

Parcours : DISCOVERY

Module : Naviguer en toute
sécurité

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

*Tous vos travaux devront être déposés sur votre
compte Github*

Sommaire

1 - Introduction à la sécurité sur Internet

2 - Créer des mots de passe forts

3 - Fonctionnalité de sécurité de votre navigateur

4 - Éviter le spam et le phishing

5 - Comment éviter les logiciels malveillants

6 - Achats en ligne sécurisés

7 - Comprendre le suivi du navigateur

8 - Principes de base de la confidentialité des médias sociaux

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

1 - Introduction à la sécurité sur Internet

Objectif : *à la découverte de la sécurité sur internet*

1/ En naviguant sur le web, consultez trois articles qui parlent de sécurité sur internet.

Pensez à vérifier la source des informations et essayez de consulter des articles

récents pour que les informations soient à jour. Saisissez le nom du site et de l'article. •

Article 1 : Kaspersky-Sécurité internet : qu'est-ce que c'est et comment vous protéger en ligne ?

Article 2 : Mes questions d'argent-Comment utiliser internet en toute sécurité.

Article 3 : MDN Web Docs-La sécurité d'un site Web

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 surfer en sécurité sur internet

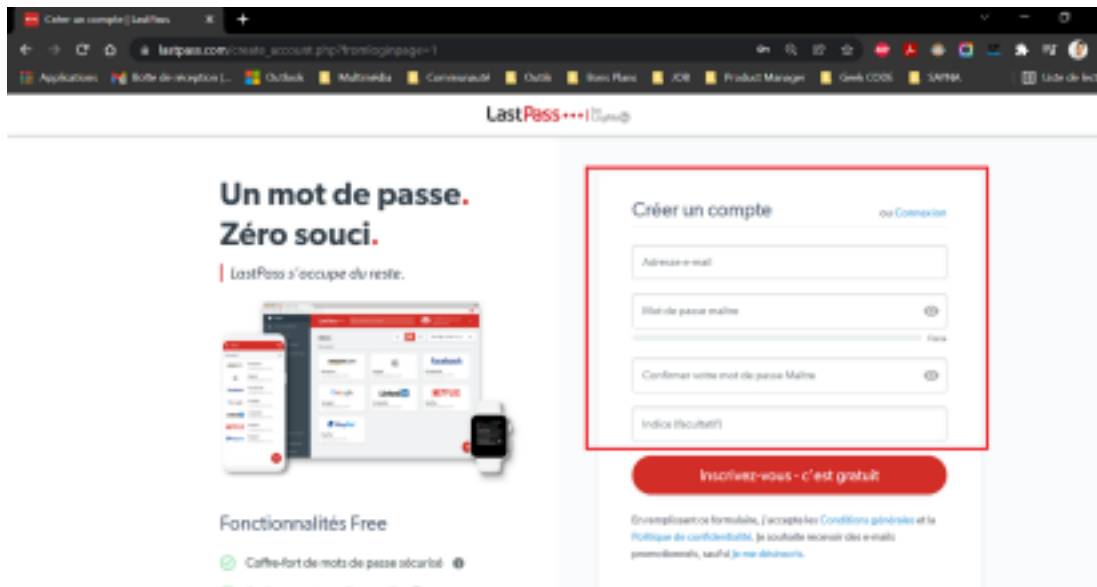
Beaucoup de notions traitées dans les articles sont également traitées dans le cours et des exercices y sont associés.

2 - Créer des mots de passe forts

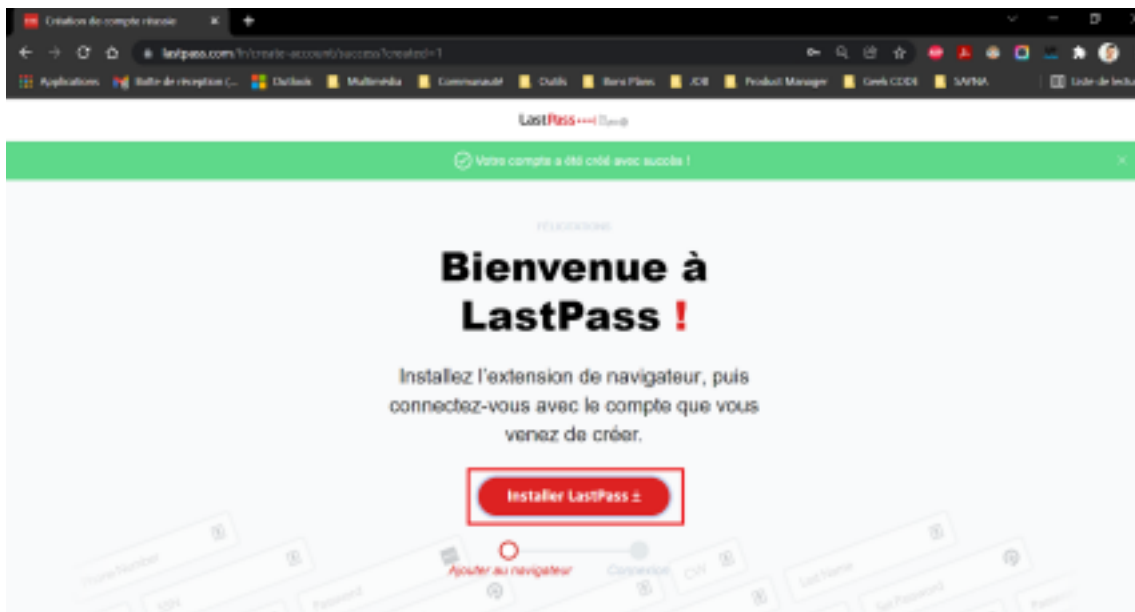
Objectif : *utiliser un gestionnaire de mot de passe LastPass*

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)

