

Module : Naviguer en toute sécurité

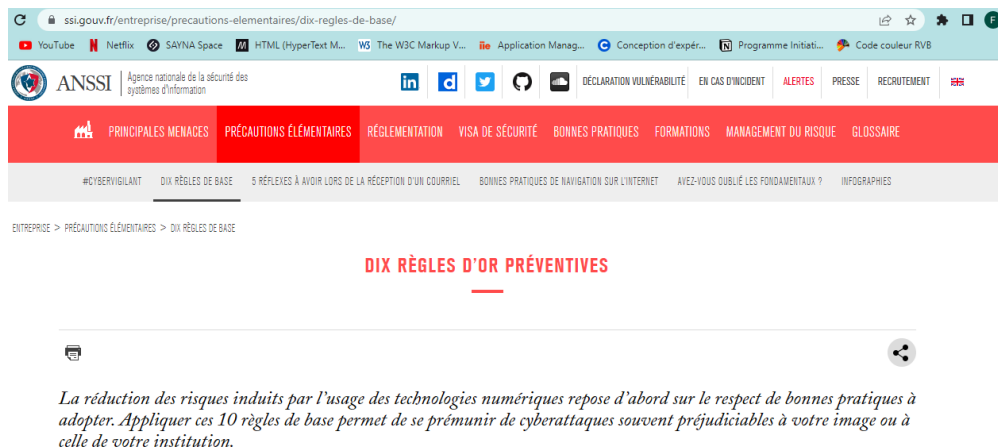
1- INTRODUCTION A LA SECURITE SUR INTERNET

1/ En naviguant sur le web, consultez trois articles qui parlent de sécurité sur internet. Pensez à vérifier la source des informations et essayez de consulter des articles récents pour que les informations soient à jour.

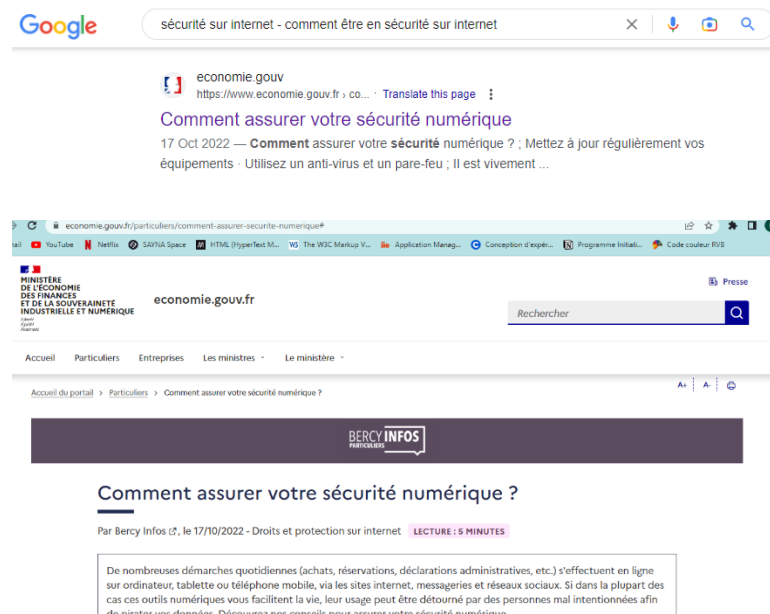
Réponses

Avec les mots-clés « sécurité et internet » et « comment être en sécurité sur internet », voici les 3 articles correspondants :

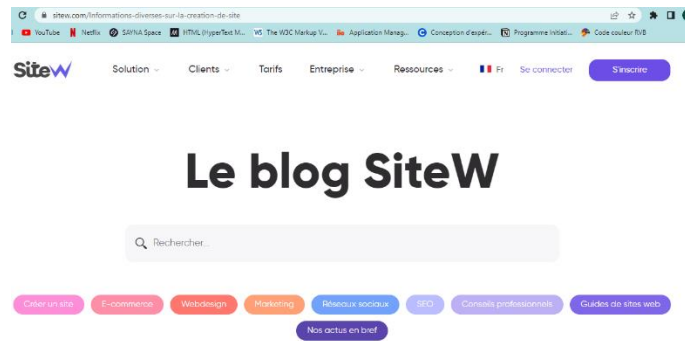
- ✓ Article 1 = [ANSSI - Dix règles de base](https://ssi.gouv.fr/entreprise/precautions-elementaires/dix-regles-de-base/)



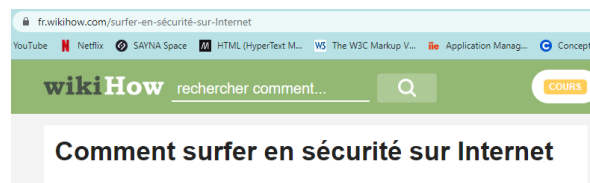
- ✓ Article 2 = [Economie.gouv – Comment assurer votre sécurité numérique](https://economie.gouv.fr/particuliers/comment-assurer-securite-numerique)



✓ Article 3 = [Site W - Naviguez en toute sécurité sur Internet](#)



* Article bonus = [wikiHow – Comment surfer en sécurité sur Internet](#)



