



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, je consulte trois articles qui parlent de sécurité sur internet. Puis je vérifie les sources des informations et j'essaierai de consulter des articles récents pour que les informations soient à jour. Je donne le nom du site et de l'article.

Réponse 1

Voici les articles que j'ai consulté (avec les mots-clés "sécurité sur internet" et "comment être en sécurité sur internet" :

Voici trois articles en français sur la sécurité sur Internet avec les mots clés "sécurité sur internet" :

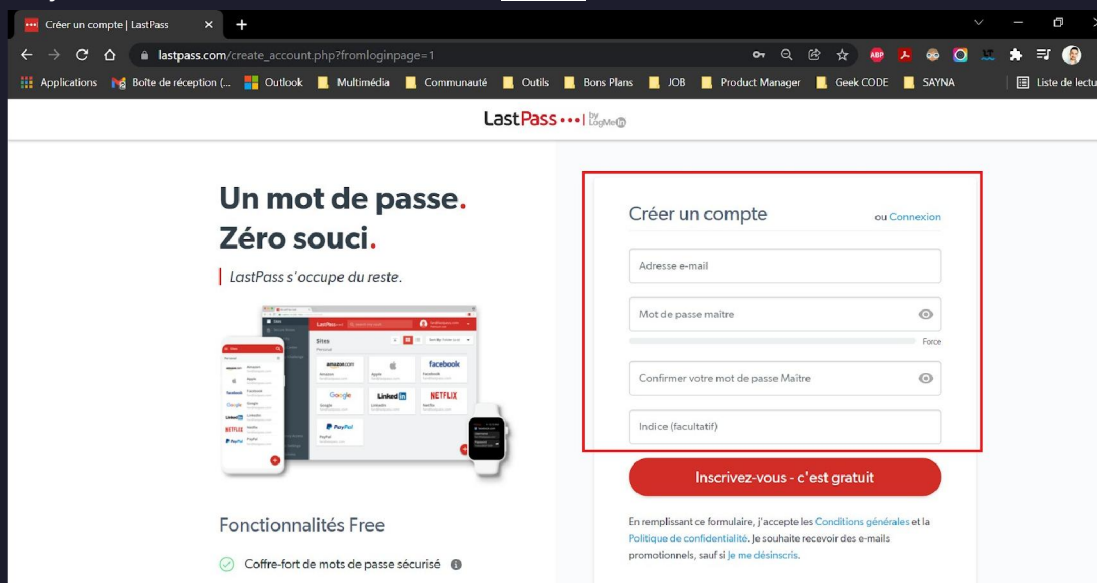
- Site : L'Express.fr Article : "Sécurité sur internet : comment bien protéger ses données ?" Source : https://www.lexpress.fr/actualite/societe/securite-sur-internet-comment-bien-protoger-ses-donnees_2052949.html
- Site : LeFigaro.fr Article : "Sécurité sur Internet : les meilleurs conseils pour éviter les pièges du web" Source : <https://www.lefigaro.fr/secteur/high-tech/securite-sur-internet-les-meilleurs-conseils-pour-eviter-les-pieges-du-web-20211119>
- Site : France24.com Article : "Cybersécurité : comment protéger ses données sur internet ?" Source : <https://www.france24.com/fr/minisite/les-experts/20220303-cybers%C3%A9curit%C3%A9-comment-prot%C3%A9ger-ses-donn%C3%A9es-sur-internet>

2 – Création des mots de passe forts

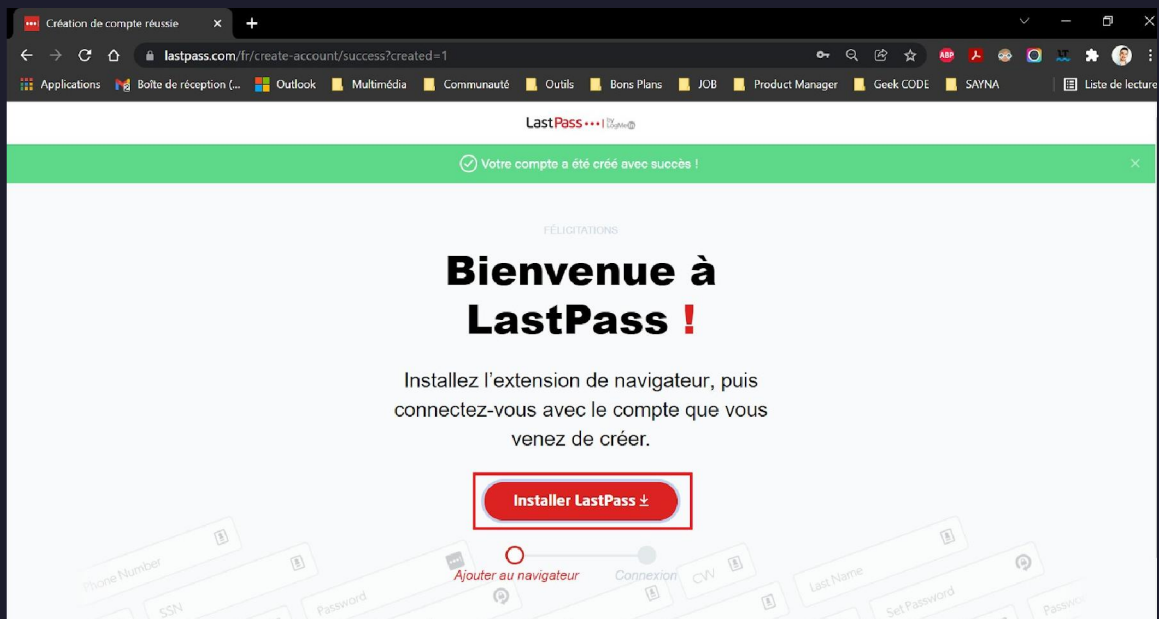
Objectif : utiliser un gestionnaire de mot de passe LastPass

1/ Dans cet exercice, je vais 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. En suivant les étapes suivantes. (case à cocher)