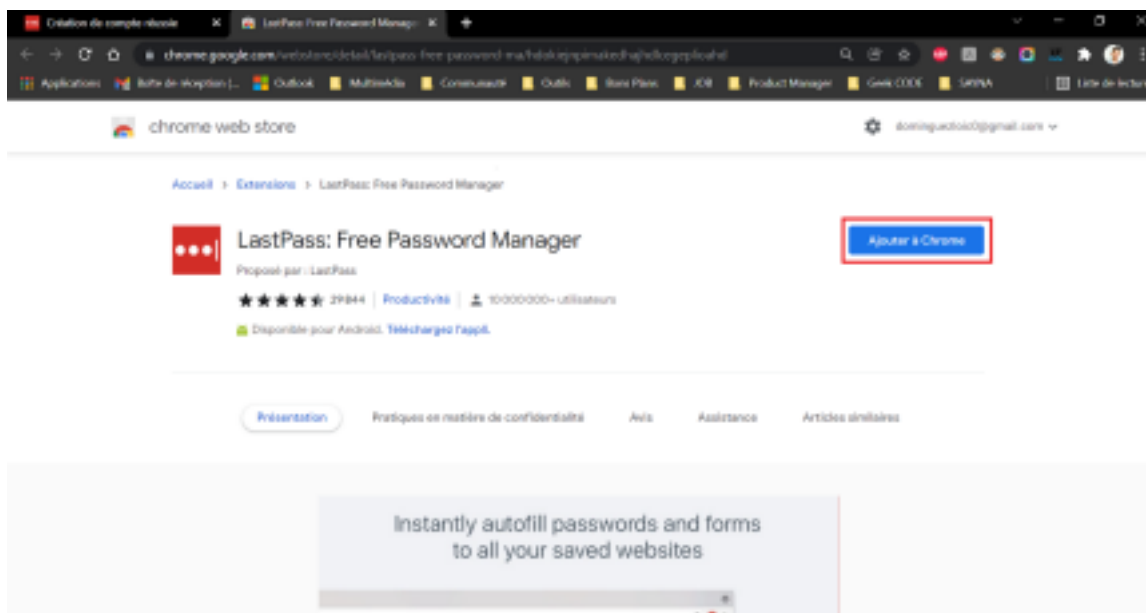
- Accède au site de LastPass avec [ce lien](#)

The image is a screenshot of a web browser displaying the LastPass website. The browser's address bar shows the URL 'lastpass.com/crea...'. The website has a light blue header with the 'LastPass' logo. The main content area is split into two columns. The left column features the text 'Un mot de passe. Zéro souci.' and 'LastPass s'occupe du reste.' above an illustration of a smartphone and a laptop. The right column contains a 'Créer un compte' form, which is highlighted with a red rectangular border. The form includes fields for 'Adresse e-mail', 'Mot de passe maître' (with a strength indicator), 'Confirmer votre mot de passe Maître', and 'Indice (facultatif)'. Below the form is a red button that says 'Inscrivez-vous - c'est gratuit'. At the bottom of the form, there is a small disclaimer about terms and conditions.

- Crée un compte en remplissant le formulaire. Un conseil, on te demande de choisir un mot de passe maître. Pour rappel, ce mot de passe sera unique et te permettra d'accéder à tous tes comptes. Choisis donc un mot de passe avec un niveau de sécurité élevé et assure-toi de pouvoir le retrouver
 - Exemple de mot de passe maître : c3c!3s!l3M0!2P@SS3 (Ceci est le mot de passe, en remplaçant le "e" par "3" le "i", "t" par "!", "a" par "@" et les premières lettres en minuscules puis majuscules à partir de "mot")
 - Tu peux également générer un mot de passe maître, mais pense à l'écrire dans un endroit sûr pour pouvoir l'utiliser lorsque tu en as besoin
- 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



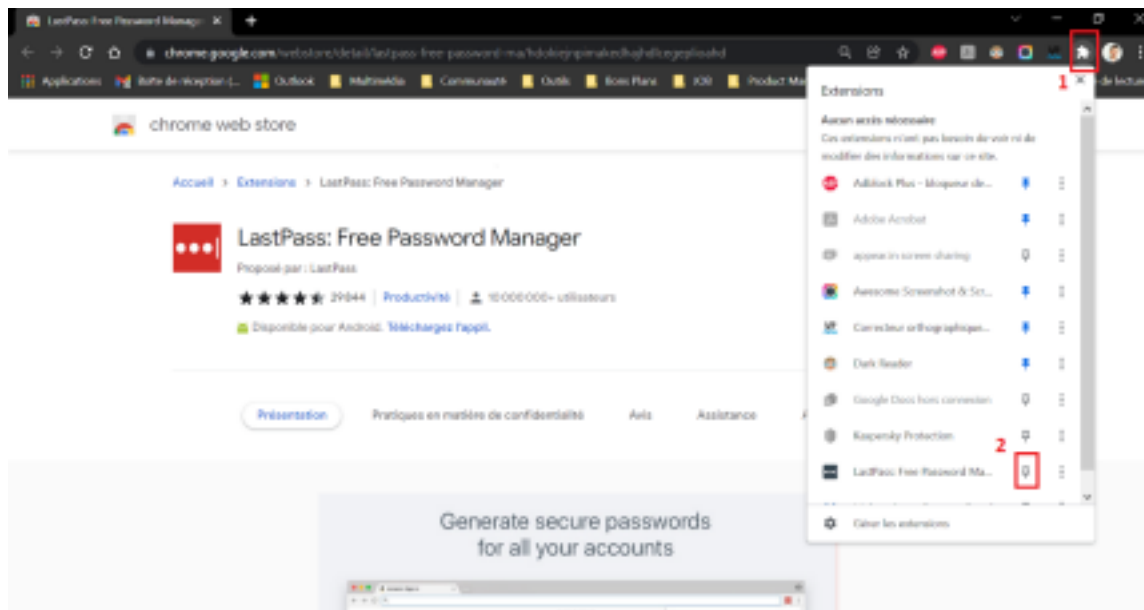
Il te suffit de valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome"



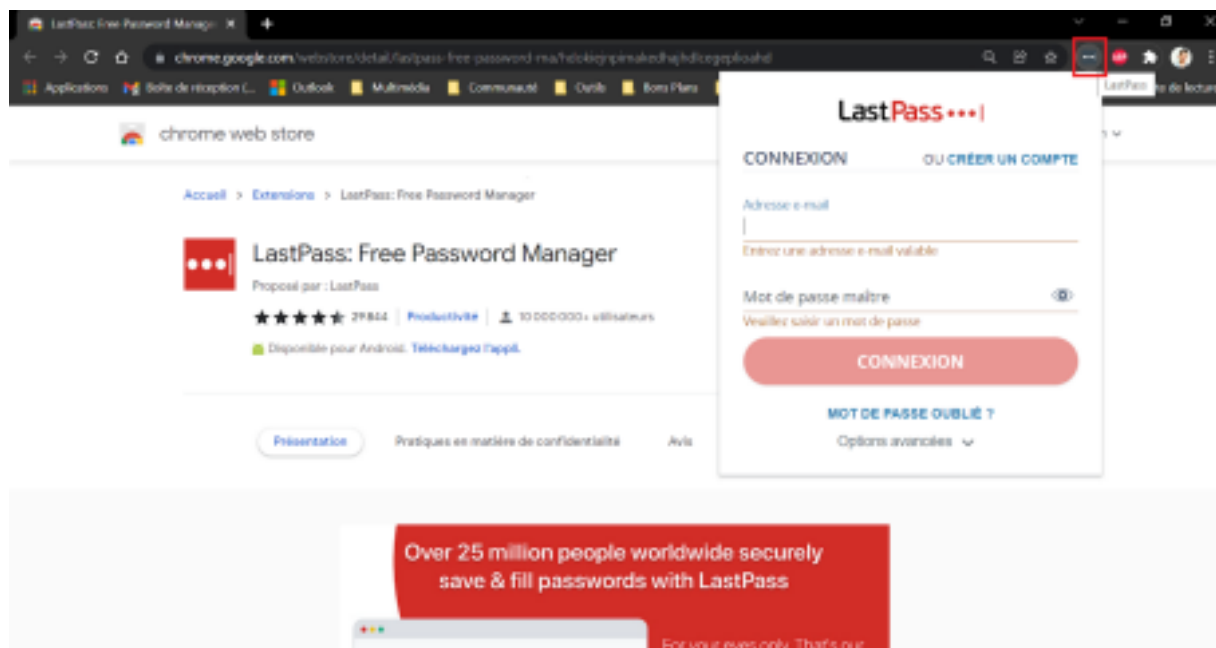
• Une fois installé, il te suffit d'accéder à cette extension et de t'y connecter