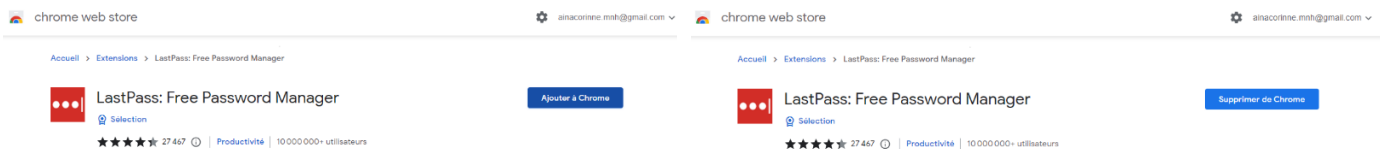
2- CREER DES MOTS DE PASSE FORTS

Objectif : utiliser un gestionnaire de mot de passe LastPass

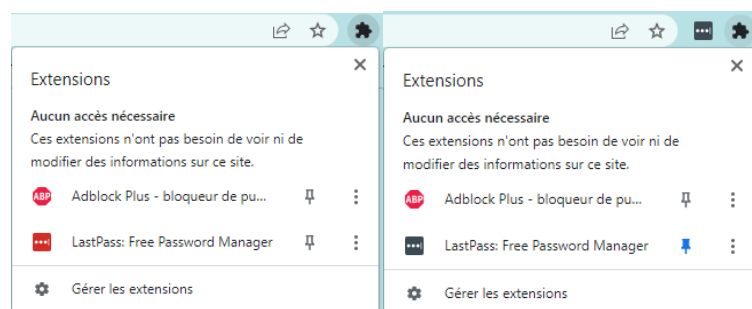
1/ Dans cet exercice, nous allons voir comment utiliser pour la première fois un gestionnaire de mot de passe nommé LastPass. Ce gestionnaire prend la forme d'une application web, accessible sur tous supports (PC, Mac, mobile). Il est simple à prendre en main et propose un niveau de sécurité optimal.

Réponses

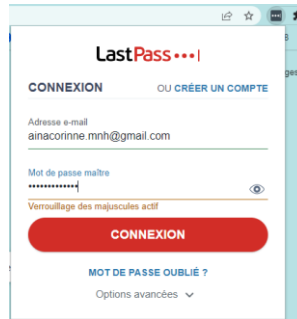
- ☒ Accède au site de LastPass.
- ☒ Crée un compte en remplissant le formulaire et fournis un mot de passe maître.
- ☒ Une fois la création du compte effectuée, tu arrives sur une page de validation qui propose le téléchargement de l'extension sur ton navigateur. Lance l'installation en effectuant un 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.
- En haut à droite du navigateur, clic sur le logo "Extensions". Epingler l'extension de LastPass avec l'icône.

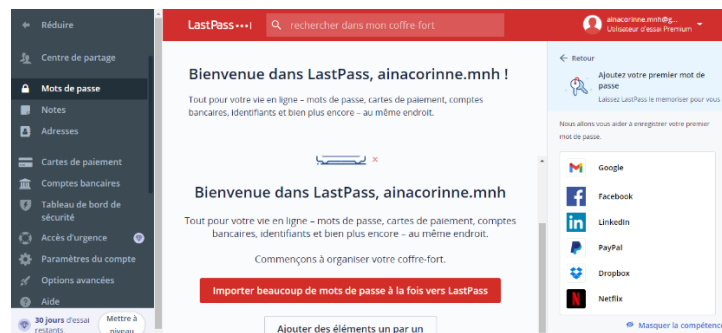


Il ne te reste plus qu'à te connecter en effectuant un clic sur l'icône de l'extension et en saisissant ton identifiant et mot de passe.

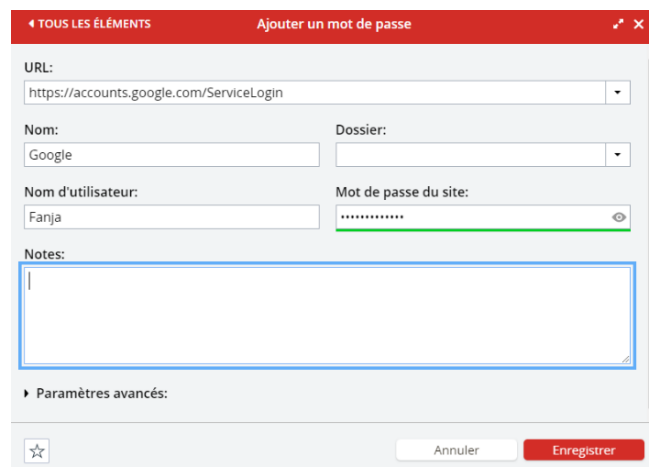
The image shows the LastPass login interface. At the top, it says 'LastPass' with a red logo. Below that, there's a 'CONNEXION' button and a link 'OU CRÉER UN COMPTE'. The form includes fields for 'Adresse e-mail' (with 'ainacorinne.mnh@gmail.com' entered) and 'Mot de passe maître' (with a masked password and an eye icon to toggle visibility). A red 'CONNEXION' button is prominent. Below it, there's a link 'MOT DE PASSE OUBLIÉ ?' and a link 'Options avancées'.

☒ 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" puis clique sur "Ajouter un élément".

