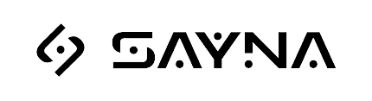
****

**Parcours : DISCOVERY**

**Module : Naviguer en toute sécurité**

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

En naviguant sur le web, consulte trois articles qui parlent de sécurité sur internet.

Voici les articles que nous avons retenus pour toi (avec les mots-clés “sécurité sur internet”

et “comment être en sécurité sur internet” :

● Article 1 = ANSSI - Dix règles de base

● Article 2 = Economie.gouv - Comment assurer votre sécurité numérique

● Article 3 = Site W - Naviguez en toute sécurité sur Internet

● Article bonus = wikiHow - Comment surfez en sécurité sur internet

**2 - Créer des mots de passe forts**

(pratique)

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

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

Les sites web qui semblent être malveillants sont :

● www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l’univers

Marvel

● www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social

du monde

● www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très

utilisé

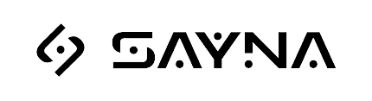
Les seuls sites qui semblaient être cohérents sont donc :

● 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)

**4 - Éviter le spam et le phishing**

****

(pratique)

**5 - Comment éviter les logiciels malveillants**

Sécuriser votre ordinateur et identifier les liens suspects

● Site n°1

○ Indicateur de sécurité

■ HTTPS

○ Analyse Google

■ Aucun contenu suspect

● Site n°2

○ Indicateur de sécurité

■ Not secure

○ Analyse Google

■ Aucun contenu suspect

● Site n°3

○ Indicateur de sécurité

■ Not secure

○ Analyse Google

■ Vérifier un URL en particulier (analyse trop générale)

**6- Achats en lignes et sécurisée**

(pratique)

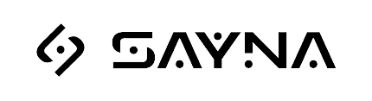
**7 - Comprendre le suivi du navigateur**

(pratique)

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

(pratique)

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

****

Proposition pour vérifier en fonction de l’appareil utilisé

Utilisez un logiciel antivirus : Assurez-vous que votre PC dispose d'un logiciel antivirus fiable et à jour. Lancez une analyse complète du système pour détecter et éliminer les virus et autres logiciels malveillants.

Proposition pour installer et utilisation un antiviru + antimalware

Recherchez un antivirus et un antimalware réputés : Effectuez une recherche en ligne pour trouver des antivirus et des antimalware bien évalués et réputés pour leur efficacité. Assurez-vous de choisir des logiciels provenant de sources fiables et sécurisées.

Téléchargez les logiciels : Rendez-vous sur les sites officiels des antivirus et des antimalware que vous avez choisis. Téléchargez les programmes d'installation sur votre PC.

Désactivez temporairement Windows Defender : Si vous avez déjà Windows Defender (l'antivirus intégré à Windows), il est recommandé de le désactiver temporairement avant d'installer un autre antivirus. Pour cela, allez dans les paramètres de sécurité de Windows et désactivez la protection en temps réel.