



Repository Name : SAYNA-SECURTY-PROJET1

Tous vos travaux devront être déposés sur votre compte GitHub en PDF.

⚠ Pensez à mettre votre dépôt en "Public". Le projet ne sera pas corrigé si le dépôt se trouve en "Privé" ⚠

## 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, 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.**

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 = *La Dépêche – A l'Agglo d'Agen, la cyberattaque venait de l'Est...*
- Article 2 = *Yahoo Life France – Caméras cachées dans les hôtels et les Airbnb : "Je me suis sentie violée, c'était traumatisant"*
- Article 3 = *BFM TV - CYBERHARCÈLEMENT, FAUSSE MORT ET ALERTE À LA BOMBE: CES FOIS OÙ LE FORUM 18-25 A FAIT PARLER DE LUI*

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

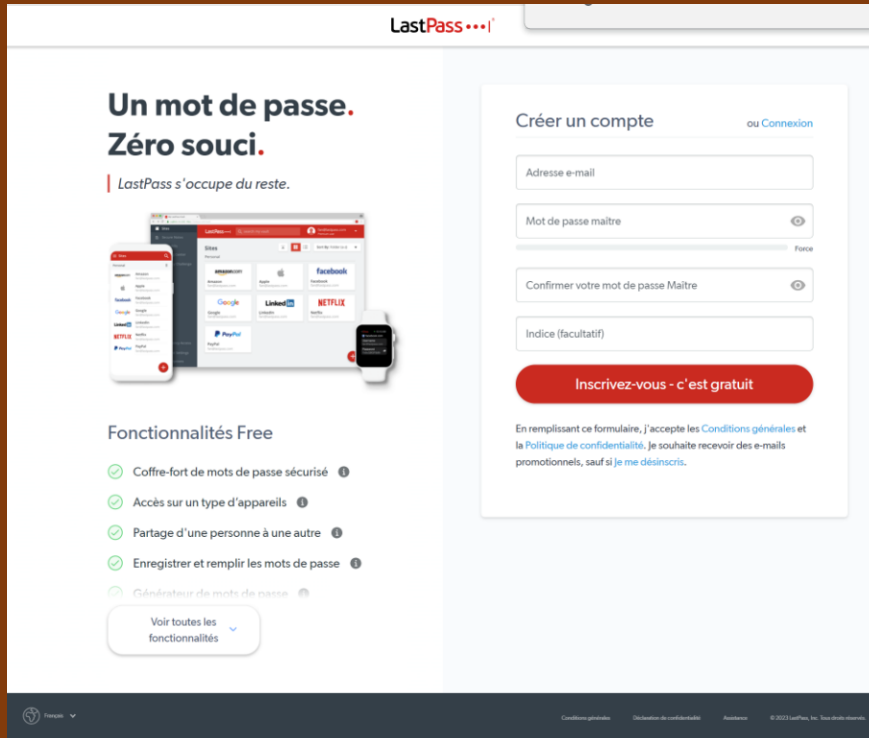
## 2- Créer des mots de passe forts

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



**Un mot de passe. Zéro souci.**  
LastPass s'occupe du reste.

**Fonctionnalités Free**

- ✓ Coffre-fort de mots de passe sécurisé ⓘ
- ✓ Accès sur un type d'appareils ⓘ
- ✓ Partage d'une personne à une autre ⓘ
- ✓ Enregistrer et remplir les mots de passe ⓘ
- ✓ Générateur de mots de passe ⓘ

[Voir toutes les fonctionnalités](#)

**Créer un compte** ou [Connexion](#)

Adresse e-mail

Mot de passe maître [Force](#)

