SAYNA

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

- ✓ Article 1 :

https://www.kaspersky.fr/resource-center/definitions/what-is-internet-security - Sécurité Internet : Qu'est-ce que c'est et comment vous protéger en ligne ?

- ✓ Article 2 :

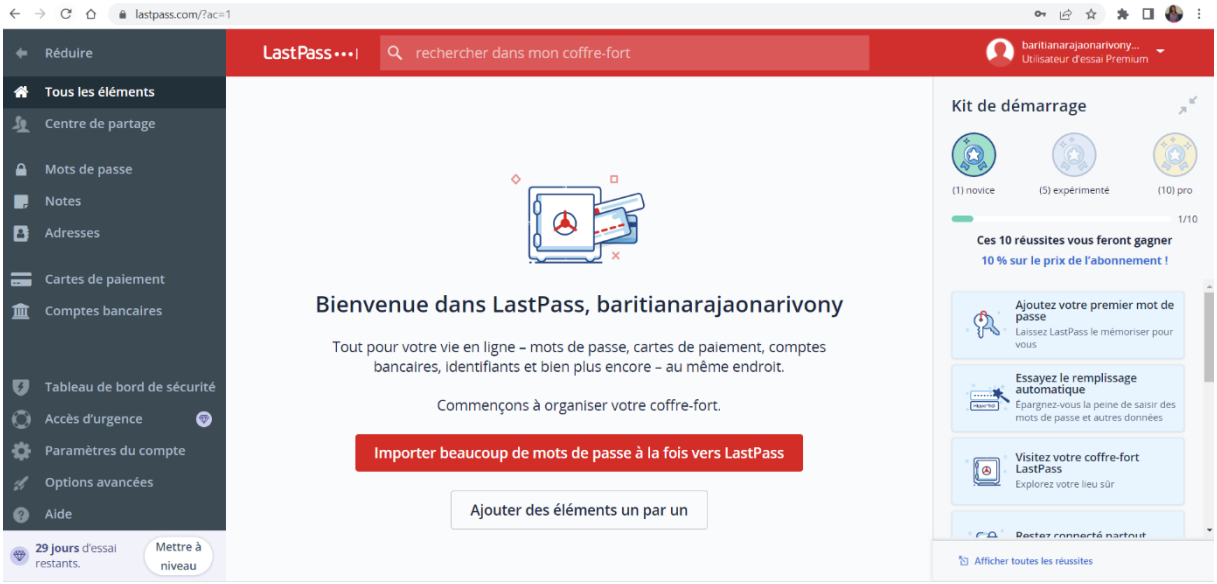
https://www.laposte.fr/professionnel/conseils-pour-etre-en-securite-sur-internet - 5 conseils pour être en sécurité sur Internet

- ✓ Article 3 :

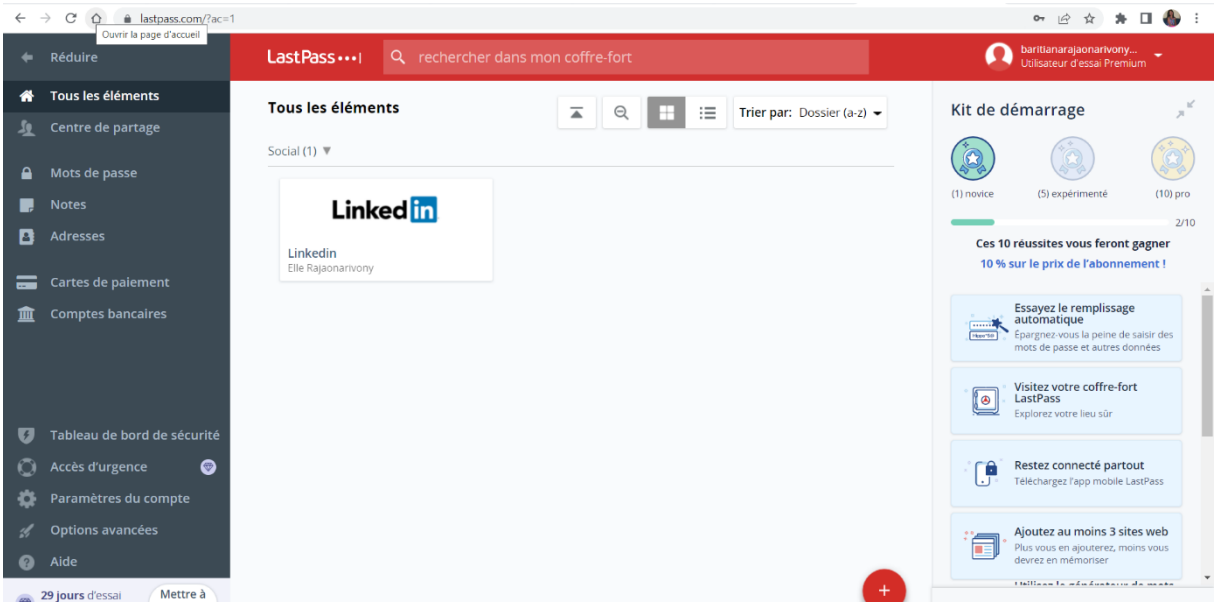
https://www.economie.gouv.fr/particuliers/comment-assurer-securite-numerique# - Comment assurer votre sécurité numérique ?

