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

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.

Article 1 = nom du site - nom de l'article

Article 2 = nom du site - nom de l'article

• Article 3 = nom du site - nom de l'article

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 = CYBER MALVEILLANCE.GOUV.FR – Comment se protéger sur Internet.

• Article 2 = Kaspersky – Confidentialité sur Internet : 5 conseils de sécurité.

• Article 3 = economie.gouv.fr – Comment assurer votre 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

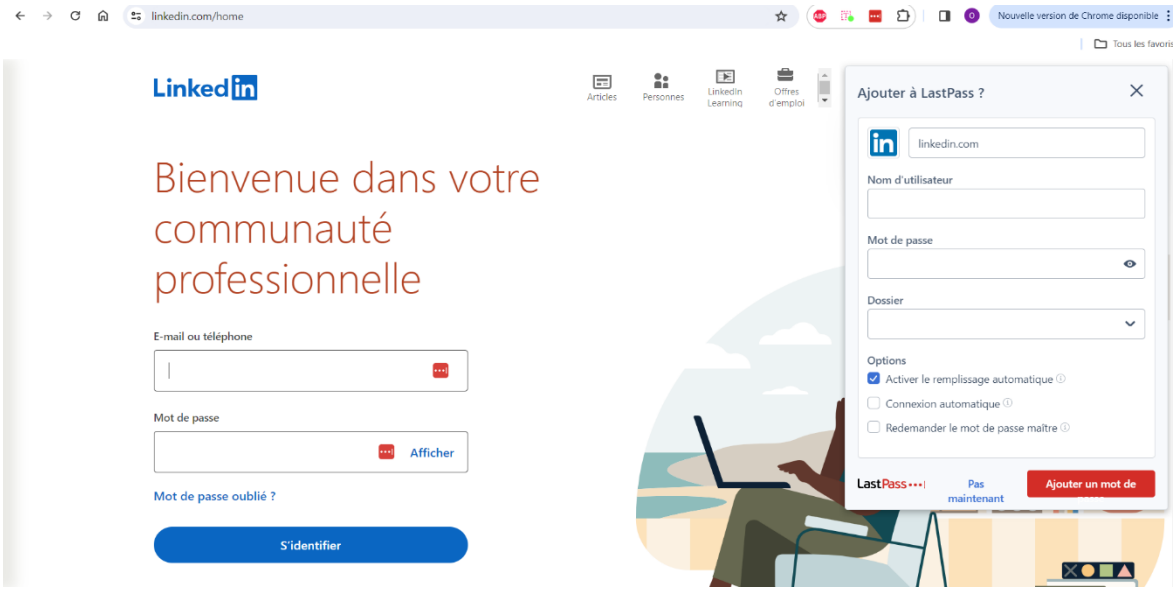
Prendre en main et propose un niveau de sécurité optimal. Suis les étapes suivantes.

(Case à cocher)