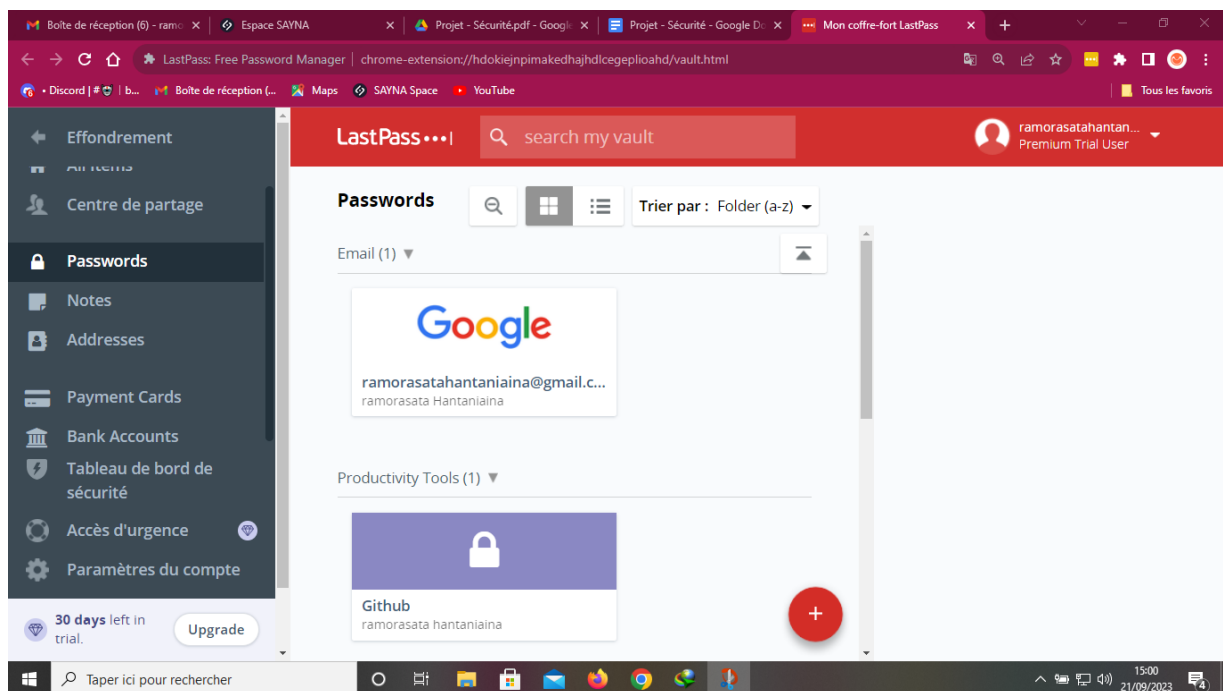
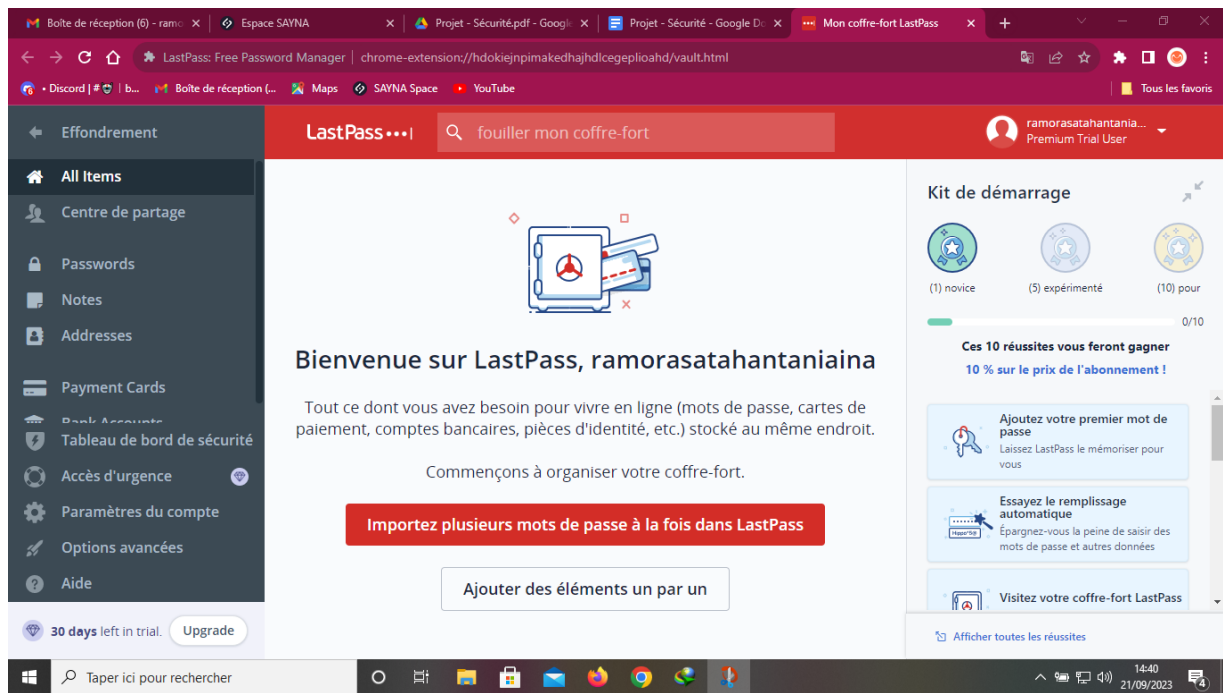
◦ (1) En haut à droite du navigateur, clic sur le logo "Extensions"

