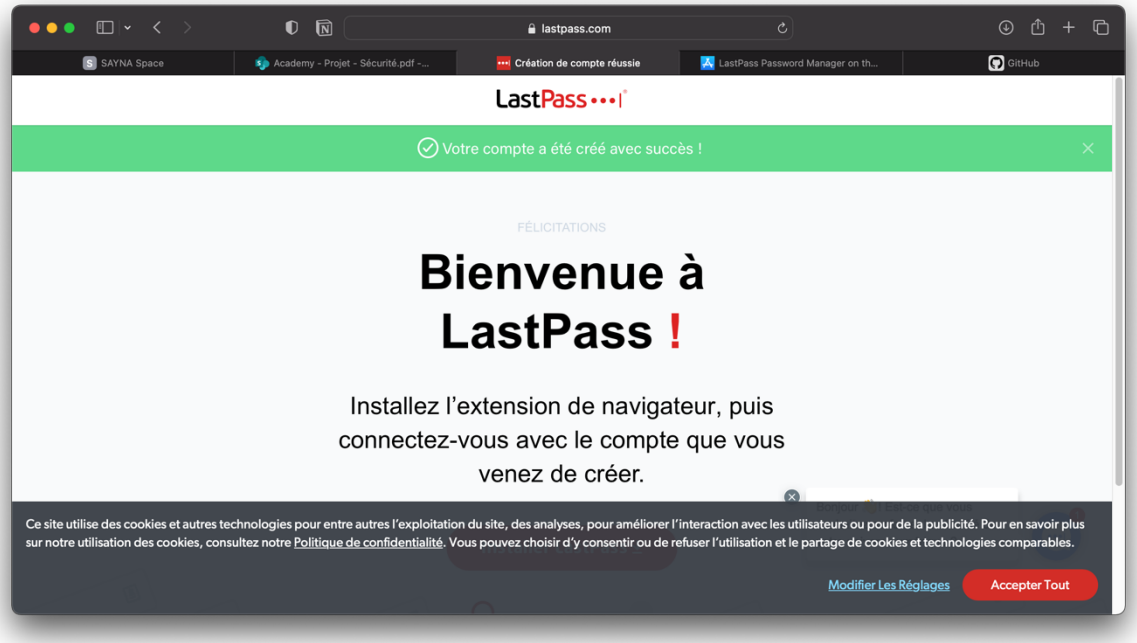
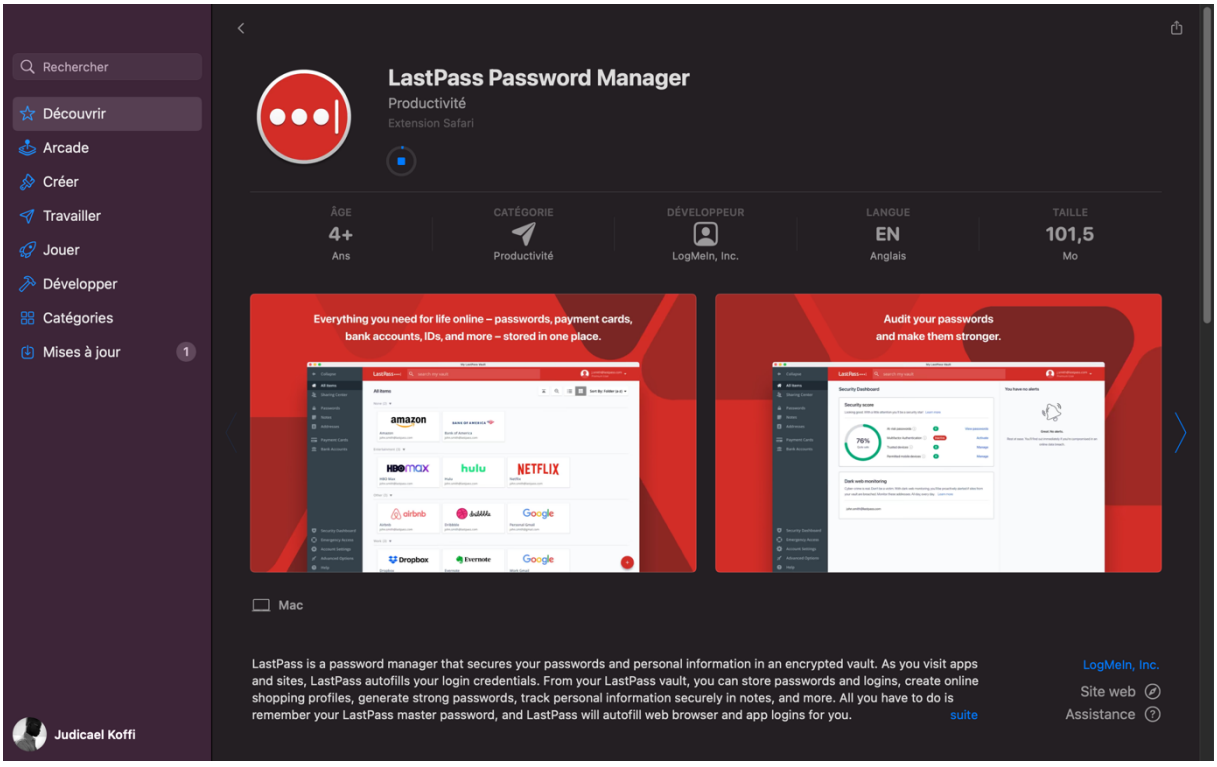
1 - Introduction à la sécurité sur Internet

