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

Objectif : à la découverte de la sécurité sur internet

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

Pense à vérifier la sources 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 = www.bestcours.com Cours sécurité informatique gratuit en PDF
Article 2 = WWW.leblocnote.fr Les 5 grands principes de la sécurité
Article 3 = www.researchgate.net Etablissement Recevant du Public

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

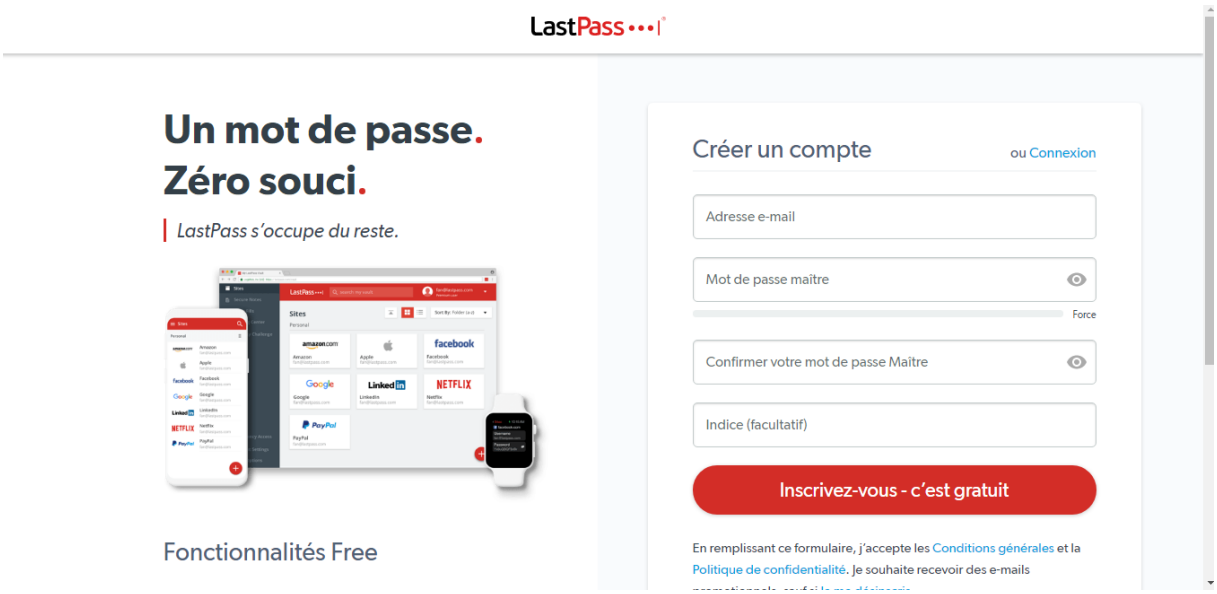
Beaucoup de notions traitées dans les articles sont également traitées dans le cours et des exercices y sont associés.

2 - Créer des mots de passe forts

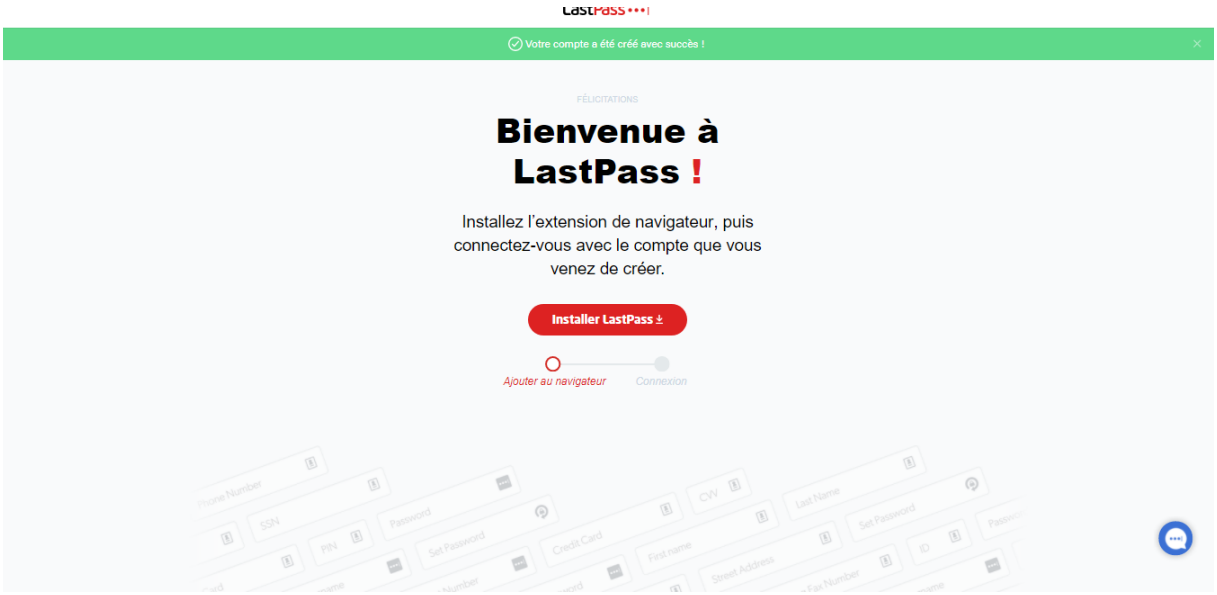
Objectif : utiliser un gestionnaire de mot de passe LastPass

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



● 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")

