

Parcours : DISCOVERY

Module : Naviguer en toute sécurité

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

1 - Introduction à la sécurité sur Internet

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

1/ En naviguant sur le web, consultez 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.

Réponse 1

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

- Article 1 = [Doctissimo - Découvrez les gestes simples pour naviguer en toute sécurité sur internet](#)
- Article 2 = [Idealogeek.fr - Les meilleures pratiques pour protéger vos données sur internet](#)
- Article 3 = [Buzzwebzine - 6 conseils pour acheter sur internet en toute sécurité](#)
- Article bonus = [Stockage en Cloud : comment choisir la solution idéale pour la sécurité de vos données ?](#)

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](#) ✓
- Créer un compte en remplissant le formulaire. ✓
- 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, cliquez 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. ✓

- 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 

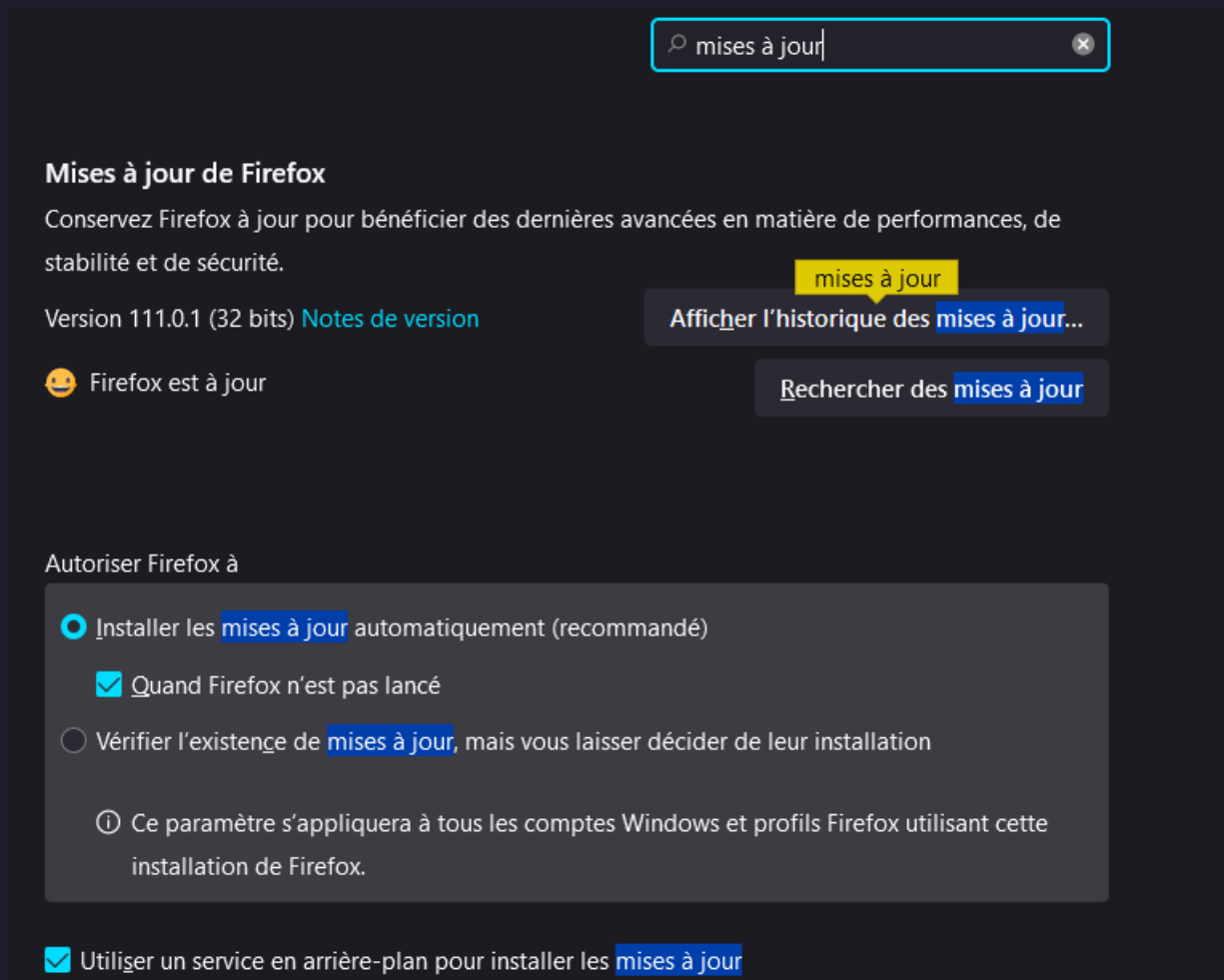
Les seuls sites qui semblaient être cohérents sont donc :

- 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) 

Conclusion : les adresses internet qui semblent provenir de sites web malveillants ont un nom de domaine qui ressemble aux sites existants. Je pourrai prendre d'autres exemples comme facbook.com, instagramhjack.com, videocall-whatsapp.com. Leur objectif est bien de tromper les utilisateurs en se faisant passer pour les services officiels.