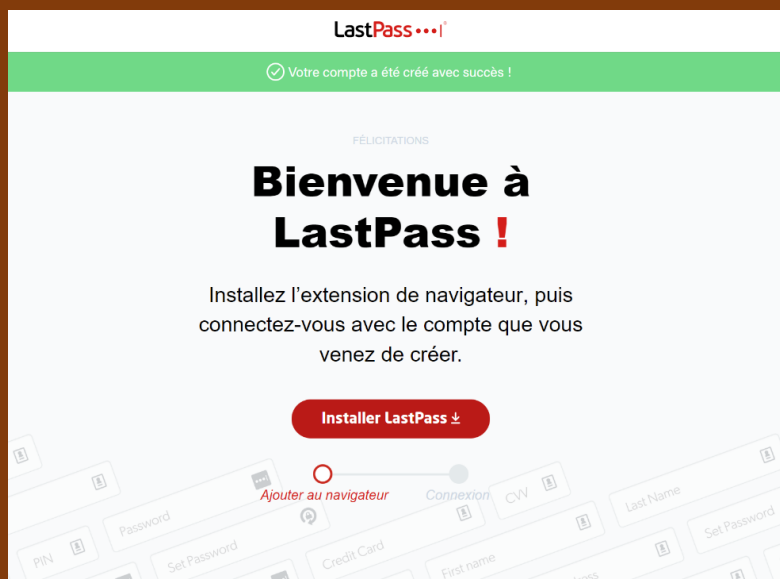
Confirmer votre mot de passe Maître

Indice (facultatif)

**Inscrivez-vous - c'est gratuit**

En remplissant ce formulaire, j'accepte les [Conditions générales](#) et la [Politique de confidentialité](#). Je souhaite recevoir des e-mails promotionnels, sauf si [je me désinscris](#).

- 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.



**LastPass**

✓ Votre compte a été créé avec succès !

FÉLICITATIONS

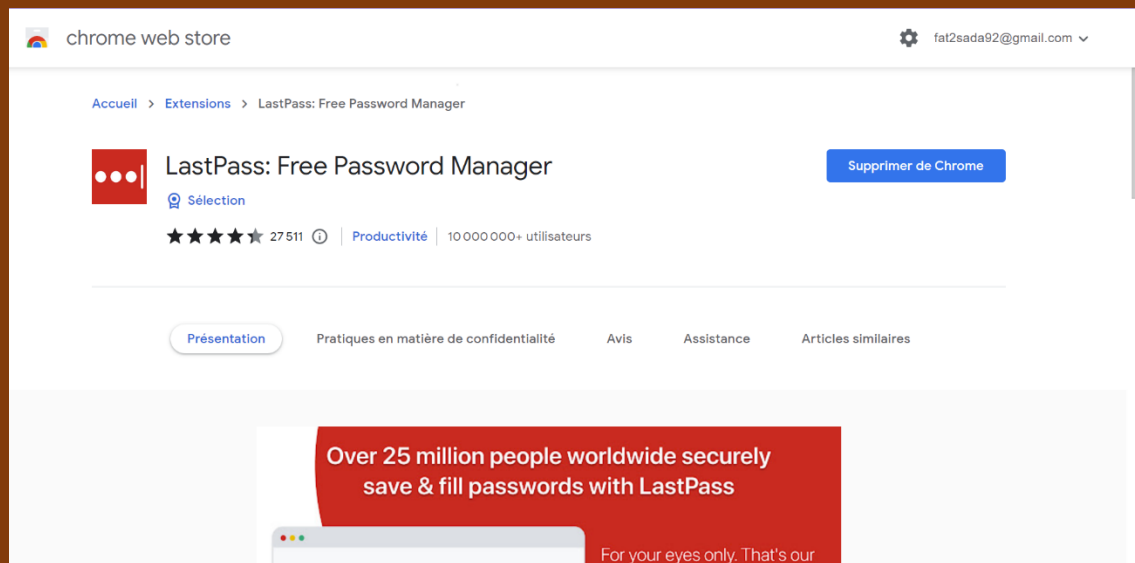
## Bienvenue à LastPass !


Installez l'extension de navigateur, puis connectez-vous avec le compte que vous venez de créer.