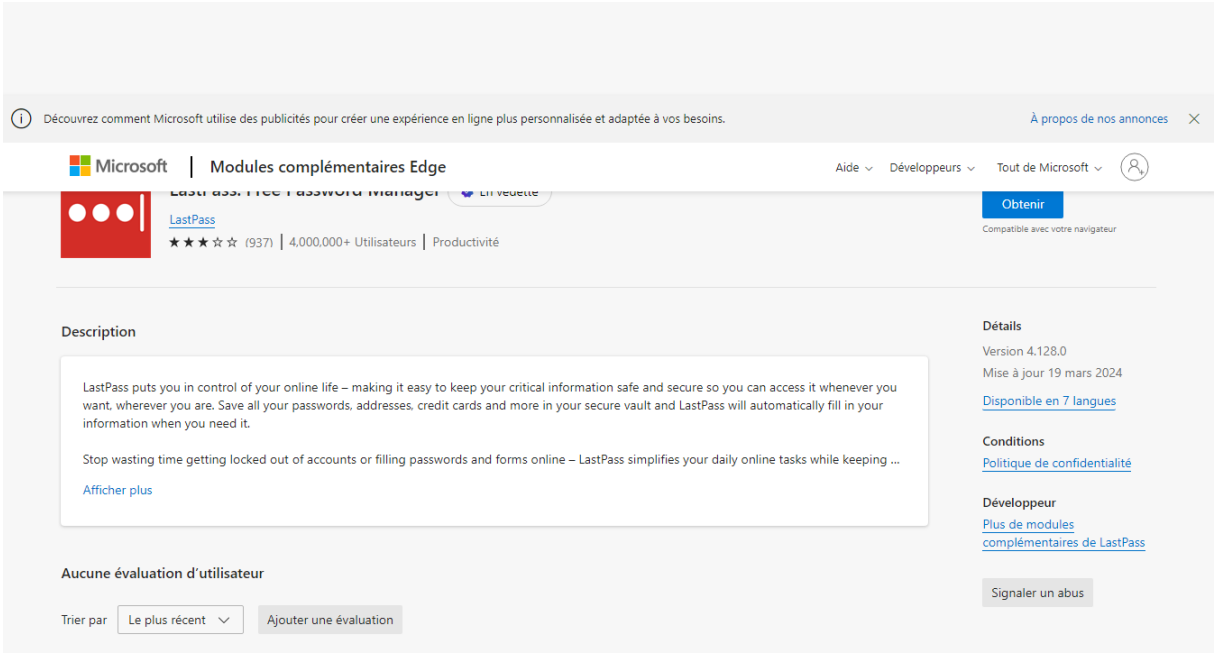
○ Tu peux également générer un mot de passe maître, mais pense à l'écrire dans un endroit sûr pour pouvoir l'utiliser lorsque tu en as besoin

● 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) Épingle 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.

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/ 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

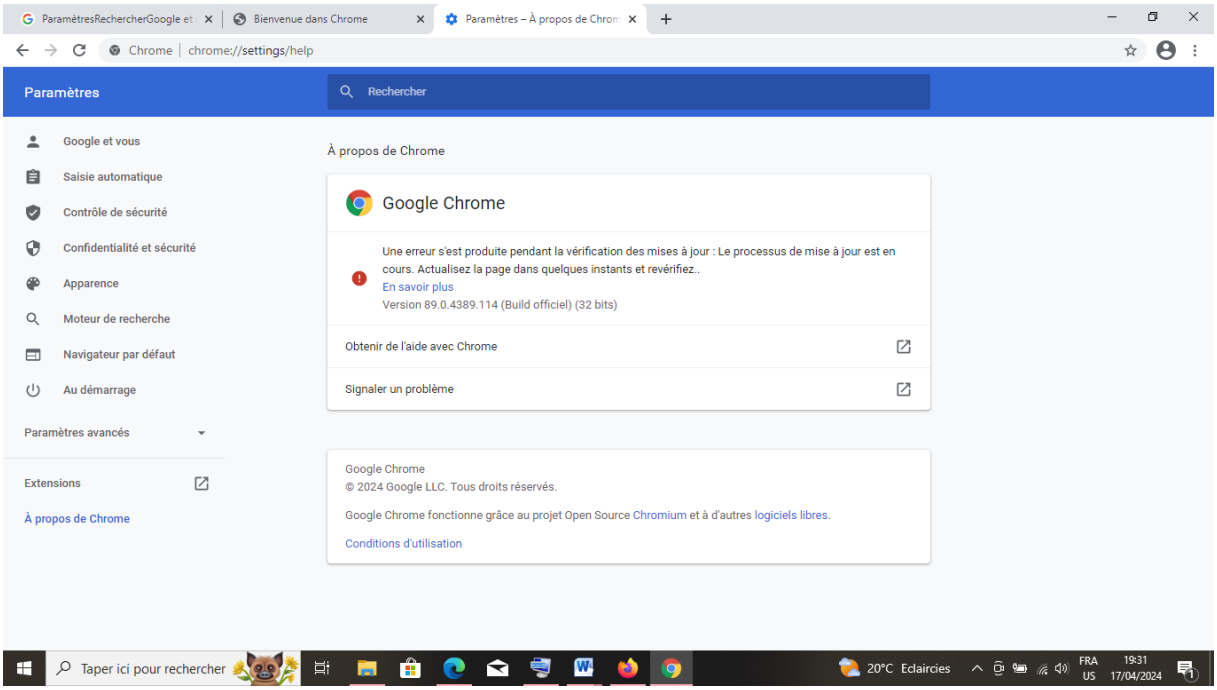
○ Ouvre le menu du navigateur et accède aux "Paramètres"

○ Clic sur la rubrique "A propose de Chrome"

○ Si tu constates le message "Chrome est à jour", c'est Ok

● Pour Firefox

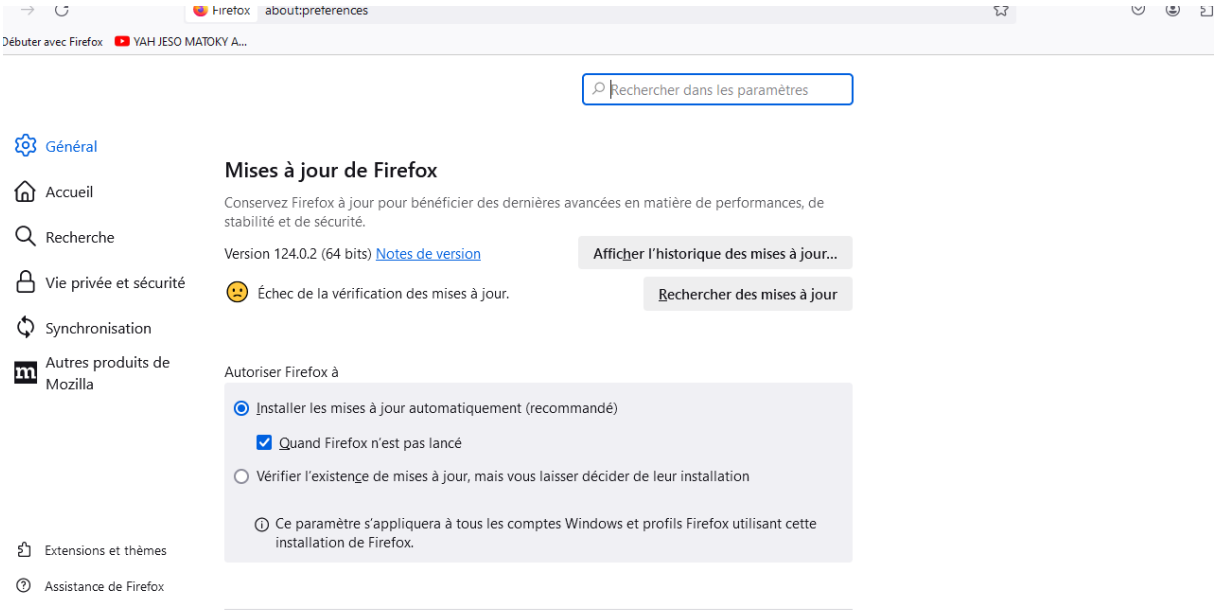
○ Ouvre le menu du navigateur et accède aux "Paramètres"



