

Parcours : DISCOVERY

Module : Naviguer en toute sécurité

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



# - 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.

* + Article 1 = Faut-il dépénaliser les hackers blancs ? sur cairn.info aborde les failles de sécurité sur Internet qui permettent l'accès non autorisé à des données sensibles.
  + Article 2 = La sécurité d'un site Web - Apprendre le développement web sur developer.mozilla.org explique les menaces courantes pour la sécurité des applications web et comment réduire les risques de piratage.
  + Article 3 = Sécuriser un site web : risques, enjeux et bonnes pratiques sur vaadata.com couvre les bonnes pratiques pour sécuriser un site web, y compris la sécurité des serveurs, l'authentification, le contrôle d'accès et la sécurité des données, ainsi que les vulnérabilités et attaques courantes des applications web.

# - Créer des mots de passe forts

Objectif : *utiliser un gestionnaire de mot de passe LastPass*

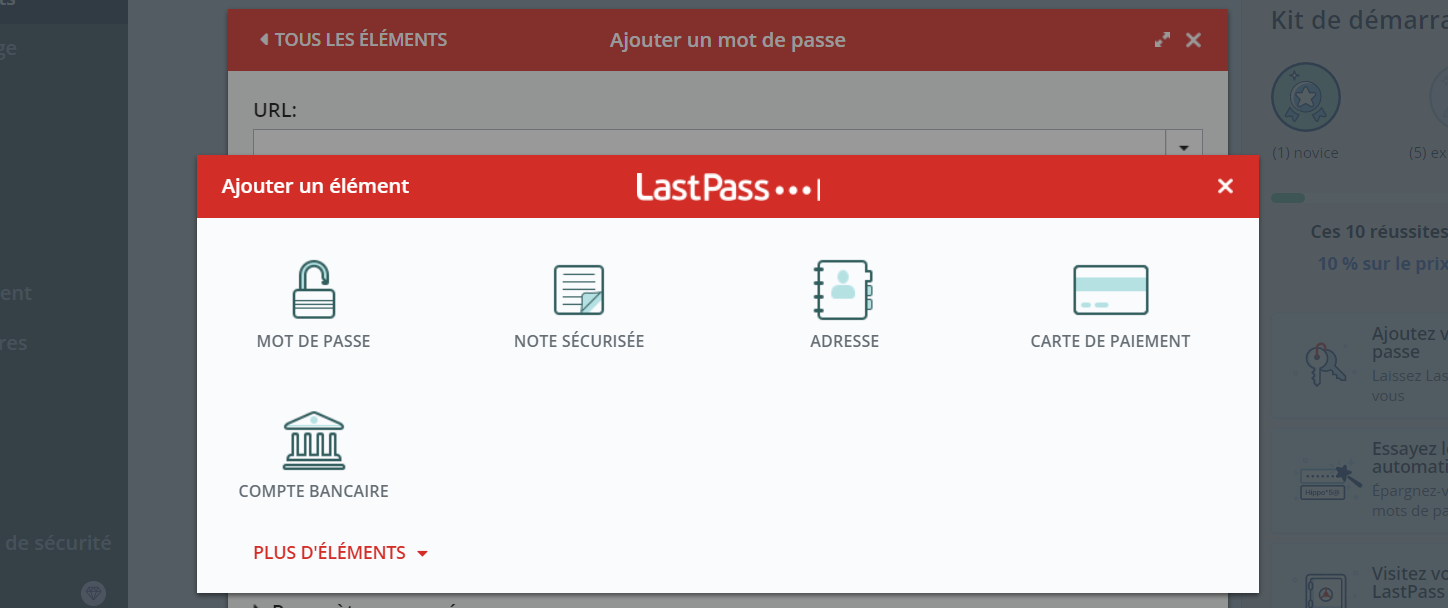
## 1/ Compte LastPass

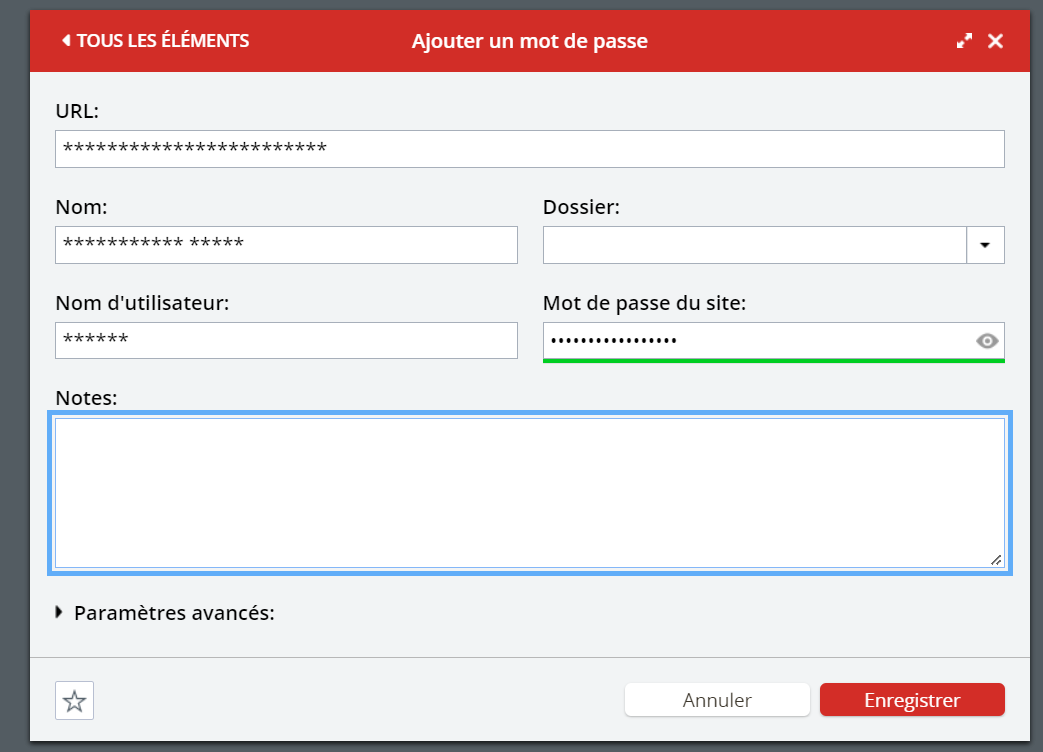
## 

## 

## 









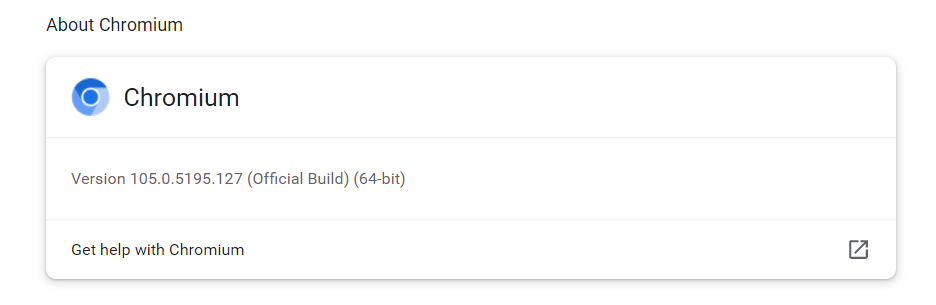
# - Fonctionnalité de sécurité de votre navigateur