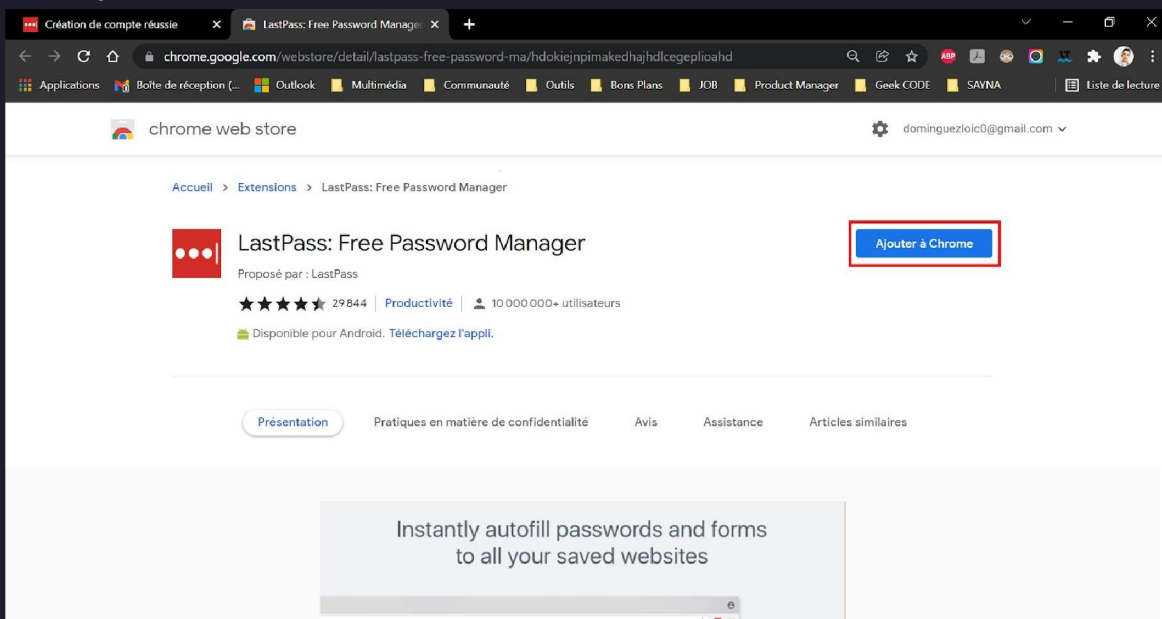
- j'accède au site de LastPass avec ce lien



- Je crée un compte en remplissant le formulaire. Un conseil, on me demande de choisir un mot de passe maître. Pour rappel, ce mot de passe sera unique et me permettra d'accéder à tous tes comptes. Choisis donc un mot de passe avec un niveau de sécurité élevé et je m'assurerais 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")
 - Je peux également générer un mot de passe maître, puis je l'écrire dans un endroit sûr pour pouvoir l'utiliser lorsque tu en as besoin
- Une fois la création du compte effectuée, j'arrive sur une page de validation qui propose le téléchargement de l'extension sur ton navigateur. Je lance l'installation en effectuant un clic sur le bouton prévu à cet effet

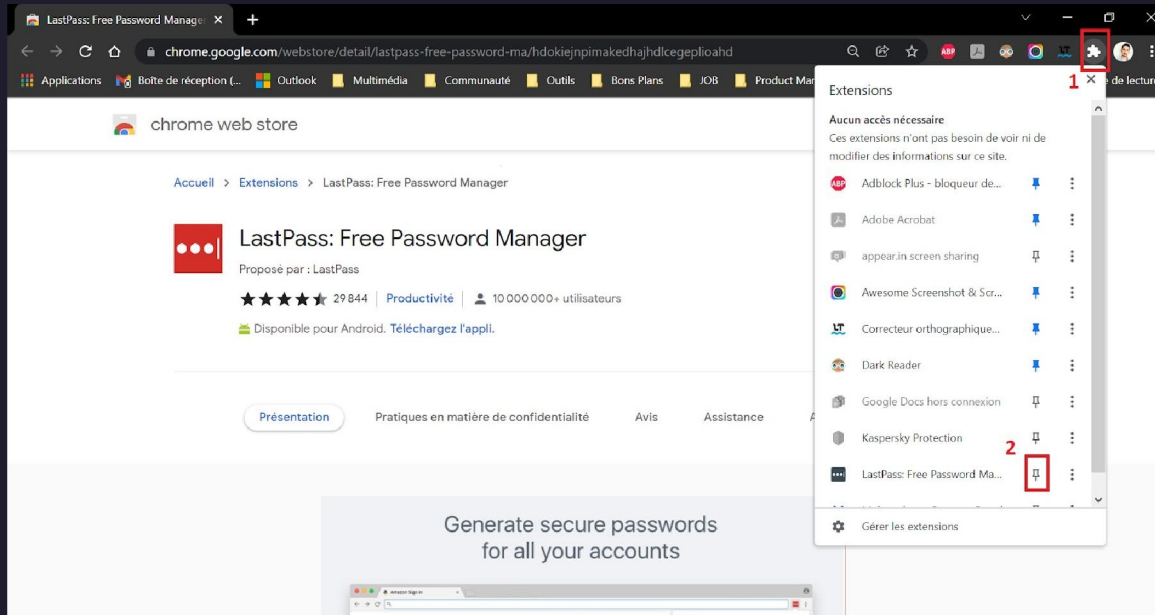


- Je valide l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome"

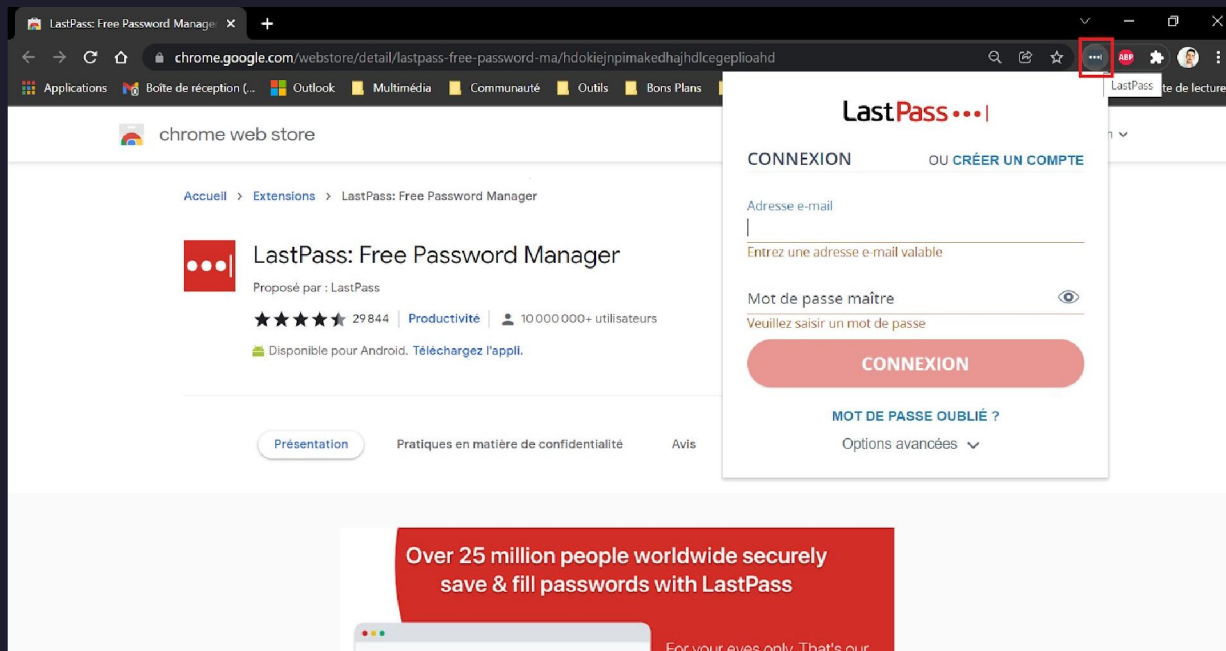


- Une fois installé, j'accéder à cette extension et de m'y connecter

- (1) En haut à droite du navigateur, je clic sur le logo "Extensions"
- (2) j'épingle l'extension de LastPass avec l'icône