○ 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

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. **Site du gouvernement cybermalveillance.gouv.fr https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconn aitre-un-mail-de-phishing-ou-dhameconnage**

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

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/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

○ 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

○ 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 :

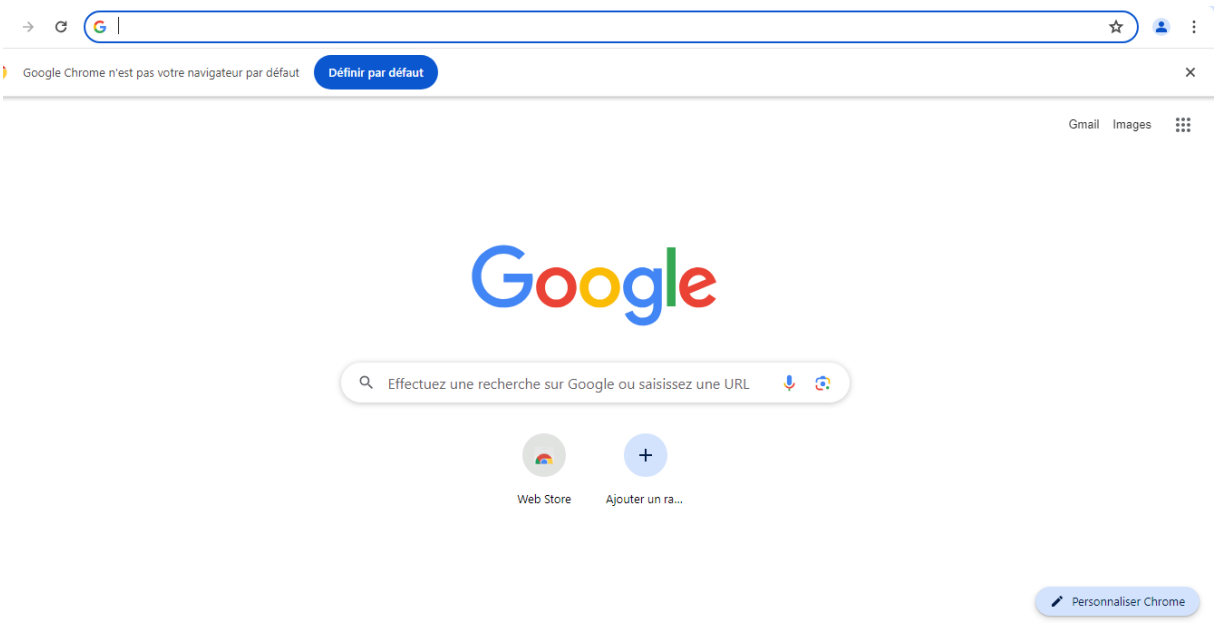
1. Créer un dossier sur ta messagerie électronique

2. Créer un dossier sur ton espace de stockage personnel (en local ou sur le

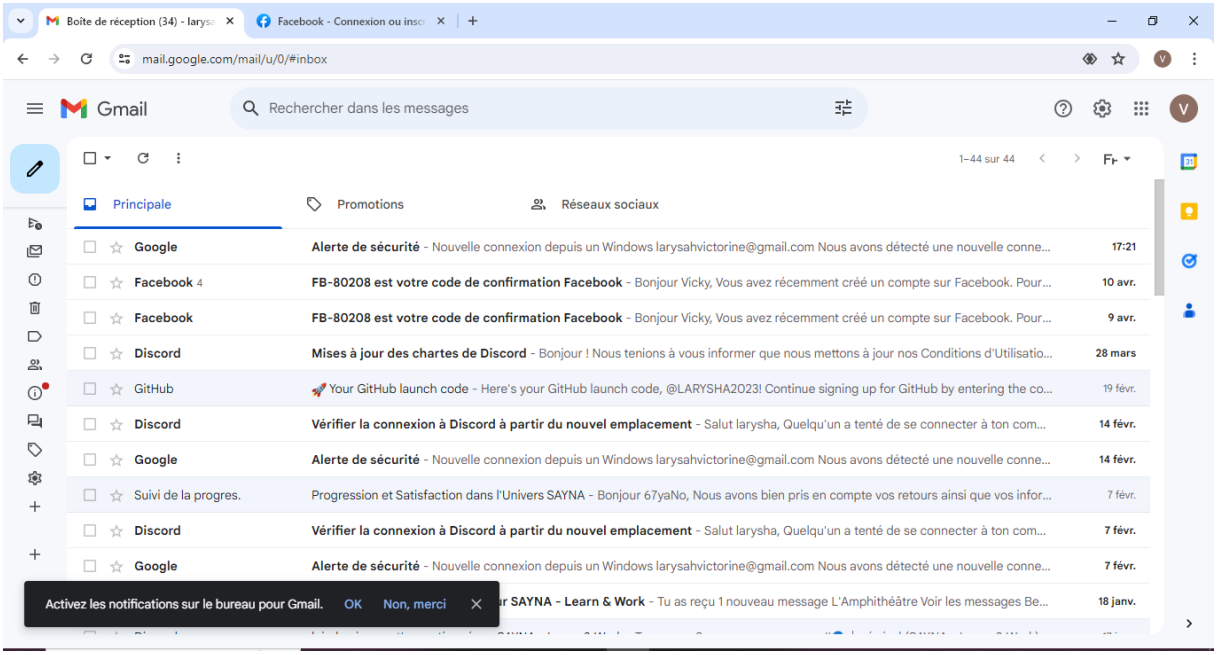
cloud)

