



## Parcours : DISCOVERY

Module : Naviguer en toute  
sécurité

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

*Tous vos travaux devront être déposés sur  
votre compte Github*

---

**Sommaire**

---

- 1 - Introduction à la sécurité sur Internet
- 2 - Créer des mots de passe forts
- 3 - Fonctionnalité de sécurité de votre navigateur
- 4 - Éviter le spam et le phishing
- 5 - Comment éviter les logiciels malveillants
- 6 - Achats en ligne sécurisés
- 7 - Comprendre le suivi du navigateur
- 8 - Principes 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

Objectif : à la découverte de la sécurité sur internet

1/ En naviguant sur le web, consulte trois articles qui parlent de sécurité sur internet. Pense à vérifier la sources des informations et essaie de consulter des articles récents pour que les informations soient à jour. Saisis le nom du site et de l'article.

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 = kapersky - Qu'est-ce que la sécurité Internet ?
- Article 2 = Wikipedia - Comment assurer votre sécurité numérique
- Article 3 = La poste - 5 conseils pour être en sécurité sur Internet

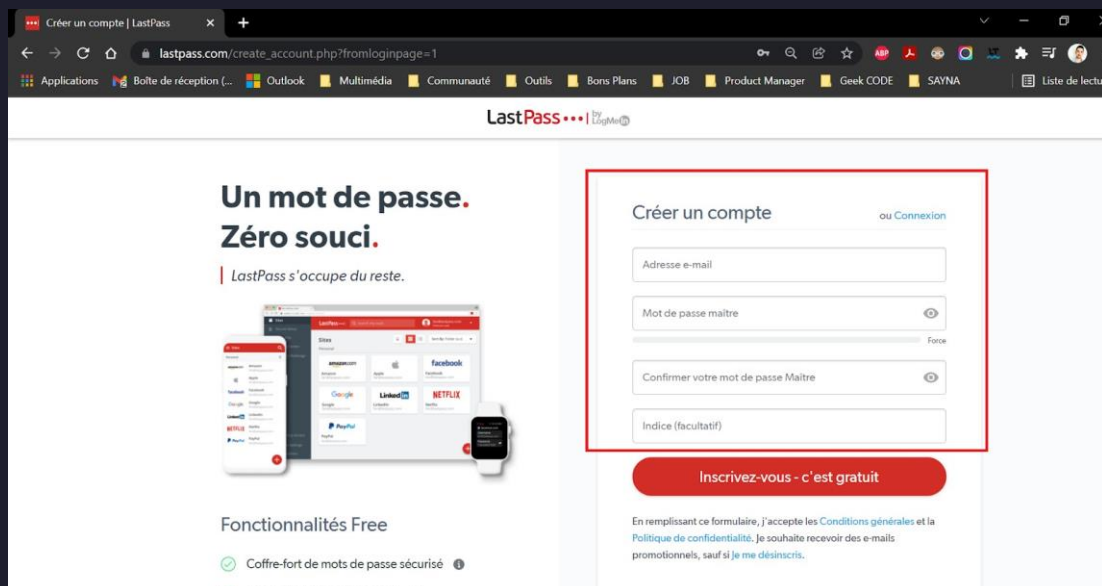
## 2 - Créer des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass

1/ Dans cet exercice, nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Ce gestionnaire prend la forme d'une application web, accessible sur tous supports (PC, Mac, mobile). Il est simple à prendre en main et propose un niveau de sécurité optimal. Suis les étapes suivantes.