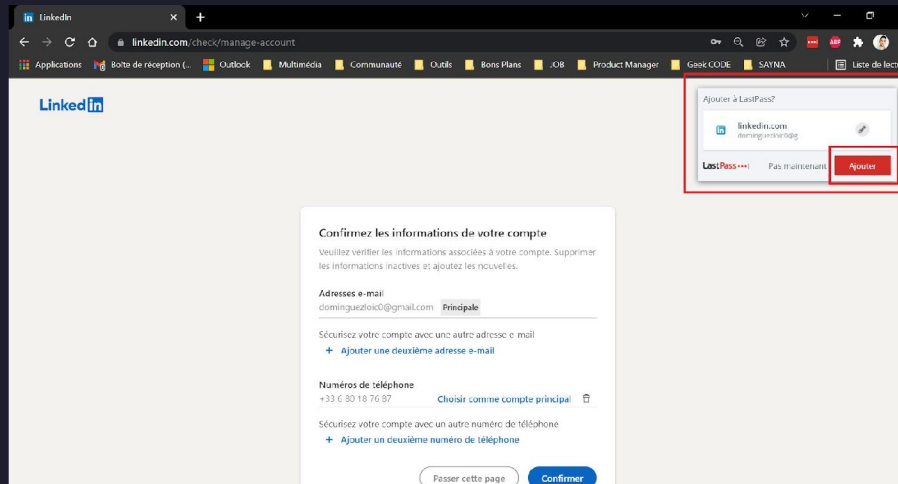


- Il ne me reste plus qu'à te connecter en effectuant un clic sur l'icône de l'extension et en saisissant mon identifiant et mot de passe

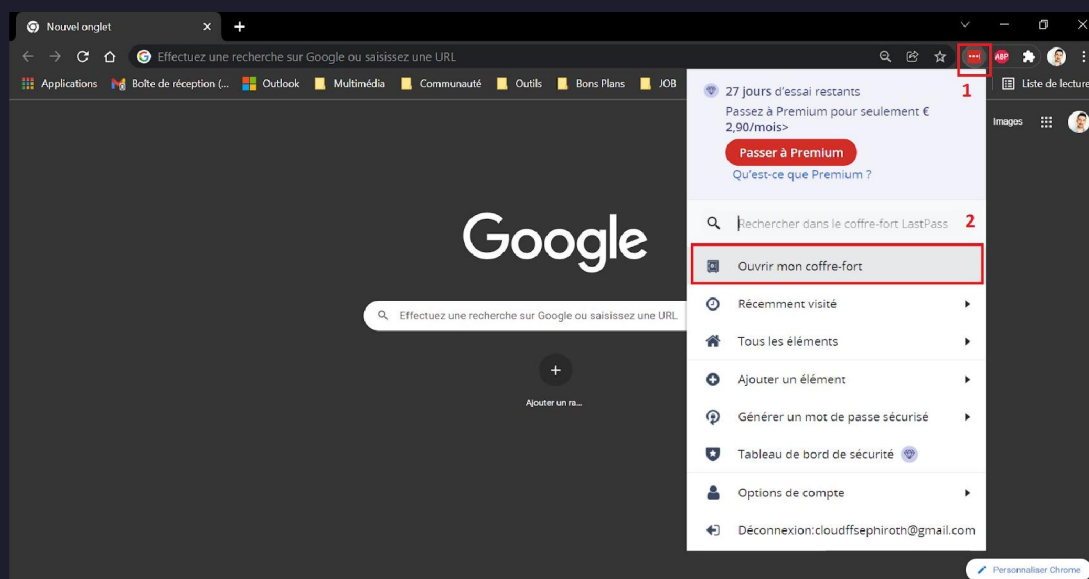


Réponse 1

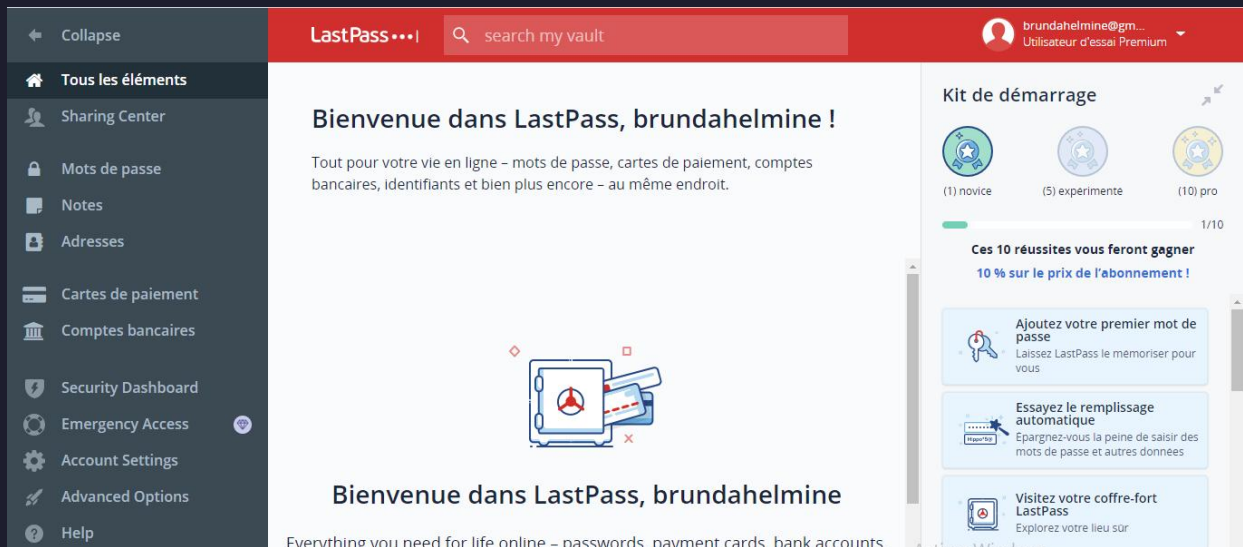
Désormais, lorsque je me connecte à mes comptes, je peux enregistrer mon mot de passe grâce à LastPass.