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)

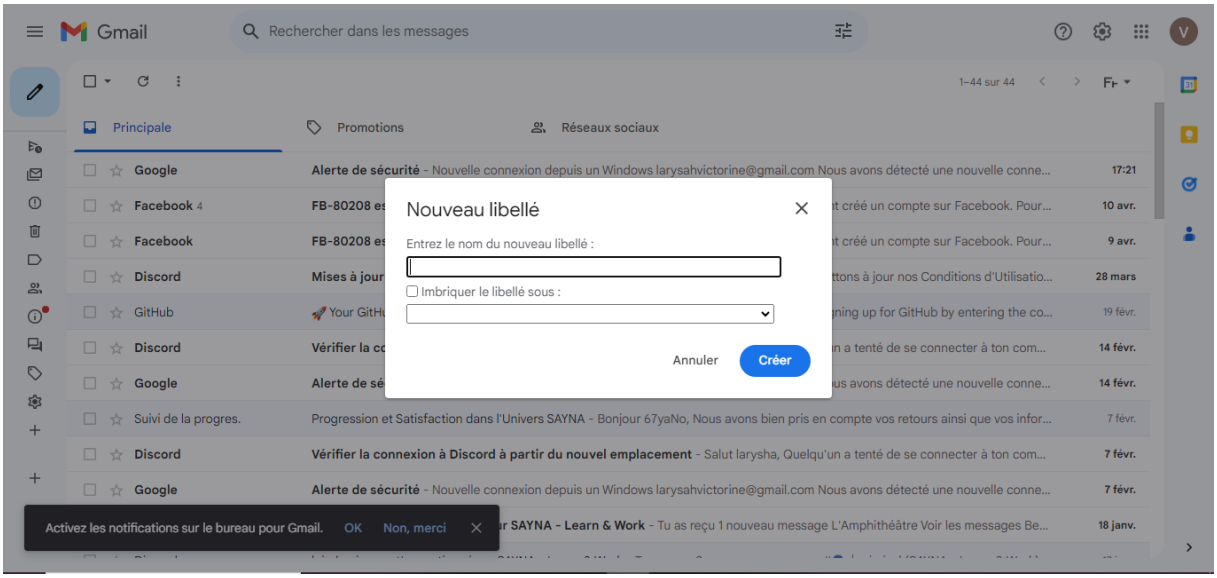
● Pour commencer, accède à ta messagerie électronique. Pour rappel, tu peux y accéder rapidement en ouvrant un nouvel onglet (dans la barre des favoris ou via le raccourci)



● Sur la page d'accueil de ta messagerie, tu trouveras sur la gauche les libellés initialement prévus (boite 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)