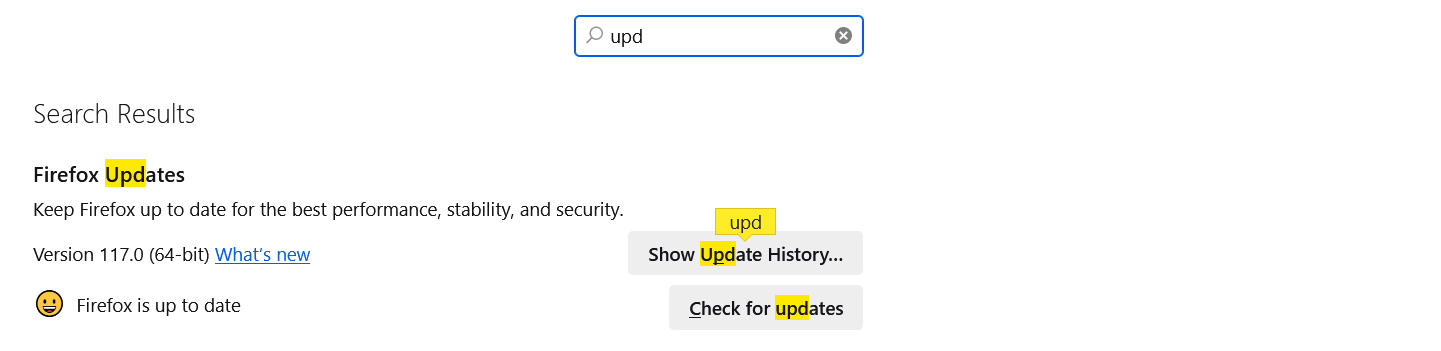
Objectif : *identifier les éléments à observer pour naviguer sur le web en toute sécurité*

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

* + [www.morvel.com](http://www.morvel.com/) [X]
  + [www.dccomics.com](http://www.dccomics.com/)
  + [www.ironman.com](http://www.ironman.com/)
  + [www.fessebook.com](http://www.fessebook.com/) [X]
  + [www.instagam.com](http://www.instagam.com/) [X]