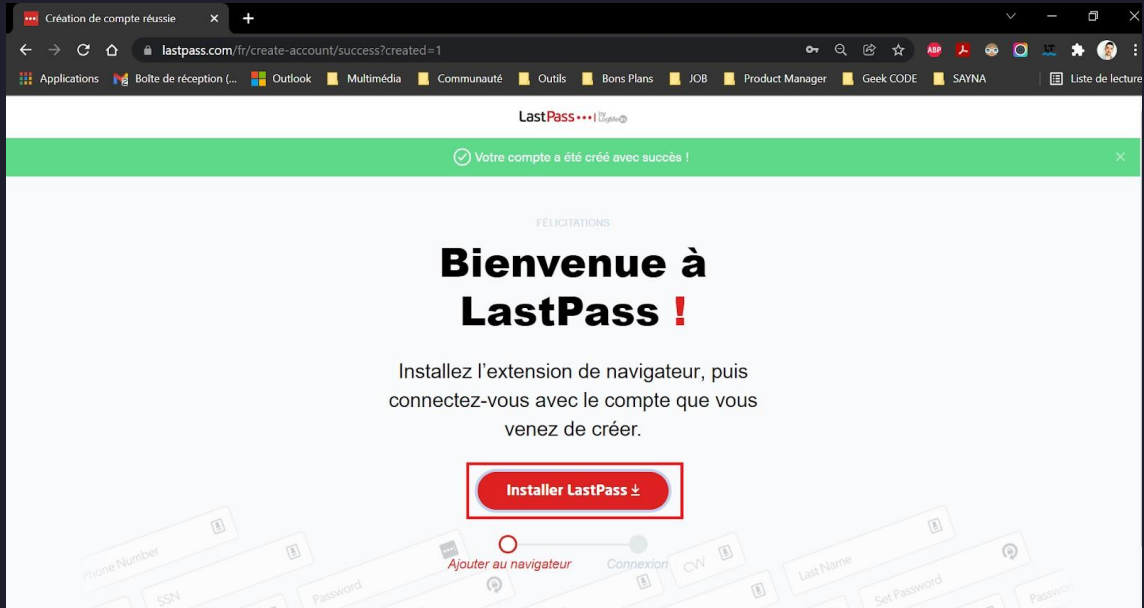
(case à cocher)

- Accède au site de LastPass avec ce lien

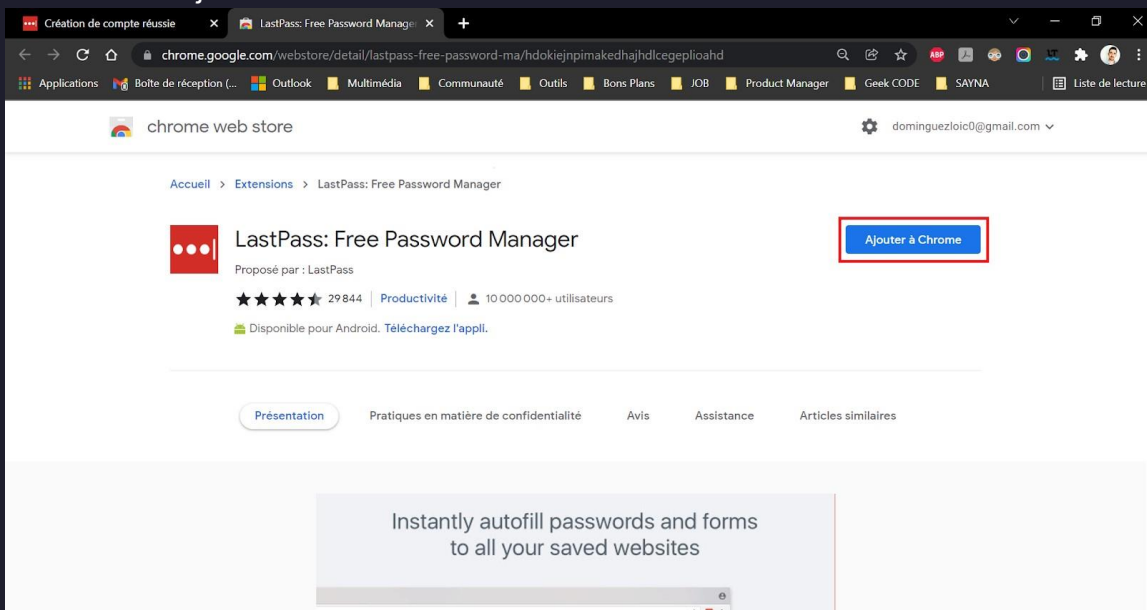



- Crée un compte en remplissant le formulaire. Un conseil, on te demande de choisir un mot de passe maître. Pour rappel, ce mot de passe sera unique et te permettra d'accéder à tous tes comptes. Choisis donc un mot de passe avec un niveau de sécurité élevé et assure-toi de pouvoir le retrouver
  - Exemple de mot de passe maître : c3c!3s!!3M0!2P@SS3 (Ceci est le mot de passe, en remplaçant le "e" par "3" le "i", "t" par "!", "a" par "@" et les premières lettres en minuscules puis majuscules à partir de "mot")
  - Tu peux également générer un mot de passe maître, mais pense à l'écrire dans un endroit sûr pour pouvoir l'utiliser lorsque tu en as besoin

