**Parcours : DISCOVERY**
**Module : Naviguer en toute**

**Sécurité**

# Projet 1 - Un peu plus desécurité, on n'en a jamais assez !

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 = 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 = 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

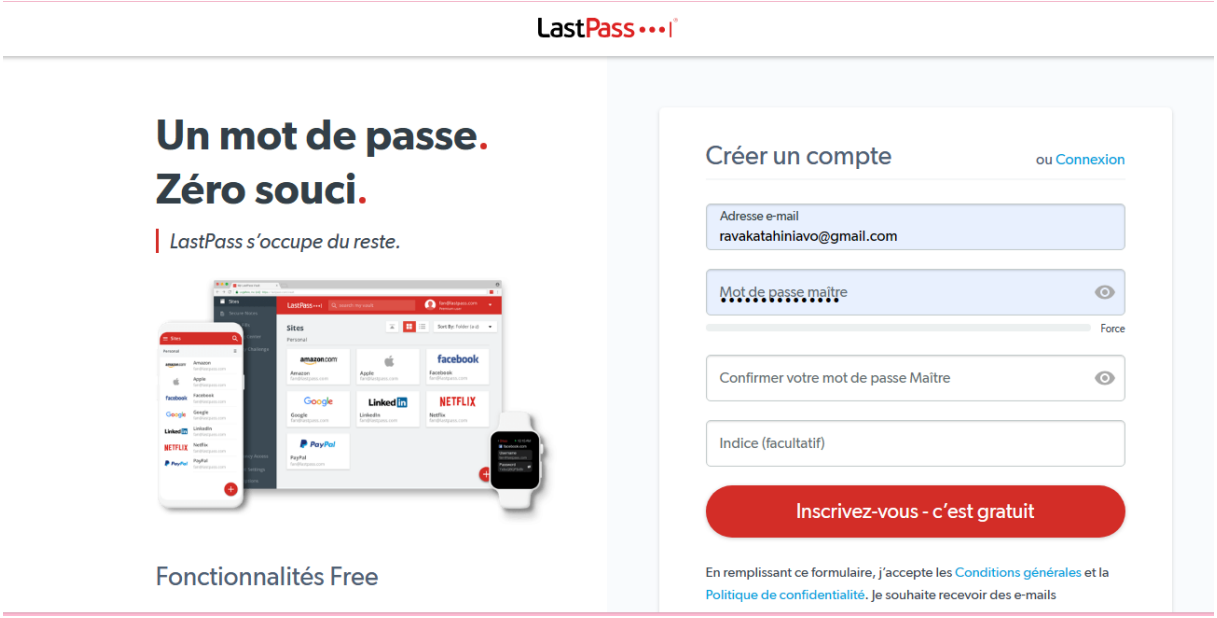
Beaucoup de notions traitées dans les articles sont également traitées dans le cours et des exercices y sont associés.

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



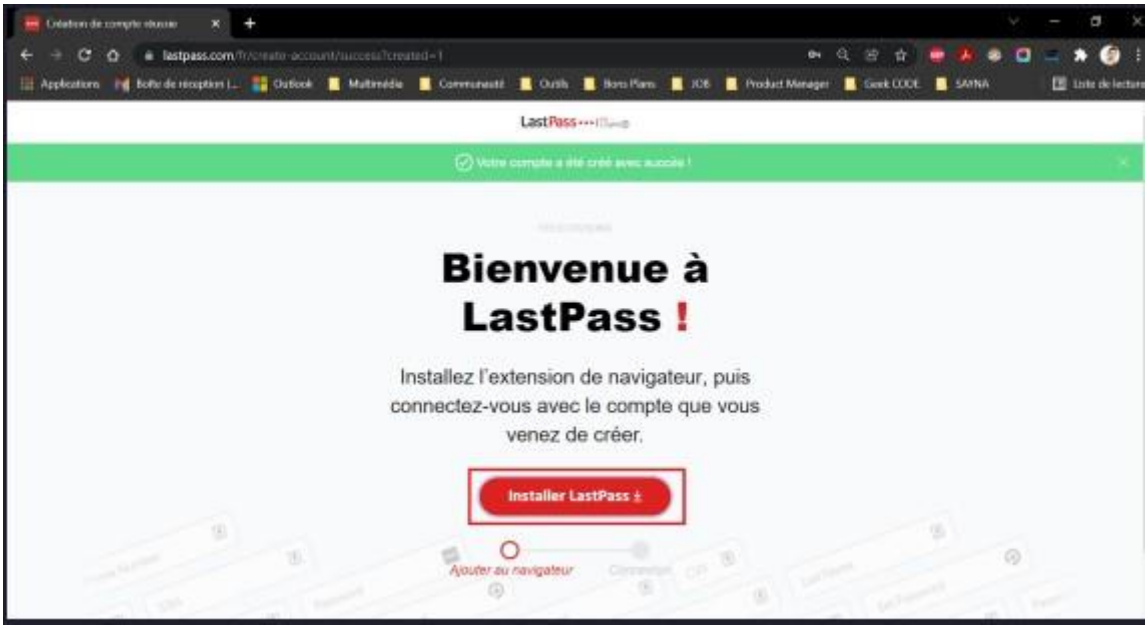

● Crée un compte en remplissant le formulaire. Un conseil, on te demande de choisir un mot de passe maître. Pour rappel, ce mot de passe sera unique et te permettra d'accéder à tous tes comptes. Choisis donc un mot de passe avec un niveau de sécurité élevé et assure-toi de pouvoir le retrouver