The image shows the LastPass dashboard. On the left is a sidebar with a menu: 'Réduire', 'Centre de partage', 'Mots de passe', 'Notes', 'Adresses', 'Cartes de paiement', 'Comptes bancaires', 'Tableau de bord de sécurité', 'Accès d'urgence', 'Paramètres du compte', 'Options avancées', and 'Aide'. The main area has a red header with 'LastPass' and a search bar. Below the header, it says 'Bienvenue dans LastPass, ainacorinne.mnh !' and 'Tout pour votre vie en ligne - mots de passe, cartes de paiement, comptes bancaires, identifiants et bien plus encore - au même endroit.' There's a red button 'Importer beaucoup de mots de passe à la fois vers LastPass' and a link 'Ajouter des éléments un par un'. On the right, there's a section 'Ajoutez votre premier mot de passe' with a list of services: Google, Facebook, LinkedIn, PayPal, Dropbox, and Netflix.

☒ 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.

The image shows the 'Ajouter un mot de passe' form in LastPass. It has a red header with 'TOUS LES ÉLÉMENTS' and 'Ajouter un mot de passe'. The form includes fields for 'URL:' (with 'https://accounts.google.com/ServiceLogin' entered), 'Nom:' (with 'Google' entered), 'Dossier:' (with a dropdown menu), 'Nom d'utilisateur:' (with 'Fanja' entered), and 'Mot de passe du site:' (with a masked password and an eye icon to toggle visibility). There's a 'Notes:' section with a text area. At the bottom, there's a 'Paramètres avancés:' section with a star icon, an 'Annuler' button, and an 'Enregistrer' button.

Comparatif des gestionnaires de mot de passe :

The image shows the header of the Clubic website. It has a red header with the 'clubic' logo and a navigation menu: 'ACTUALITÉS', 'TESTS', 'GUIDES D'ACHAT', 'TÉLÉCHARGER', 'BONS PLANS', and 'TUTORIELS'. Below the menu, there's a sub-menu: 'Informatique', 'Mobile', 'Image & Son', 'Gaming', 'Maison connectée', 'Streaming', and 'Auto'. At the bottom, there's a link 'Accueil / Guides d'achat / Guides Gestionnaire de mot de passe'.

Meilleur gestionnaire de mots de passe, le comparatif 2023

3- FONCTIONNALITE DE SECURITE 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 :

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

Explications

Les sites web qui semblent être malveillants sont :

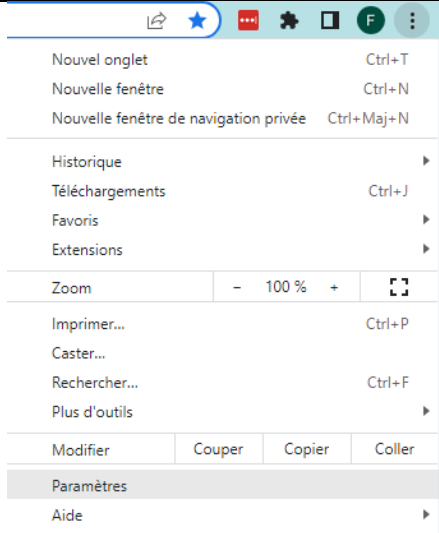
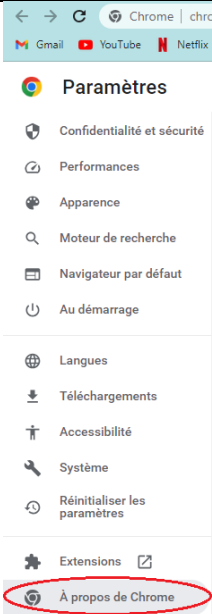
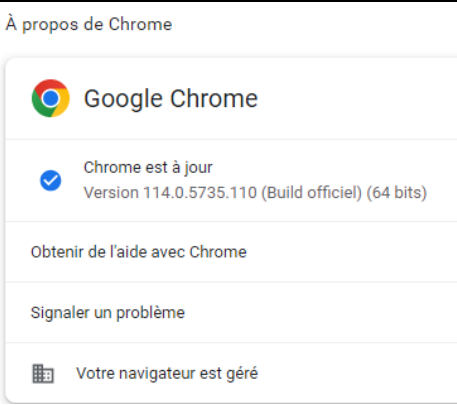
- www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel
- www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde
- www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très utilisé

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.

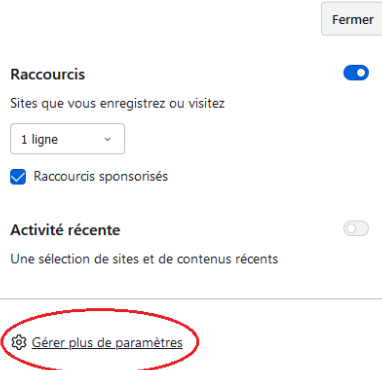
Réponses

Pour Chrome		
<input checked="" type="checkbox"/> Ouvre le menu du navigateur et accède aux "Paramètres"	<input checked="" type="checkbox"/> Clique sur la rubrique "À propos de Chrome"	<input checked="" type="checkbox"/> 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 "mises à jour" pour tomber directement dessus)



Mises à jour de Firefox

Conservez Firefox à jour pour bénéficier des dernières avancées en matière de performances, de stabilité et de sécurité.

