Parcours : DISCOVERY
Module : Naviguer en toute sécurité

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

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 source 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.

	Nom du site	Nom de l'article
Article 1	cybermalveillance.gouv.fr	Comment se protéger sur Internet?
Article 2	kaspersky.fr	Sécurité Internet : Qu'est-ce que c'est et comment vous protéger en ligne ?
Article 3	pandasecurity.com	Les bonnes pratiques pour naviguer en toute sécurité sur l'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.

Accède au site de LastPass avec ce lien	✓
Crée un compte en remplissant le formulaire	✓
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	✓
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

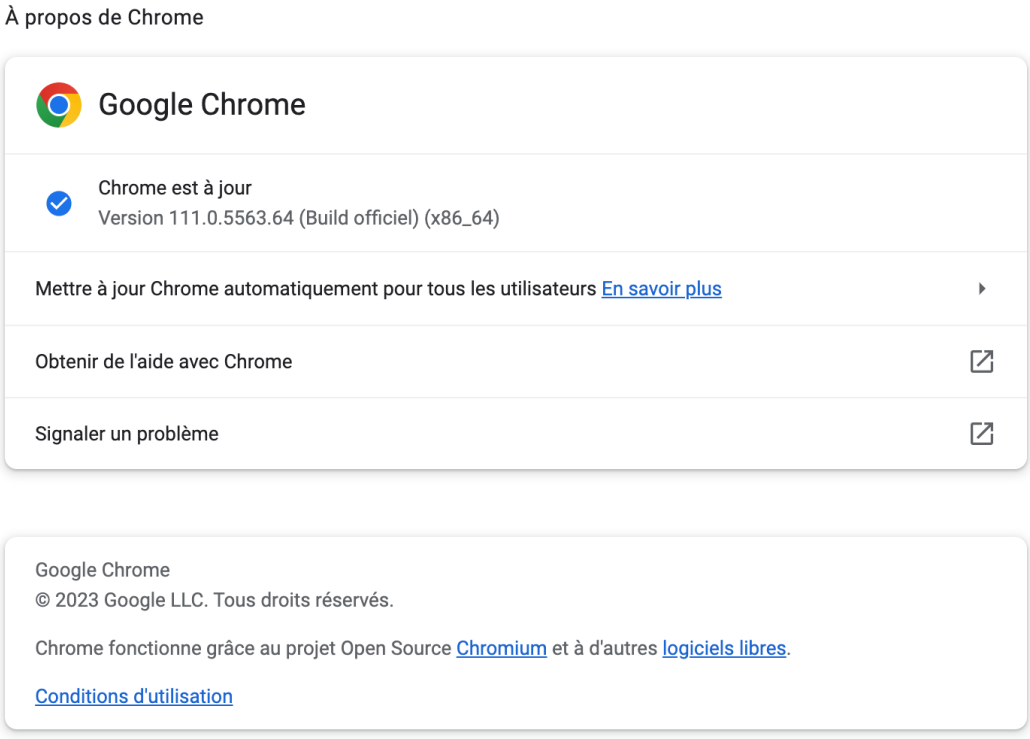
1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants.

www.morvel.com	❌	Site web malveillant dérivé du site marvel
www.dccomics.com	✔	Site officiel
www.ironman.com	✔	Site officiel
www.fessebook.com	❌	Site web malveillant dérivé du site Facebook
www.instagam.com	❌	Site web malveillant pour dérivé du site d'Instagram

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

Pour Chrome

Ouvre le menu du navigateur et accède aux "Paramètres"	✔
Clic sur la rubrique "A propose 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	✔

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.

- ✔ Exercice effectué avec un score de 8/8

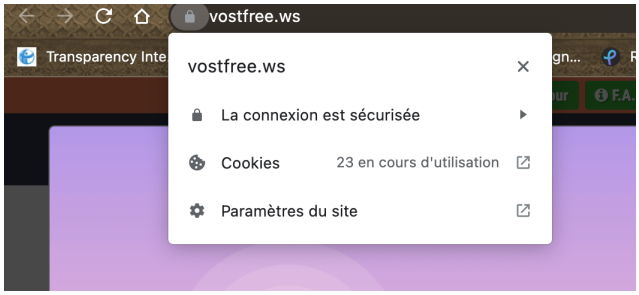
5 - Comment éviter les logiciels malveillants