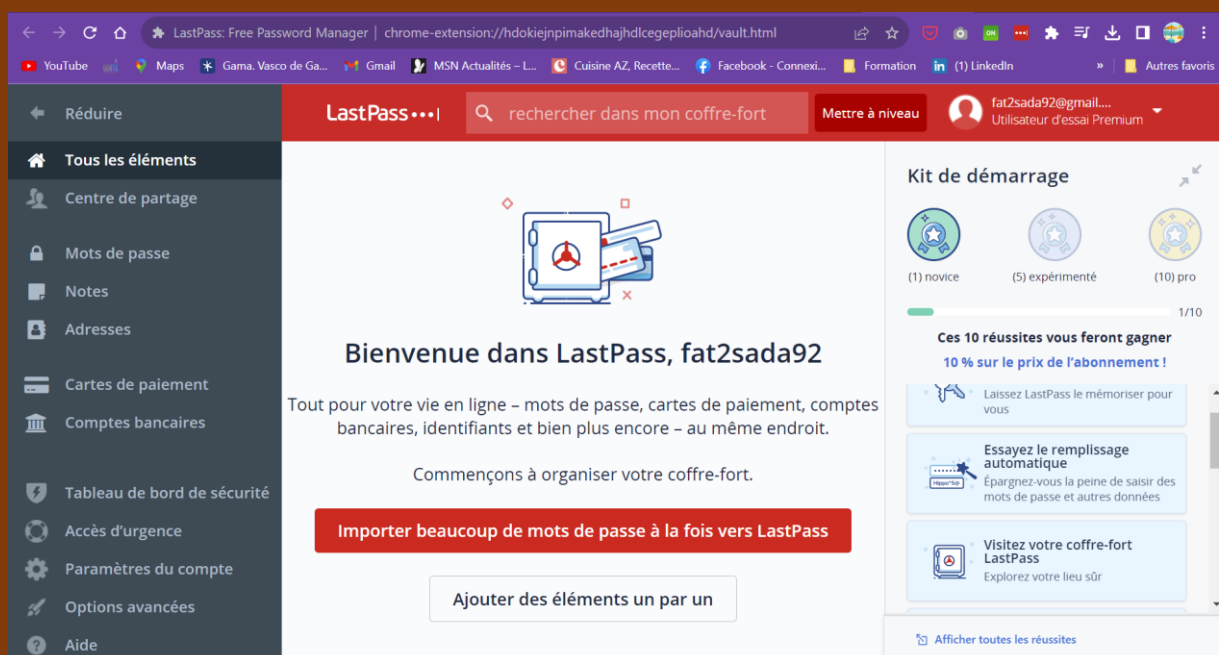
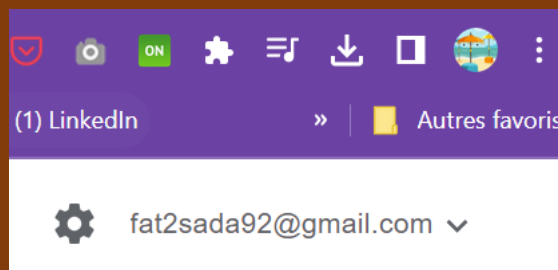
**Installer LastPass**

[Ajouter au navigateur](#)

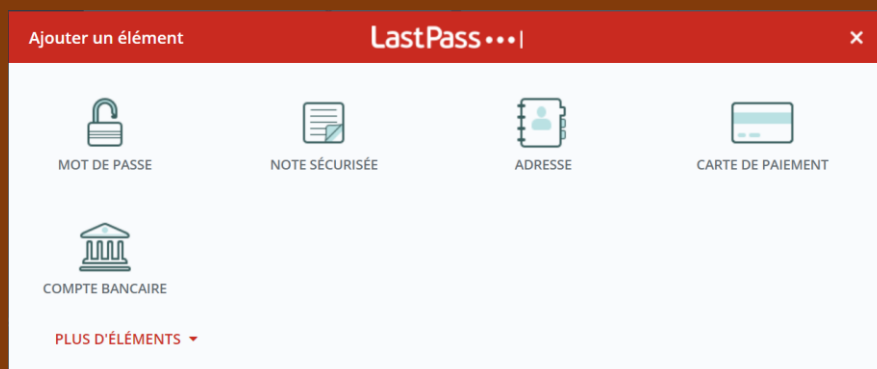
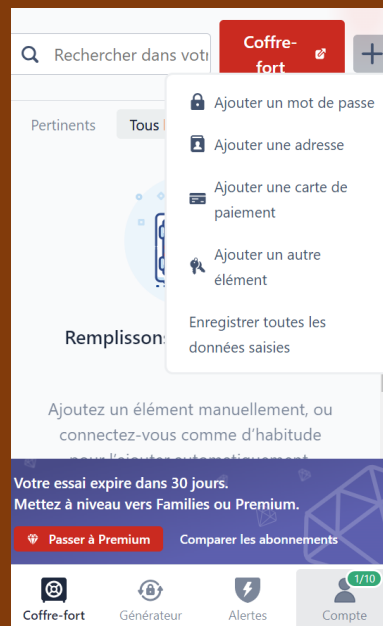
- Il te suffit de valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome".