○ 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



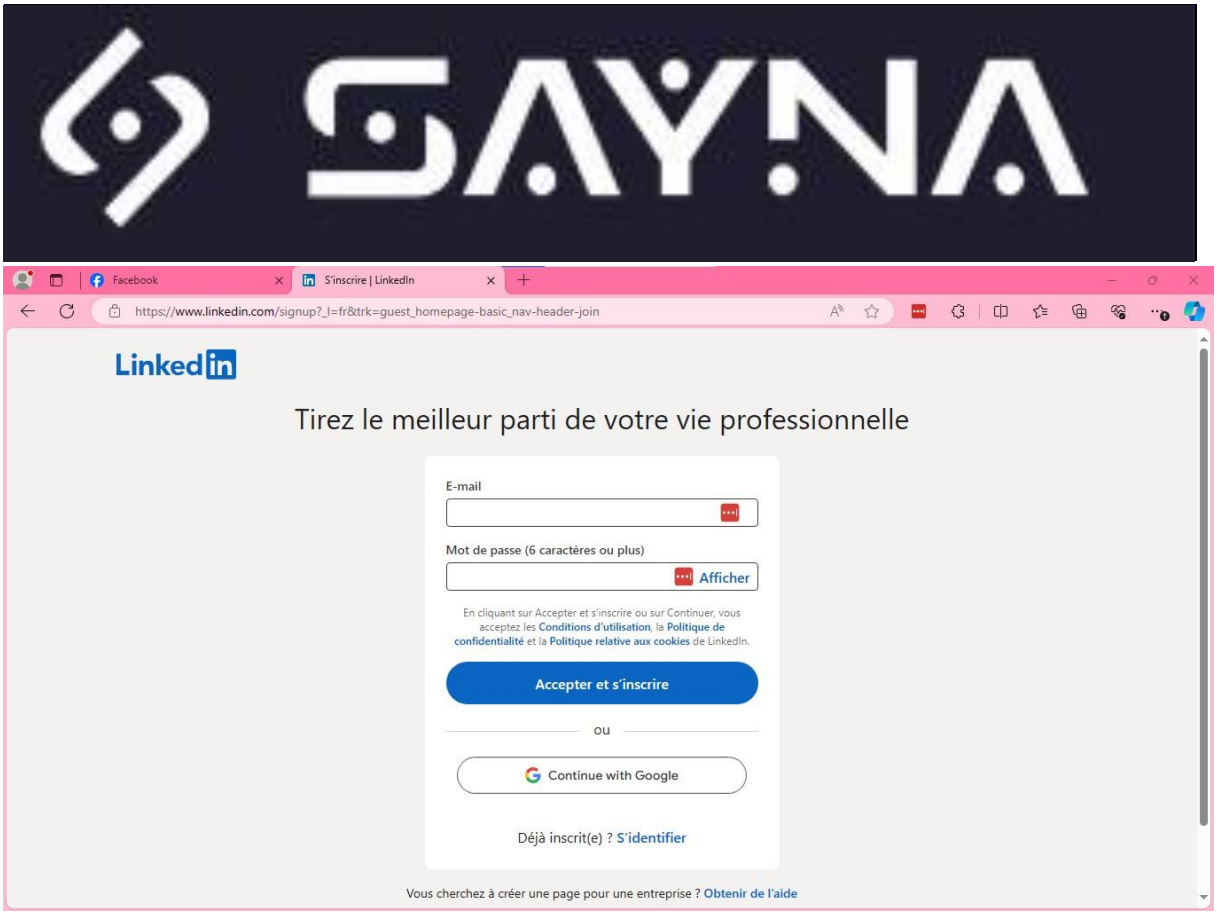

● Il te suffit de valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome"