Objectif : sécuriser votre ordinateur et identifier les liens suspects

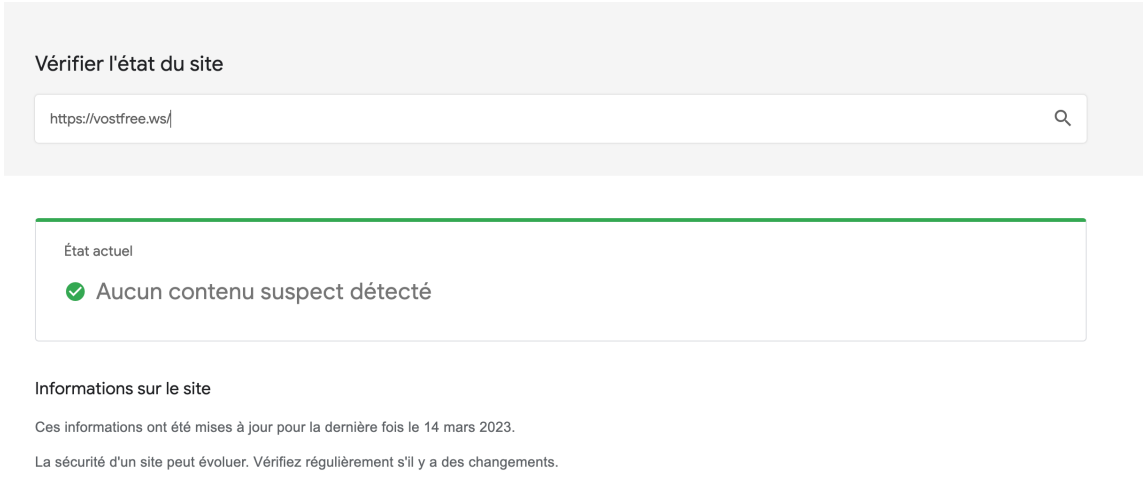
3/ Indicateur de sécurité et le rapport d'analyse de l'outil Google