## 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
  + 
  + Pour Firefox

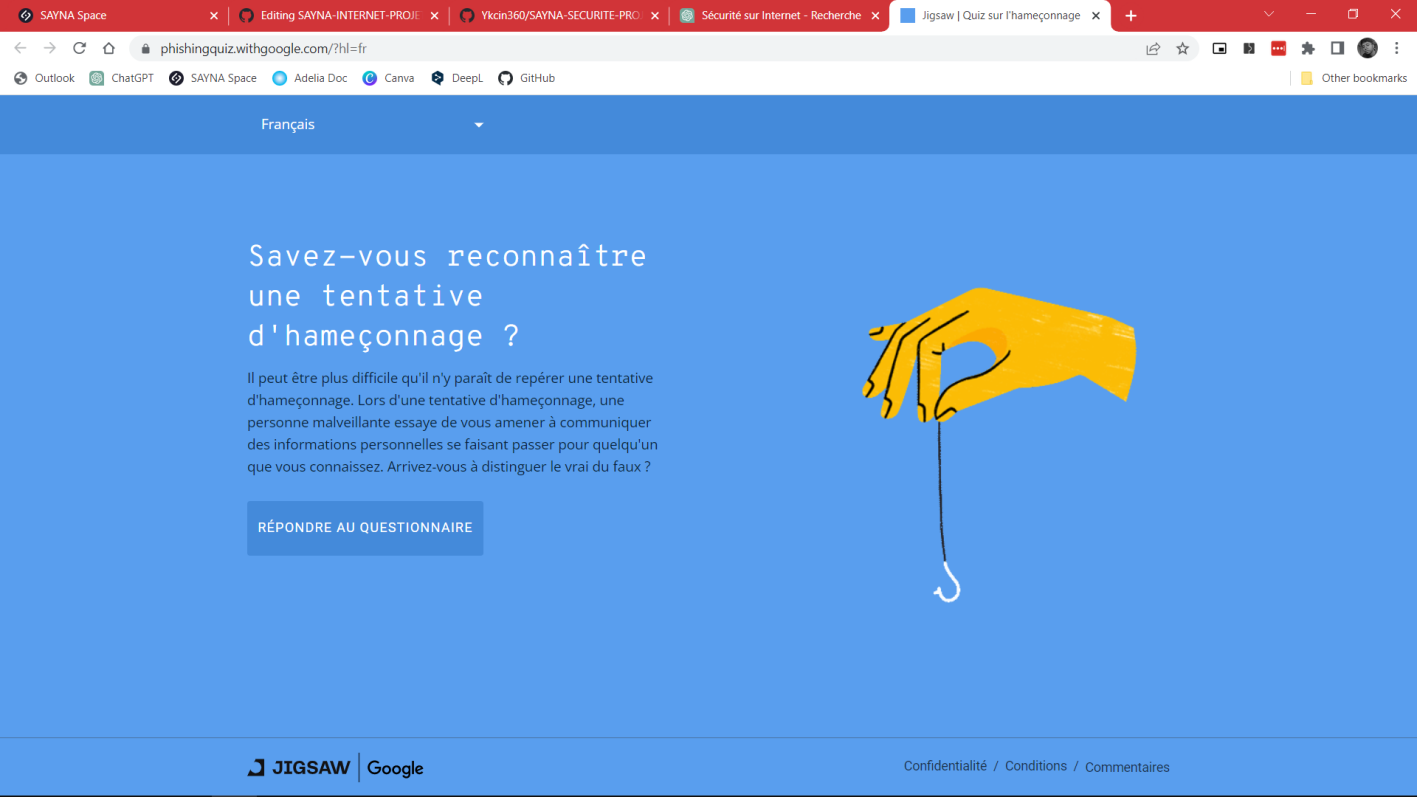




# - Éviter le spam et le phishing

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.





# - Comment éviter les logiciels malveillants

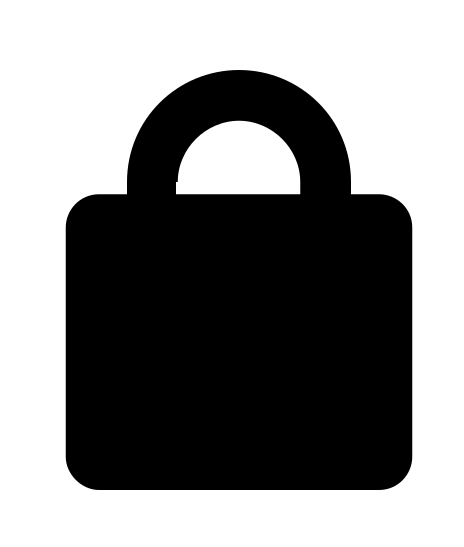
Objectif : *sécuriser votre ordinateur et identifier les liens suspects*

## 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.

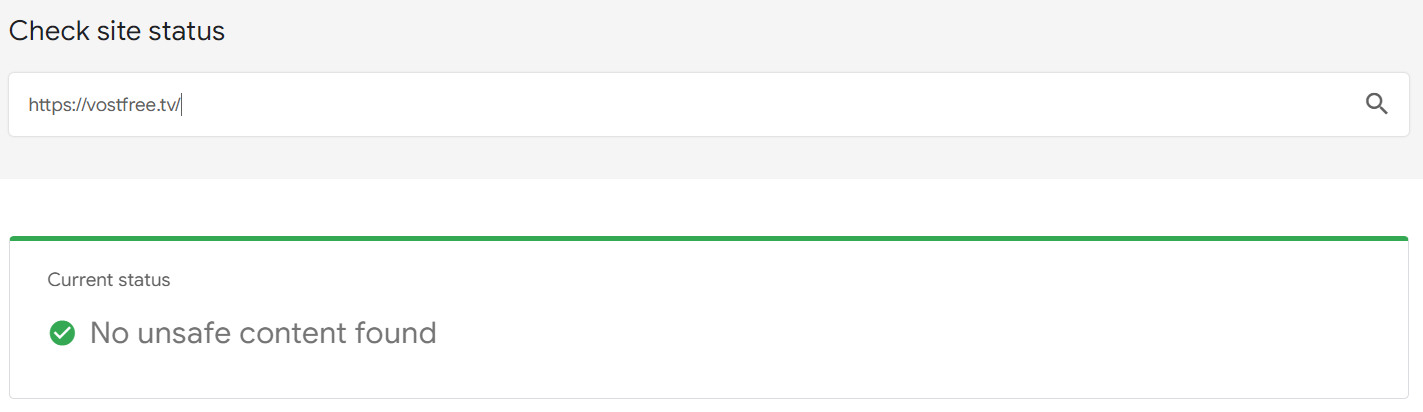
**Lorsque le doute persiste tu peux t’appuyer sur un outil proposé par Google : [Google](https://transparencyreport.google.com/safe-browsing/search?hl=en) [Transparency Report](https://transparencyreport.google.com/safe-browsing/search?hl=en) (en anglais) ou [Google Transparence des Informations](https://transparencyreport.google.com/safe-browsing/search?hl=fr) (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)**