◦ (2) Épingler l'extension de LastPass avec l'icône



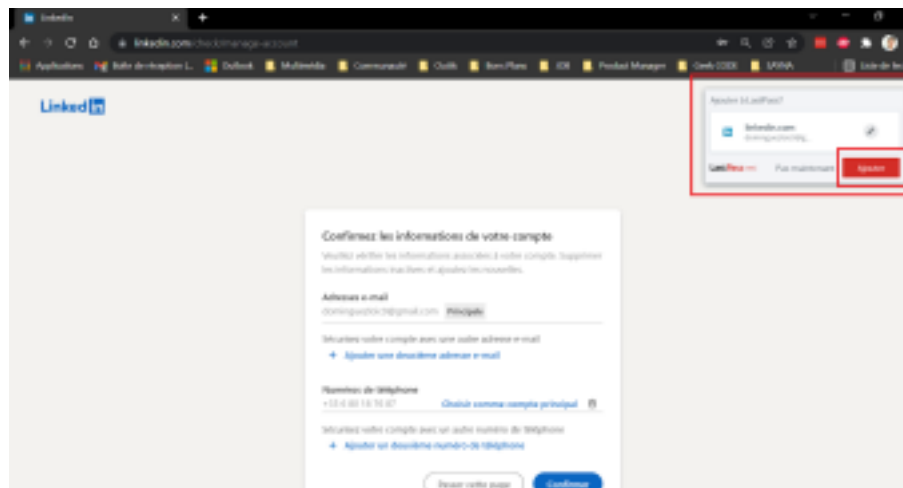
- Il ne te reste plus qu'à te connecter en effectuant un clic sur l'icône de l'extension et en saisissant ton identifiant et mot de passe



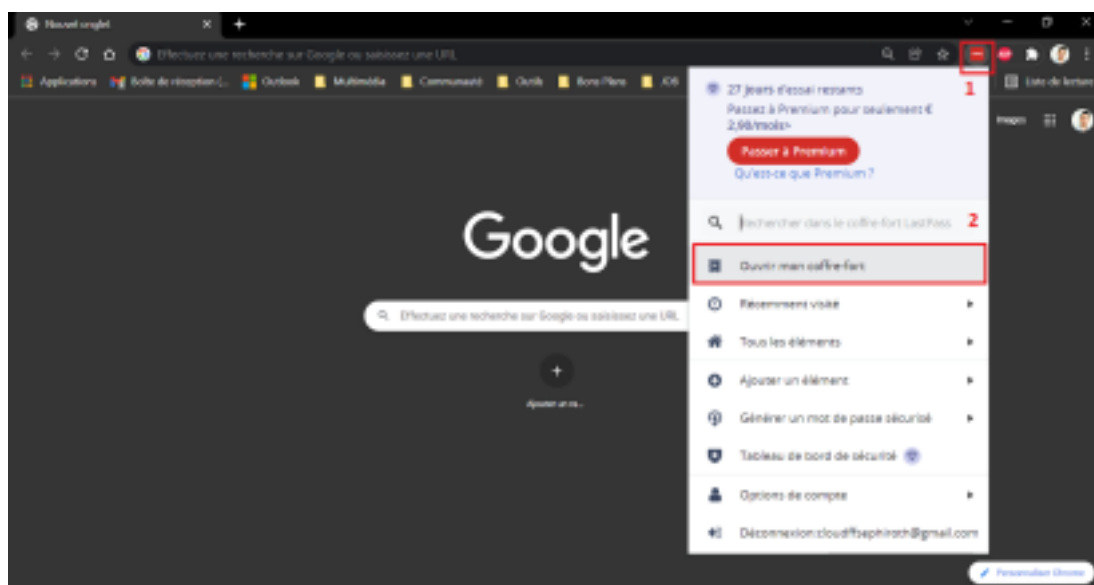


Réponse 1

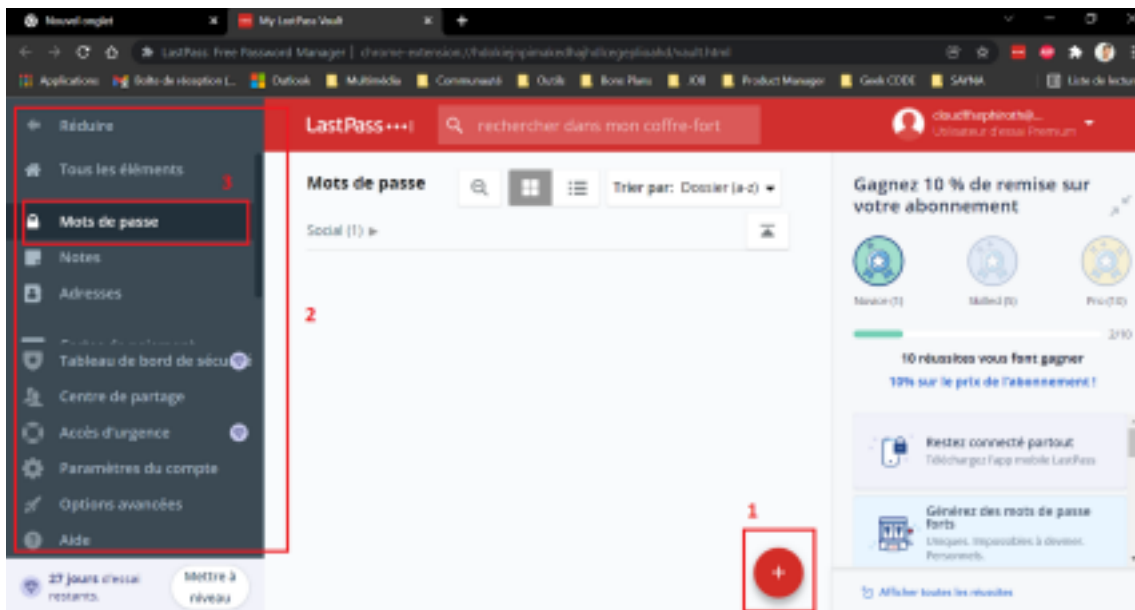
Désormais, lorsque tu te connectes à tes comptes, tu peux enregistrer le mot de passe grâce à LastPass.