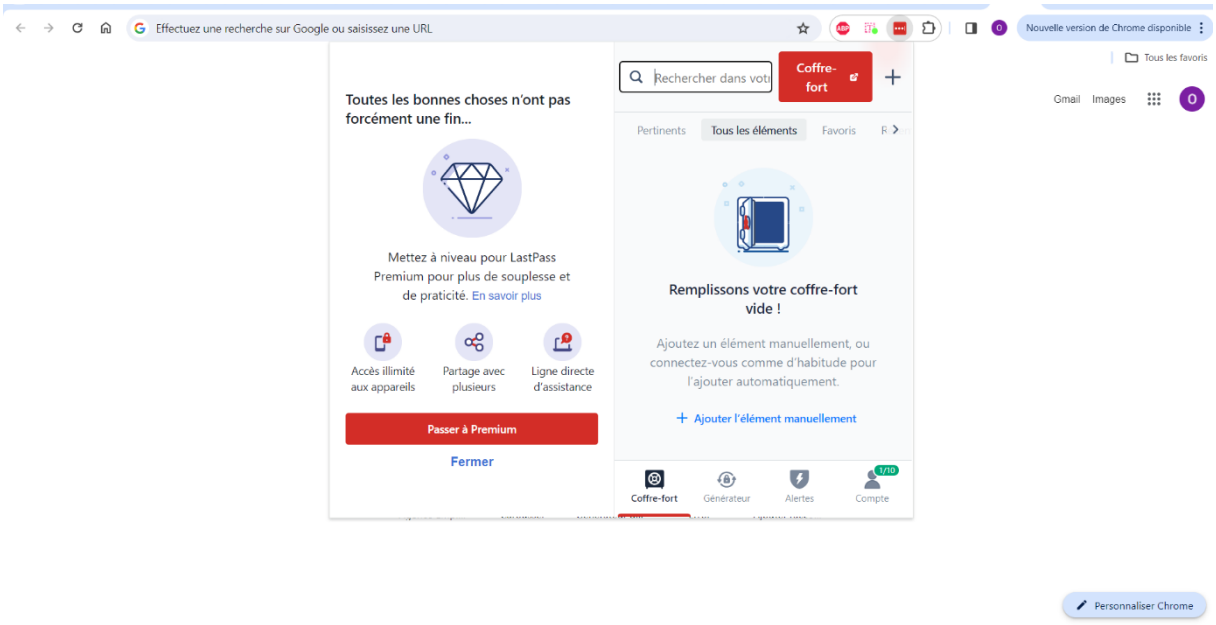
Réponse 1

Désormais, lorsque tu te connectes à tes comptes, tu peux enregistrer le mot de passe

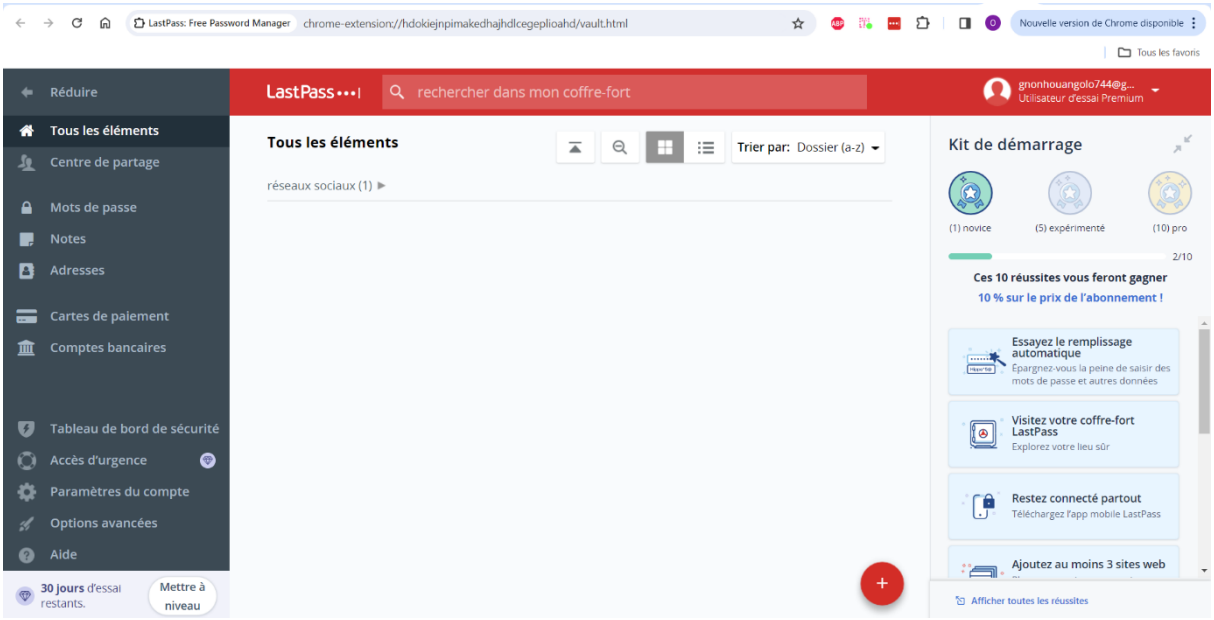
Grâce à LastPass.