Site n°1

Indicateur de sécurité : HTTPS

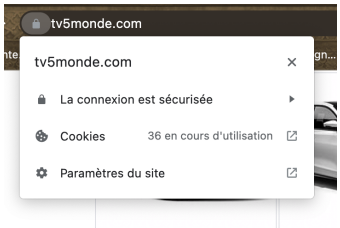


Analyse Google : aucun contenu suspect

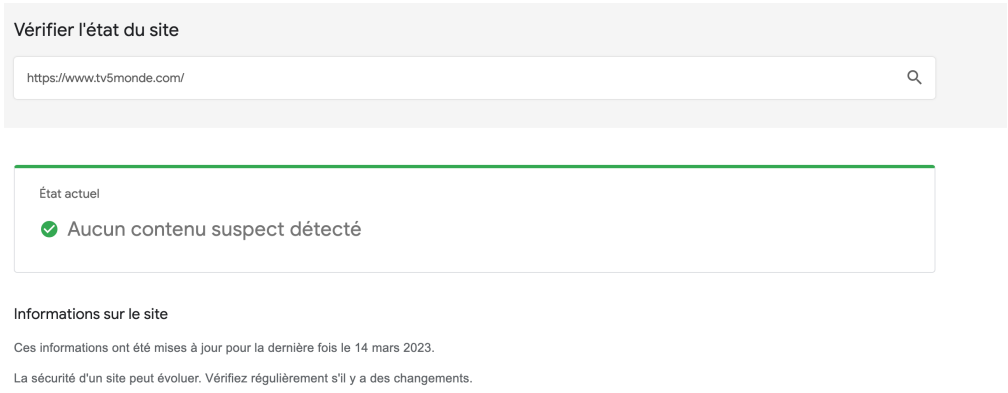


Site n°2

Indicateur de sécurité : HTTPS

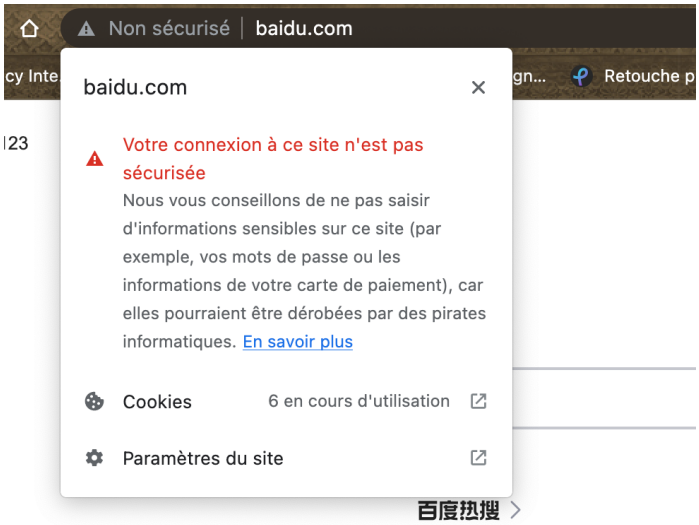


Analyse Google : aucun contenu suspect

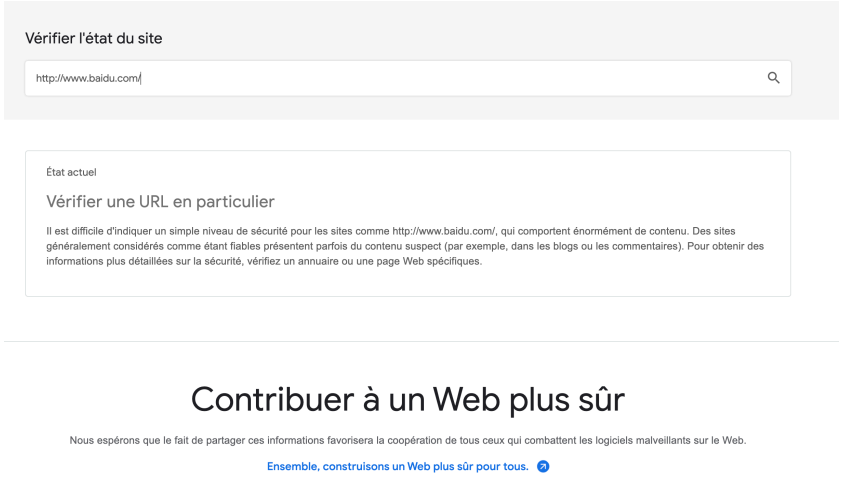


Site n°3

Indicateur de sécurité : Not secure



Analyse Google : Vérifier un URL en particulier (analyse trop générale)



6 - Achats en ligne sécurisés

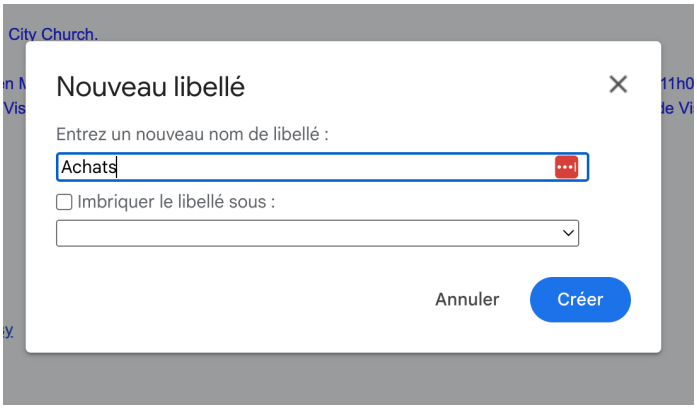
Objectif : créer un registre des achats effectués sur internet

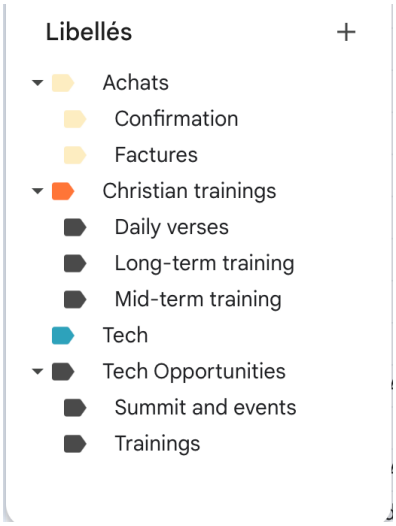
1/ Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le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

Deux possibilités s'offrent à toi pour organiser ce registre :
1. Créer un dossier sur ta messagerie électronique
2. Créer un dossier sur ton espace de stockage personnel

Un dossier sur ta messagerie électronique

Pour commencer, accède à ta messagerie électronique. Pour rappel, tu peux y accéder rapidement en ouvrant un nouvel onglet (dans la barre des favoris ou via le raccourci)	✓
Sur la page d'accueil de ta messagerie, tu trouveras sur la gauche les libellés initialement prévus (boite de réception, messages envoyés, etc.) C'est dans cette partie que tu vas créer ta rubrique des achats. Pour ce faire, clic sur "Plus" et va tout en bas des libellés. Pour créer un libellé rapidement il te suffit d'effectuer un clic sur "Créer un libellé" et de le nommer "ACHATS" (pour notre exercice)	✓
Effectuer un clic sur le bouton "Créer" pour valider l'opération	✓
Tu peux également gérer les libellés en effectuant un clic sur "Gérer les libellés"(1).	✓
Tu as maintenant un libellé pour stocker tous tes messages électroniques relatifs aux achats effectués sur internet : confirmation de l'achat, détail de la commande, modalités de livraison	✓