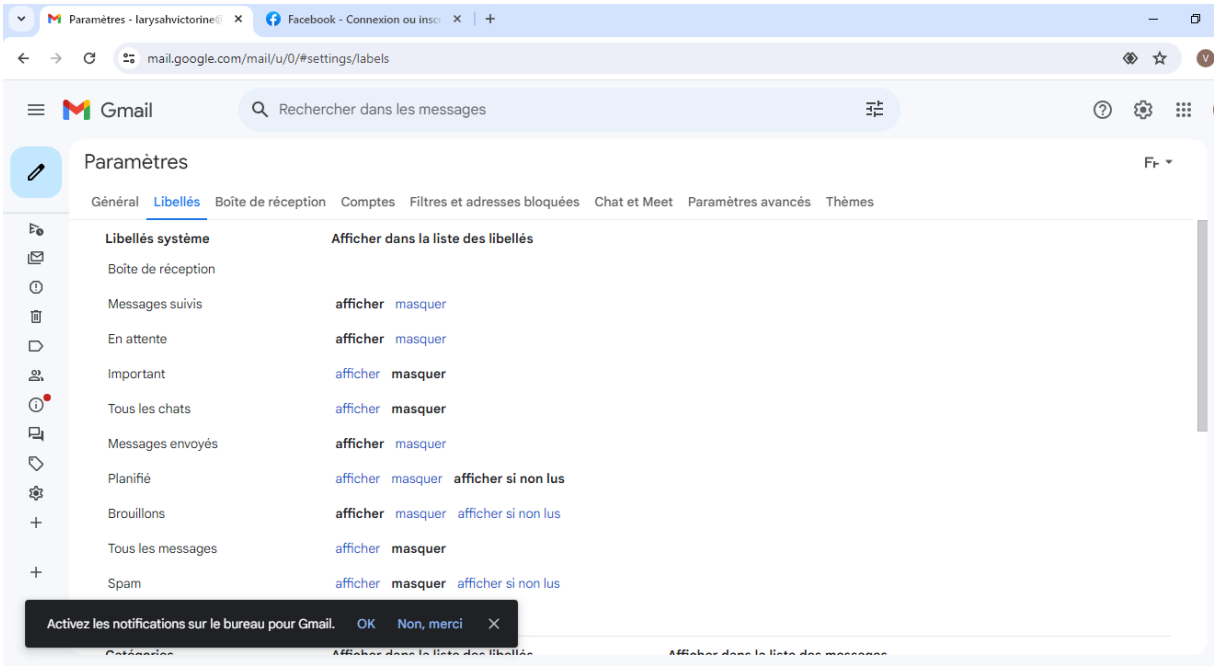


● Effectuer un clic sur le bouton “Créer” pour valider l’opération

● 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

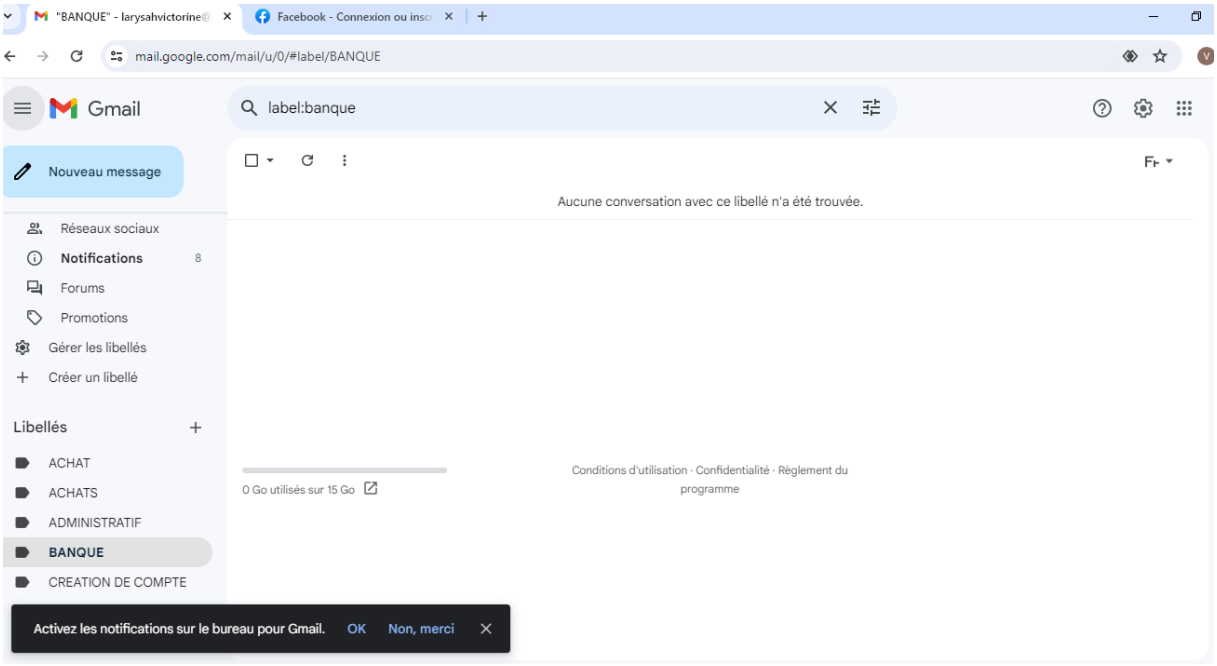
● Administratif : toutes les démarches administratives

● 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

médias sociaux

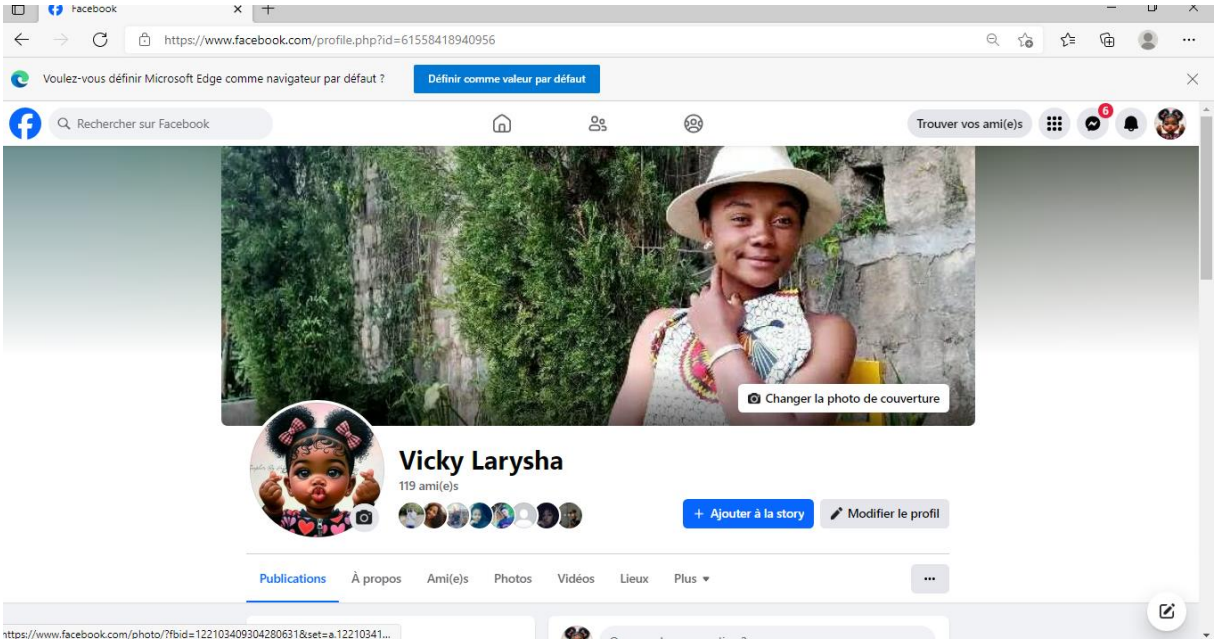
Objectif : Régler les paramètres de confidentialité de Facebook

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

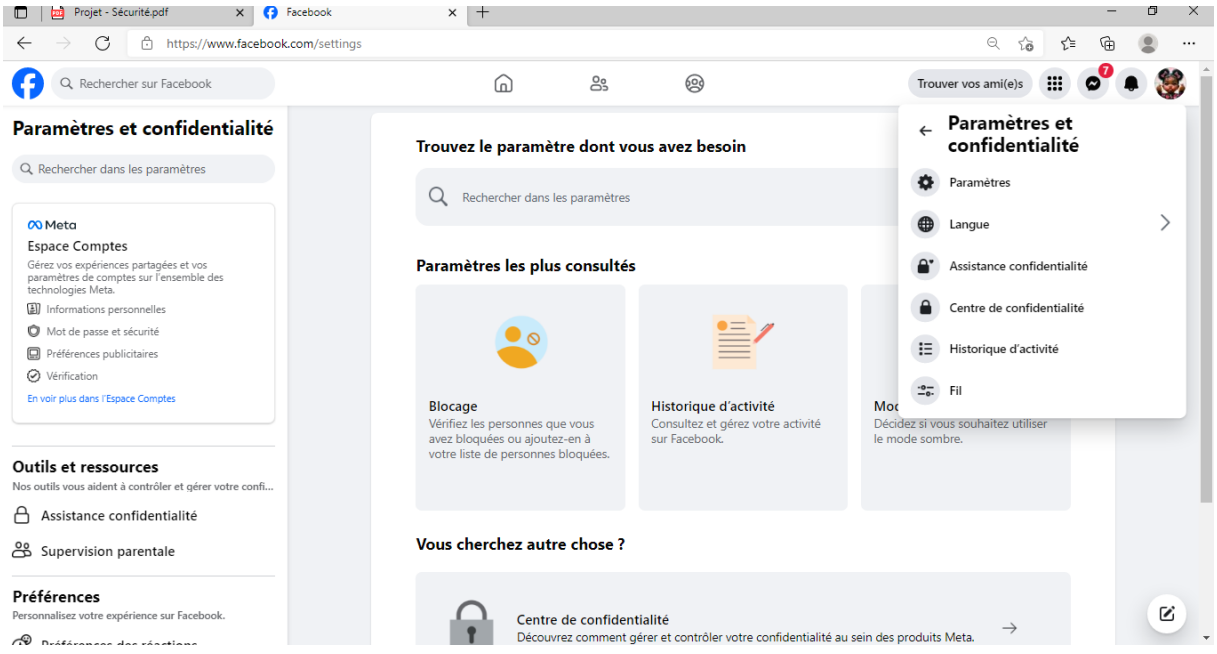
paramètres de confidentialité pour Facebook. Suis les étapes suivantes. (case à cocher)