- Une fois la création du compte effectuée, tu arrives sur une page de validation qui propose le téléchargement de l'extension sur ton navigateur. Lance l'installation en effectuant un clic sur le bouton prévu à cet effet

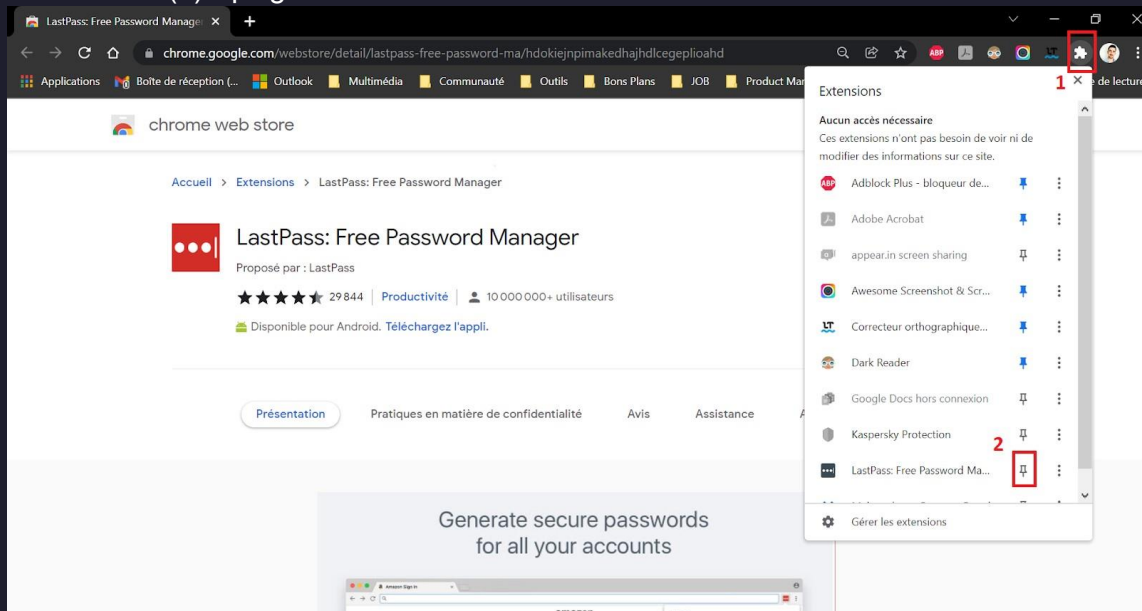


- Il te suffit de valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome"