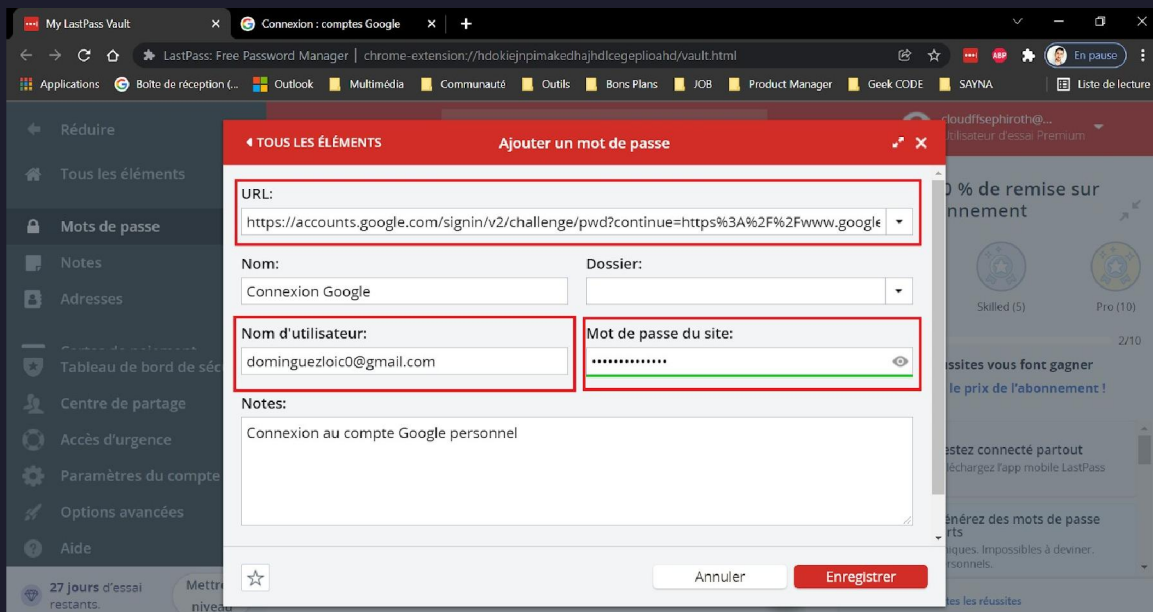
Je peux également ajouter des comptes manuellement en accédant au coffre-fort, espace de stockage de tous tes mots de passe. Pour y accéder, je clic sur l'icône de l'extension puis sur "Ouvrir mon coffre-fort".



J'arrive alors sur une page de gestion de mon compte LastPass. Pour ajouter un site et une connexion associée (identifiant + mot de passe), j'accède à la rubrique "Mot de passe" (2) et (3) puis je 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 ; je mets l'URL de la **page de connexion du site**. Ensuite préciser l'id et le mot de passe. Je peux personnaliser mon nom, un commentaire associé ou encore un dossier si besoin.



Je 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/ J'identifie les adresses internet qui me semblent provenir de sites web malveillants. (Case à cocher)


- www.morvel.com
- www.dccomics.com
- www.ironman.com
- www.fessebook.com
- www.instagam.com

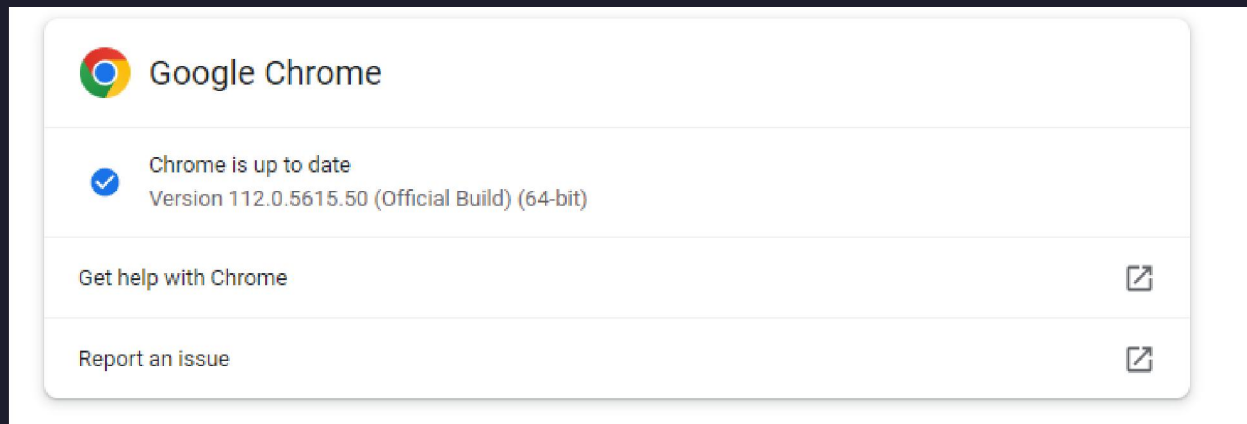
Réponse 1

Les sites web qui semblent être malveillants sont :


- "www.morvel.com" semble suspecte car l'adresse correcte est "www.marvel.com".
- "www.fessebook.com" est également suspecte car elle semble être une tentative de copie frauduleuse du site web "Facebook".
- www.instagam.com
L'utilisation de ces sites web peut présenter des risques pour la sécurité en raison de la possibilité de phishing, de logiciels malveillants et de tentatives de vol de données personnelles.

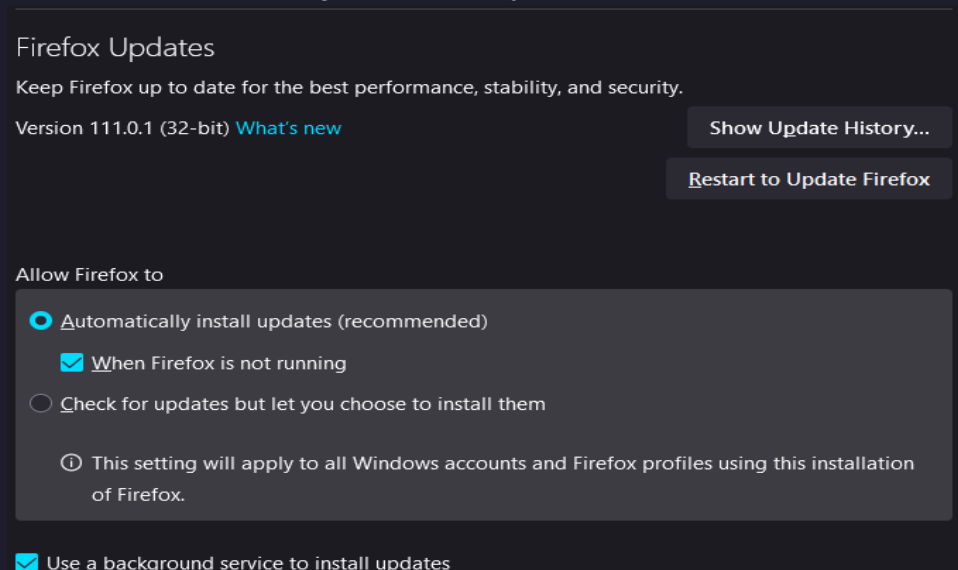
2/ je vérifie si les navigateurs que j'utilise sont à jour : Chrome et Firefox Pour ce faire, je suivrais les étapes suivantes. (case à cocher)

- Pour Chrome
 - J'ouvre le menu du navigateur  et j'accède aux "Paramètres"
 - Je clic sur la rubrique "A propose de Chrome"
 - Si je constate le message "Chrome est à jour", donc c'est Ok



- Pour Firefox

- J'ouvre le menu du navigateur  et j'accède aux "Paramètres"



- ☒ Use a background service to install updates

Dans la rubrique "Général", je fais défiler jusqu'à voir la section "Mise à jour de Firefox (astuce : je peux également saisir dans la barre de recherche (2) "mises à jour" pour tomber directement dessus)

- Je vérifie que les paramètres sélectionnés sont identiques que sur la photo

Réponse 2

En effet, les paramètres par défaut de ces deux navigateurs sont réglés pour réaliser les mises à jour automatiquement. Puisque Les mises à jour automatiques sont également activées par défaut et les utilisateurs reçoivent des notifications lorsqu'une nouvelle mise à jour est disponible. Les mises à jour sont téléchargées et installées en arrière-plan sans que l'utilisateur ait à fermer et redémarrer le navigateur.