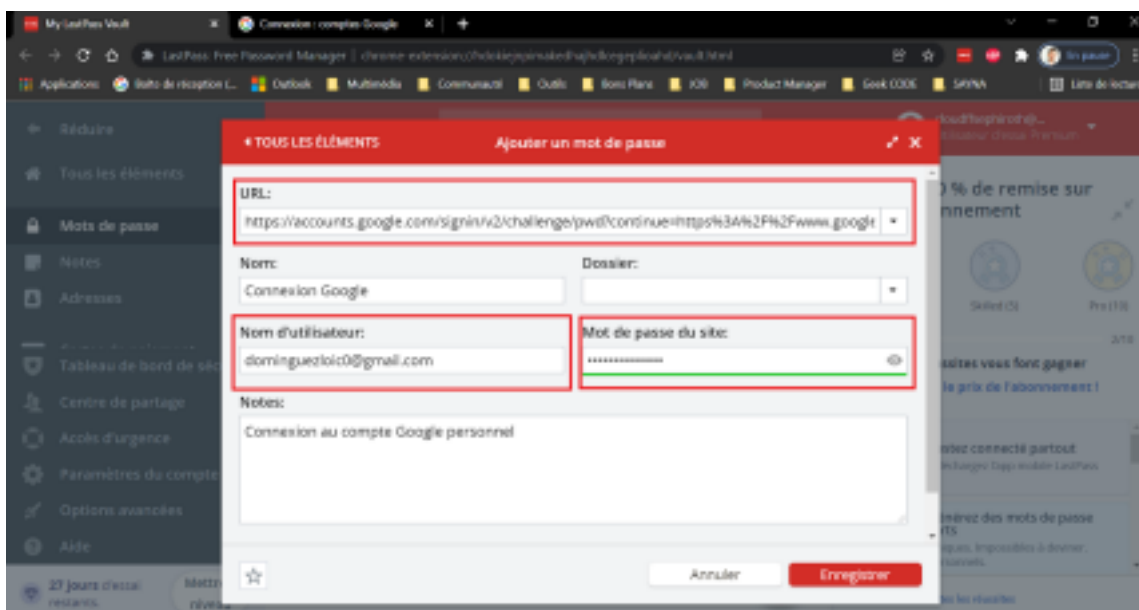
Tu peux également ajouter des comptes manuellement en accédant au coffre-fort, espace de stockage de tous tes mots de passe. Pour y accéder, clic sur l'icône de l'extension puis sur "Ouvrir mon coffre-fort".



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'id 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.

Pour aller plus loin :

L'abonnement gratuit (freemium) te permet de faire les tâches principales. Si tu trouves cet outil incontournable, tu peux passer au compte premium. Il te permettra notamment de synchroniser ton compte LastPass sur tous les supports utilisés.

- Comparatif des gestionnaires de mot de passe :

<https://www.clubic.com/application-web/article-854952-1-gestionnaires-mots-meilleur-logiciel-gratuit-windows.html>

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)

www.morvel.com site web malveillant
www.dccomics.com site sécurisé
www.ironman.com site sécurisé
www.fessebook.com site web malveillant
www.instagram.com site web malveillant

Réponse 1


Les sites web qui semblent être malveillants sont :

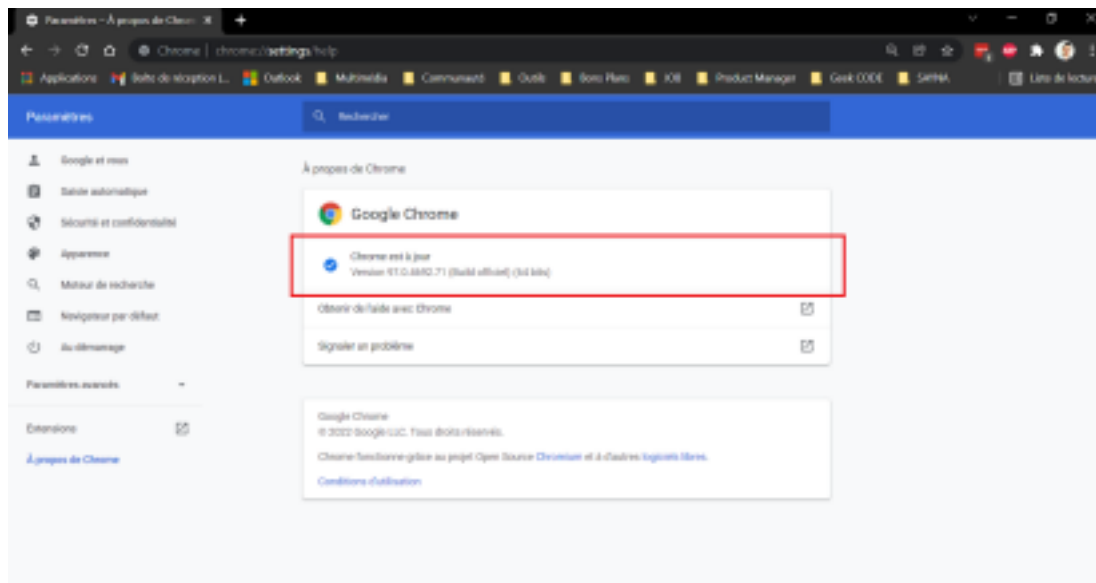
- www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel
- www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde
- www.instagram.com, un dérivé de www.instagram.com, un autre réseau social très utilisé

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)

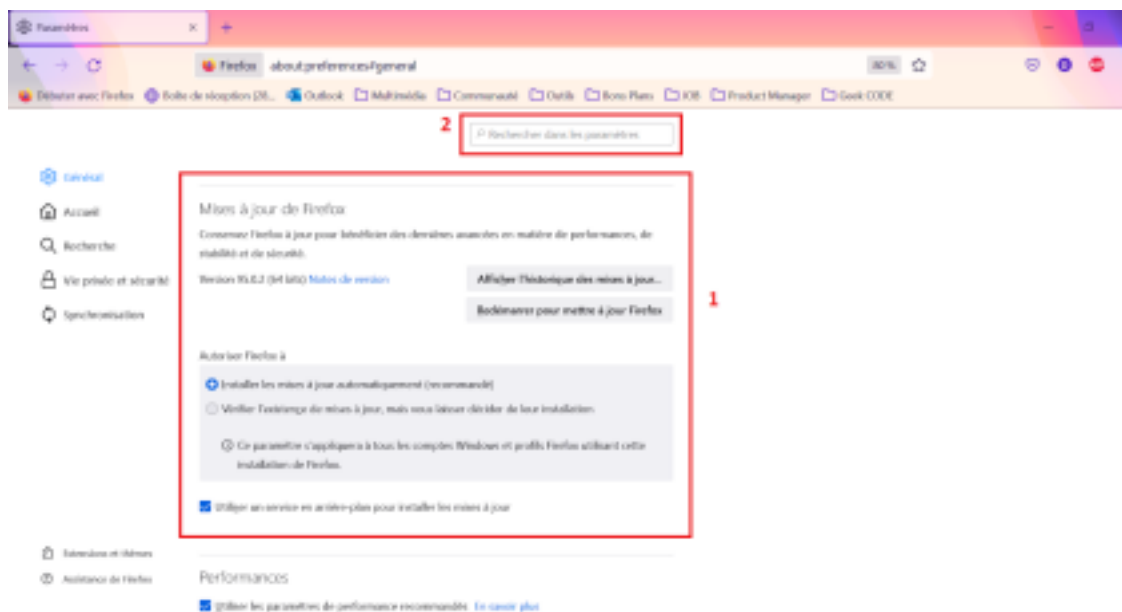
2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes. (case à cocher)