● 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

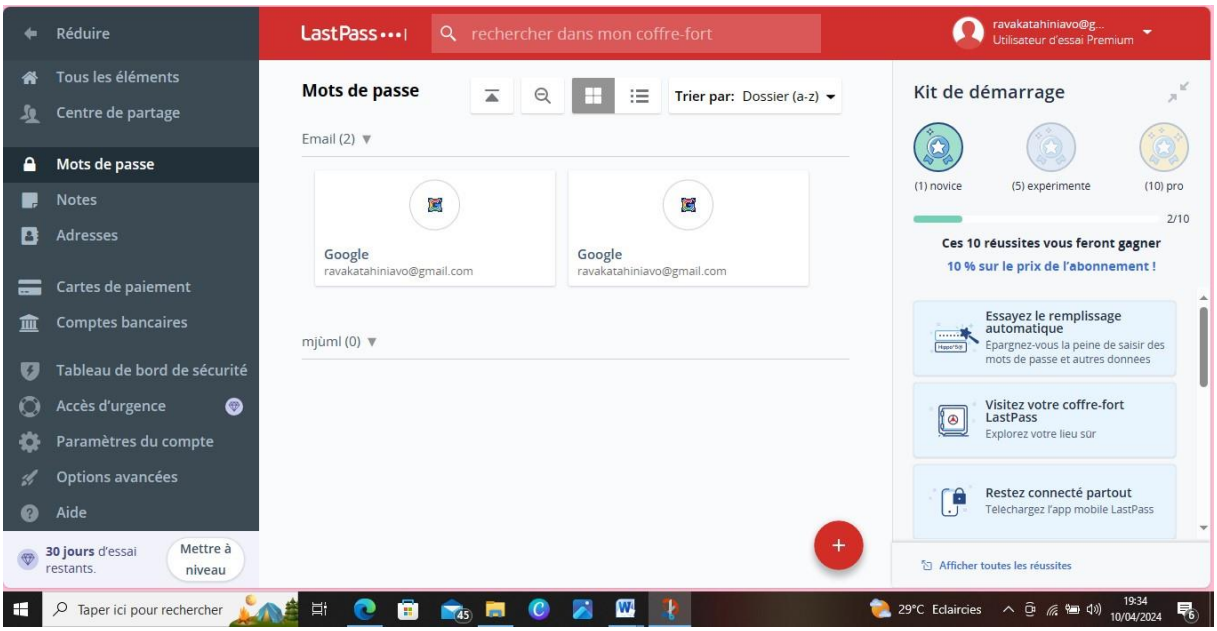



Réponse 1

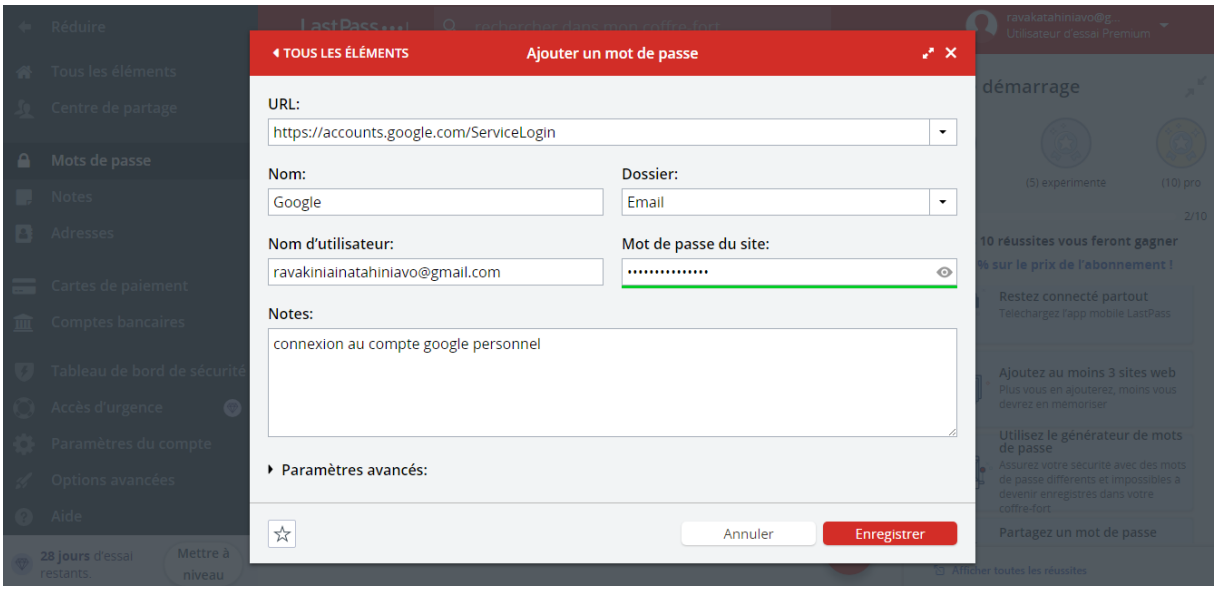
Désormais, lorsque tu te connectes à tes comptes, tu peux enregistrer le mot de passe grâce à LastPass.

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.

(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, 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)

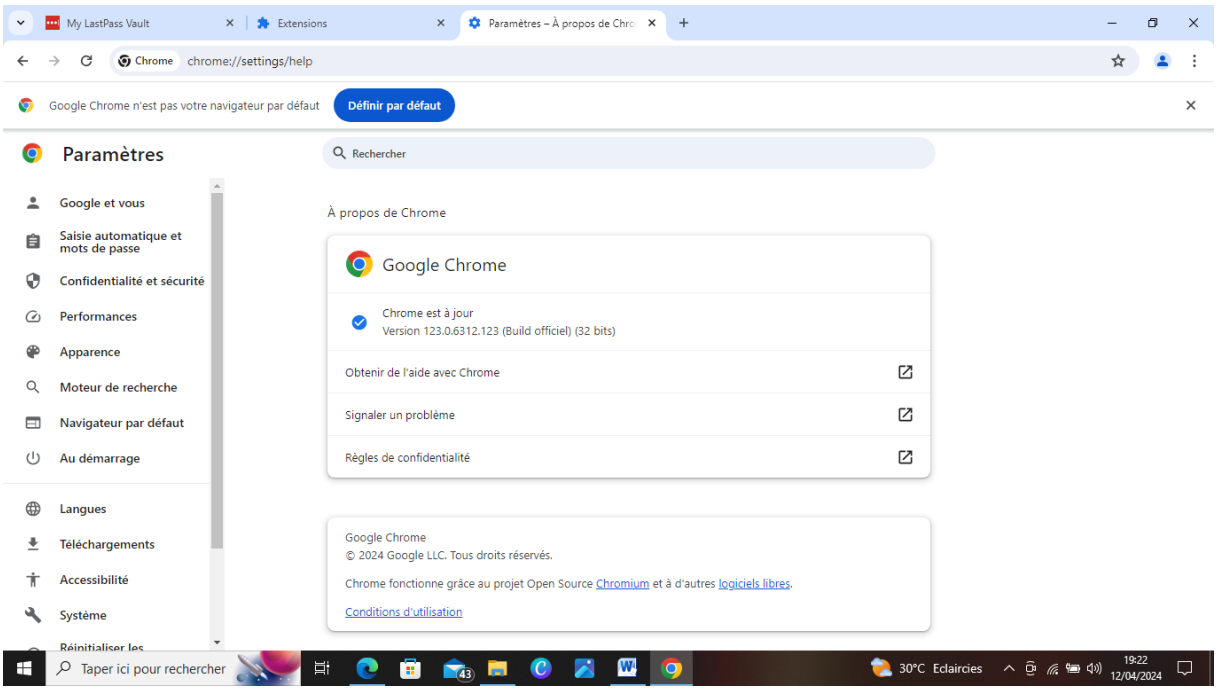
2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes. (case àcocher)