● Connecte-toi à ton compte Facebook

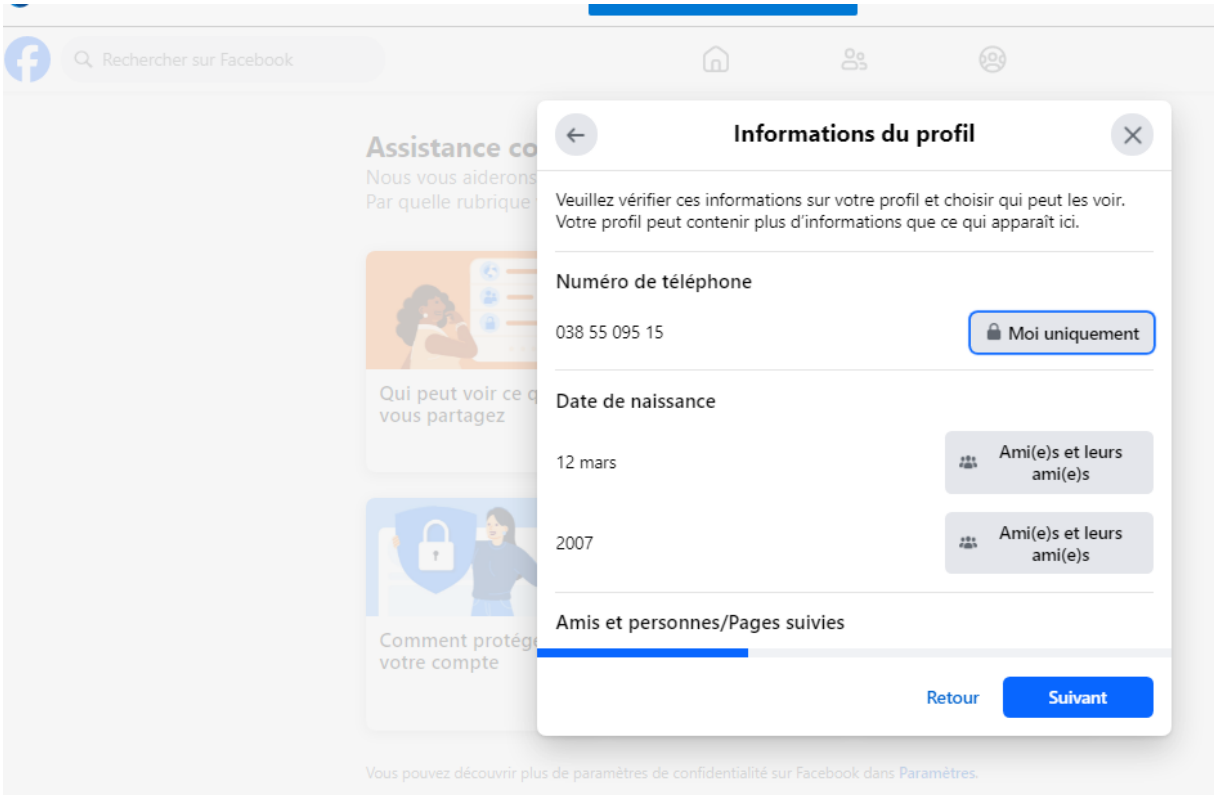


- UNE FOIS SUR LA PAGE D'ACCUEIL, OUVRE LE MENU FACEBOOK , PUIS EFFECTUE UN CLIC SUR

"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

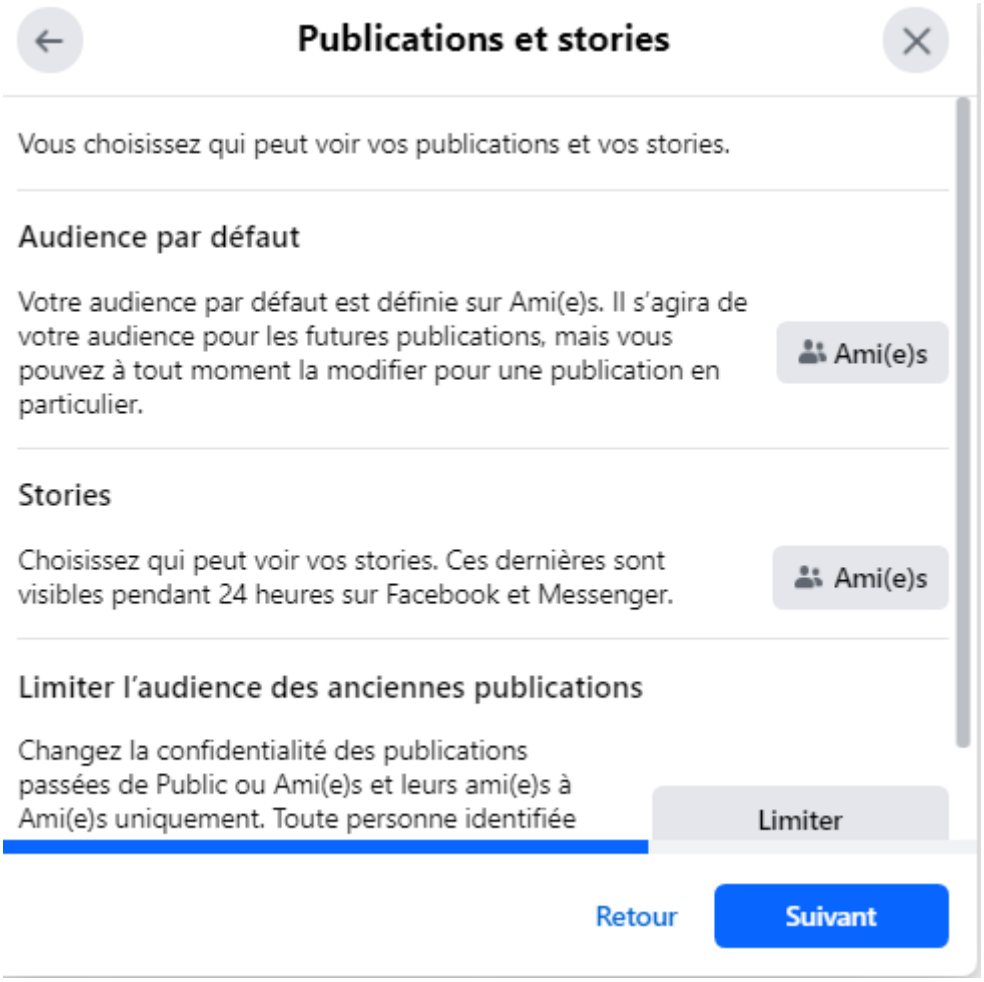
● Retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à gauche. Tu peux continuer à explorer les rubriques pour personnaliser tes