- Pour Chrome
 - Ouvre le menu du navigateur  et accède aux "Paramètres"
 - Clic sur la rubrique "A propos 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 (astuce : tu peux également saisir dans la barre de recherche (2) “mises à jour” pour tomber directement dessus)



- Vérifie que les paramètres sélectionnés sont identiques que sur la photo

À propos de Chrome

 **Google Chrome**

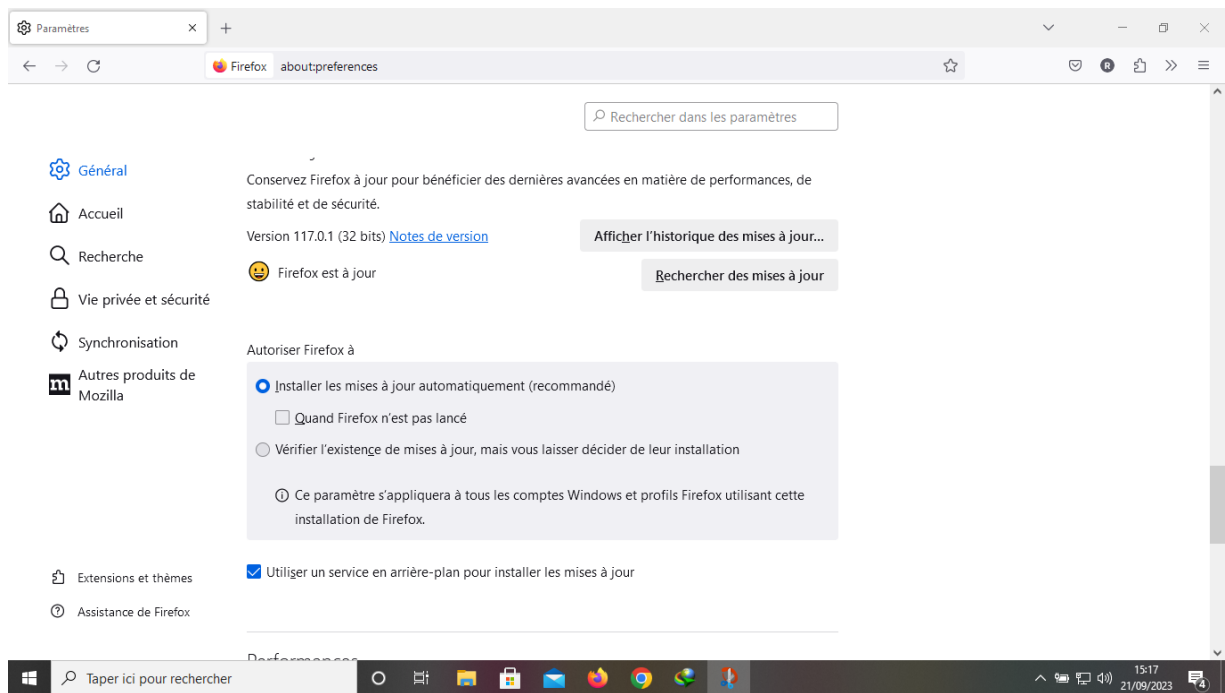
 Mise à jour de Chrome... (5%)
Version 116.0.5845.188 (Build officiel) (64 bits)

Obtenir de l'aide avec Chrome

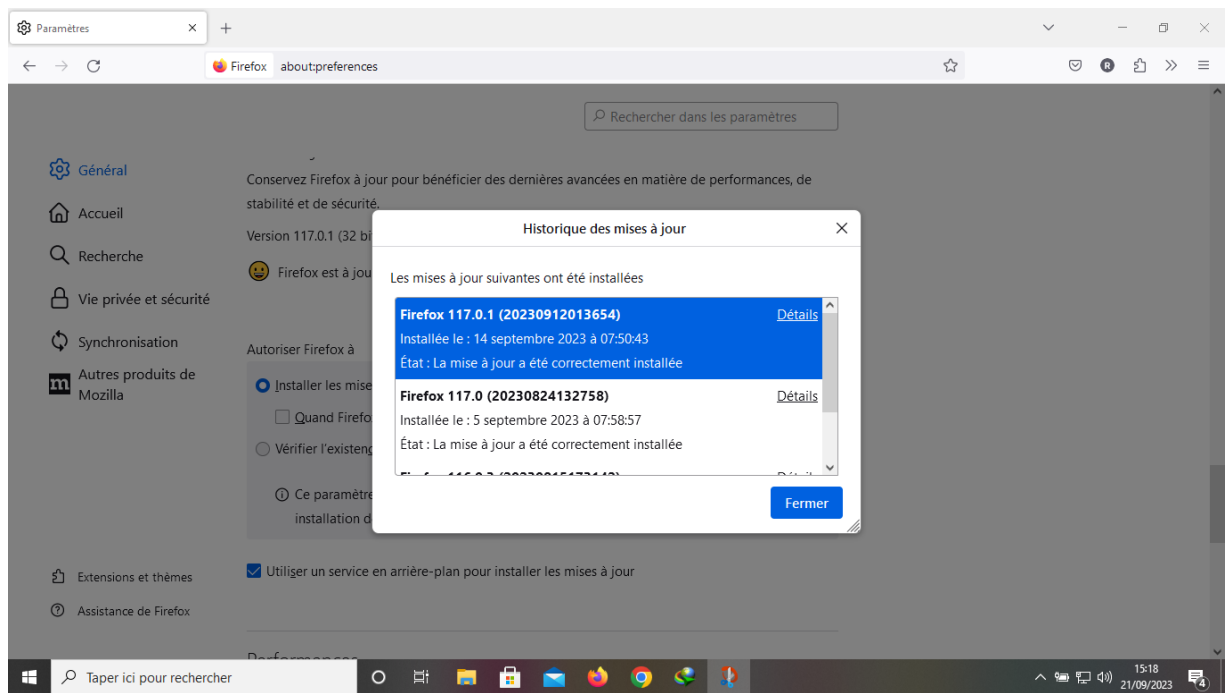
Signaler un problème

Chrome

n'est pas mis à jour.



The screenshot shows the Firefox 'about:preferences' page. The left sidebar contains a menu with 'Général' (selected), 'Accueil', 'Recherche', 'Vie privée et sécurité', 'Synchronisation', and 'Autres produits de Mozilla'. The main content area under 'Général' includes a search bar, a version update notice for 117.0.1 (32 bits) with a 'Notes de version' link, a status 'Firefox est à jour' with a smiley face icon, and a section 'Autoriser Firefox à' with three radio button options: 'Installer les mises à jour automatiquement (recommandé)' (selected), 'Quand Firefox n'est pas lancé', and 'Vérifier l'existence de mises à jour, mais vous laisser décider de leur installation'. A note below states that the selected parameter applies to all Windows accounts and Firefox profiles. At the bottom, there is a checkbox 'Utiliser un service en arrière-plan pour installer les mises à jour' which is checked. The top of the browser window shows the address bar with 'about:preferences' and standard navigation buttons. The Windows taskbar at the bottom shows the search bar and several application icons.