2-Créer des mots de passe forts

➢ Création d'un compte LastPass



➢ Ajout d'un site et d'une connexion associée

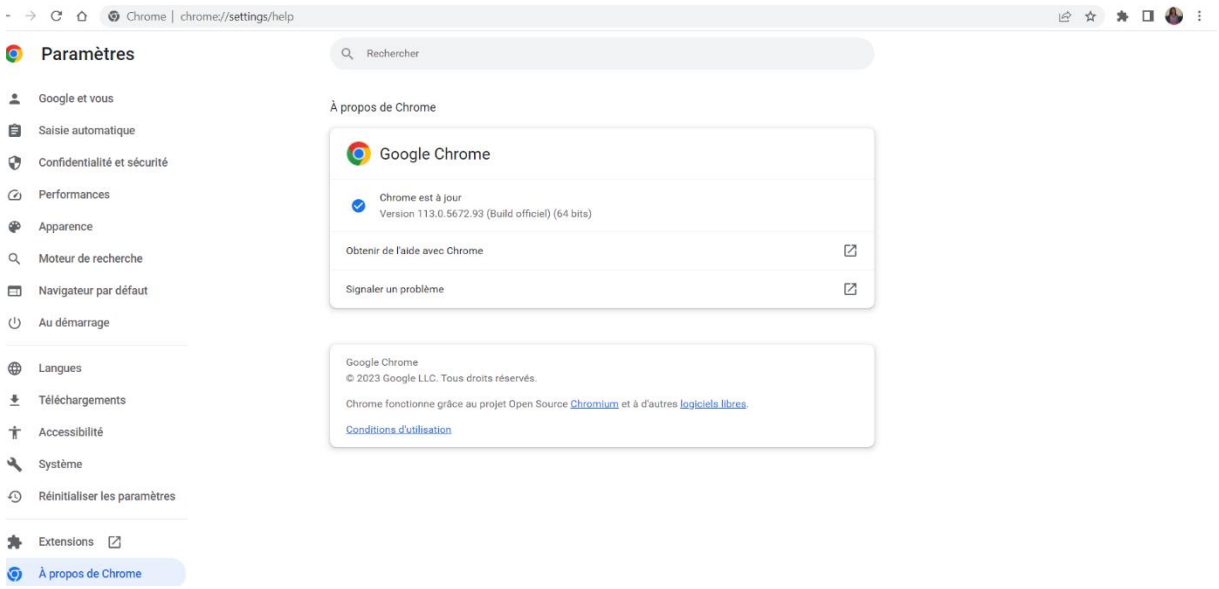


3-Fonctionnalité de sécurité de votre navigateur

1- Identification des adresses internet qui semblent malveillants

- www.morvel.com