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) 



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

Bravo, Fano !
Vous avez obtenu un
score de 8/8.

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 :



RECOMMENCER LE QUESTIONNAIRE

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*

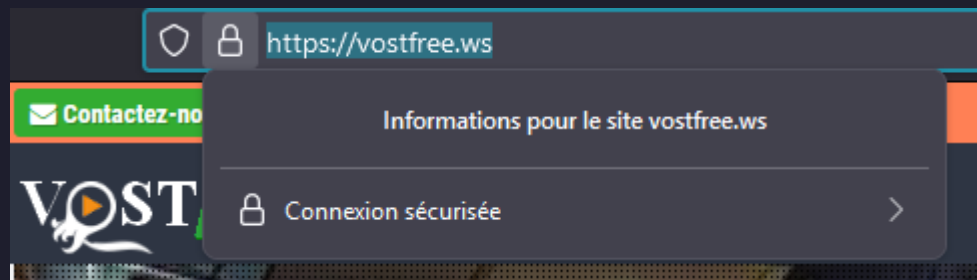
3/ Lors de la navigation sur le web, il arrive d'avoir des doutes sur la sécurité de certains sites. Comme tu as pu le voir précédemment, le premier niveau de vigilance à avoir se trouve dans la barre d'adresse des navigateurs web. La plupart affichent des indicateurs de sécurité pour donner une information 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 ✓