Firefox est mise à jour

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

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.

Pour ce faire accède au lien suivant et suis les étapes qui y sont décrites : [Exercice 4 - Spam et Phishing](#)

Bon travail, hary
ravelo !
Vous avez obtenu un
score de 4/8.

Plus vous vous entraînez, 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 :

réponse 1

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

Pour aller plus loin :

- Site du gouvernement [cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr)
<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage>

5 - 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 Transparency 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)

- Site n°1

<https://www.baidu.com/>

- **Indicateur de sécurité**

- HTTPS

- HTTPS Not secure ☐

- Not secure aucune donnée disponible

- **Analyse Google**

- Aucun contenu suspect

- Vérifier un URL en particulier
sécurisé

- Site n°2

<https://www.w3.org/>

- **Indicateur de sécurité**

- HTTPS ☐

- HTTPS Not secure ☐

- Not secure aucune donnée disponible

- **Analyse Google**

- Aucun contenu suspect

- Vérifier un URL en particulier
sécurisé cadenas

- Site n°3

<https://www.gov.cn/>

- **Indicateur de sécurité**

- HTTPS ☐

- HTTPS Not secure ☐

- Not secure aucune donnée disponible

- **Analyse Google**

- Aucun contenu suspect

- Vérifier un URL en particulier
sécurisé cadenas

- Site n°4 (site non sécurisé)

<http://xinhuanet.com/> par Google et aucune donnée disponible par Google

Transparence des Informations

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)

Tu peux tester la sécurité d'autres sites à partir de [ce lien](#). Ce site référence et explique les défauts de sécurité des sites dans le monde.

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 (en local ou sur le cloud)**

La première est la plus pratique à utiliser et la plus facile à mettre en place. Nous prendrons pour exemple la messagerie de Google (les autres messageries fonctionnent sensiblement de la même manière). Suis les étapes suivantes pour créer un registre des achats sur ta messagerie électronique. (case à cocher)

- 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 (boîte de réception, messages envoyés, etc.)



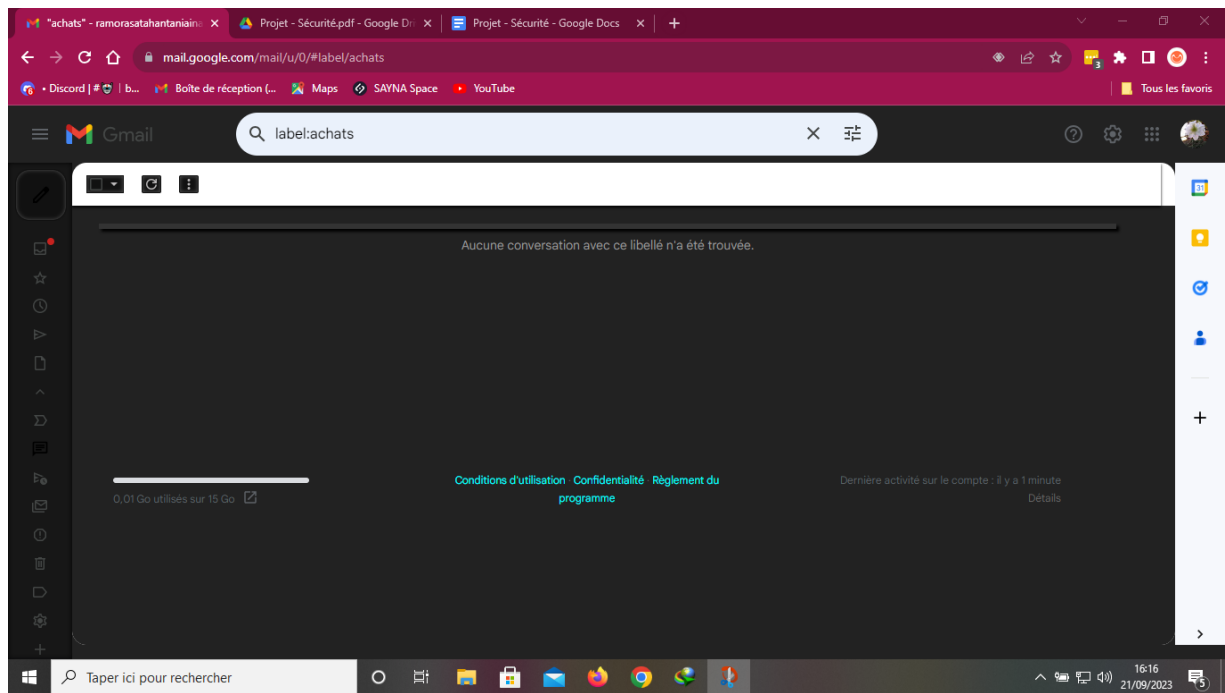
C'est dans cette partie que tu vas créer ta rubrique des achats. Pour ce faire, clic sur "Plus" et va tout en bas des libellés. Pour créer un libellé rapidement il te suffit d'effectuer un clic sur "Créer un libellé" et de le nommer "ACHATS" (pour notre exercice)



- 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). Sur cette page, tu peux gérer l’affichage des libellés initiaux (2) et gérer les libellés personnels (3)



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



Réponse 1

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

- Achats : historique, facture, conversations liés 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

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


Gestion des cookies : clic Menu, clic Paramètres, clic menu principal, clic Confidentialité et sécurité, clic Cookies tiers et bloquer les cookies tiers.