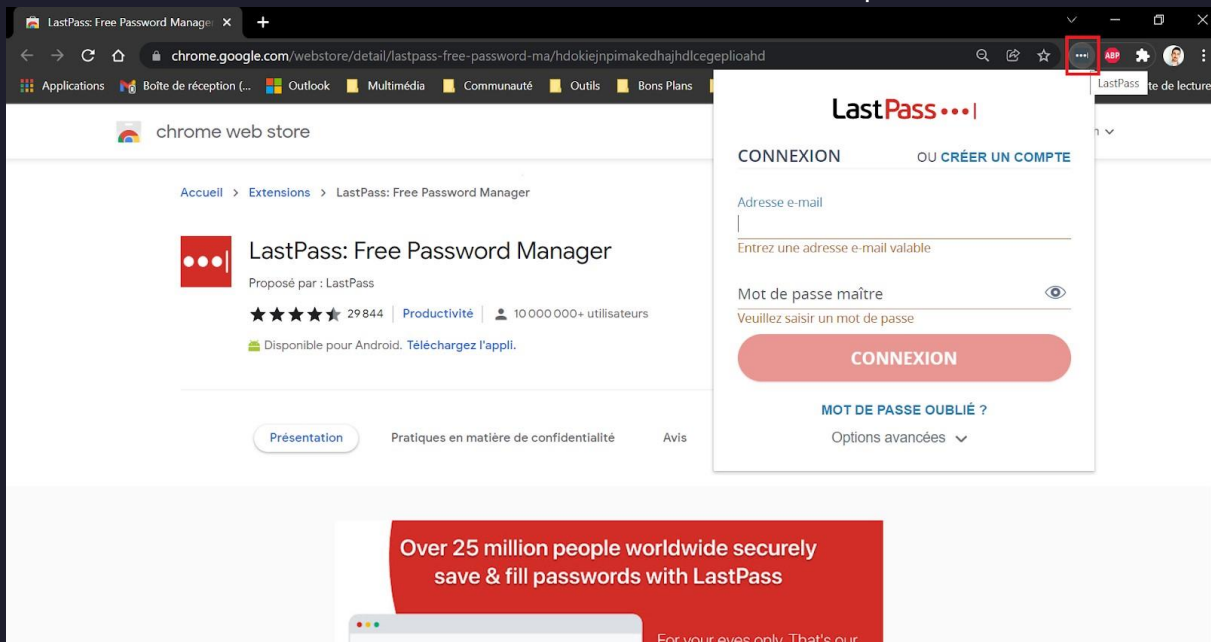


- Une fois installé, il te suffit d'accéder à cette extension et de t'y connecter
  - (1) En haut à droite du navigateur, clic sur le logo "Extensions" 

- (2) Épingler l'extension de LastPass avec l'icône



- Il ne te reste plus qu'à te connecter en effectuant un clic sur l'icône de l'extension et en saisissant ton identifiant et mot de passe



## 3 - Fonctionnalité de sécurité de votre navigateur

Objectif : identifier les éléments à observer pour naviguer sur le web en toute sécurité

- 1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants.  
(Case à cocher)

- www.morvel.com
- www.dccomics.com
- www.ironman.com

- [www.fessebook.com](http://www.fessebook.com)
- [www.instagram.com](http://www.instagram.com)

## Réponse 1


Les sites web qui semblent être malveillants sont :

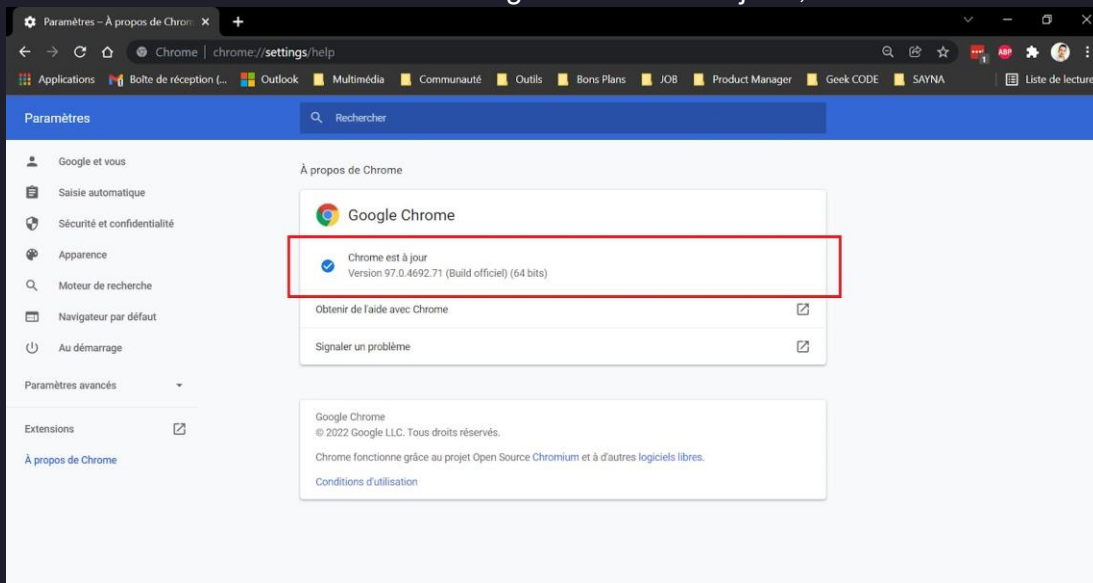
- [www.morvel.com](http://www.morvel.com), un dérivé de [www.marvel.com](http://www.marvel.com), le site web officiel de l'univers Marvel
- [www.fessebook.com](http://www.fessebook.com), un dérivé de [www.facebook.com](http://www.facebook.com), le plus grand réseau social du monde
- [www.instagram.com](http://www.instagram.com), un dérivé de [www.instagram.com](http://www.instagram.com), un autre réseau social très utilisé