4 - Éviter le spam et le phishing

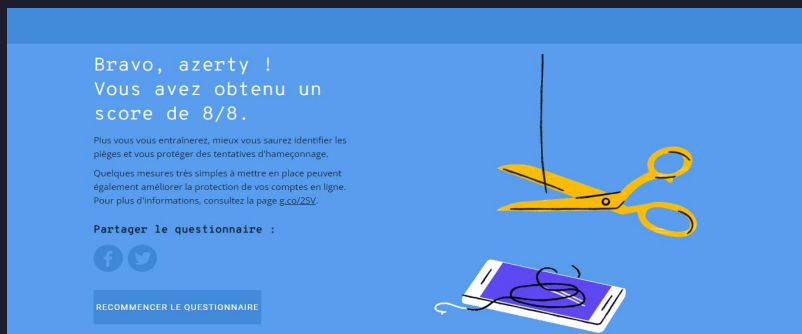
Objectif : *Reconnaître plus facilement les messages frauduleux*

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

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

Réponse 1





Je veux réessayer pour continuer à m'exercer, c'est possible ! Je peux également consulter des ressources annexes pour m'exercer.





5 - Eviter 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 j'ai 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 je peux m'appuyer sur un outil proposé par Google : [Google Transparency Report](#) (en anglais) ou [Google Transparence des Informations](#) (en français). Afin d'améliorer ma lecture de la sécurité sur internet, je vais devoir analyser les informations de plusieurs sites. Pour chaque site je devrais préciser l'indicateur de sécurité et le rapport d'analyse de l'outil Google. J'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
 - **Indicateur de sécurité**
 - HTTPS 
 - HTTPS Not secure 
 - Not secure
 - **Analyse Google**
 - Aucun contenu suspect
 - Vérifier un URL en particulier
- Site n°2
 - **Indicateur de sécurité**
 - HTTPS 
 - HTTPS Not secure 
 - Not secure
 - **Analyse Google**

- Aucun contenu suspect
 - Vérifier un URL en particulier
- Site n°3
 - **Indicateur de sécurité**
 - HTTPS 
 - HTTPS Not secure 
 - Not secure
 - **Analyse Google**
 - Aucun contenu suspect
 - Vérifier un URL en particulier
- Site n°4 (site non sécurisé)

Réponse 1

- Site n°1
 - **Indicateur de sécurité**
 - HTTPS
 - **L'analyse de Google indique qu'il n'y a aucun contenu suspect et permet de vérifier l'URL en particulier.**
- Site n°2
 - **Indicateur de sécurité**
 - Not secure
 - **Il n'y a pas de rapport d'analyse de l'outil Google fourni.**
- Site n°3
 - **Indicateur de sécurité**
 - Not secure
 - **Analyse Google : aucun contenu suspect et permet de vérifier l'URL en particulier.**
- Site n°4
 - **Indicateur de sécurité**
 - Not secure
 - **Analyse Google : Ne dispose pas de certificat SSL pour chiffrer les données échangées entre le navigateur et le serveur. Il est donc plus vulnérable aux attaques de type man-in-the-middle ou phishing.**

6 - Achats en ligne sécurisés

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

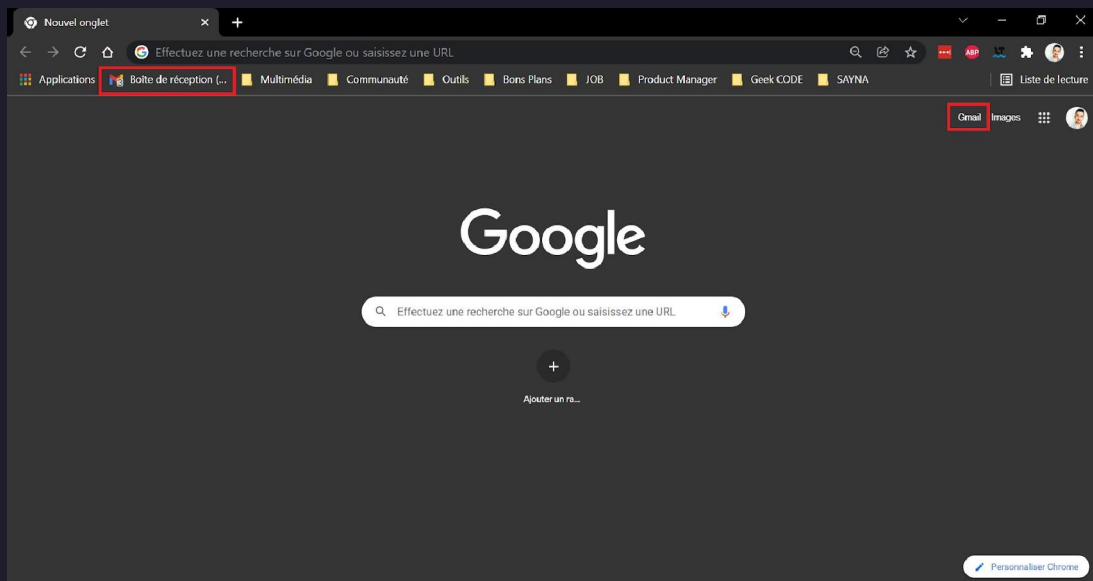
1/ Dans cet exercice, on va m'aider à créer un registre des achats. Dans le cours, ce registre a pour but de conserver les informations relatives à mes achats en ligne. Très pratique lorsque je fais face à un litige, un problème sur ma commande ou tout simplement pour faire le bilan de tes dépenses du mois.

Deux possibilités s'offrent à moi pour organiser ce registre :