Utilisation de la navigation privée : clic sur le menu de Chrome (navigateur par défaut) puis clic sur les paramètres puis on choisit « sécurité et confidentialité » puis « effacer les données de la navigation » pour effacer l'historique. Enfin, on ouvre une nouvelle fenêtre de navigation privée (Ctrl+maj+N)

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. (case à cocher) • 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



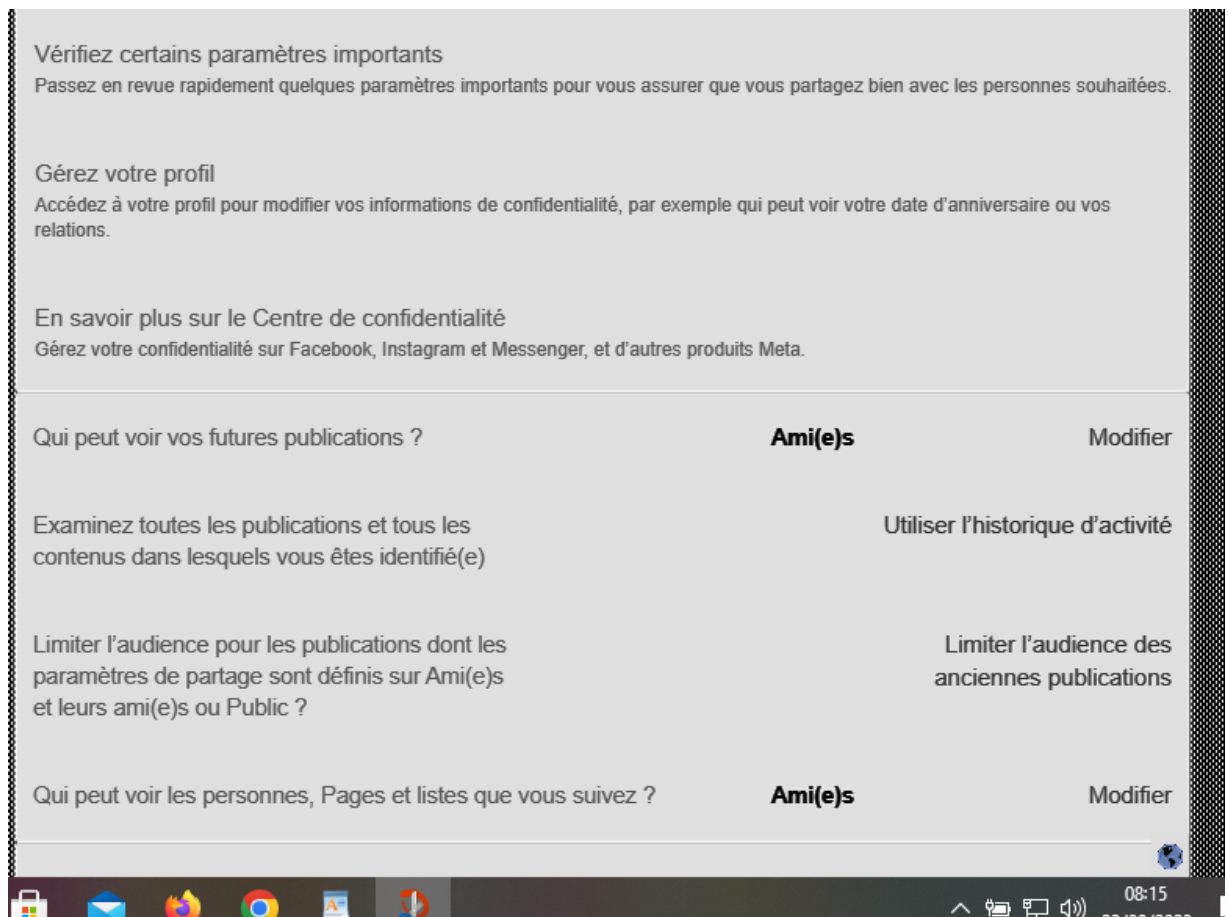
Cette rubrique résume les grandes lignes de la confidentialité sur Facebook

- 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. 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 :

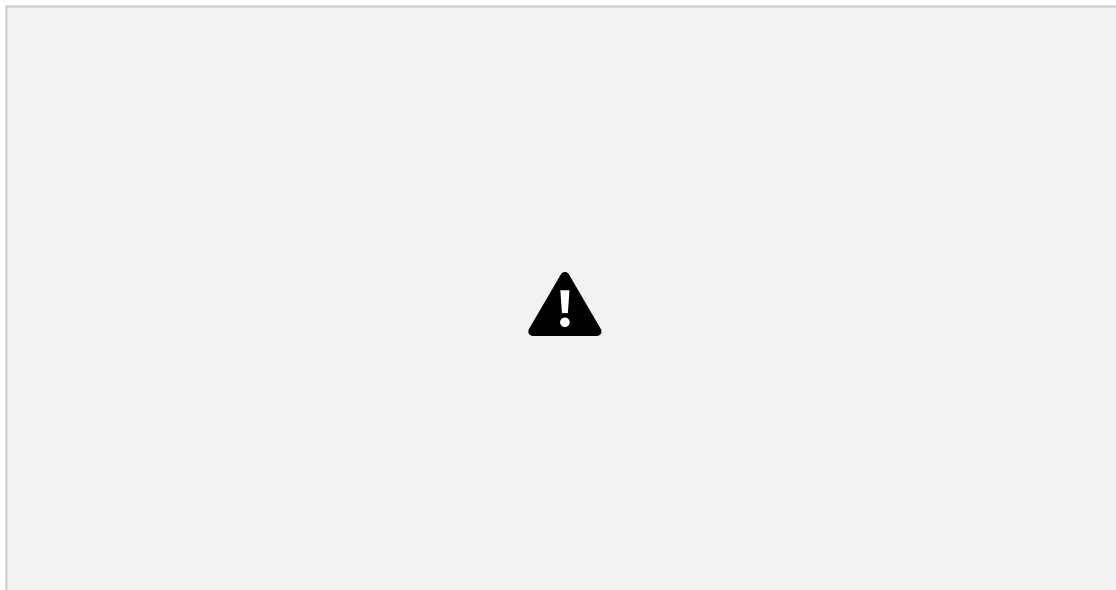
- Si tu utilises ton compte Facebook uniquement pour communiquer avec tes amis, règle les paramètres en conséquence en choisissant une visibilité "Amis" ou "Amis de leurs amis".
- Beaucoup de personnes utilisent Facebook en mêlant réseau professionnel et réseau personnel. Il n'y a pas vraiment de contre-indication, 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"
- 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.



Réponse 1

Voici un exemple de paramétrage de compte Facebook pour une utilisation privilégiant les échanges avec les amis, mais autorisant le contact avec des inconnus (limite de leurs actions) :

- Confidentialité



- Publications publiques



Sur les autres médias sociaux, tu retrouveras sensiblement le même type de paramétrage. Maîtrise ton utilisation de ces outils en paramétrant selon tes souhaits.

Pour aller plus loin :

- [Les conseils pour utiliser en toute sécurité les médias sociaux](#)

9 - 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 ????????

1-comment faire pour vérifier la sécurité contre virus en fonction de l'appareil utilisé

Mise à jour régulière du navigateur

Eviter les sites malveillants, les phishings, rechercher les sites HTTPS

Sécuriser l'appareil avec un antivirus

Sauvegarder les données dans un support externe

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

Installer un antivirus et antimalware

Faire une analyse complète pour voir leur fonctionnement

Si virus il y a, le supprimer. Si il demeure, faire un formatage.

Mettre à jour régulièrement l'antivirus

2/Proposerunexercicepour installeretutiliserunantivirus+antimalwareenfonctionde l'appareil utilisé.