3. Dans la nouvelle fenêtre, vérifiez que tous les curseurs sont activés.
4. Votre antivirus Windows Defender est activé, votre ordinateur est protégé.