* + [Site n°1](https://vostfree.tv/)

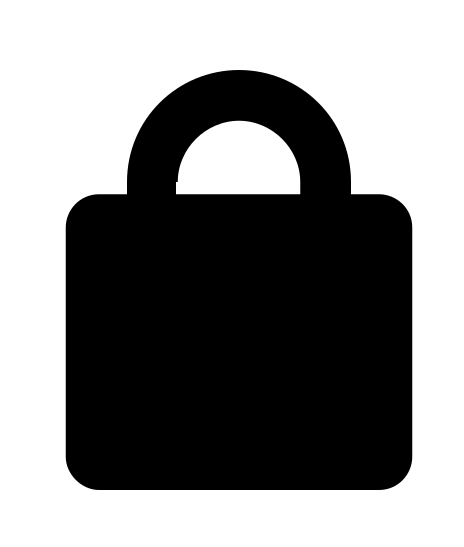
## Indicateur de sécurité

* + - HTTPS 

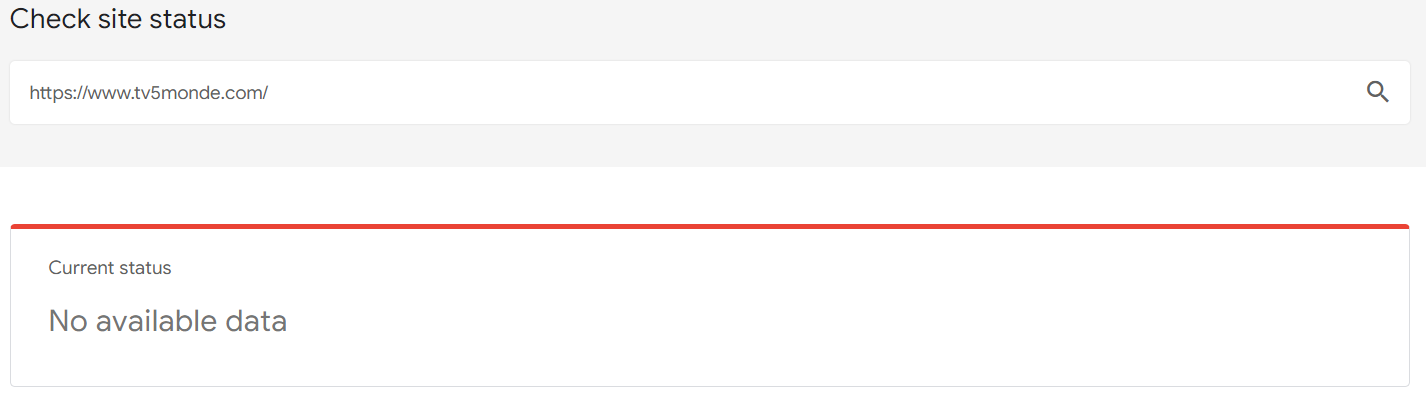
## Analyse Google

* + [Site n°2](http://www.tv5monde.com/)