Version 114.0.1 (64 bits) [Notes de version](#)

[Afficher l'historique des mises à jour...](#)

😊 Firefox est à jour

[Rechercher des mises à jour](#)

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

Photo modèle

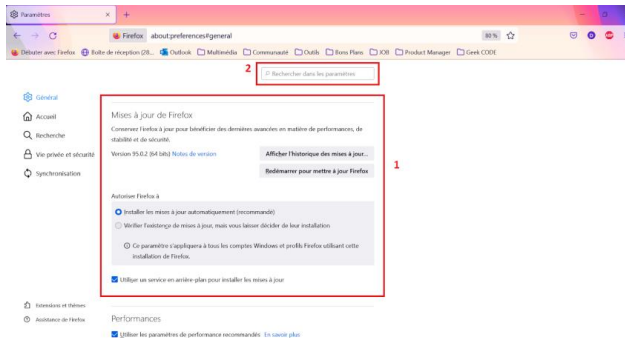
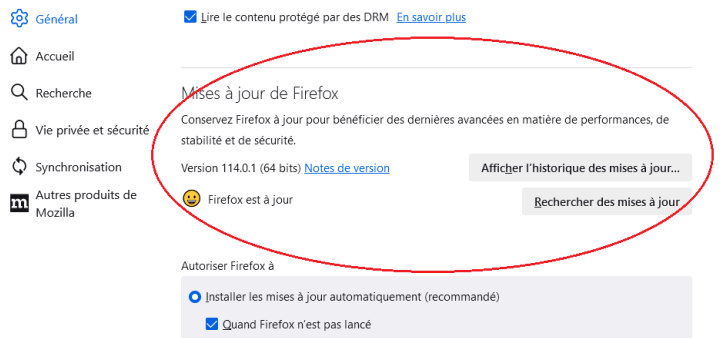


Photo de mon navigateur Firefox



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 <https://phishingquiz.withgoogle.com/?hl=fr> suivant et suis les étapes qui y sont décrites : **Exercice 4 - Spam et Phishing**

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

Réponses

<p>Etape 1</p> <p>https://phishingquiz.withgoogle.com/?hl=fr</p> <p>Français</p> <p>Savez-vous reconnaître une tentative d'hameçonnage ?</p> <p>Il peut être plus difficile qu'il n'y paraît de repérer une tentative d'hameçonnage. Lors d'une tentative d'hameçonnage, une personne malveillante essaye de vous amener à communiquer des informations personnelles se faisant passer pour quelqu'un que vous connaissez. Arrivez-vous à distinguer le vrai du faux ?</p> <p>RÉPONDRE AU QUESTIONNAIRE</p>	<p>Etape 2</p> <p>Créer un nom et une adresse e-mail.</p> <p>Pour rendre ce questionnaire plus réaliste, créez un nom d'utilisateur et une adresse e-mail (ceux-ci peuvent être fictifs). Ne vous inquiétez pas, ces informations ne sortiront pas de votre appareil. Plus d'infos</p> <p>Fanja</p> <p>Nom</p> <p>ainacorinne.mnh@gmail.com</p> <p>E-mail</p> <p>COMMENCER</p>
<p>Etape 3</p> <p>Il s'agit bien d'un e-mail d'hameçonnage.</p> <p>L'URL semble correcte, mais il s'agit en fait d'une adresse trompeuse. Prenez garde aux liens hypertexte et aux pièces jointes que vous ouvrez à partir des e-mails, car ils peuvent rediriger vers des sites Web frauduleux qui vous invitent à saisir des informations sensibles.</p> <p>MONTREZ-MOI</p> <p>Luke Johnson luke.john800@gmail.com à moi</p> <p>07:16</p> <p>Luke Johnson a partagé un lien vers le document suivant :</p> <p>Budget département 2023.docx</p> <p>Bonjour. Voici le document demandé. N'hésitez pas à me contacter si vous avez besoin d'autre chose !</p> <p>Ouvrir dans Docs</p>	<p>Etape 4</p> <p>Luke Johnson a partagé un lien vers le document suivant :</p> <p>Budget département 2023.docx</p> <p>En passant la souris sur ce lien ou en appuyant de manière prolongée dessus, vous verrez qu'il ouvre le domaine non sécurisé "drive-google.com", qui n'appartient pas à Google.</p> <p>Suivant</p> <p>N'hésitez pas à me contacter si vous avez</p>

Pour aller plus loin :

- Site du gouvernement cybermalveillance.gouv.fr [Comment reconnaître un mal de phishing](#)

Aperçu du site



Comment reconnaître un mail de phishing ou d'hameçonnage ?