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 :

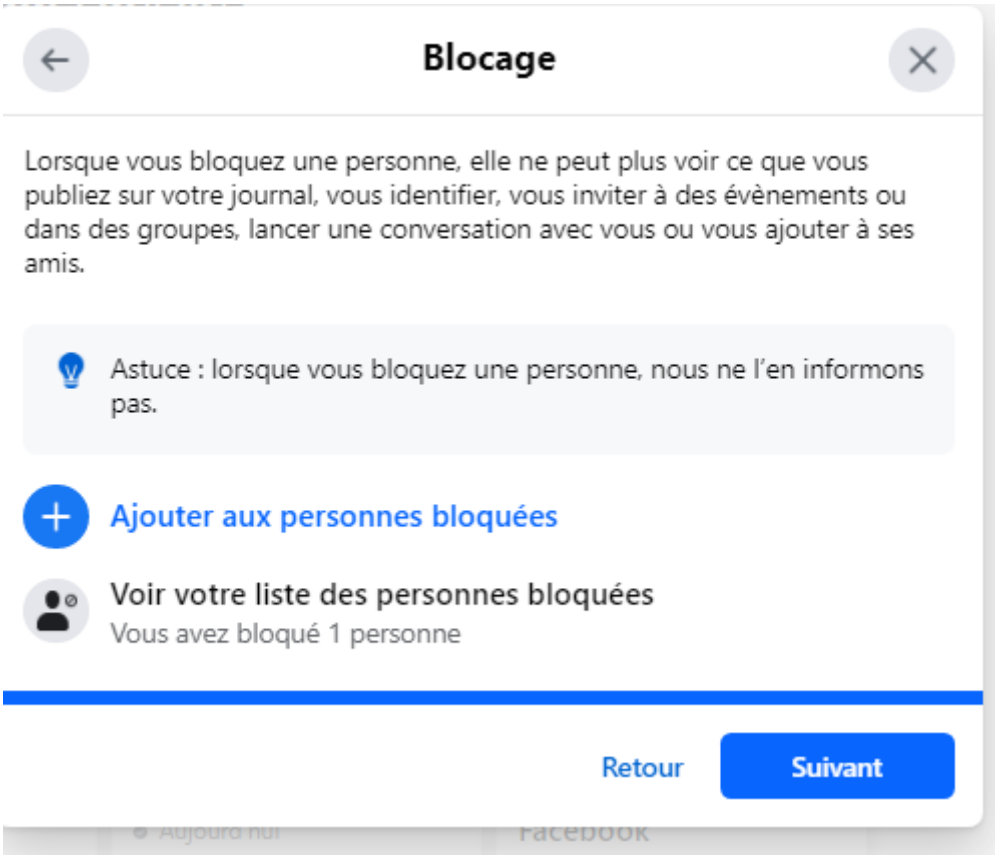
○ Si tu utilises ton compte Facebook uniquement pour communiquer avec tes amis, règles les paramètres en conséquence en choisissant une visibilité "Amis" ou "Amis de leurs amis".

○ 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. **Analyse des autorisations des applications** : Passez en revue les autorisations accordées à chaque application installée sur votre smartphone. Demandez-vous si chaque application a vraiment besoin des autorisations demandées pour fonctionner correctement. Si une application demande des autorisations excessives ou non pertinentes, envisagez de la désinstaller ou de limiter ses autorisations.
2. **Test des réglages de confidentialité** : Explorez les paramètres de confidentialité de votre smartphone et assurez-vous qu'ils sont configurés de manière à protéger vos données personnelles. Vérifiez les autorisations des applications, les paramètres de localisation, les options de partage de données, etc.
3. **Analyse des connexions réseau** : Utilisez des outils ou des applications de sécurité réseau pour analyser les connexions actives sur votre smartphone. Assurez-vous qu'il n'y a pas de connexions suspectes ou non autorisées en cours et que seuls les appareils et les réseaux approuvés y ont accès.
4. **Test de vulnérabilité des réseaux sans fil** : Utilisez un scanner de réseau sans fil pour détecter les réseaux Wi-Fi à proximité de votre smartphone. Vérifiez s'il y a des réseaux non sécurisés ou potentiellement malveillants à éviter, et assurez-vous que votre smartphone ne se connecte qu'à des réseaux Wi-Fi sécurisés et fiables.
5. **Évaluation des applications tierces** : Si vous avez des applications provenant de sources tierces (c'est-à-dire en dehors du Google Play Store pour Android ou de l'App Store pour iOS), examinez-les attentivement pour détecter les signes de logiciels malveillants ou de comportements suspects. Évitez de télécharger des applications à partir de sources non fiables.
6. **Test de phishing et de sécurité des e-mails** : Envoyez-vous un e-mail de test de phishing à partir d'un compte sécurisé vers votre propre adresse e-mail. Vérifiez si votre smartphone détecte l'e-mail comme une tentative de phishing et si les mesures de sécurité appropriées sont en place pour vous protéger.
7. **Analyse des comportements inhabituels** : Soyez attentif aux signes de comportements inhabituels ou suspects sur votre smartphone, tels que des performances lentes, une durée de vie de la batterie anormalement courte, des pop-ups indésirables, des applications qui se ferment inopinément, etc. Ces signes pourraient indiquer une infection par un logiciel malveillant.
8. **Sauvegarde des données et plan de récupération** : Assurez-vous que vos données importantes sont sauvegardées régulièrement sur une autre source sécurisée, comme un stockage cloud chiffré. Avoir un plan de récupération des données en cas de perte ou de vol de votre smartphone est essentiel pour garantir que vos informations importantes ne sont pas perdues définitivement.