● 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



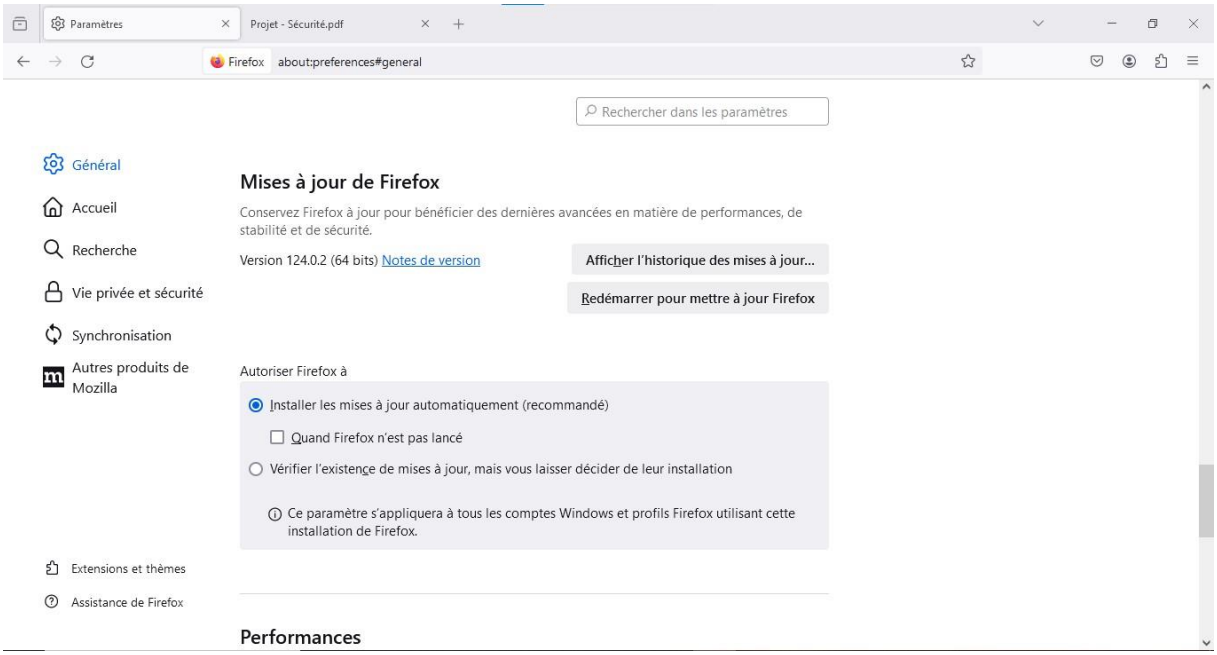

● Pour Firefox

○ 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.

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-reconn

aitre-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 lecloud)

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)

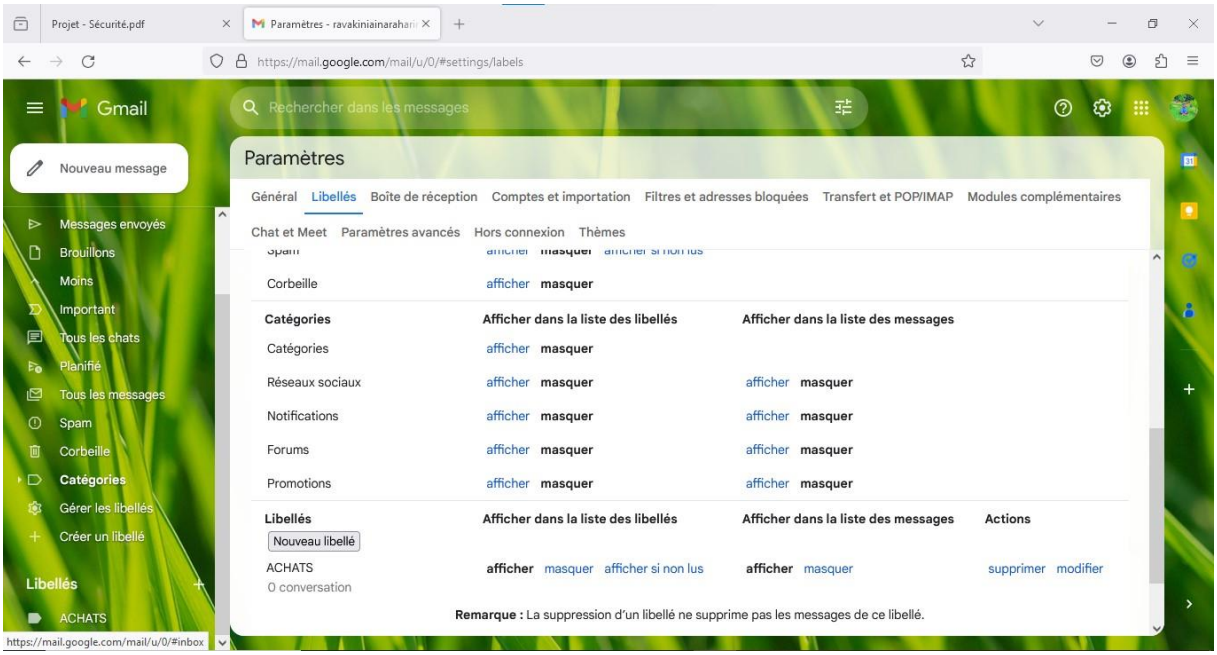
● Sur la page d'accueil de ta messagerie, tu trouveras sur la gauche les libellés initialement prévus (boite de réception, messages envoyés, etc.)

● 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

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

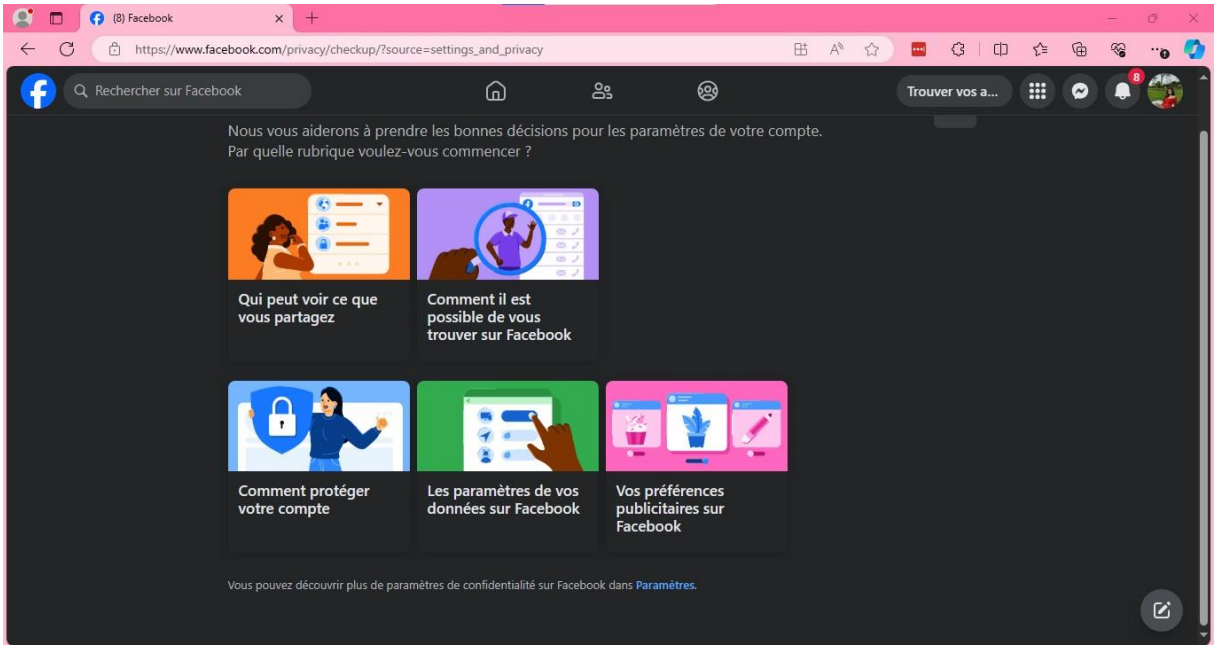
○ La deuxième rubrique (bleu) te permet de changer ton mot de passe