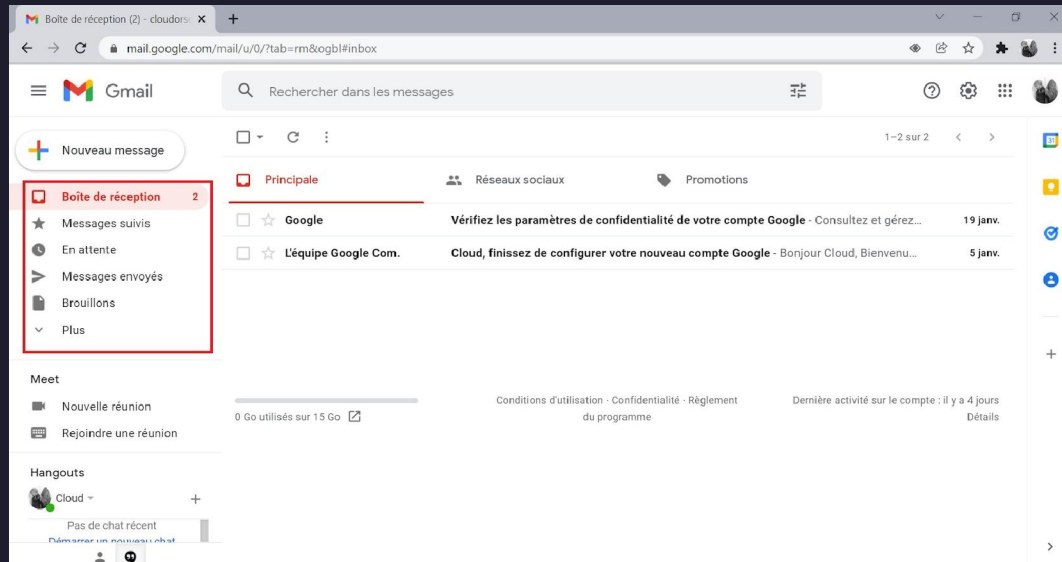
1. Créer un dossier sur ma messagerie électronique
2. Créer un dossier sur mon espace de stockage personnel (en local ou sur le cloud)

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). Je suis les étapes suivantes pour créer un registre des achats sur ta messagerie électronique. (case à cocher)

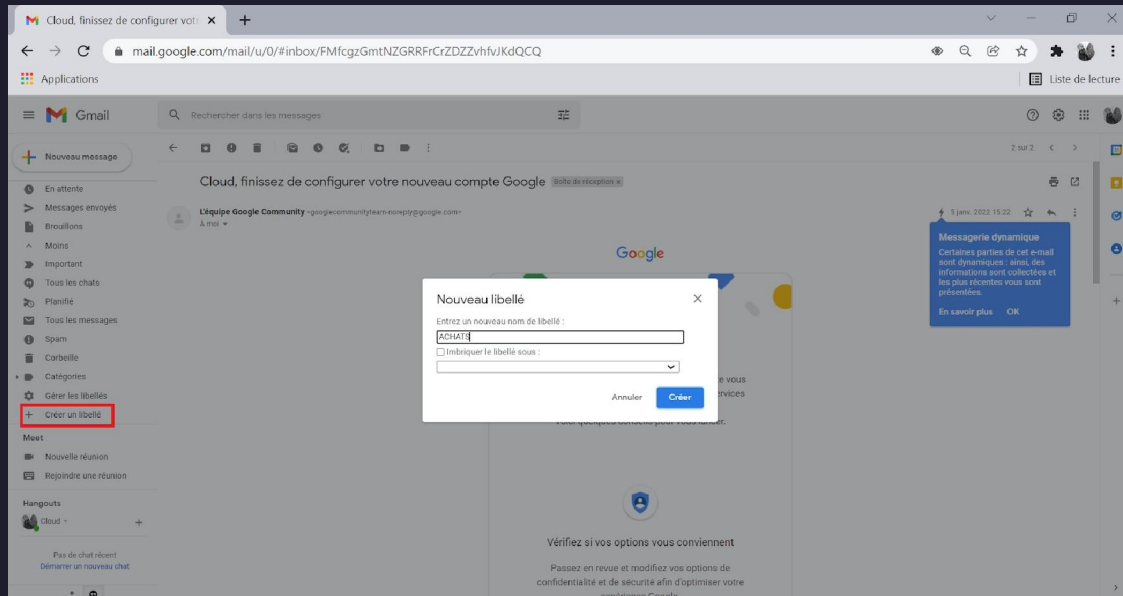
- Pour commencer, j'accède à ma messagerie électronique. Pour rappel, je peux y accéder rapidement en ouvrant un nouvel onglet (dans la barre des favoris ou via le raccourci)



- Sur la page d'accueil de ma messagerie, je trouverais sur la gauche les libellés initialement prévus (boîte de réception, messages envoyés, etc.)



- C'est dans cette partie que je vais créer ta rubrique des achats. Pour ce faire, clic sur "Plus" et va tout en bas des libellés. Pour créer un libellé rapidement j'effectuerai un clic sur "Créer un libellé" et de le nommer "ACHATS" (pour notre exercice)



- J'effectue un clic sur le bouton "Créer" pour valider l'opération
- Je peux également gérer les libellés en effectuant un clic sur "Gérer les libellés"(1). Sur cette page, je peux gérer l'affichage des libellés initiaux (2) et gérer les libellés personnels (3)
- J'ai maintenant un libellé pour stocker tous mes 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 :

Personnel : tous les messages personnels non liés au travail ou aux achats

- Social : tous les messages liés aux réseaux sociaux
- Spam : tous les messages indésirables ou suspects
- Tâches : tous les messages liés aux tâches à accomplir ou à suivre
- Travail : tous les messages liés à mon travail actuel
- Voyages : tous les messages liés à mes voyages passés ou futurs (réservations, confirmations)

7 - Comprendre le suivi du navigateur

Le suivi du navigateur, la gestion des cookies et l'utilisation de la navigation privée sont des concepts liés à la vie privée et à la sécurité en ligne.

Le suivi du navigateur fait référence à la capacité des sites web de suivre les actions de l'utilisateur sur le web en utilisant des technologies telles que les cookies, les pixels de suivi et les empreintes digitales du navigateur. Ce suivi peut être utilisé pour collecter des informations sur l'utilisateur, telles que ses préférences d'achat, ses habitudes de navigation et ses informations personnelles.

Les cookies sont des petits fichiers stockés sur l'ordinateur de l'utilisateur qui sont utilisés pour stocker des informations sur les visites passées sur un site web et pour personnaliser l'expérience de l'utilisateur sur ce site web. Les cookies peuvent être utilisés pour suivre l'utilisateur à travers différents sites web pour diffuser des publicités ciblées, ou pour collecter des informations personnelles.

La navigation privée est une fonctionnalité offerte par les navigateurs web qui permet à l'utilisateur de naviguer sur le web sans que les informations de navigation ne soient enregistrées sur l'ordinateur. Cela signifie que les cookies et autres données de navigation ne sont pas enregistrés, offrant une expérience de navigation plus privée. Cependant, cela ne


signifie pas que l'utilisateur est totalement anonyme sur le web, car les activités de navigation peuvent toujours être surveillées par les FAI (fournisseurs d'accès à Internet) ou par les sites web eux-mêmes.