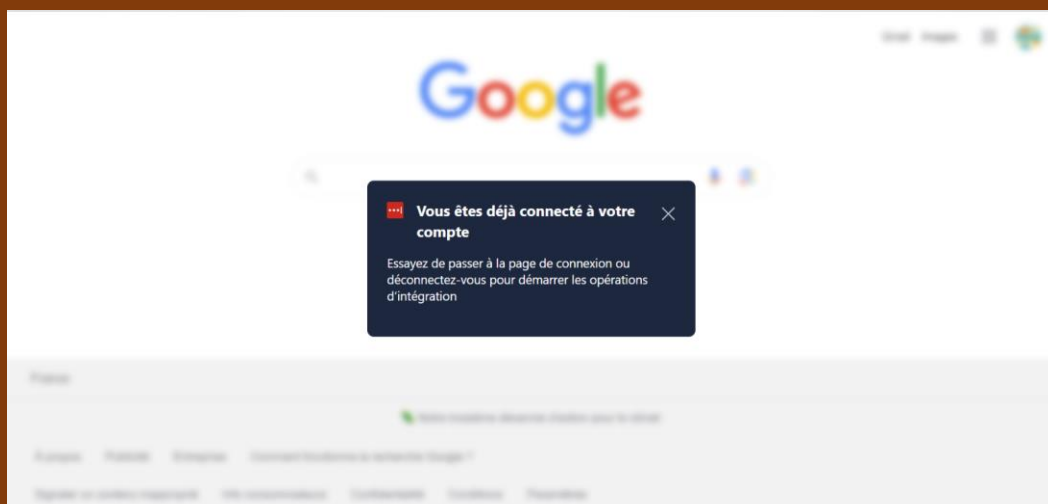
- Une fois installé, il te suffit d'accéder à cette extension et de t'y connecter
  - (1) En haut à droite du navigateur, clic sur le logo "Extensions" .



- 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 .



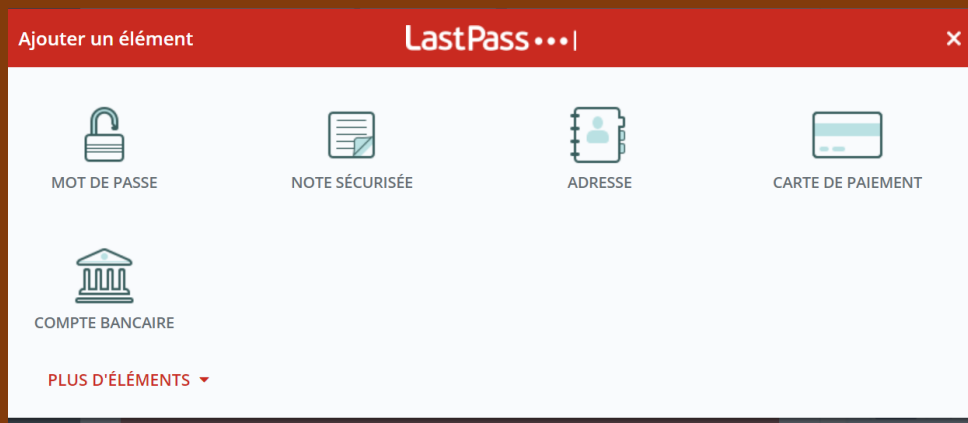
Désormais, lorsque tu te connectes à tes comptes, tu peux enregistrer le mot de passe grâce à LastPass puisque le compte est épinglé.



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. Une mise à jour automatique est faite sur les navigateurs installés.