○ 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, 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"

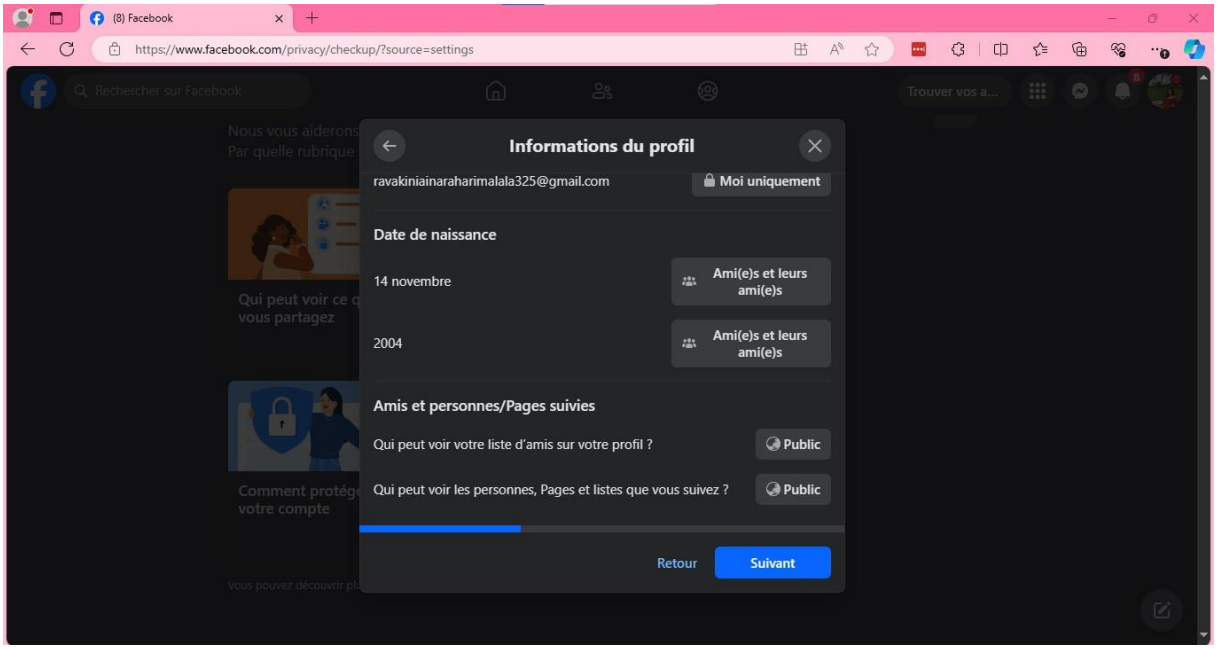
● Dans les paramètres de Facebook tu as également un onglet "Cookies". On t'en a parlé dans le cours précédent (Comprendre le suivi du navigateur). Maintenant que

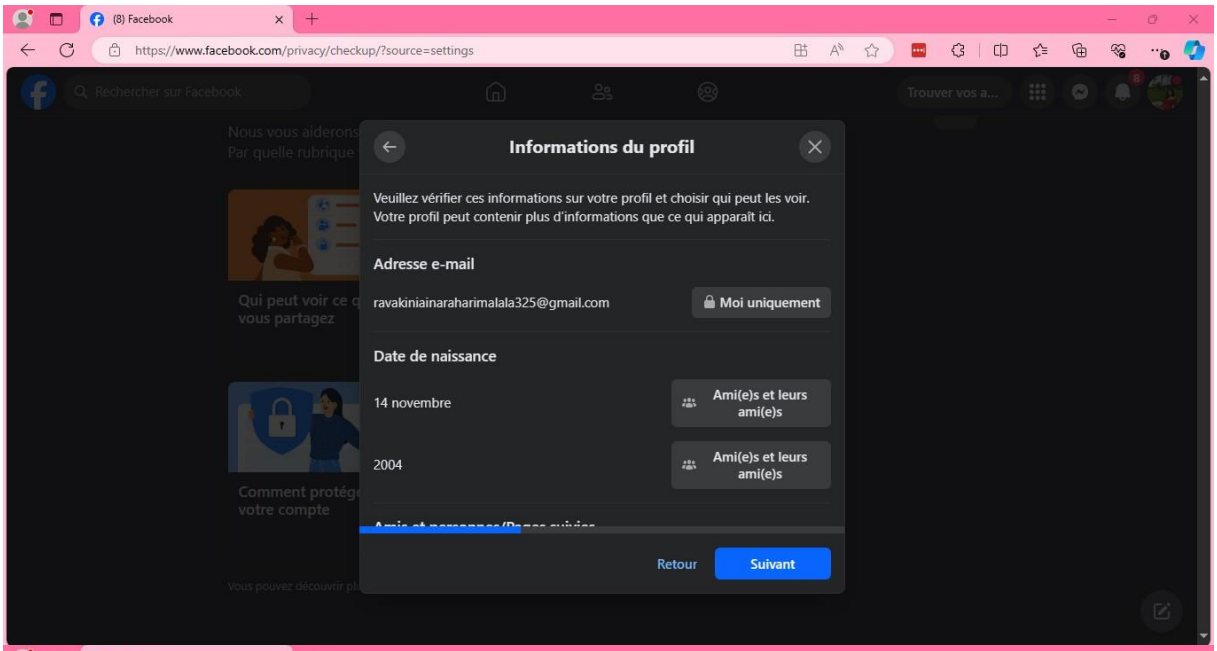
tu sais comment sont utilisées tes données, tu es capable de choisir en pleine conscience ce que tu souhaites partager.