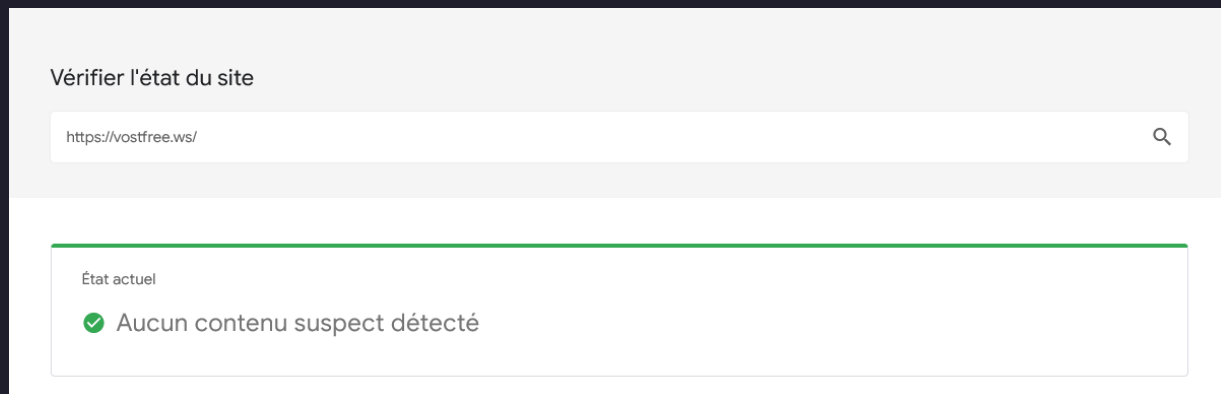


- HTTPS Not secure ✗

- Not secure ✗

- Analyse Google

- Aucun contenu suspect ✓

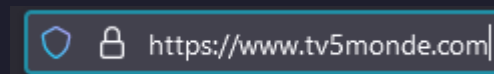


- Vérifier un URL en particulier ✗

- Site n°2

- Indicateur de sécurité

- HTTPS ✓



- HTTPS Not secure ✗

- Not secure ✗

- Analyse Google

- Aucun contenu suspect ✓

Vérifier l'état du site

https://www.tv5monde.com/

État actuel

✓ Aucun contenu suspect détecté

■ Vérifier un URL en particulier ✗

- Site n°3

- Indicateur de sécurité

■ HTTPS ✓

https://www.baidu.com

■ HTTPS Not secure ✗

■ Not secure ✗

- Analyse Google

■ Aucun contenu suspect ✗

■ Vérifier un URL en particulier ✓

Vérifier l'état du site




https://www.baidu.com/

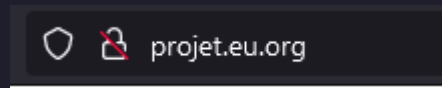
État actuel

Vérifier une URL en particulier


- Site n°4

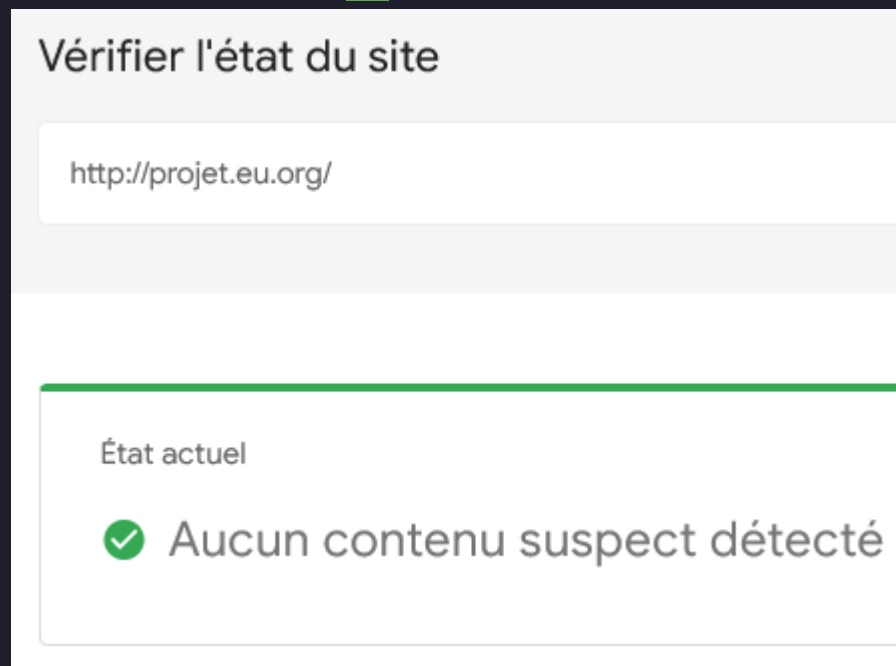
- Indicateur de sécurité

- HTTPS 
 - HTTPS Not secure 
 - Not secure 




- Analyse Google

- Aucun contenu suspect 



- Vérifier un URL en particulier 

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.

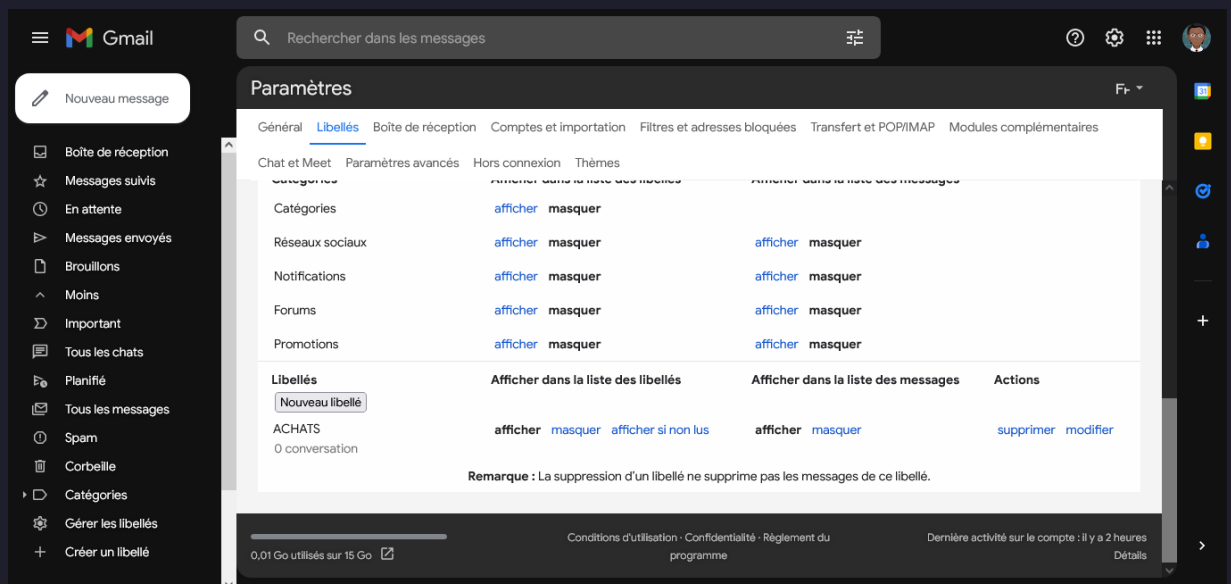
Deux possibilités s'offrent à toi pour organiser ce registre :