Publié le 25 Oct 2021

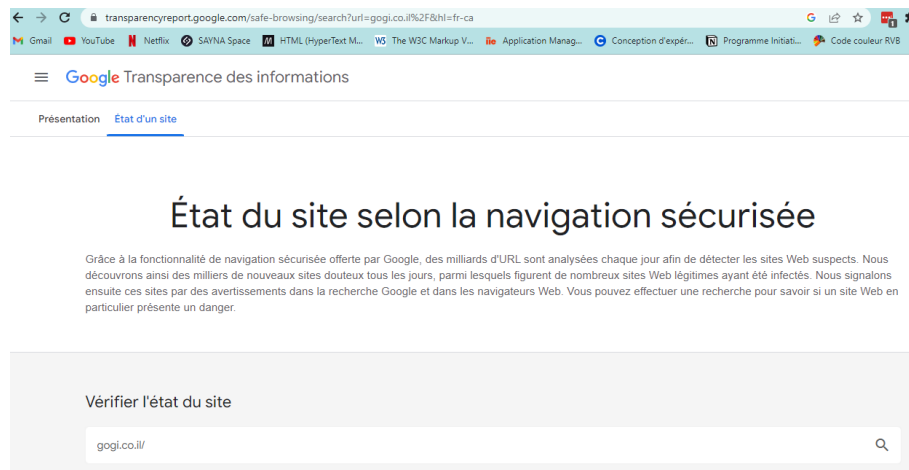
Mail frauduleux phishing

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).

Google Transparence des informations

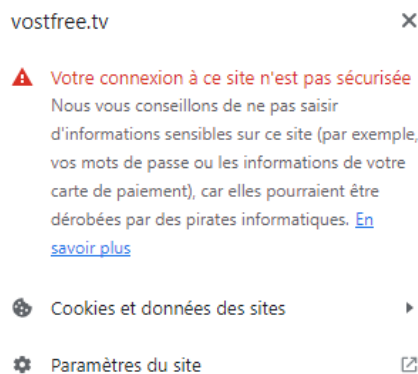


Afin d'améliorer ta lecture de la sécurité sur internet, tu vas devoir analyser les informations de plusieurs sites. Pour chaque site tu devras préciser l'indicateur de sécurité et le rapport d'analyse de l'outil Google. Il te suffit d'accéder aux liens proposés ci-dessous pour observer l'indicateur de sécurité et de copier-coller l'URL du site dans l'outil Google.

Réponses

● Site n°1 : <https://vostfree.tv/>

○ Indicateur de sécurité

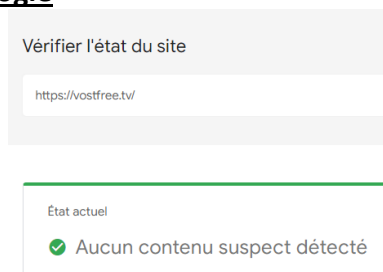


☐ HTTPS

☒ HTTPS Not secure

☐ Not secure

○ Analyse Google



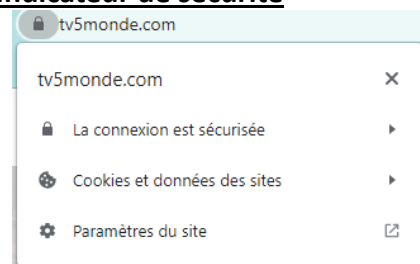
☒ Aucun contenu suspect

☐ Vérifier un URL en particulier

● Site n°2

<https://www.tv5monde.com/>

○ Indicateur de sécurité

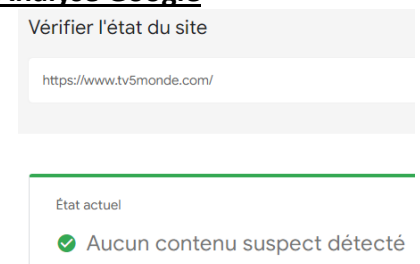


☒ HTTPS

☐ HTTPS Not secure

☐ Not secure

○ Analyse Google

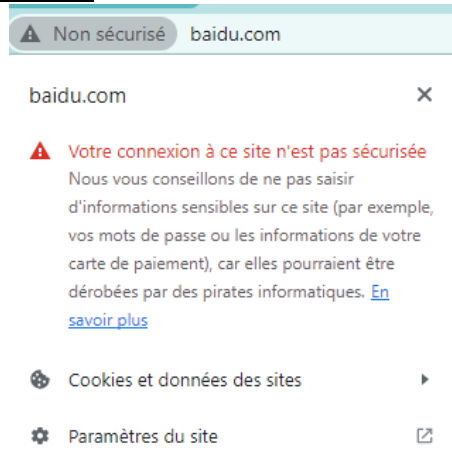


☒ Aucun contenu suspect

☐ Vérifier un URL en particulier

● Site n°3 <http://www.baidu.com/>

○ Indicateur de sécurité



☐ HTTPS

☐ HTTPS Not secure

☒ Not secure

○ Analyse Google



Etat actuel

Vérifier une URL en particulier

Il est difficile d'indiquer un simple niveau de sécurité pour les sites comme <http://www.baidu.com/>, qui comportent énormément de contenu. Des sites généralement considérés comme étant fiables présentent parfois du contenu suspect (par exemple, dans les blogs ou les commentaires). Pour obtenir des informations plus détaillées sur la sécurité, vérifiez un annuaire ou une page Web spécifiques.

☐ Aucun contenu suspect

☒ Vérifier un URL en particulier

● Site n°4 (non sécurisé)

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 :

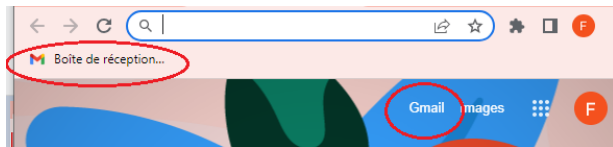
1. Créer un dossier sur ta messagerie électronique

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

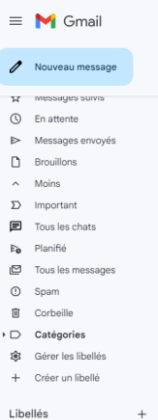
La première est la plus pratique à utiliser et la plus facile à mettre en place. Nous prendrons pour exemple la messagerie de Google (les autres messageries fonctionnent sensiblement de la même manière).