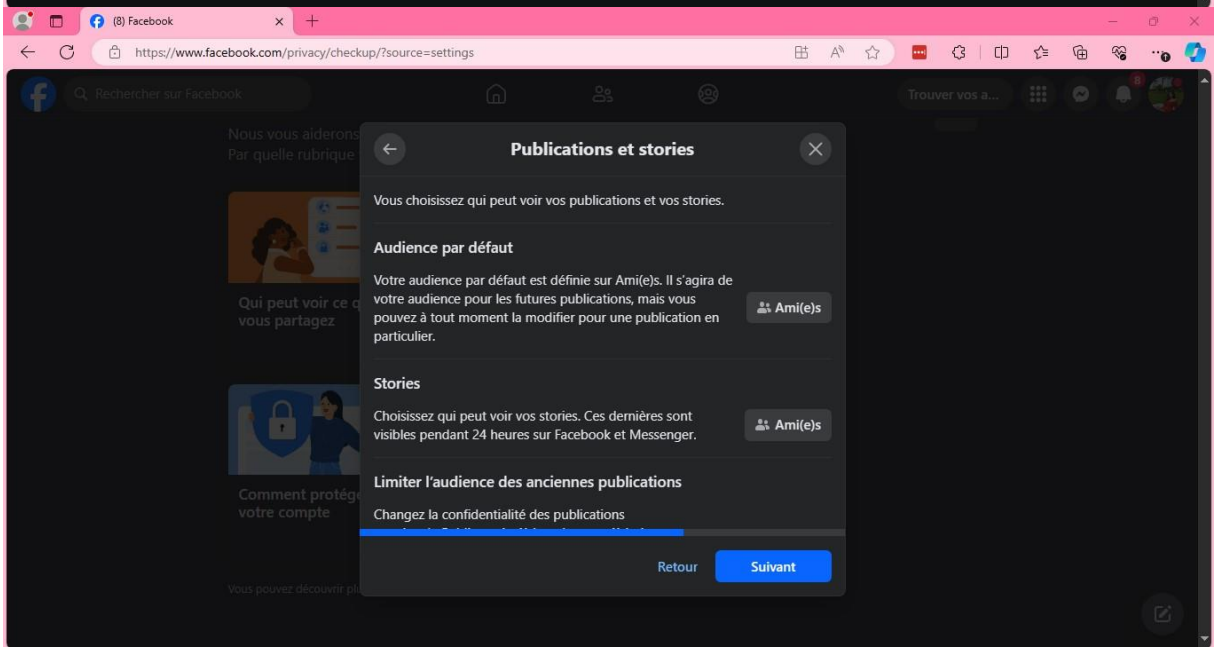
Réponse 1

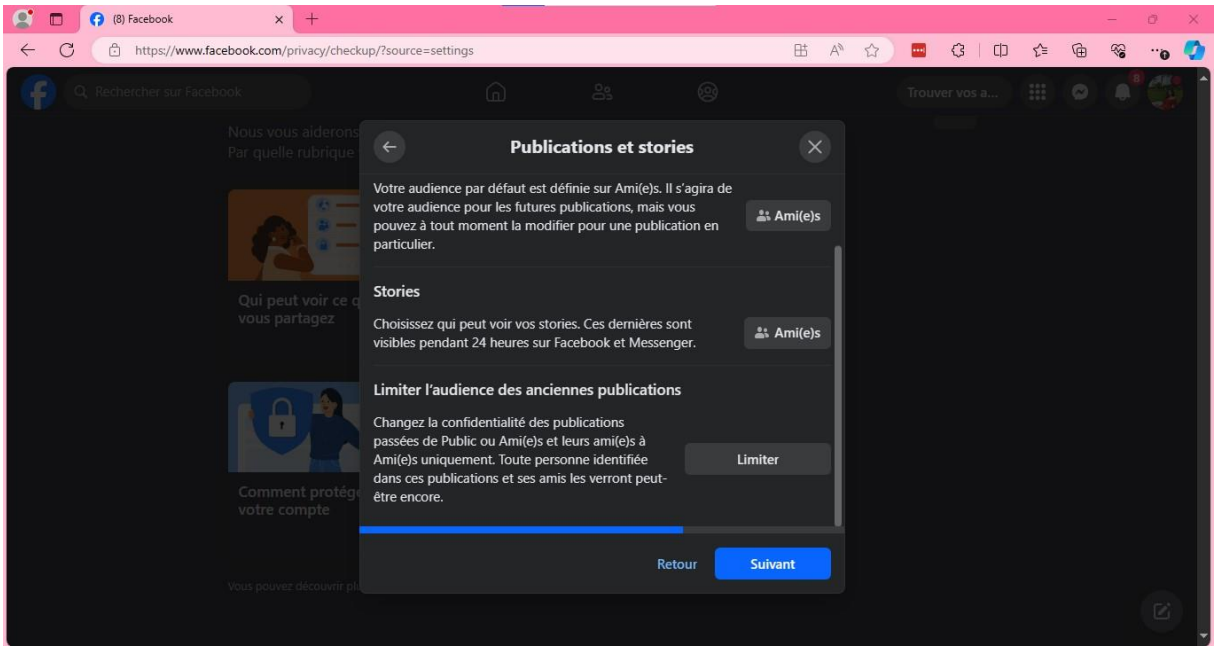
Voici un exemple de paramétrage de compte Facebook pour une utilisation privilégiant les échanges avec les amis, mais autorisant le contact avec des inconnus (limite de leurs actions) :