Réponse 1
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 = ANSSI - Dix règles de base
● Article 2 = Economie.gouv - Comment assurer votre sécurité numérique
● Article 3 = Site W - Naviguez en toute sécurité sur Internet
● Article bonus = wikiHow - Comment surfez en sécurité sur internet
Beaucoup de notions traitées dans les articles sont également traitées dans le cours et des exercices y sont associés.

2 - Créer des mots de passe forts





3 - Fonctionnalité de sécurité de votre navigateur

1)

Réponse 1

Les sites web qui semblent être malveillants sont :
● www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel

● www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde
● www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très Utilisé
Les seuls sites qui semblaient être cohérents sont donc :
● www.dccomics.com, le site officiel de l'univers DC Comics
● www.ironman.com, le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

2)

4 - Éviter le spam et le phishing

Bon travail, Jude ! Vous avez obtenu un score de 5/8.

Plus vous vous entraînerez, 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.

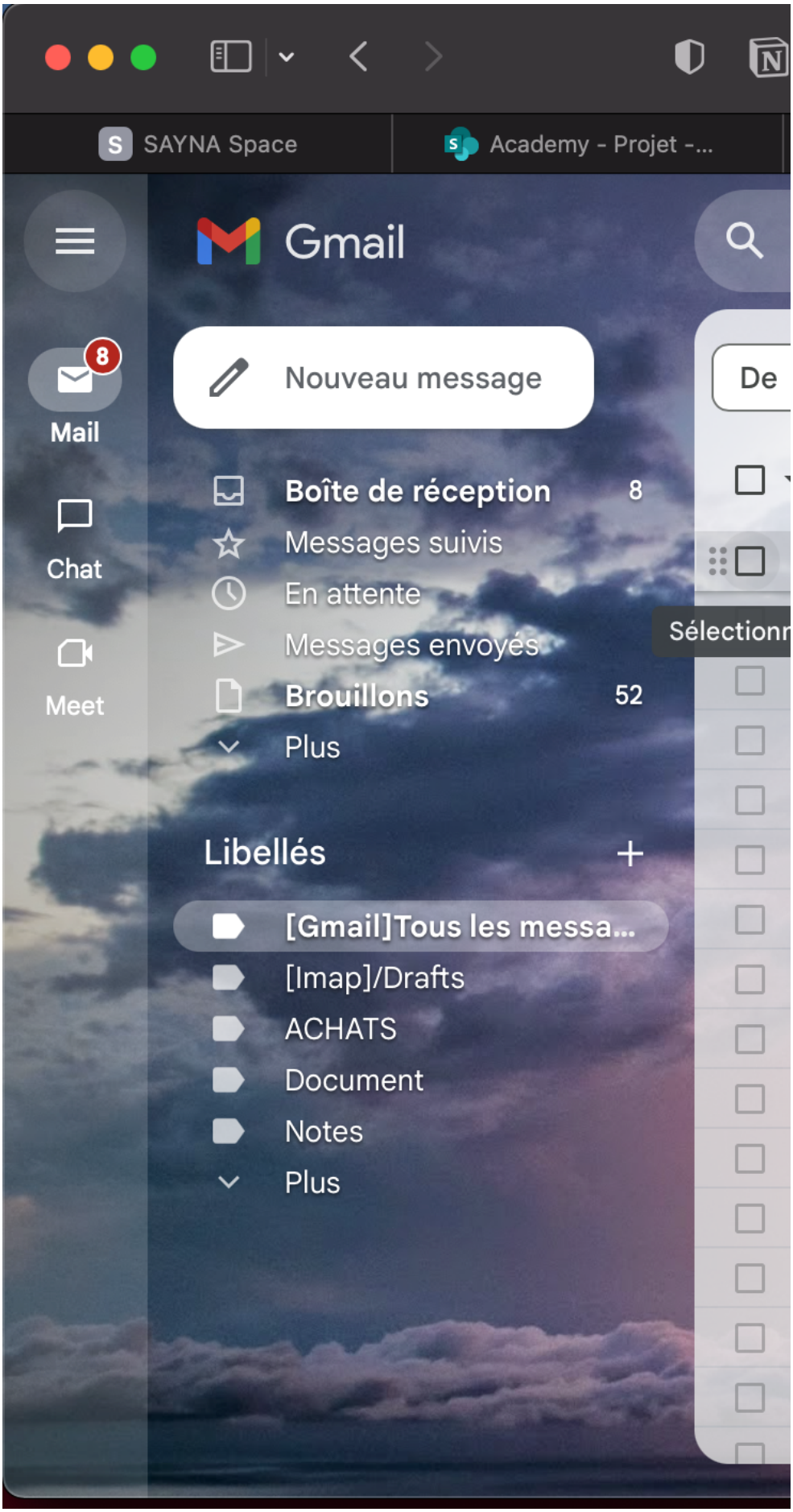
Partager le questionnaire :