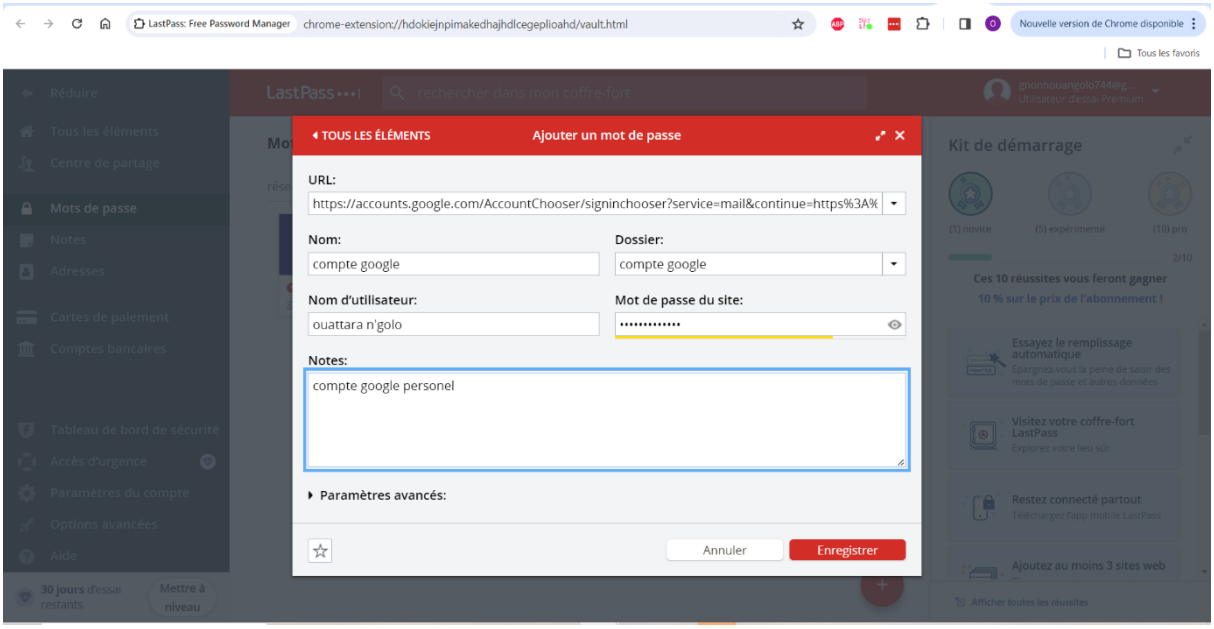
Tu peux également ajouter des comptes manuellement en accédant au coffre-fort, espace De stockage de tous tes mots de passe. Pour y accéder, clic sur l'icône de l'extension puis Sur "Ouvrir mon coffre-fort".



Tu arrives alors sur une page de gestion de ton compte LastPass. Pour ajouter un site et Une connexion associée (identifiant + mot de passe), accède à la rubrique "Mot de passe" (2) et (3) puis clic sur "Ajouter un élément" (1).



Une fenêtre s'ouvre pour y insérer toutes les informations à retenir pour automatiser la Prochaine connexion. LastPass demande l'URL du site en question ; on conseille de mettre l'URL de la page de connexion du site. Ensuite préciser l'I et le mot de passe. On peut Personnaliser le nom, un commentaire associé ou encore un dossier si besoin.



Tu connais maintenant les grandes lignes de l'utilisation du gestionnaire de mot de passe LastPass.

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)

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

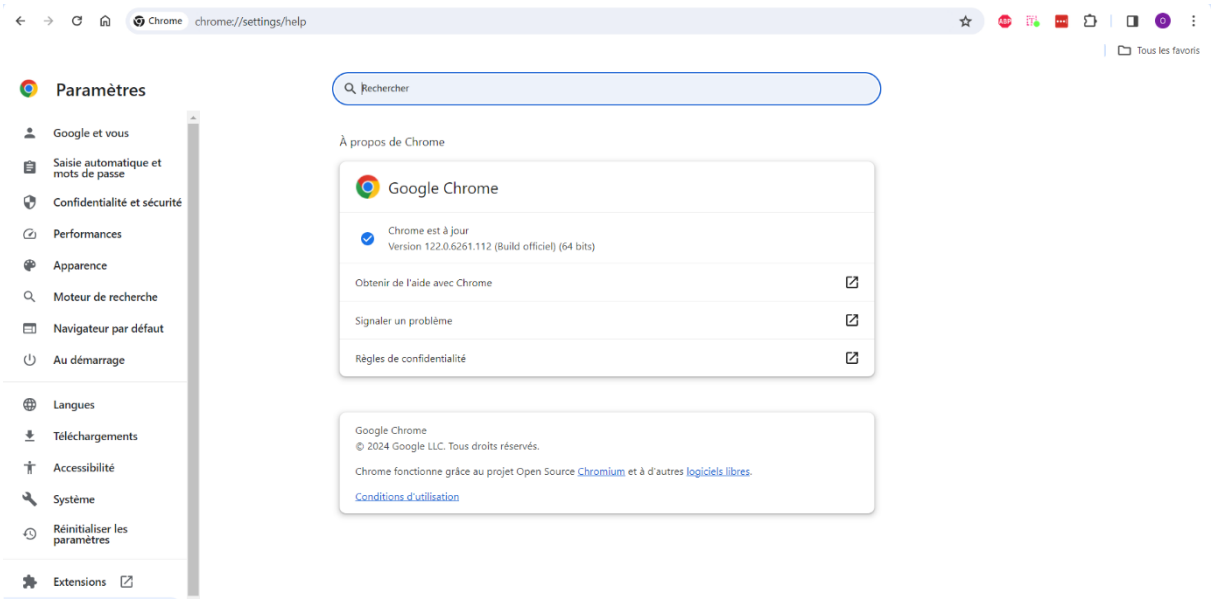
• www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très utilisé