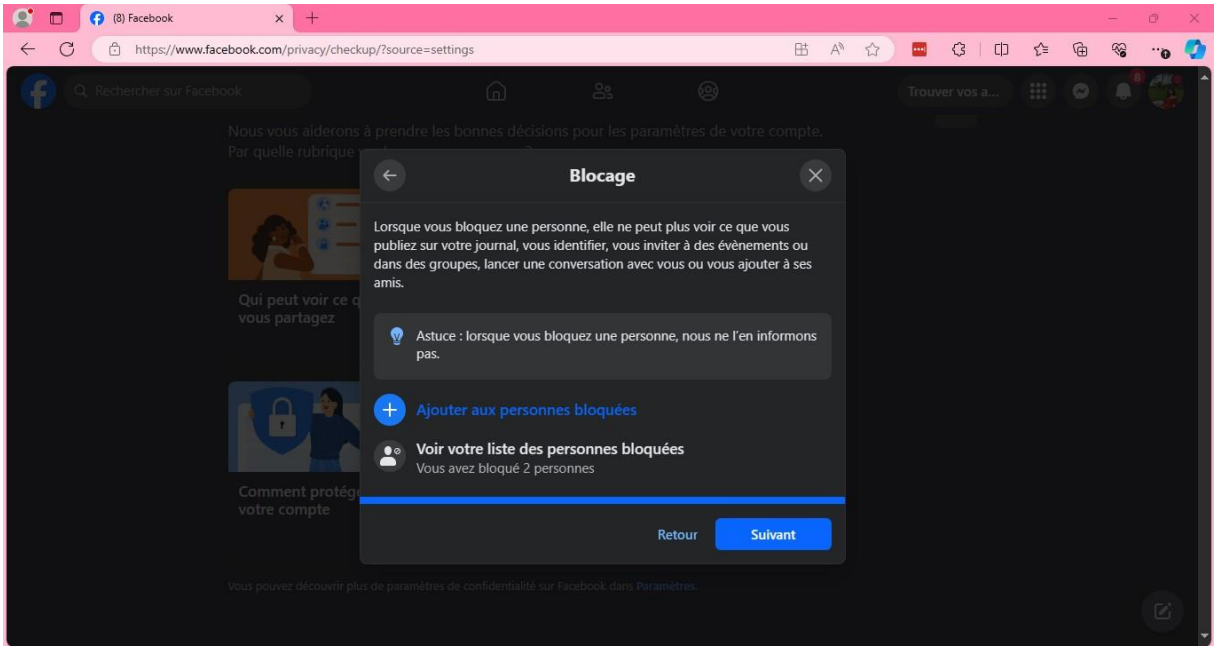
● Confidentialité




(8) Facebook
https://www.facebook.com/privacy/checkup/?source=settings
Rechercher sur Facebook
Trouver vos a...
Nous vous aiderons
Par quelle rubrique
Qui peut voir ce q
vous partagez
Comment protég
votre compte
Vous pouvez découvrir pl
Informations du profil
Veuillez vérifier ces informations sur votre profil et choisir qui peut les voir. Votre profil peut contenir plus d'informations que ce qui apparaît ici.
Adresse e-mail
ravakiniainaraharimalala325@gmail.com
Moi uniquement
Date de naissance
14 novembre
Ami(e)s et leurs ami(e)s
2004
Ami(e)s et leurs ami(e)s
Retour
Suivant


(8) Facebook
https://www.facebook.com/privacy/checkup/?source=settings
Rechercher sur Facebook
Trouver vos a...
Nous vous aiderons
Par quelle rubrique
Qui peut voir ce q
vous partagez
Comment protég
votre compte
Vous pouvez découvrir pl
Publications et stories
Vous choisissez qui peut voir vos publications et vos stories.
Audience par défaut
Votre audience par défaut est définie sur Ami(e)s. Il s'agira de votre audience pour les futures publications, mais vous pouvez à tout moment la modifier pour une publication en particulier.
Ami(e)s
Stories
Choisissez qui peut voir vos stories. Ces dernières sont visibles pendant 24 heures sur Facebook et Messenger.
Ami(e)s
Limiter l'audience des anciennes publications
Changez la confidentialité des publications
Retour
Suivant




● 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/ exercice pour vérifier la sécurité en fonction de l'appareil :

Pour un smartphone :

- Vérifiez les applications
- Vérifiez les permissions
- Recherchez les mises à jours
- Scannez avec un logiciel antivirus
- Vérifiez qu'il n'y ait pas de fuites de données

Pour un ordinateur :

- Analyse antivirus : Exécutez un scan complet avec un logiciel antivirus à jour pour détecter les éventuelles infections par des logiciels malveillants.
- Test des ports ouverts : Utilisez un outil de scan de ports pour vérifier qu'aucun port non nécessaire n'est ouvert sur votre ordinateur.
- Vérification des mises à jour : Assurez-vous que votre système d'exploitation, vos logiciels et vos applications sont tous à jour pour bénéficier des derniers correctifs de sécurité.
- Test de vulnérabilité : Utilisez des outils de test de vulnérabilité pour identifier les éventuelles faille²s de sécurité dans votre système.
- Examen des autorisations des applications : Passez en revue les autorisations accordées à chaque application installée sur votre ordinateur pour vous assurer qu'elles ne disposent que des privilèges nécessaires.
- Test de phishing et de sécurité des mots de passe : Effectuez des tests de phishing pour évaluer la capacité de reconnaissance des attaques de phishing par les utilisateurs, et vérifiez la robustesse des mots de passe utilisés.
- Audit des politiques de sécurité : Passez en revue les politiques de sécurité de votre organisation (le cas échéant) pour vous assurer qu'elles sont bien appliquées sur votre ordinateur.
- Formation à la sécurité informatique : Suivez des cours ou des formations en ligne sur la sécurité informatique pour vous tenir au courant des dernières menaces et des meilleures pratiques de sécurité.
- Audit des paramètres de sécurité du système : Vérifiez que les pare-feu, les antivirus, les filtres anti-spam et d'autres outils de sécurité sont correctement configurés et activés.

2/ un exercice pour installer et utiliser un antivirus antimalware en fonction de l'appareil utilisée

Pour  un ordinateur :

Recherche : Faites des recherches pour trouver un antivirus et un logiciel antimalware de confiance. Consultez des avis d'experts et des comparaisons pour choisir celui qui convient le mieux à vos besoins et à votre système d'exploitation.

Téléchargement : Accédez au site web de l'antivirus sélectionné et téléchargez la version compatible avec votre système d'exploitation (Windows, macOS, Linux, etc.).

Étape 2 : Installation de l'Antivirus/Antimalware

Exécution du programme d'installation : Une fois le téléchargement terminé, ouvrez le fichier d'installation en double-cliquant dessus.

Suivre les instructions : Suivez les instructions à l'écran pour installer le logiciel. Cela peut impliquer d'accepter les conditions d'utilisation, de choisir un emplacement d'installation et de personnaliser les options d'installation.

Redémarrage : Après l'installation, il est recommandé de redémarrer votre ordinateur pour finaliser le processus.