Suis les étapes suivantes pour créer un registre des achats sur ta messagerie électronique.

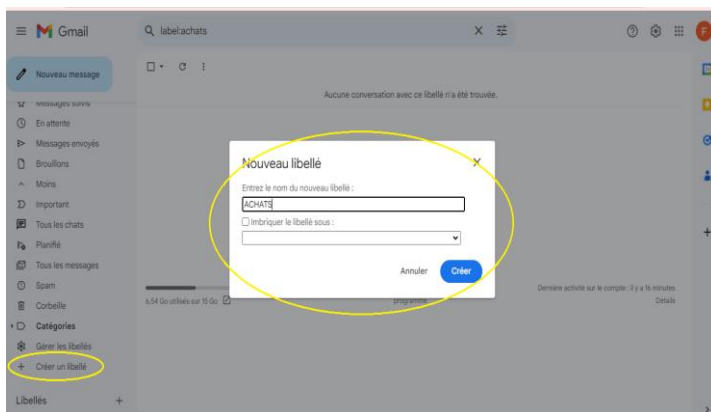
Réponses



☒ 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).



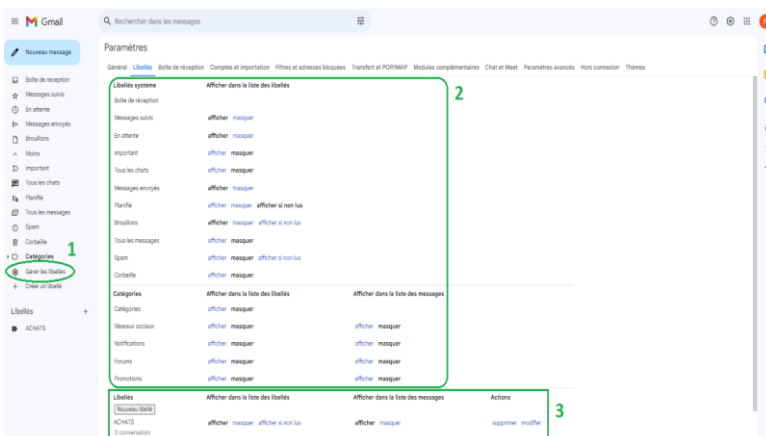
☒ Sur la page d'accueil de ta messagerie, tu trouveras sur la gauche les libellés initialement prévus (boîte de réception, messages envoyés, etc.)



☒ 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)

<div> <div>Libellés</div> <div>+</div> <div> <div>ACHATS</div> <div>ADMINISTRATIF</div> <div>BANQUE</div> <div>CREATION DE COMPTE</div> <div>JOB</div> <div>SAYNA</div> </div> </div>	<div> <div> <input checked="" type="checkbox"/> 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... </div> <div> <div>● ACHATS : historique, facture, conversations liées aux achats...</div> <div>● ADMINISTRATIF : toutes les démarches administratives</div> <div>● BANQUE : tous les documents et les conversations liés à la banque personnelle</div> <div>● CREATION DE COMPTE : tous les messages liés à la création d'un compte (message de bienvenue, résumé du profil, etc.)</div> <div>● JOB : tous les messages liés à mon projet professionnel</div> <div>● SAYNA : tous les messages liés mon activité avec SAYNA</div> </div> </div>
---	---

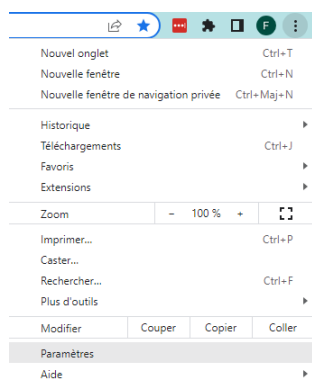
7. Comprendre le suivi du navigateur

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

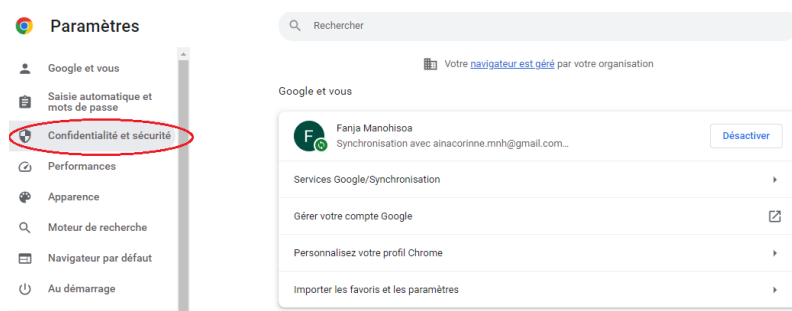
Réponses

GESTION DES COOKIES

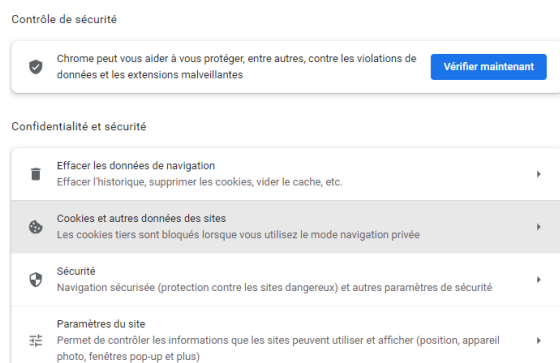
1/ Ouvrir le menu du navigateur et accéder aux Paramètres