## Indicateur de sécurité

* + HTTPS 

## Analyse Google

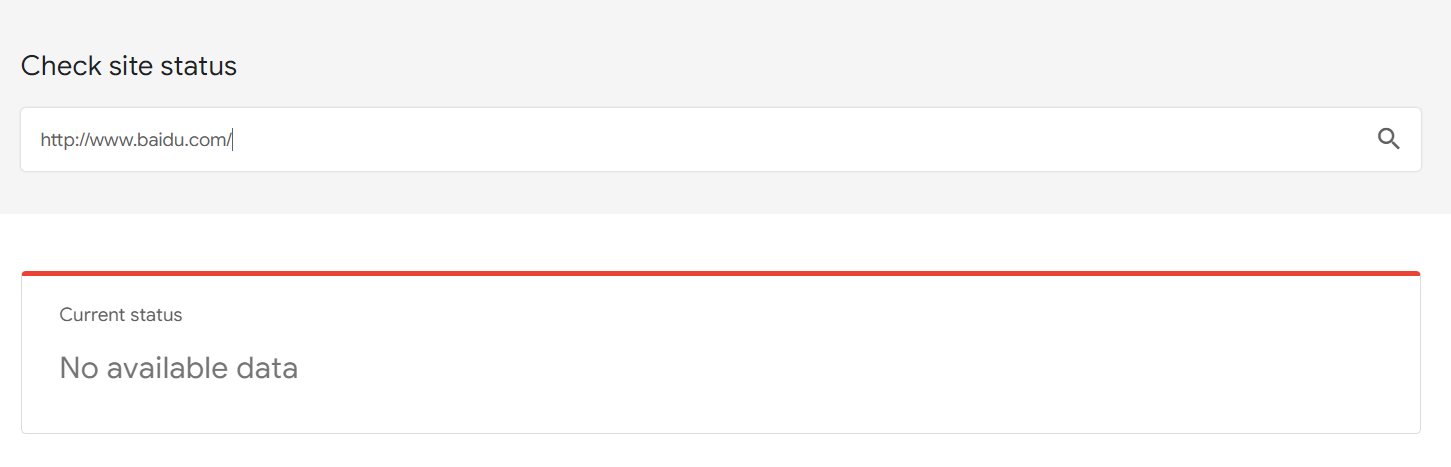


[Site n°3](http://www.baidu.com/)

## Indicateur de sécurité

* + - Not secure

## Analyse Google



# - Achats en ligne sécurisés

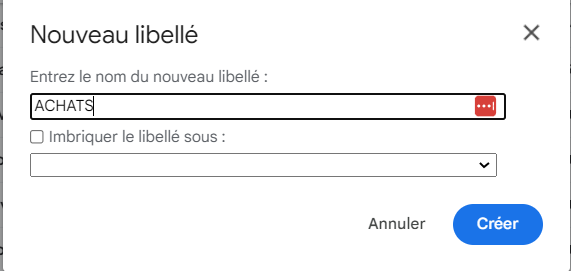
Objectif : *créer un registre des achats effectués sur internet*

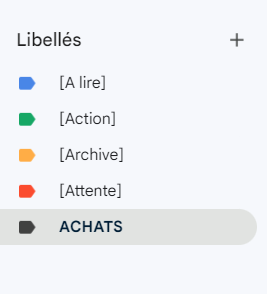
## 1/ Dans cet exercice, on va t’aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire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

**Deux possibilités s’offrent à toi pour organiser ce registre :**

## Créer un dossier sur ta messagerie électronique

1. **Créer un dossier sur ton espace de stockage personnel (en local ou sur le cloud)**