En effectuant ces exercices régulièrement, vous pouvez évaluer et renforcer la sécurité de votre smartphone, réduisant ainsi les risques d'exploitation et de compromission de vos données personnelles.

2 / P r o p o s e r u n e x e r cic e p o u r in s t alle r e t u tilis e r u n a n tivir u s + a n tim alw a r e e n fo n c tio n d e l'appareil utilisé

1. **Choisir un logiciel antivirus/antimalware** : Il existe de nombreux programmes antivirus et antimalware disponibles sur le marché. Faites des recherches pour trouver celui qui correspond le mieux à vos besoins et à votre budget. Des exemples populaires incluent Avast, Norton, Bitdefender, Kaspersky, Malwarebytes, et Windows Defender (intégré à Windows 10).
2. **Télécharger et installer le logiciel** : Rendez-vous sur le site web du fournisseur de l'antivirus que vous avez choisi et téléchargez la version appropriée pour votre système d'exploitation (Windows, macOS, Linux, etc.). Suivez les instructions d'installation fournies par le programme d'installation pour installer le logiciel sur votre ordinateur.
3. **Mise à jour du logiciel** : Une fois installé, assurez-vous de mettre à jour votre logiciel antivirus/antimalware pour obtenir les dernières définitions de virus et les mises à jour de sécurité. La plupart des programmes ont une fonction de mise à jour automatique que vous pouvez activer.
4. **Analyse initiale du système** : Après l'installation, lancez une analyse complète de votre système pour détecter et supprimer tout logiciel malveillant déjà présent. Cette analyse peut prendre un certain temps en fonction de la taille de votre disque dur et du nombre de fichiers à analyser.
5. **Planifier des analyses régulières** : Configurez votre logiciel antivirus/antimalware pour effectuer des analyses régulières de votre système, par exemple une fois par semaine. Cela vous aidera à détecter rapidement tout nouveau logiciel malveillant qui pourrait infecter votre ordinateur.
6. **Surveillance en temps réel** : Activez la fonction de surveillance en temps réel de votre logiciel antivirus/antimalware pour détecter et bloquer les menaces en temps réel pendant que vous utilisez votre ordinateur.
7. **Analyse des téléchargements et des pièces jointes** : Avant d'ouvrir ou d'exécuter tout fichier téléchargé ou pièce jointe à un e-mail, analysez-le d'abord avec votre logiciel antivirus/antimalware pour vous assurer qu'il est sûr.
8. **Mises à jour du système d'exploitation et des applications** : Assurez-vous que votre système d'exploitation et toutes vos applications sont régulièrement mis à jour avec les derniers correctifs de sécurité pour réduire les risques d'exploitation de vulnérabilités.
9. **Prudence lors de la navigation sur Internet** : Soyez prudent lorsque vous naviguez sur Internet et évitez de cliquer sur des liens suspects ou de télécharger des fichiers à partir de sources non fiables.

En suivant ces étapes, vous pourrez installer et utiliser un logiciel antivirus/antimalware efficace pour protéger votre ordinateur contre les logiciels malveillants et autres menaces en ligne.

Pour smartphone.

1. **Choisir une application antivirus/antimalware** : Tout d'abord, recherchez une application antivirus/antimalware fiable sur le magasin d'applications de votre smartphone. Assurez-vous de choisir une application bien notée et réputée pour sa capacité à détecter et à supprimer les logiciels malveillants.
2. **Télécharger et installer l'application** : Une fois que vous avez choisi une application, téléchargez-la et installez-la sur votre smartphone en suivant les instructions fournies par le magasin d'applications.
3. **Configurer l'application** : Après l'installation, ouvrez l'application antivirus/antimalware et suivez les instructions pour la configurer selon vos préférences. Cela peut inclure des

paramètres tels que la planification des analyses, l'activation de la protection en temps réel et la configuration des notifications.

4. **Mettre à jour l'application** : Assurez-vous de maintenir l'application antivirus/antimalware à jour en téléchargeant les dernières mises à jour disponibles dans le magasin d'applications. Les mises à jour régulières garantissent que votre application dispose des dernières définitions de virus et des fonctionnalités de sécurité les plus récentes.
5. **Lancer une analyse initiale** : Après avoir configuré l'application, lancez une analyse complète de votre smartphone pour détecter et supprimer tout logiciel malveillant potentiellement présent. Cette analyse peut prendre un certain temps en fonction de la capacité de stockage de votre téléphone et du nombre de fichiers à analyser.
6. **Planifier des analyses régulières** : Configurez l'application antivirus/antimalware pour effectuer des analyses régulières de votre smartphone, par exemple une fois par semaine. Cela vous aidera à détecter rapidement tout nouveau logiciel malveillant qui pourrait infecter votre appareil.
7. **Surveillance en temps réel** : Activez la fonction de surveillance en temps réel de l'application antivirus/antimalware pour détecter et bloquer les menaces en temps réel pendant que vous utilisez votre smartphone.
8. **Analyser les nouvelles applications** : Avant d'installer de nouvelles applications sur votre smartphone, analysez-les d'abord avec votre application antivirus/antimalware pour vous assurer qu'elles sont sûres et exemptes de logiciels malveillants.
9. **Mettre à jour le système d'exploitation et les applications** : Assurez-vous que votre système d'exploitation et toutes vos applications sont régulièrement mis à jour avec les derniers correctifs de sécurité pour réduire les risques d'exploitation de vulnérabilités.

En suivant ces étapes, vous pourrez installer et utiliser efficacement un antivirus/antimalware sur votre smartphone pour protéger vos données personnelles et votre vie privée contre les menaces en ligne.