7 - Comprendre le suivi du navigateur

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

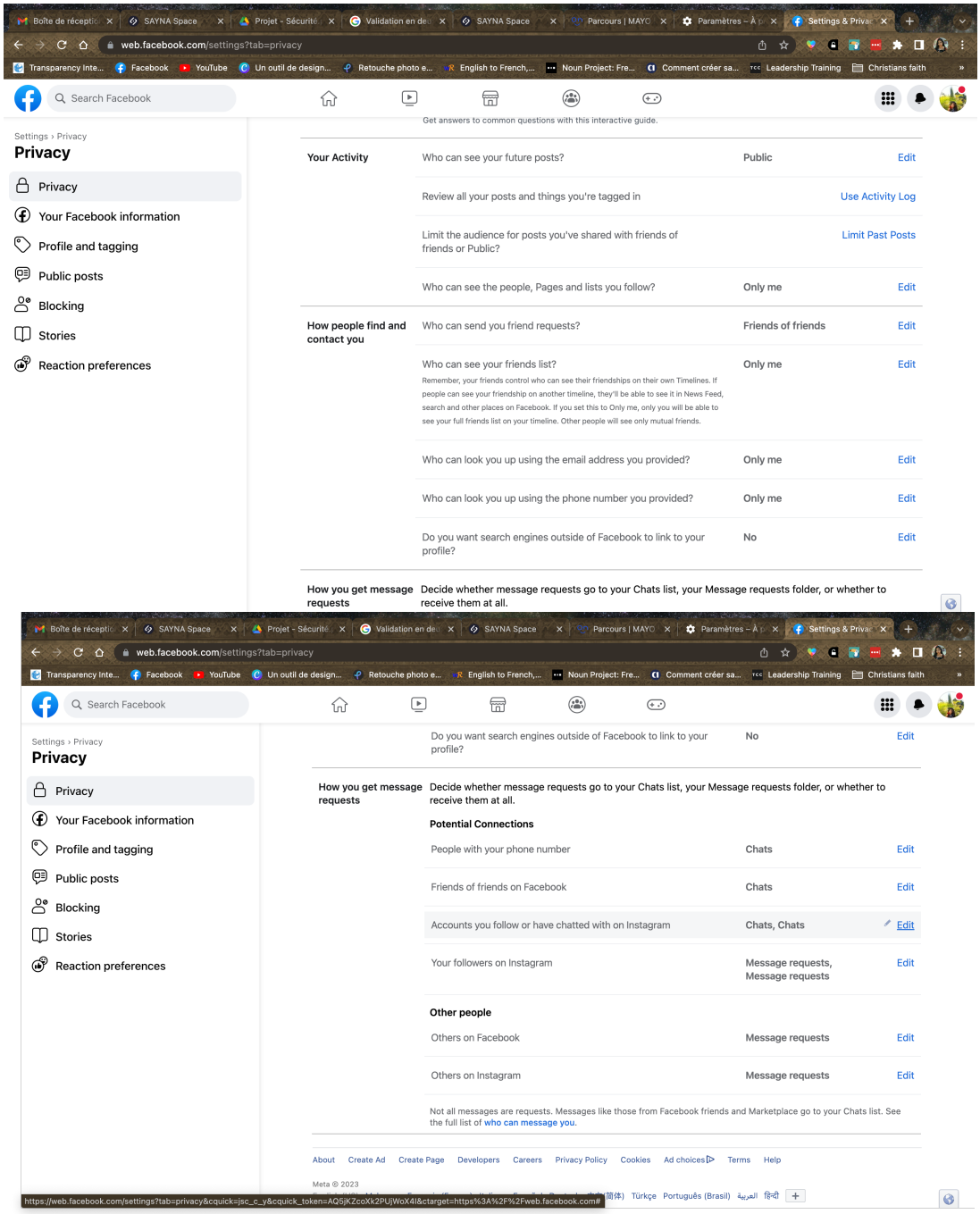
8 - Principes de base de la confidentialité des

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.