5 - Comment éviter les logiciels malveillants

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 (analyse trop générale

6 - Achats en ligne sécurisés


SAYNA Space
Academy - Projet -...
Gmail
Nouveau message
Mail
Chat
Meet
Boîte de réception 8
Messages suivis
En attente
Messages envoyés
Brouillons 52
Plus
Libellés
[Gmail]Tous les messa...
[Imap]/Drafts
ACHATS
Document
Notes
Plus
De

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

1. Vérification de la sécurité de l'appareil :

- Analyse de l'appareil : Exécutez un scan complet de l'ordinateur pour rechercher tout logiciel malveillant ou virus. Pour ce faire, utilisez l'antivirus installé sur l'appareil ou téléchargez un logiciel antimalware fiable.
- Vérification des mises à jour : Assurez-vous que le système d'exploitation et les logiciels installés sont à jour. Les mises à jour contiennent souvent des correctifs de sécurité importants.
- Examen des connexions réseau : Surveillez les connexions réseau de votre appareil pour détecter toute activité inhabituelle ou non autorisée.
- Contrôle des programmes installés : Passez en revue les programmes installés sur votre appareil et supprimez ceux qui sont inutiles ou suspects.
- Audit des paramètres de sécurité : Vérifiez les paramètres de sécurité du système d'exploitation et des applications utilisées (firewall, paramétrage de confidentialité, etc.).

2. Installer et utiliser un antivirus et un antimalware :

- Choix du logiciel : Choisissez un logiciel antivirus et antimalware fiable, adapté à votre appareil (ordinateur, smartphone, tablette). Consultez les avis d'utilisateurs et les comparatifs en ligne pour vous aider à faire votre choix.
- Installation : Téléchargez le logiciel à partir d'un site de confiance et suivez les instructions d'installation.
- Mise à jour automatique : Assurez-vous que le logiciel est configuré pour se mettre à jour automatiquement afin de bénéficier de la dernière protection contre les menaces.
- Paramétrage : Configurez les paramètres de sécurité selon vos besoins, notamment les analyses automatiques, la quarantaine des fichiers suspects et les alertes de sécurité.
- Exécution d'analyses régulières : Programmez des analyses automatiques régulières de votre appareil pour détecter et éliminer les menaces.
- Formation et sensibilisation : Familiarisez-vous avec les bonnes pratiques de sécurité pour éviter les sites web dangereux, les liens suspects et les pièces jointes malveillantes.