- www.fessebook.com
- www.instagam.com

2- Vérification de la mise à jour de mon navigateur

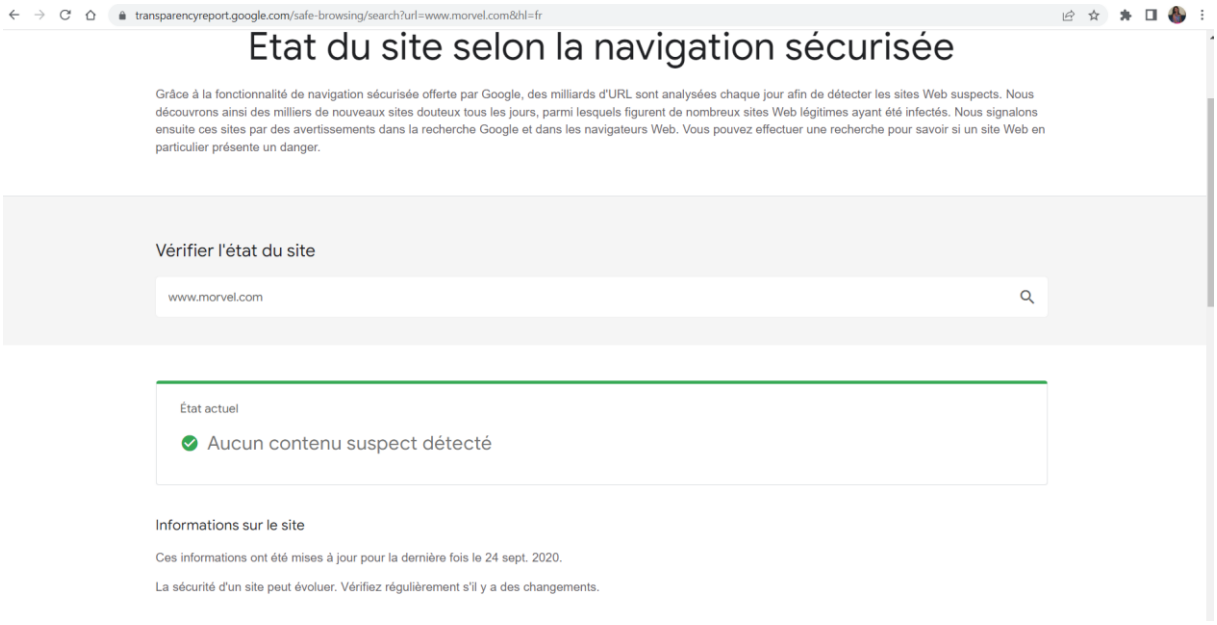


4-Eviter le spam et le phishing

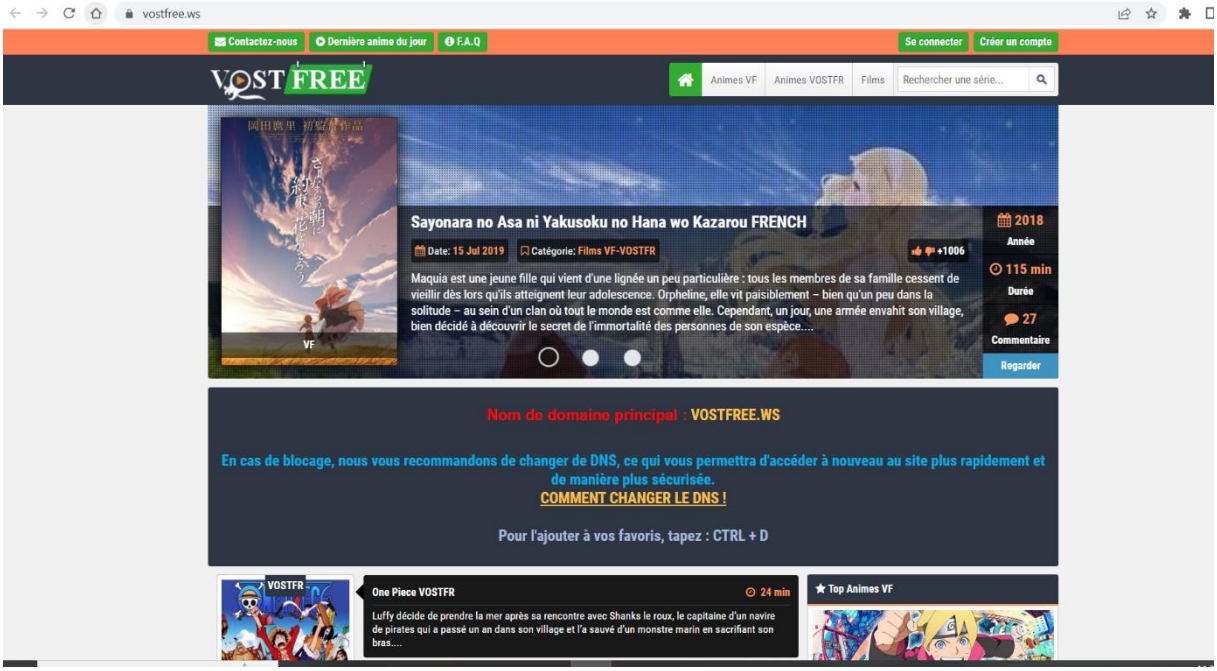
✓ Test fait

5-Comment éviter les logiciels malveillants