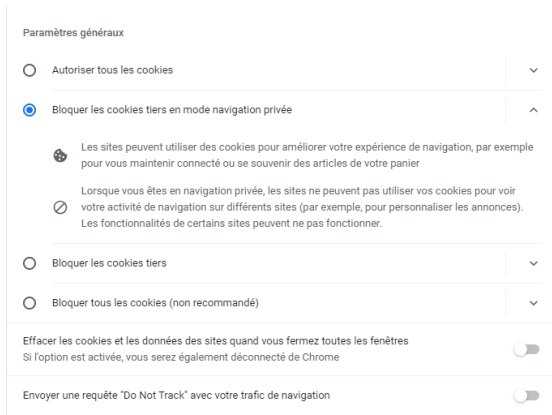
2/ Cliquer sur Confidentialité et sécurité



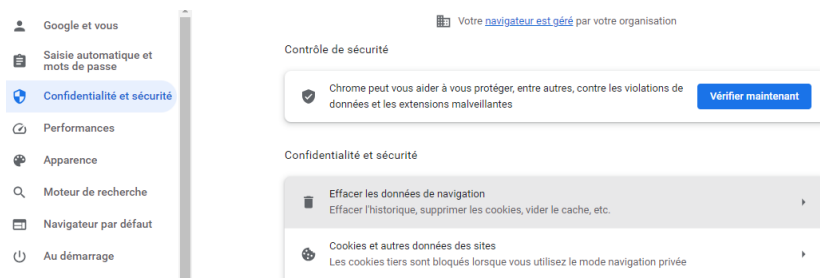
3/ Ouvrir Cookies et autres données du site



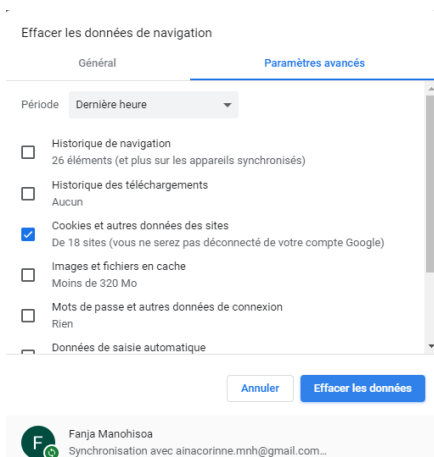
4/ Paramétrer les cookies en choisissant de **Bloquer les cookies tiers en mode navigation privée**



5/ Revenir dans Confidentialité et Sécurité et cliquer sur **Effacer les données de navigation**

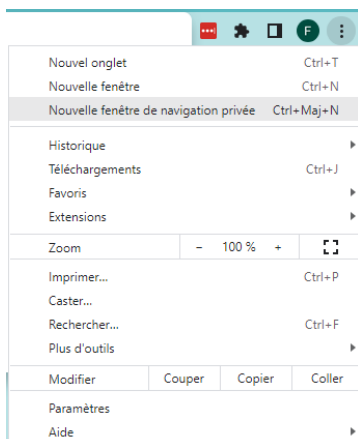


6/ Pour effacer les cookies, cocher **Cookies et autres données du site**, puis cliquer sur **Effacer les données**

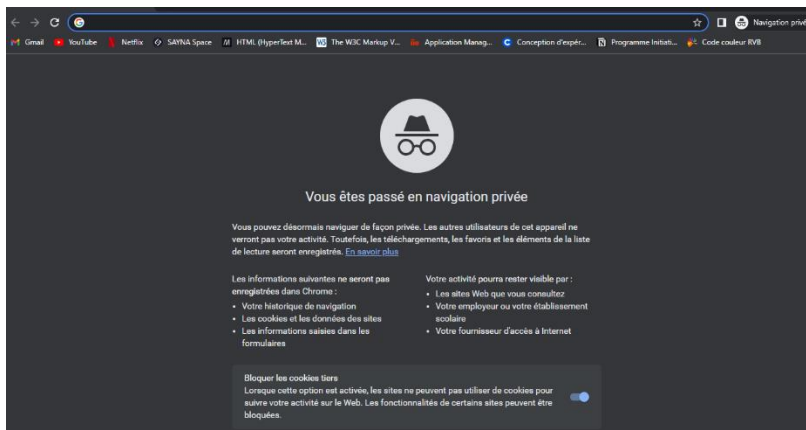


UTILISATION DE LA NAVIGATION PRIVEE

1/ Ouvrir le menu du navigateur et accéder à **Nouvelle fenêtre de navigation privée**



2/ Limiter les transferts d'informations en bloquant les cookies tiers et commencer la navigation



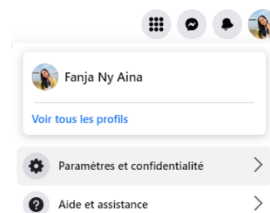
8. Principes de base de la confidentialité des médias sociaux*

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.