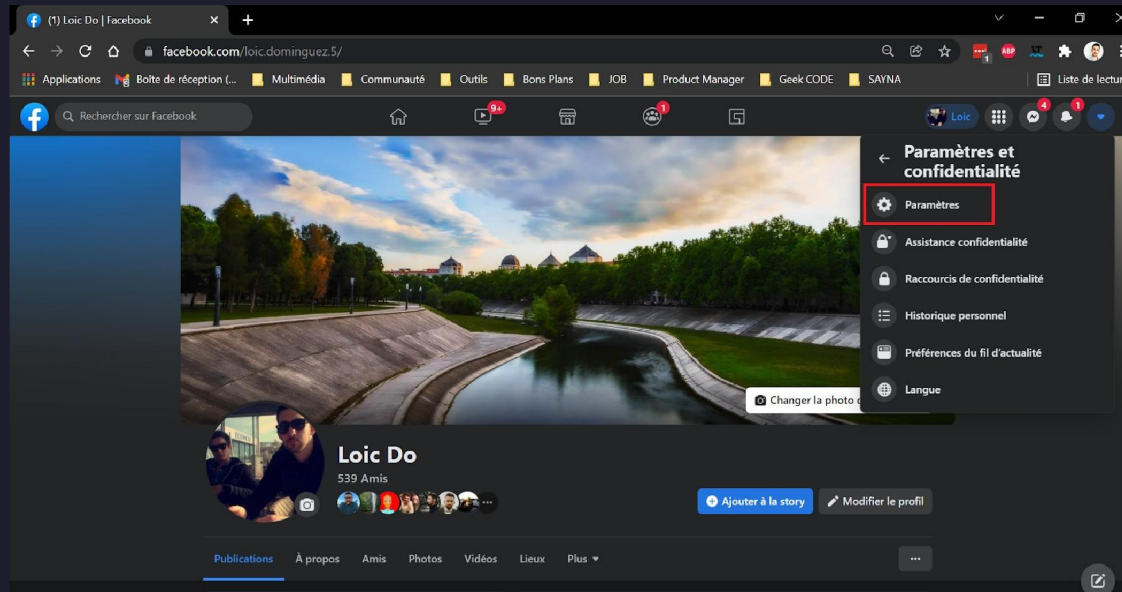
- Principes de base de la confidentialité des médias sociaux

Objectif : *Régler les paramètres de confidentialité de Facebook*

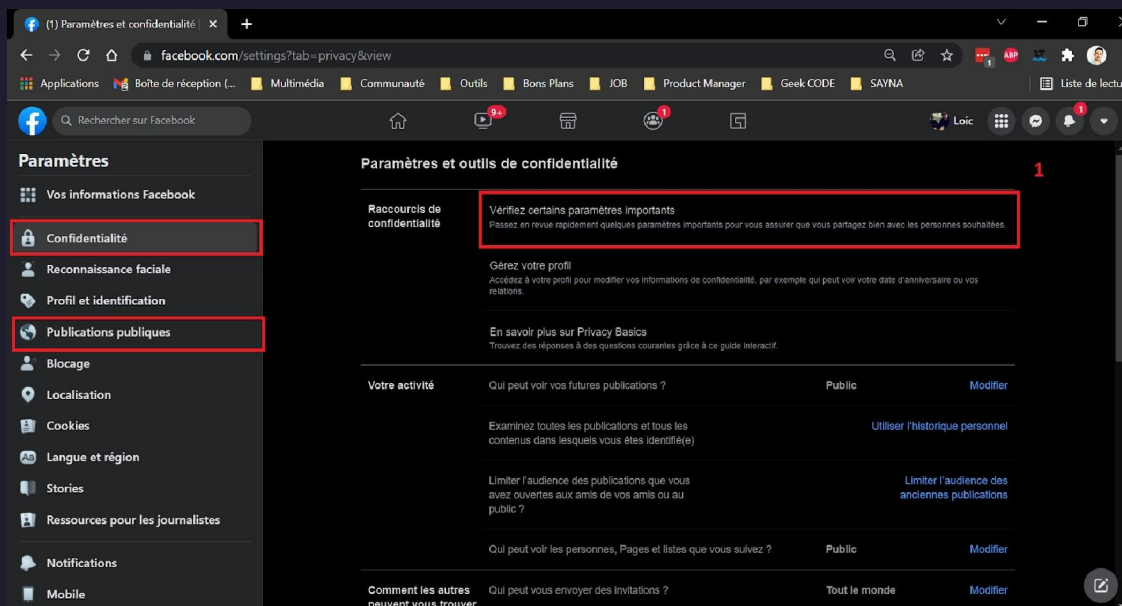
1/ Plus tôt dans le cours (Internet de base) j'ai déjà été amené à utiliser ce réseau social en partageant une publication. Dans cet exercice on va me montrer le réglage des paramètres de confidentialité pour Facebook. Je suis les étapes suivantes. (case à cocher)

Je me connecte à mon compte Facebook

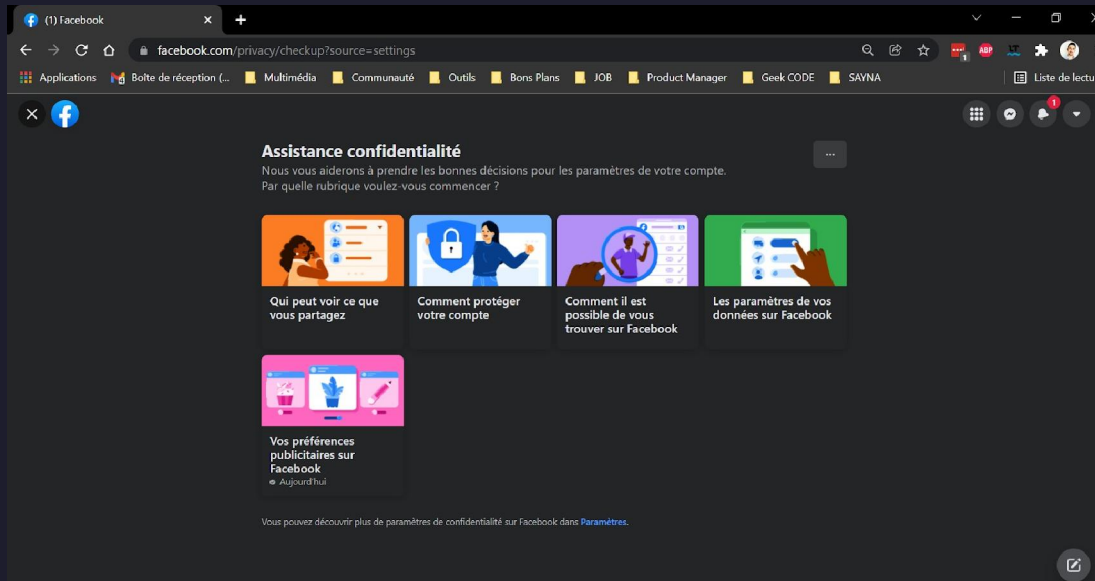
Une fois sur la page d'accueil, j'ouvre le menu Facebook , puis j'effectue un clic sur "Paramètres et confidentialité". Pour finir, je clic sur "Param



- Ce sont les onglets “Confidentialité” et “Publications publiques” qui intéressent. J’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) me permettra de régler la visibilité de mes informations personnelles
 - La deuxième rubrique (bleu) me permet de changer mon mot de passe
 - La troisième rubrique (violet) me permet de gérer la visibilité de mon 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