✓ Utilisation de l'outil google transparence en cas de doute



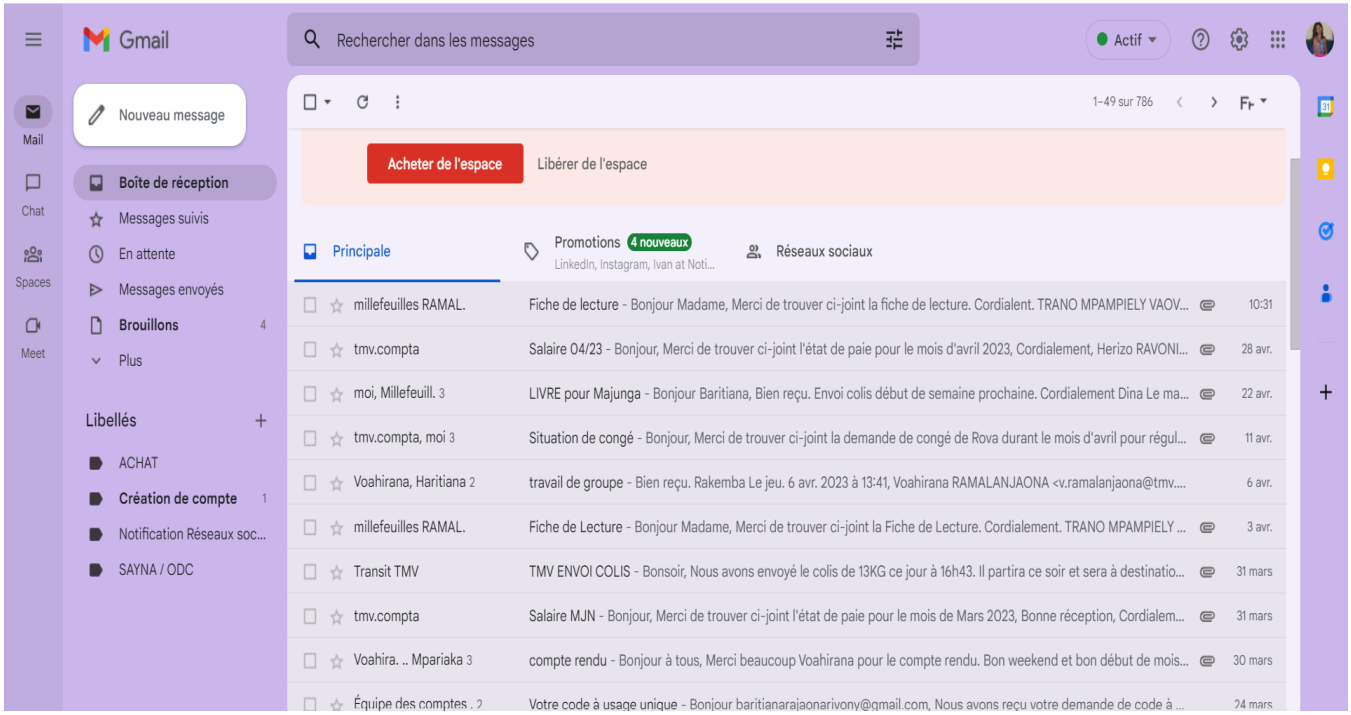
✓ Exemple de site sécurisé et non sécurisé



✓ Exemple de site non sécurisé

6-Achat en ligne sécurisés

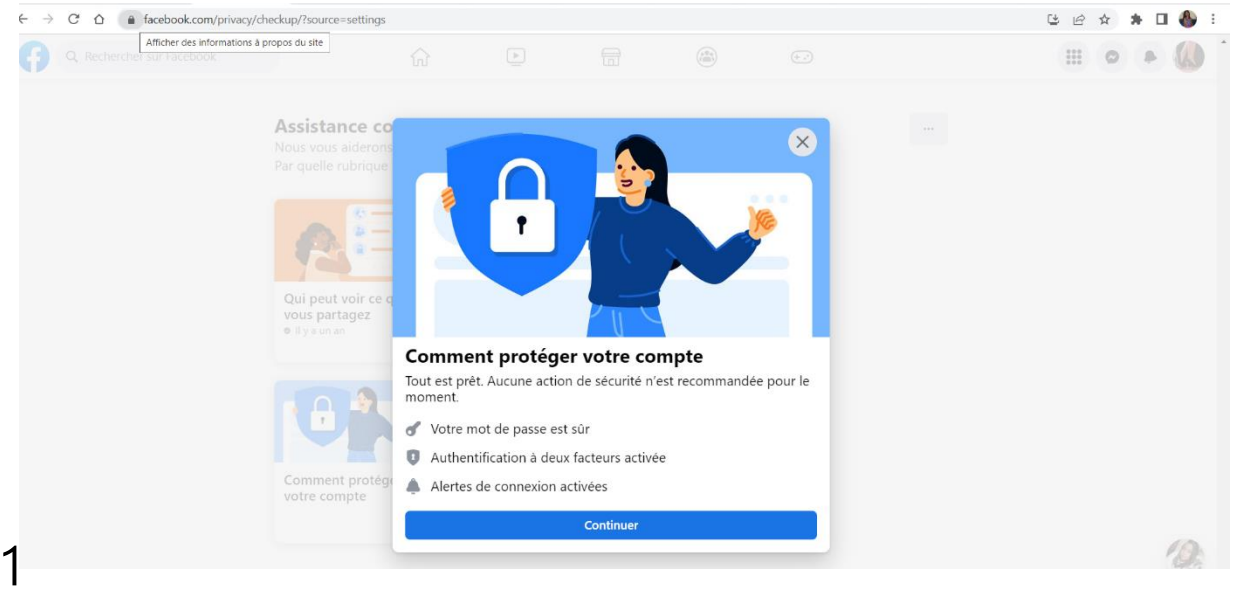
✓ Création du libellé ACHAT et organisation des autres libellés