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

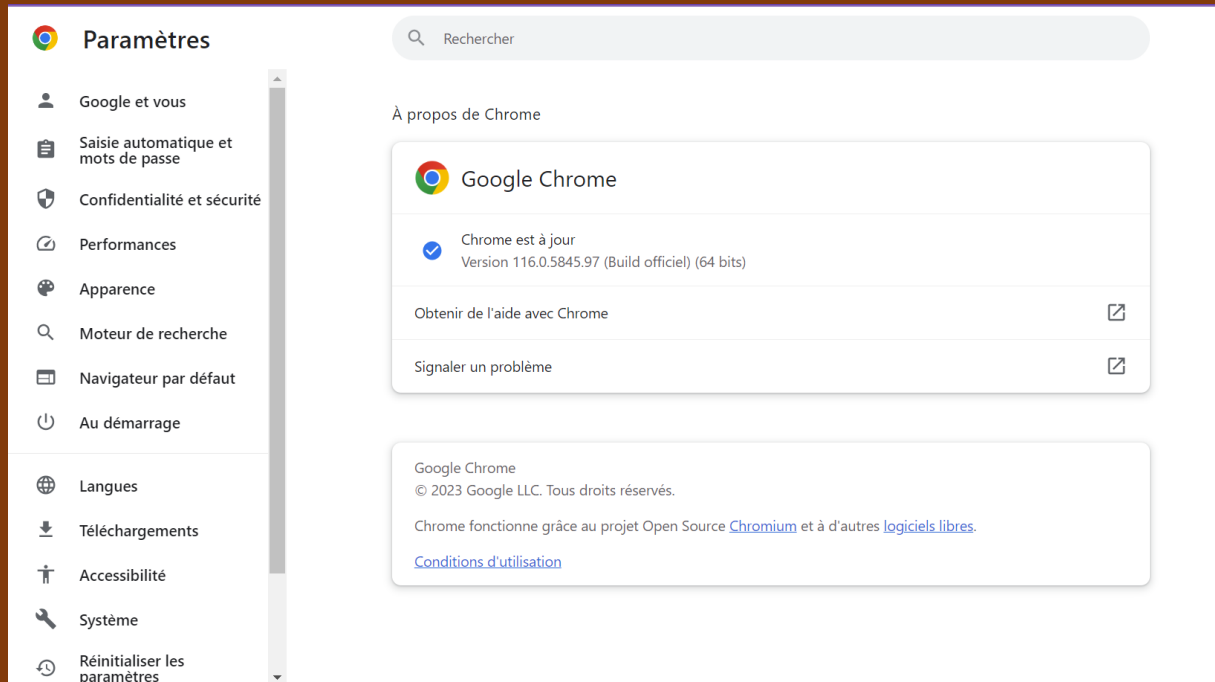
Les seuls sites qui semblaient être cohérents sont donc :


- 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).

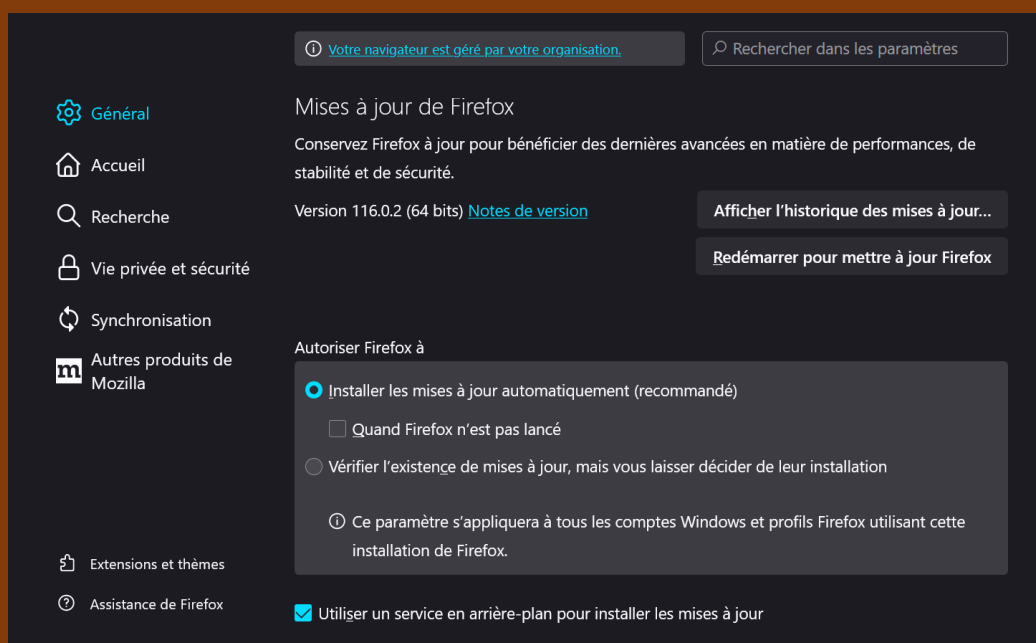
**2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes. (case à cocher)**

- ☐ Pour Chrome

- Ouvre le menu du navigateur  et accède aux “Paramètres” ;
- Clic sur la rubrique “À 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).