Étape 3 : Configuration de l'Antivirus/Antimalware

Mise à jour : Ouvrez le logiciel nouvellement installé et recherchez l'option de mise à jour. Assurez-vous que la base de données des définitions de virus est à jour pour garantir une protection maximale.

Scan initial : Effectuez un scan complet de votre ordinateur pour détecter les éventuelles menaces déjà présentes. Ce scan peut prendre un certain temps en fonction de la taille de votre disque dur.

Planification des scans : Configurez le logiciel pour qu'il effectue des scans réguliers automatiquement à des moments où vous n'utilisez pas activement votre ordinateur, comme tard dans la nuit.

Étape 4 : Utilisation quotidienne

Surveillance en temps réel : Activez la protection en temps réel pour que le logiciel surveille constamment les activités et les fichiers entrants et sortants de votre ordinateur.

Analyse des fichiers téléchargés : Si votre antivirus dispose d'une fonction de vérification des fichiers téléchargés, assurez-vous de l'activer. Elle peut empêcher les logiciels malveillants d'être téléchargés sur votre ordinateur.

Prudence en ligne : Même avec un antivirus installé, soyez prudent lorsque vous naviguez sur Internet et évitez les sites web suspects, les liens non sécurisés et les téléchargements douteux.

Étape 5 : Maintenance continue

Mises à jour régulières : Assurez-vous de maintenir votre antivirus et votre antimalware à jour en téléchargeant et en installant les mises à jour régulières fournies par le fabricant.

Analyse périodique : Effectuez régulièrement des scans complets de votre ordinateur pour détecter les menaces potentielles et les éliminer.

Formation continue : Tenez-vous informé des dernières menaces et techniques d'attaque en participant à des formations en ligne ou en lisant des articles sur la cybersécurité.

Pour un smartphone :

Choix de l'application : Sur le Play Store (pour les appareils Android) ou l'App Store (pour les appareils iOS), recherchez des applications antivirus/antimalware bien notées et fiables. Des exemples populaires incluent Avast Mobile Security, Bitdefender Mobile Security, AVG AntiVirus, McAfee Mobile Security, etc.

Téléchargement et installation : Sélectionnez l'application de votre choix et installez-la sur votre smartphone. Suivez les instructions à l'écran pour terminer le processus d'installation.

Configuration initiale : Une fois l'application installée, lancez-la et suivez les instructions pour effectuer une configuration initiale. Cela peut inclure la création d'un compte, la configuration des paramètres de sécurité, etc.

Analyse du système : Utilisez la fonction d'analyse de l'application pour scanner votre smartphone à la recherche de logiciels malveillants, de virus et d'autres menaces potentielles. Selon l'application, vous pouvez effectuer une analyse rapide ou complète.

Mises à jour des définitions de virus : Assurez-vous que les définitions de virus de l'application sont à jour. Cela garantit que votre antivirus/antimalware dispose des informations les plus récentes sur les menaces.

Planification des analyses régulières : Configurez l'application pour effectuer des analyses régulières de votre smartphone, par exemple une fois par semaine. Cela aide à détecter rapidement les nouvelles menaces.

Fonctionnalités supplémentaires : Explorez les fonctionnalités supplémentaires de l'application, telles que le verrouillage d'applications, la localisation de l'appareil perdu, la protection de la vie privée, etc. Activez celles qui correspondent le mieux à vos besoins.

Sensibilisation à la sécurité : Profitez des ressources éducatives fournies par l'application pour en savoir plus sur les menaces de sécurité mobiles et les meilleures pratiques pour protéger votre smartphone.

Gestion des permissions d'application : Assurez-vous d'examiner attentivement les autorisations demandées par l'application antivirus/antimalware et limitez-les au strict nécessaire pour préserver votre vie privée.

Suivi et maintenance : Assurez-vous de maintenir votre application antivirus/antimalware à jour en installant les mises à jour régulières disponibles sur le Play Store ou l'App Store. Surveillez également les alertes et les notifications de l'application pour toute activité suspecte détectée sur votre smartphone.

Recherche d'un antivirus/antimalware fiable : Faites des recherches pour trouver un logiciel antivirus/antimalware réputé et fiable. Des exemples populaires incluent Avast, AVG, Norton, Bitdefender, Kaspersky, Malwarebytes, etc.

Téléchargement du logiciel : Rendez-vous sur le site officiel du fournisseur de l'antivirus/antimalware que vous avez choisi. Téléchargez la version la plus récente du logiciel compatible avec votre système d'exploitation.

Installation du logiciel : Une fois le téléchargement terminé, double-cliquez sur le fichier téléchargé pour lancer le programme d'installation. Suivez les instructions à l'écran pour installer le logiciel sur votre ordinateur.

Configuration initiale : Après l'installation, le logiciel antivirus/antimalware peut vous demander de procéder à une configuration initiale. Cela peut inclure la création d'un compte, la sélection des paramètres de protection, etc.

Mise à jour des définitions de virus : Assurez-vous que les définitions de virus de l'antivirus/antimalware sont à jour. Généralement, le logiciel se met automatiquement à jour, mais vous pouvez également le faire manuellement depuis les paramètres.

Analyse du système : Utilisez la fonction d'analyse de l'antivirus/antimalware pour scanner votre ordinateur à la recherche de logiciels malveillants, de virus et d'autres menaces potentielles. Vous pouvez généralement choisir entre une analyse rapide et une analyse complète.

Planification des analyses régulières : Configurez le logiciel pour qu'il effectue des analyses régulières de votre ordinateur, par exemple une fois par semaine. Cela garantit que votre système est constamment protégé contre les menaces.

Exploration des fonctionnalités supplémentaires : Explorez les fonctionnalités supplémentaires de l'antivirus/antimalware, telles que la protection en temps réel, le pare-feu intégré, la protection contre le phishing, etc. Activez celles qui correspondent le mieux à vos besoins.

Sensibilisation à la sécurité : Profitez des ressources éducatives fournies par le logiciel antivirus/antimalware pour en savoir plus sur les menaces de sécurité informatique et les meilleures pratiques pour protéger votre ordinateur.

Suivi et maintenance : Assurez-vous de maintenir votre logiciel antivirus/antimalware à jour en installant les mises à jour régulières disponibles. Surveillez également les alertes et les notifications du logiciel pour toute activité suspecte détectée sur votre ordinateur.