7 - Comprendre le suivi du navigateur

8 - Principes de base de la confidentialité des médias sociaux

- ✓ Régler les paramètres de confidentialité de Facebook



1

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

Pour maintenir la sécurité des appareils, qu'il s'agit d'un ordinateur, d'un smartphone ou d'un objet connecté, il est recommandé d'avoir des bonnes pratiques. Ces dernières auront un impact significatif et positif sur votre sécurité en ligne et votre vie privée.

La première de toute est de bien vérifier avant de donner des infirmations sensibles sur votre vie privée à qui que ce soit. N'oubliez pas aussi de faire la sauvegarde régulière de vos données importantes. Puis après viennent les spécificités en fonction de l'appareil :

- Pour les ordinateurs :

1- Installez un logiciel antivirus et anti-malware de qualité pour protéger votre système contre les virus ou les logiciels malveillants en ligne
2- Mettre à jour périodiquement le système d'exploitation, ainsi que les logiciels installés afin de bénéficier des dernières mises à jour de sécurité
3- Utiliser des mots de passe forts et différents pour chaque compte.
4- Bien vérifier le site avant de faire des téléchargements
5- Ne pas cliquer sur des liens suspects ou des offres tentants

- Pour tablettes et smartphones :
  1- Mettre à jour régulièrement les applications installées pour bénéficier des améliorations proposées
  2- Activer le verrouillage automatique suivi d'un mot de passe, les empreintes digitales ou les reconnaissances faciales pour éviter que quelqu'un ait accès facilement à vos données personnelles
  3- Ne pas télécharger des applications à partir des sources non vérifiés ou inconnus
  4- Désactiver les connexions sans fil (Wi-Fi, données mobiles, Bluetooth) quand ce n'est pas nécessaire

- Pour les appareils connectés :
  1- Eviter de les connecter à un réseau Wi-Fi public
  2- Changer les mots de passe par défaut fournis par le producteur
  3- Ne pas oubliez de les mises à jour de sécurité
  4- Vérifier les autorisations d'accès de ces objets à vos données personnelles

2. Proposer un exercice pour installer et utiliser un antivirus + antimalware en fonction d'un appareil utilisé

- Pour les ordinateurs :
  1- Lancer une recherche d'antivirus et antimalware fiable sur un navigateur web
  2- Vérifier les sites fiables qui propose des téléchargement (gratuit ou payant)
  3- Normalement, un téléchargement ne demande pas des données personnelles
  4- Télécharger puis exécuter dans le programme
  5- Ne pas oublier de faire régulièrement des mises à jour pour obtenir les dernières mesures de sécurité

- Pour les tablettes et smartphones :
  1- Aller dans Playstore ou l'app Store de votre mobile
  2- Dans la barre de recherche trouver un antivirus et ou antimalware adapté à votre mobile
  3- Vérifier les sources des applications
  4- Regarder les avis concernant l'application
  5- Télécharger et mettre à jour régulièrement

- Pour les appareils connectés :
    1- A partir de votre smartphone, rechercher des antivirus et ou antimalwares adaptés à l'objet
    2- En cas d'hésitations ou de doutes, rechercher les plus populaires ou celles qui ont beaucoup d'étoiles
    3- Sélectionner puis télécharger le plus fiable
    4- Ne pas oublier de faire des mises à jour régulières

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

Objectif :