Les seuls sites qui semblaient être cohérents sont donc :

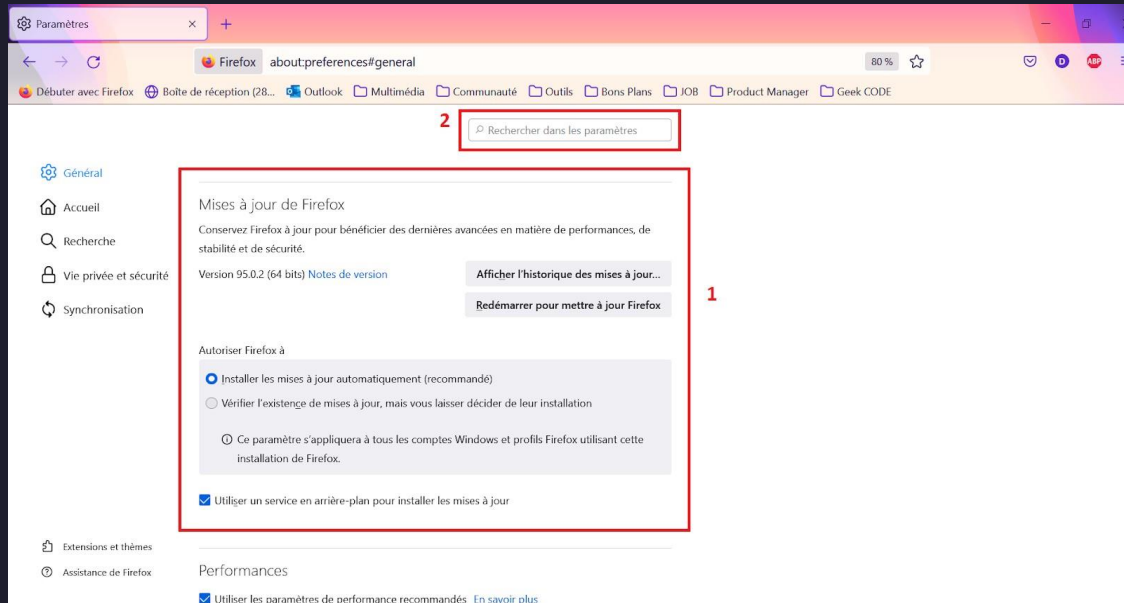
- [www.dccomics.com](http://www.dccomics.com), le site officiel de l'univers DC Comics
- [www.ironman.com](http://www.ironman.com), le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

**2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes. (case à cocher)**

- Pour Chrome
  - Ouvre le menu du navigateur  et accède aux "Paramètres"
  - Clic sur la rubrique "À propos de Chrome"
  - Si tu constates le message "Chrome est à jour", c'est Ok



- Pour Firefox
  - Ouvre le menu du navigateur  et accède aux "Paramètres"
  - Dans la rubrique "Général", fais défiler jusqu'à voir la section "Mise à jour de Firefox (astuce : tu peux également saisir dans la barre de recherche (2) "mises à jour" pour tomber directement dessus)



- Vérifie que les paramètres sélectionnés sont identiques que sur la photo

## 4 - Éviter le spam et le phishing

Objectif : *Reconnaître plus facilement les messages frauduleux*

**1/ Dans cet exercice, on va exercer ta capacité à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.**

Pour ce faire accède au lien suivant et suis les étapes qui y sont décrites : Exercice 4 -  
Spam et Phishing

### Réponse 1

Bon travail, RAJAONA  
HERINJARA Aristote  
Méa !

Vous avez obtenu un  
score de 7/8.

Plus vous vous entraînez, mieux vous saurez identifier les  
pièges et vous protéger des tentatives d'hameçonnage.

Quelques mesures très simples à mettre en place peuvent  
également améliorer la protection de vos comptes en ligne.  
Pour plus d'informations, consultez la page [g.co/2SV](https://g.co/2SV).