# - Comprendre le suivi du navigateur

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

# - 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)

* Connecte-toi à ton compte Facebook [X]
* Une fois sur la page d’accueil, ouvre le menu Facebook , puis effectue un clic sur “Paramètres et confidentialité”. Pour finir, clic sur “Paramètres” [X]
* Ce sont les onglets “Confidentialité” et “Publications publiques” qui nous intéressent. Accède à “Confidentialité” pour commencer et clic sur la première rubrique [X]
* Cette rubrique résume les grandes lignes de la confidentialité sur Facebook [X]
  + - La première rubrique (orange) te permettra de régler la visibilité de tes informations personnelles
    - La deuxième rubrique (bleu) te permet de changer ton mot de passe
    - La troisième rubrique (violet) te permet de gérer la visibilité de ton profil pour la gestion des invitations
    - La quatrième rubrique (vert) permet de gérer la connexion simplifiée sur des applications ou des sites utilisés qui permettent cela
    - La dernière rubrique (rose) permet de gérer les informations récoltées par Facebook utiles pour les annonceurs
* Retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à gauche. Tu peux continuer à explorer les rubriques pour personnaliser tes paramètres. On ne peut pas te dire ce que tu dois faire. [X]
* C’est à toi de choisir les informations que tu souhaites partager et celles que tu veux garder privées. Voici tout de même quelques conseils :
  + - Si tu utilises ton compte Facebook uniquement pour communiquer avec tes amis, règles les paramètres en conséquence en choisissant une visibilité “Amis” ou “Amis de leurs amis”.
    - Beaucoup de personnes utilisent Facebook en mêlant réseau professionnel et réseau personnel. Il n’y a pas vraiment de contre-indication, mais on te conseille tout de même de ne pas trop mélanger les deux. Il existe LinkedIn pour utiliser un média social pour le réseau professionnel
    - Pour limiter les haters et les commentaires malveillants, tu peux restreindre les commentaires de tes publications. Ça se passe dans l’onglet “Publications publiques” [X]
* 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. [X]

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

Objectif :

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

Si votre ordinateur est infecté par un virus, voici quelques étapes à suivre pour vérifier la sécurité de votre appareil, en fonction des conseils provenant des sources mentionnées :

Déconnectez l'appareil d'Internet pour empêcher la propagation du virus et protéger vos données.

Identifiez la source de l'infection en vérifiant les téléchargements récents, les e-mails suspects ou les sites web douteux. Vous pouvez suivre les conseils de cybermalveillance.gouv.fr.

Effectuez une analyse antivirus complète à l'aide d'un logiciel antivirus fiable. Désinstallez tous les logiciels que vous ne reconnaissez pas. Kaspersky recommande cette étape pour éliminer le virus.

Dans le cas d'un PC Windows, vous pouvez utiliser Microsoft Defender pour rechercher des programmes malveillants, des virus ou d'autres menaces, comme décrit dans les instructions de support.microsoft.com.



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

Pour installer et utiliser un antivirus et un antimalware en fonction de l'appareil utilisé, suivez cet exercice simple :

Exercice : Installer et Utiliser un Antivirus et Antimalware

Objectif : Assurer la sécurité de votre appareil contre les menaces en installant et utilisant un antivirus et un antimalware.

Étapes :

Identification de l'appareil : Déterminez l'appareil que vous utilisez (ordinateur Windows, Mac, smartphone Android, etc.).

Recherche de logiciels de sécurité : Consultez les liens des sources fournies, notamment fr.malwarebytes.com, pour comprendre la différence entre un antivirus et un antimalware. Choisissez un logiciel adapté à votre appareil.

Téléchargement : Rendez-vous sur le site web du logiciel de sécurité choisi (par exemple, Malwarebytes, Bitdefender, ou Windows Defender pour Windows). Téléchargez le logiciel en suivant les instructions spécifiques à votre appareil.

Installation : Installez le logiciel en suivant les étapes d'installation.

Mise à jour : Assurez-vous que le logiciel est à jour pour une protection optimale.

Analyse du système : Effectuez une analyse complète de votre appareil à l'aide du logiciel de sécurité pour détecter et supprimer les menaces éventuelles.

Planification des analyses : Configurez un calendrier d'analyses régulières pour maintenir votre appareil en sécurité.

Éducation en cybersécurité : Familiarisez-vous avec les bonnes pratiques de cybersécurité, telles que la prudence lors du téléchargement de fichiers et la mise à jour régulière de votre système d'exploitation.