Réponses

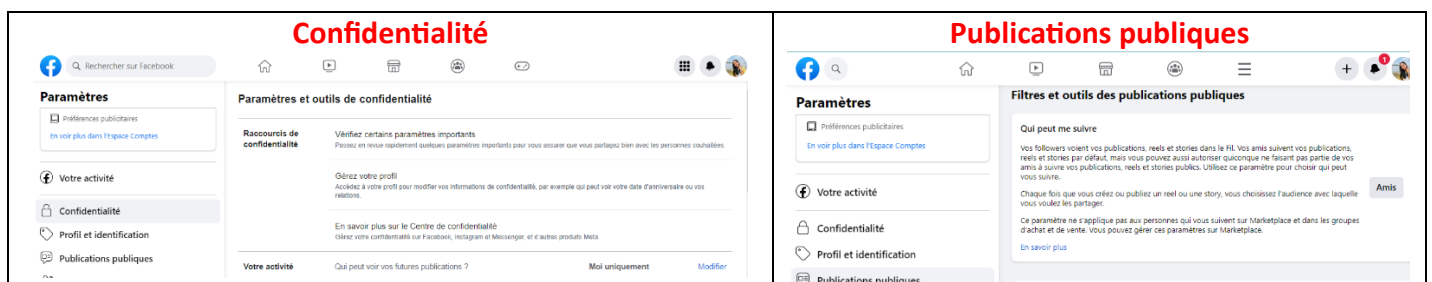
☒ Connecte-toi à ton compte Facebook.



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



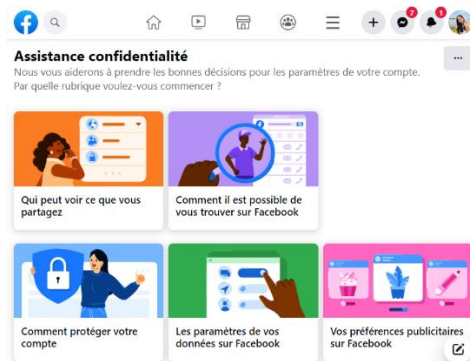
☒ Ce sont les onglets "Confidentialité" et "Publications publiques" qui nous intéressent. Accède à "Confidentialité" pour commencer et clique sur la première rubrique.



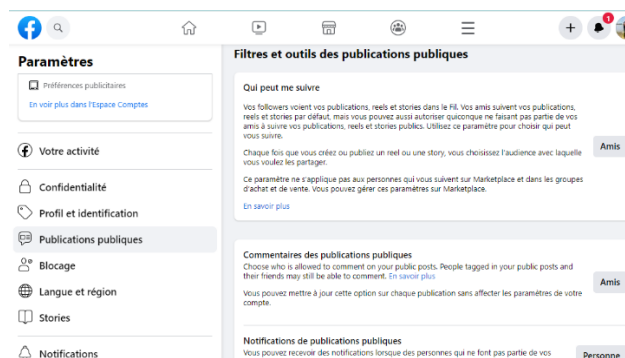
● Cette rubrique résume les **grandes lignes de la confidentialité sur Facebook** :

☒ 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.



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

1/ Comment vérifier la sécurité en fonction de l'appareil utilisé ?

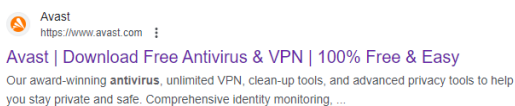
Réponses

- > Il faut installer un logiciel antivirus si l'appareil n'a pas de programme antivirus.
- > Faire analyser le système par l'antivirus : analyse rapide ou analyse complète.
- > Examiner les menaces découvertes avec les actions recommandées
- > Si l'antivirus peut supprimer les menaces, le laisser faire.

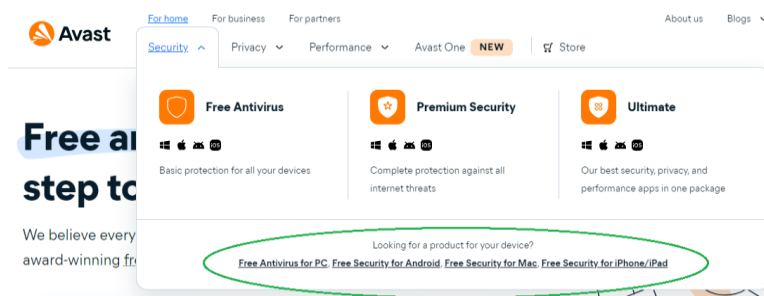
2/ Proposer un exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé.

Réponses

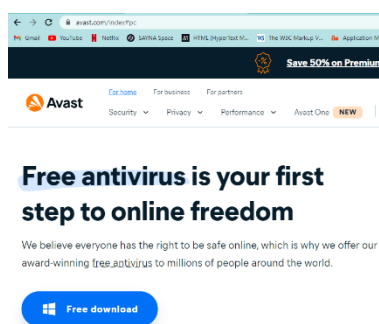
- > Faire des recherches d'antivirus sur internet :



- > Voir l'option compatible à l'appareil :



- > Télécharger et installer le logiciel antivirus :



Avast possède aussi un antimalware qu'on peut télécharger :