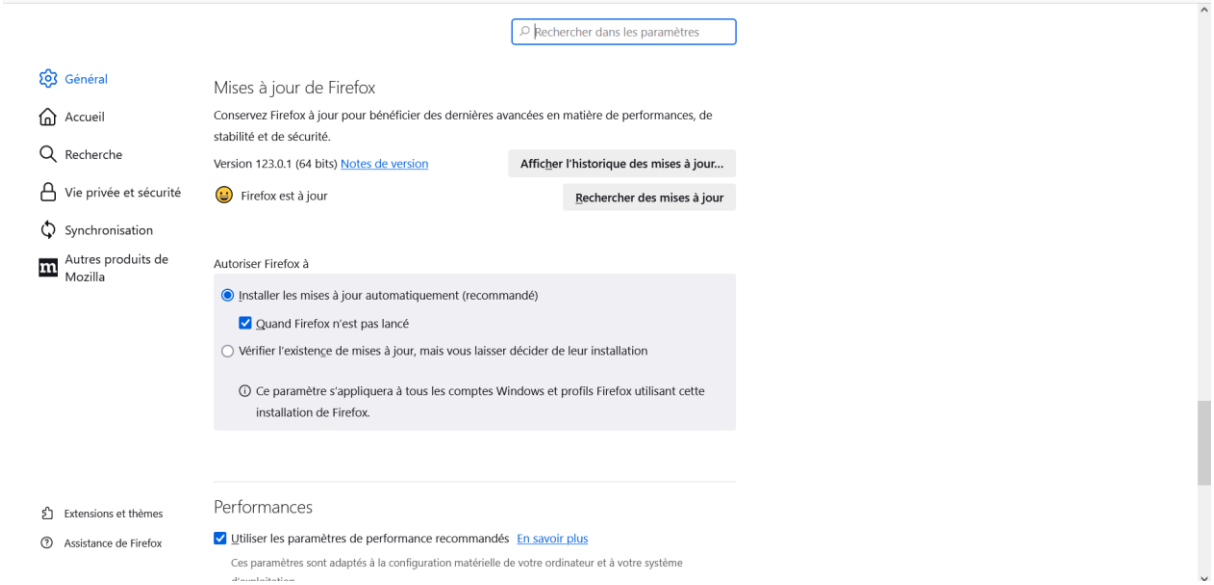
2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox

Dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes. (Case à cocher)

Réponse 2

Comme tu as pu le constater, les paramètres par défaut de ces deux navigateurs sont réglés pour réaliser les mises à jour automatiquement. Comme d'habitude, Firefox affiche une personnalisation des paramètres un peu plus poussée.