Partager le questionnaire :



RECOMMENCER LE QUESTIONNAIRE

## 5 - Comment éviter les logiciels malveillants


Objectif : *sécuriser votre ordinateur et identifier les liens suspects*

3/ Lors de la navigation sur le web, il arrive d'avoir des doutes sur la sécurité de certains sites. Comme tu as pu le voir précédemment, le premier de niveau de vigilance à avoir se trouve dans la barre d'adresse des navigateurs web. La plupart affichent des indicateurs de sécurité pour donner une information sur la protection d'un site internet.

Lorsque le doute persiste tu peux t'appuyer sur un outil proposé par Google : Google Transparency Report (en anglais) ou Google Transparence des Informations (en français). Afin d'améliorer ta lecture de la sécurité sur internet, tu vas devoir analyser les informations de plusieurs sites. Pour chaque site tu devras préciser l'indicateur de sécurité et le rapport d'analyse de l'outil Google. Il te suffit d'accéder aux liens proposés ci-dessous pour observer l'indicateur de sécurité et de copier-coller l'URL du site dans l'outil Google. (choix multiples)

### Réponse 1

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

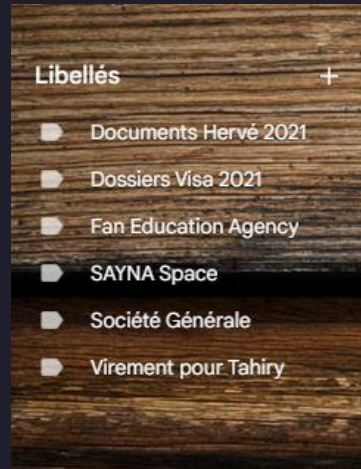
- **Indicateur de sécurité**
  - Not secure ○
- Analyse Google**
  - Vérifier un URL en particulier

## 6 - Achats en ligne sécurisés

Objectif : *créer un registre des achats effectués sur internet*

1 / Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le bilan de tes dépenses du mois.





## 7 - Comprendre le suivi du navigateur

Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée

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

Objectif : *Régler les paramètres de confidentialité de Facebook*

1 / Plus tôt dans le cours ( Internet de base) tu as déjà été amené à utiliser ce réseau social en partageant une publication. Dans cet exercice on va te montrer le réglage des paramètres de confidentialité pour Facebook. Suis les étapes suivantes. (Case à cocher)



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

1/ Exercice : Analyse comparative de la sécurité des appareils

Objectif : Évaluer la sécurité des différents appareils utilisés.

Instructions :

Sélectionnez quatre appareils couramment utilisés, tels que 2 ordinateurs portables, un smartphone et une tablette. Assurez vous que les appareils ont des niveaux de sécurité différents.

Définissez les critères de sécurité pertinents à évaluer, par exemple :

- a. Niveau de cryptage des données
- b. Mesures de protection contre les logiciels malveillants
- c. Possibilité de verrouillage biométrique (empreinte digitale, reconnaissance faciale, etc.)
- d. Mises à jour régulières du système d'exploitation
- e. Options de sauvegarde des données
- f. Politiques de confidentialité et de partage des données

Créez un tableau comparatif avec les critères de sécurité en colonnes et les appareils en lignes

Recherchez des informations sur chaque appareil et remplissez le tableau avec les détails correspondants à chaque critère de sécurité.

Analysez les résultats et déterminez lesquels des appareils semblent offrir le niveau de sécurité le plus élevé.

2/ Exercice pour installer et utiliser un antivirus et antimalware en fonction de l'appareil utilisé

Instructions :

Avec un ordinateur fonctionnant sous Windows (version de votre choix) rechercher et sélectionner un antivirus avec antimalware de confiance. Il existe de nombreuses options disponibles, telles qu'Avast, AVG, Norton, McAfee, etc. Choisissez celle qui vous convient le mieux.

- Rendez vous sur le site Web officiel de l'antivirus choisi et télécharger.
- Une fois le téléchargement terminé, suivez attentivement les instructions.
- Ouvrez l'interface de l'antivirus en cliquant sur son icône et recherchez l'option de mise à jour.
- Une fois les mises à jour effectuées, recherchez une option de scan ou d'analyse.
- Laissez l'antivirus terminer l'analyse. Cela peut prendre un certain temps.
- Une fois l'analyse faite configurez votre antivirus.