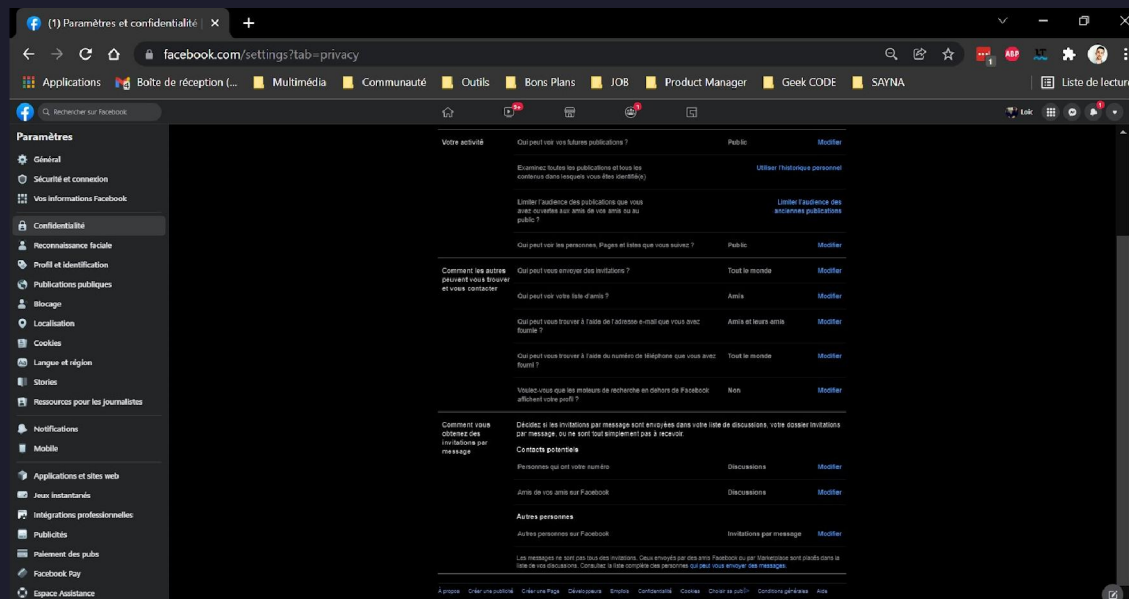


- Je retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à gauche. Je peux continuer à explorer les rubriques pour personnaliser tes paramètres. On ne peut pas me dire ce que je dois faire. C'est à moi de choisir les informations que tu souhaites partager et celles que tu veux garder privées. Voici tout de même quelques conseils :
 - Si j'utilise mon compte Facebook uniquement pour communiquer avec mes 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 il est conseillé 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, je peux restreindre les commentaires de tes publications. Ça se passe dans l'onglet "Publications publiques"
- Dans les paramètres de Facebook j'ai également un onglet "Cookies". On m'en a parlé dans le cours précédent (Comprendre le suivi du navigateur). Maintenant que je sais comment sont utilisées tes données, je suis capable de choisir en pleine conscience ce que je souhaite partager.

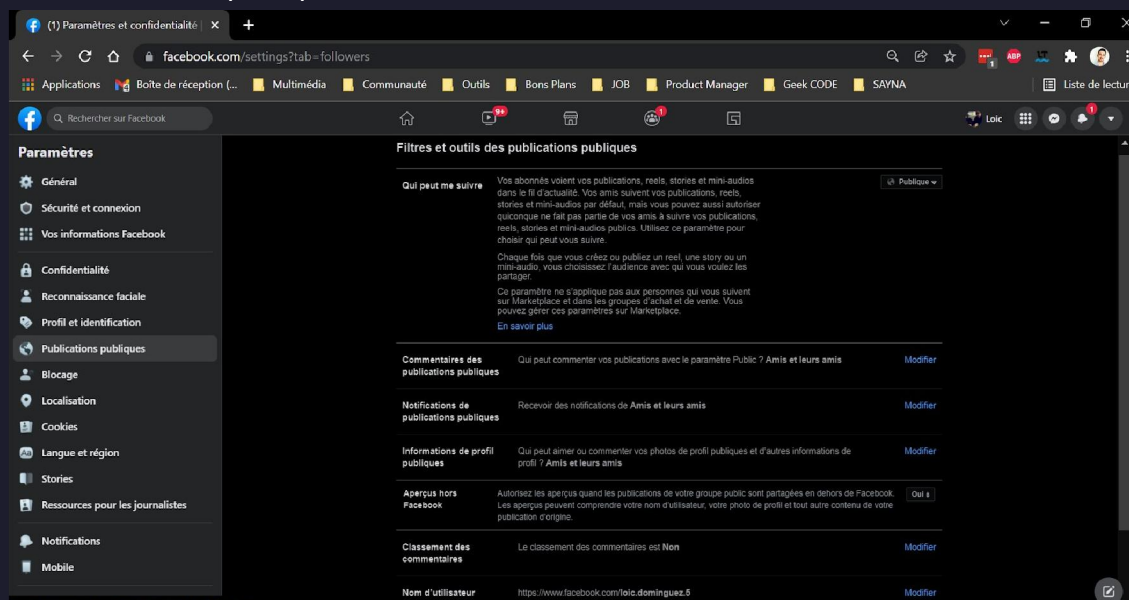
Réponse 1

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) :

- Paramètres de confidentialité :
- Paramètres de messagerie :
- Paramètres de confidentialité des photos :
- Paramètres de confidentialité des applications :



● Publications publiques



Sur les autres médias sociaux, je retrouverais sensiblement le même type de paramétrage. Maîtrise mon utilisation de ces outils en paramétrant selon tes souhaits.

Pour aller plus loin :

- Les conseils pour utiliser en toute sécurité les médias sociaux

8 – Ce qu’il faut faire quand un ordinateur est infecté par un virus

Objectif :

1/ je propose un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé en expliquant comment le faire :

1. Vérifier la sécurité d'un ordinateur Windows :
 - Effectuez une analyse complète de votre ordinateur avec un antivirus et un antimalware : installez un logiciel antivirus et un logiciel antimalware de confiance, mettez-les à jour et effectuez une analyse complète de votre ordinateur en suivant les instructions du

logiciel.

- Assurez-vous que votre pare-feu est activé et que toutes les mises à jour Windows sont installées : allez dans les paramètres de sécurité de Windows, activez votre pare-feu si ce n'est pas déjà fait et vérifiez que toutes les mises à jour Windows sont installées.
- Utilisez un scanner de vulnérabilités pour détecter les faiblesses dans votre système et prendre les mesures nécessaires pour les corriger : utilisez un scanner de vulnérabilités en ligne ou installez un logiciel dédié pour détecter les faiblesses dans votre système

2/ je propose un exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé :

1. Pour un ordinateur Windows :
 - Téléchargez un antivirus fiable tel que Bitdefender, Norton ou Kaspersky.
 - Installez le logiciel en suivant les instructions.
 - Une fois l'installation terminée, effectuez une analyse complète de votre ordinateur.
 - Si des menaces sont détectées, suivez les instructions de l'antivirus pour les supprimer.
2. Pour un Mac :
 - Téléchargez un antivirus spécialement conçu pour les Mac tels que Bitdefender, Norton ou McAfee.
 - Installez le logiciel en suivant les instructions.
 - Une fois l'installation terminée, effectuez une analyse complète de votre ordinateur.
 - Si des menaces sont détectées, suivez les instructions de l'antivirus pour les supprimer.