4 - Éviter le spam et le phishing

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

Réponse 1

Tu veux réessayer pour continuer à t'exercer, c'est possible ! Tu peux également consulter des ressources annexes pour t’exercer. ·

5 - Comment éviter les logiciels malveillants

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 Transparence 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 (analyse trop générale)

6- Achats en ligne sécurisés

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 (en local ou sur le cloud)

Réponse 1

Voici un exemple d'organisation de libellé pour gérer sa messagerie électronique :

- Achats historique, facture, conversations liées aux achats
- Administratif : toutes les démarches administratives
- Banque tous les documents et les conversations liés à la banque personnelle
- Création de compte tous les messages liés à la création d'un compte (message de bienvenue, résumé du profil, etc.)
- Job : tous les messages liés à mon projet professionnel
- SAYNA tous les messages liés mon activité avec SAYNA

7 - Comprendre le suivi du navigateur

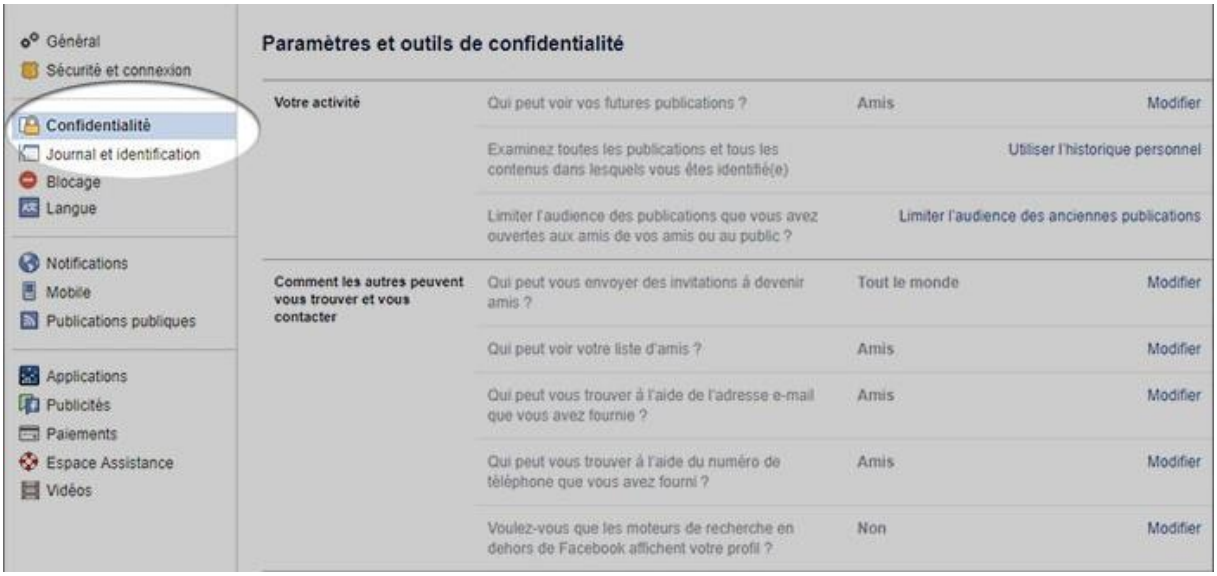
8 - Principes de base de la confidentialité des médias sociaux

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)

Réponses 1

Exemple de compte de paramétrage compte Facebook pour une utilisation privilégié.

Confidentialité



Publication Publique

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

1/ Propose moi un exercice pour vérifier la sécurité en fonction de l'appareil ???? comment faire ????

Exercice pour vérifier la sécurité en fonction de l'appareil

1. Identifiez vos appareils :

- Commencez par dresser une liste de tous les appareils que vous utilisez, y compris les ordinateurs portables, les tablettes, les smartphones, les routeurs, les imprimantes et les objets connectés.

2. Évaluez les risques :

- Pour chaque appareil, réfléchissez aux informations sensibles qu'il contient, telles que des mots de passe, des données bancaires ou des informations personnelles.
- Identifiez les risques potentiels pour chaque appareil, tels que les logiciels malveillants, les attaques de phishing ou les vols.

3. Appliquez les mesures de sécurité appropriées :

- Mettez à jour le système d'exploitation et les logiciels de chaque appareil.
- Installez un antivirus et un pare-feu sur chaque appareil.
- Activez l'authentification à deux facteurs pour vos comptes en ligne.
- Utilisez des mots de passe forts et uniques pour chaque compte.
- Sauvegardez régulièrement vos données importantes.

4. Restez informé des dernières menaces :

- Abonnez-vous à des sources d'information fiables sur la sécurité informatique.
- Soyez prudent lorsque vous cliquez sur des liens ou ouvrez des pièces jointes provenant de sources inconnues.
- Ne donnez jamais vos informations personnelles à des personnes que vous ne connaissez pas.