Connecte-toi à ton compte Facebook	✓
Une fois sur la page d'accueil, ouvre le menu Facebook, puis effectue un clic sur "Paramètres et confidentialité".	✓
Pour finir, clic sur "Paramètres"Ce sont les onglets "Confidentialité" et "Publications publiques" qui nous intéressent. Accède à "Confidentialité" pour commencer et clic sur la première rubrique Retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à gauche.	✓
Dans les paramètres de Facebook tu as également un onglet "Cookies". On t'en a parlé dans le cours précédent (Comprendre le suivi du navigateur). Maintenant que tu sais comment sont utilisées tes données, tu es capable de choisir en pleine conscience ce que tu souhaites partager.	✓



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

1/ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé ? Comment faire ?

ORDINATEUR

Exécuter un scan complet du système à l'aide d'un logiciel antivirus. Voici comment procéder :

1. Ouvrir le logiciel antivirus et s'assurer que les définitions de virus sont à jour.
2. Lancer une analyse complète du système. On peut également exécuter une analyse rapide, mais une analyse complète est recommandée pour détecter les virus plus profonds.
3. Attendre que l'analyse soit terminée et examiner le rapport d'analyse pour voir s'il y a des virus ou des programmes malveillants détectés.
4. Si un virus est détecté, suivre les instructions du logiciel antivirus afin de supprimer le virus.
5. Si aucun virus n'est détecté, on peut considérer que l'ordinateur est relativement sûr, mais il faut continuer à utiliser l'antivirus et à le mettre à jour régulièrement pour assurer la sécurité

TÉLÉPHONE/TABLETTE

Exécuter une analyse à l'aide d'une application antivirus. Voici comment procéder :

1. Télécharger et installer une application antivirus fiable sur le téléphone à partir du Google Play Store ou de l'App Store.
2. Lancer l'application antivirus et assurer que les définitions de virus sont à jour.
3. Exécuter une analyse complète du téléphone.
4. Attendre que l'analyse soit terminée et examiner le rapport d'analyse pour voir s'il y a des virus ou des programmes malveillants détectés.
5. Si un virus est détecté, suivre les instructions de l'application antivirus pour supprimer le virus.
6. Si aucun virus n'est détecté, continuer à utiliser l'application antivirus et à la mettre à jour régulièrement pour assurer la sécurité du téléphone.

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

ORDINATEUR

1. Rechercher une solution antivirus + antimalware fiable et de confiance adaptée à l'ordinateur.
2. Télécharger le logiciel antivirus + antimalware à partir du site Web du fournisseur
3. Lancer le programme d'installation et suivre les instructions pour installer le logiciel sur l'ordinateur.
4. Mettre à jour le logiciel pour avoir la dernière version avec les dernières définitions de virus.
5. Configurer les paramètres du logiciel antivirus + antimalware selon les préférences de sécurité, tels que les fréquences de scan et les types de scan.
6. Exécuter une analyse complète de l'ordinateur pour détecter la présence de virus et de logiciels malveillants, Supprimer le virus si un virus est détecté.
7. Garder le logiciel antivirus + antimalware à jour en téléchargeant régulièrement les mises à jour proposées par le fournisseur.

Les fonctionnalités et les options peuvent varier selon le logiciel antivirus + antimalware choisi et

selon le système d'exploitation de votre ordinateur.

TÉLÉPHONE/TABLETTE

1. Chercher une solution antivirus + antimalware fiable et de confiance adaptée au téléphone, ne pas hésiter à voir des comparateurs.
   NB : Pour les appareils iOS, Apple fournit des fonctionnalités de sécurité intégrées pour protéger les utilisateurs contre les logiciels malveillants et les menaces en ligne ; Apple dispose de mesures de sécurité intégrées pour protéger les utilisateurs. Mais il existe des solution antivirus tierce disponible.
   Voici une liste non-exhaustive :

Android	iOS
– Avast Mobile Security & Antivirus – Bitdefender Mobile Security & Antivirus – Norton Mobile Security & Antivirus – Kaspersky Mobile Antivirus: AppLock & Web Security – McAfee Mobile Security & Lock	– Norton Mobile Security & Antivirus – McAfee Mobile Security – Trend Micro Mobile Security – Avast Mobile Security & Antivirus – Kaspersky Internet Security

2. Télécharger l'antivirus + antimalware à partir de PlayStore ou AppStore
3. Configurer les paramètres selon les préférences de sécurité, tels que les fréquences de scan et les types de scan.
4. Exécuter une analyse complète du téléphone pour détecter la présence de virus et de logiciels malveillants. Supprimer le virus si un virus est détecté.
5. Garder l'antivirus + antimalware à jour en téléchargeant régulièrement les mises à jour proposées