- 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 ✓

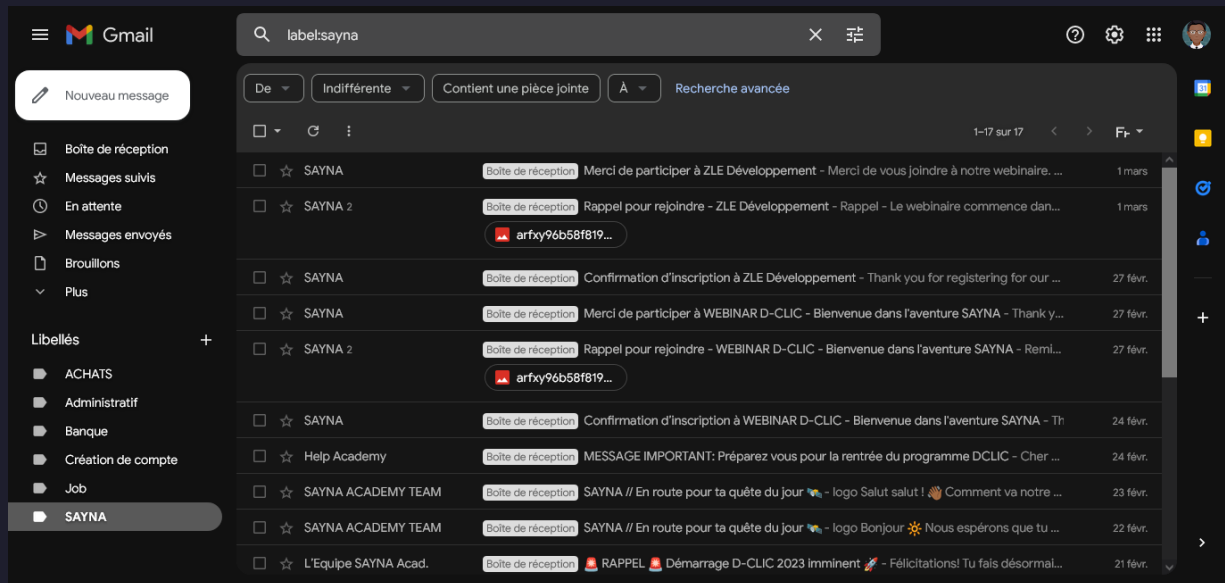
Réponse 1

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



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 ????????

Voici quelques exemples d'exercices qui peuvent être utilisés pour vérifier la sécurité en fonction de l'appareil utilisé :

1. Pour un ordinateur portable ou de bureau :
 - Vérifiez que votre antivirus et votre pare-feu sont activés et à jour.
 - Essayez d'accéder à un site Web suspect pour voir si votre antivirus le bloque.
 - Ouvrez un fichier suspect dans un environnement virtuel pour éviter d'infecter votre système principal.
 - Essayez de trouver des vulnérabilités dans votre propre réseau en utilisant des outils de test de pénétration.
2. Pour un smartphone :
 - Installez un logiciel antivirus sur votre téléphone et exécutez une analyse de virus.
 - Assurez-vous que votre téléphone est à jour avec les derniers correctifs de sécurité.
 - Vérifiez que votre téléphone est configuré pour verrouiller automatiquement après une période d'inactivité.
 - Essayez de télécharger une application douteuse pour voir si votre téléphone vous avertit d'un danger.
3. Pour un routeur sans fil :
 - Assurez-vous que votre routeur utilise un mot de passe fort et unique.
 - Vérifiez que votre routeur est configuré pour utiliser un cryptage de données fort.
 - Vérifiez que les mises à jour de sécurité sont installées sur votre routeur.
 - Vérifiez les journaux du routeur pour voir si des activités suspectes ont été détectées.

2/Proposer un exercice pour installer un antivirus+antimalware en fonction de l'appareil utilisé.

Pour un ordinateur portable ou de bureau :

- Choisissez un antivirus et un antimalware réputés et fiables. Faites des recherches pour trouver celui qui convient le mieux à vos besoins.
- Téléchargez les fichiers d'installation de l'antivirus et de l'anti-malware à partir du site Web du fournisseur.
- Fermez toutes les applications ouvertes et désactivez temporairement votre pare-feu.
- Double-cliquez sur les fichiers d'installation pour lancer l'installation. Suivez les instructions à l'écran pour terminer l'installation.
- Une fois l'installation terminée, redémarrez votre ordinateur pour que les modifications prennent effet.
- Activez votre antivirus et antimalware et effectuez une analyse complète de votre ordinateur pour détecter les menaces potentielles.

- Si des menaces sont détectées, suivez les instructions fournies par l'antivirus et l'anti-malware pour les supprimer ou les mettre en quarantaine.
- Assurez-vous que votre antivirus et votre anti-malware sont mis à jour régulièrement pour protéger votre ordinateur contre les dernières menaces.