



**Parcours : DISCOVERY**

**Module : Navigateur en toute sécurité**

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

---

### ***Sommaire***

---

- 1 - Introduction à la sécurité sur Internet
- 2 - Créés de mot de passe forts
- 3 - Fonctionnalité de sécurité de votre navigateur
- 4 - Eviter le spam et le phishing
- 5 - Comment éviter les logiciels malveillants
- 6 - Achats en ligne sécurisées
- 7 - Comprendre le suivi du navigateur
- 8 - Principale de base de la confidentialité des médias sociaux
- 9 - Que faire si votre ordinateur est infecté par un virus

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

Mesures de sécurité et précautions pour protéger les informations personnelles et les appareils contre les menaces en ligne.

### **Objectif :**

L'objectif de la sécurité sur Internet est de protéger les données personnelles et les appareils contre les menaces en ligne.

**Réponse 1 :** Voici les articles que nous avons retenus (avec les mots-clés "sécurité sur internet" et "comment être en sécurité sur internet" :

- 1- ANSSI : Dix règles de base pour une sécurité sur internet optimale.
- 2- Economie.gouv : Comment protéger votre sécurité numérique avec plusieurs astuces pratiques.
- 3- Site W : Conseils et astuces pour naviguer en toute sécurité sur Internet.
- Bonus - wikiHow : Comment naviguer en toute sécurité sur Internet pour éviter les menaces en ligne.

## **2 - Créer des mots de passe forts**

### **Objectif :**

L'objectif de créer des mots de passe forts est de protéger les comptes et les informations personnelles contre les pirates informatiques.

- ◆ Comment créer un mot de passe fort?

Pour créer un mot de passe fort : Utilisez des combinaisons complexes de lettres, chiffres et symboles, évitez les mots courants et personnels, et utilisez des phrases mnémotechniques.

Pour créer un Mot de Passe Fort & Facile à Retenir allez sur ce

lien: [https://fr.wizcase.com/blog/astuces-pour-creer-un-mot-de-passe/?](https://fr.wizcase.com/blog/astuces-pour-creer-un-mot-de-passe/?gclid=Cj0KCQjwz6ShBhCMARIsAH9A0qU0lw1v2L3KjP6DlxZPVgvfgwIqDaJvoK4Z6g_TDUU9WX)

[gclid=Cj0KCQjwz6ShBhCMARIsAH9A0qU0lw1v2L3KjP6DlxZPVgvfgwIqDaJvoK4Z6g\\_TDUU9WX](https://fr.wizcase.com/blog/astuces-pour-creer-un-mot-de-passe/?gclid=Cj0KCQjwz6ShBhCMARIsAH9A0qU0lw1v2L3KjP6DlxZPVgvfgwIqDaJvoK4Z6g_TDUU9WX)  
[Ckp3xtStUaAq2cEALw\\_wcB](https://fr.wizcase.com/blog/astuces-pour-creer-un-mot-de-passe/?gclid=Cj0KCQjwz6ShBhCMARIsAH9A0qU0lw1v2L3KjP6DlxZPVgvfgwIqDaJvoK4Z6g_TDUU9WX)

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

Protection de votre navigation en ligne contre les logiciels malveillants, les programmes espions et les attaques de phishing.

### **Objectif :**

L'objectif des fonctionnalités de sécurité des navigateurs est de protéger l'utilisateur contre les menaces en ligne telles que les logiciels malveillants et les sites frauduleux.

### **Réponse 1**

Les sites web malveillants sont [www.morvel.com](http://www.morvel.com), [www.fessebook.com](http://www.fessebook.com) et [www.instagram.com](http://www.instagram.com). Les sites fiables sont [www.dccomics.com](http://www.dccomics.com) et [www.ironman.com](http://www.ironman.com).

#### **4 - Éviter le spam et le phishing**

##### **Objectif :**

Le spam et le phishing ont pour objectif de tromper l'utilisateur pour obtenir des informations personnelles ou financières sensibles.

Pour en savoir plus clic ce lien :

<https://www.ing.lu/content/siteing/fr/Individuals/my-money/categories/techtalk/6-ways-to-avoid-falling-victim-to-phishing-scams.html>

#### **5 - Comment éviter les logiciels malveillants**

Pour éviter les logiciels malveillants : Utilisez des programmes antivirus, évitez les sites douteux, ne cliquez pas sur les liens inconnus et évitez de télécharger des fichiers suspects.

##### **Objectif :**

Eviter les attaques informatiques, protéger les données personnelles et éviter les pertes financières ou de productivité.

Pour en savoir plus clic ce lien : <https://support.google.com/google-ads/answer/2375413?hl=fr>

#### **7 - Comprendre le suivi du navigateur**

Les sites web suivent l'activité de navigation pour personnaliser les publicités et améliorer l'expérience utilisateur grâce aux cookies et autres technologies.

##### **Objectif :**

Personnaliser les publicités et l'expérience utilisateur, analyser le comportement en ligne et améliorer les produits et services.

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

Paramétrez les options de confidentialité, partagez seulement ce que vous êtes à l'aise de rendre public et évitez de publier des informations sensibles.

##### **Objectif :**

Protéger la vie privée et la sécurité en ligne, contrôler la visibilité de l'information et réduire les risques d'abus.

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

Les chose qu'on va faire si notre ordinateur est infecté par un virus :

Désactivez la connexion Internet, exécutez une analyse antivirus, puis supprimez le logiciel malveillant ou demandez l'aide d'un professionnel.

**Objectif pour comment faire si UN ordinateur est infecté par un virus:**

Éliminer le virus pour éviter les pertes de données, les blocages et les autres problèmes informatiques.

**1/** Pour vérifier la sécurité, exécutez une analyse antivirus, configurez les options de confidentialité et évitez les sites douteux.

**2/** Téléchargez et installez un logiciel antivirus et antimalware, exécutez une analyse complète et configurez les paramètres de protection.