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 puisque le navigateur est un outil des développeurs.

## 4- Éviter le spam et le phishing

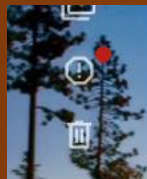
Objectif : *Reconnaître plus facilement les messages frauduleux*

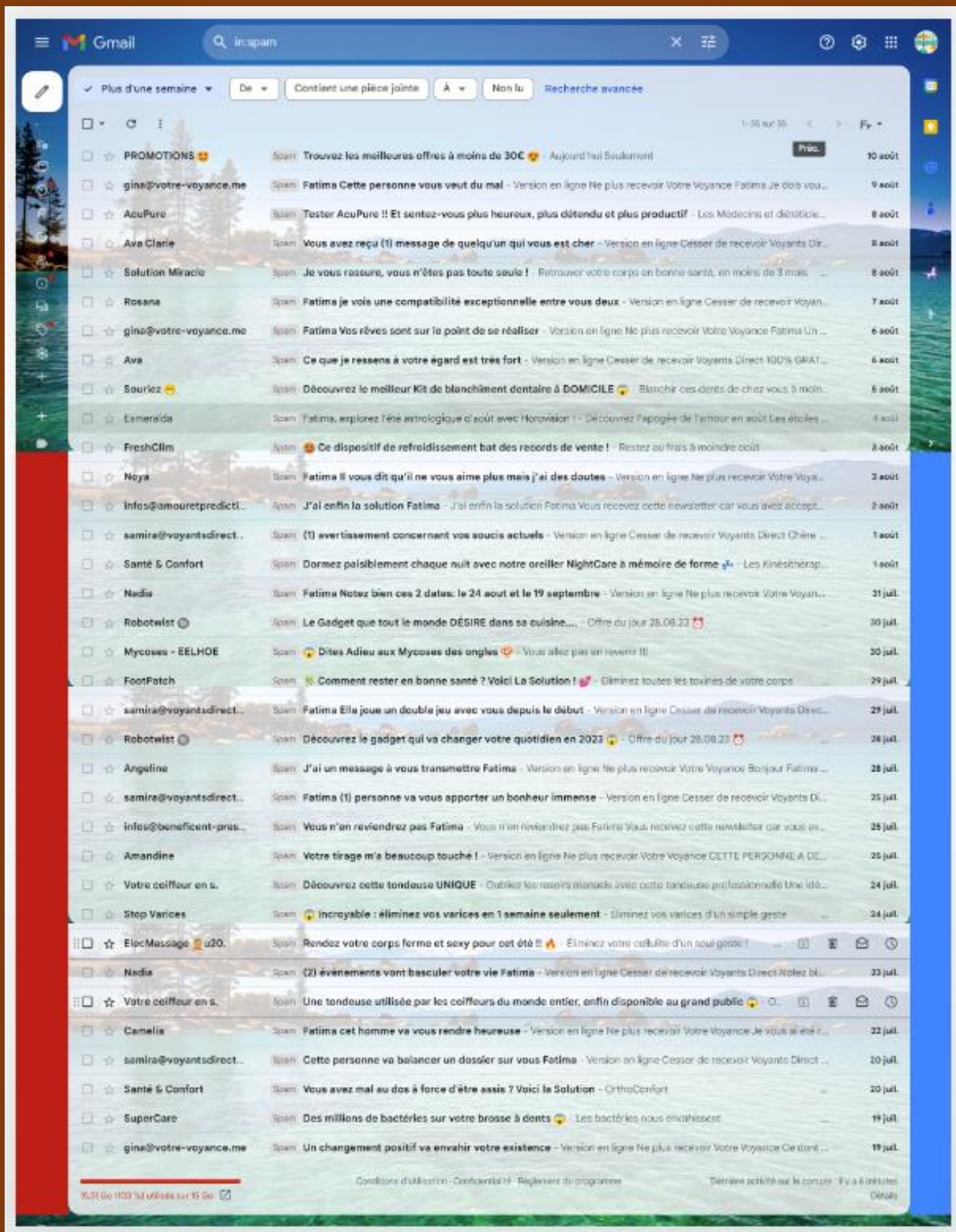
**1/ Dans cet exercice, on va exercer ta capacité à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.**

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 :

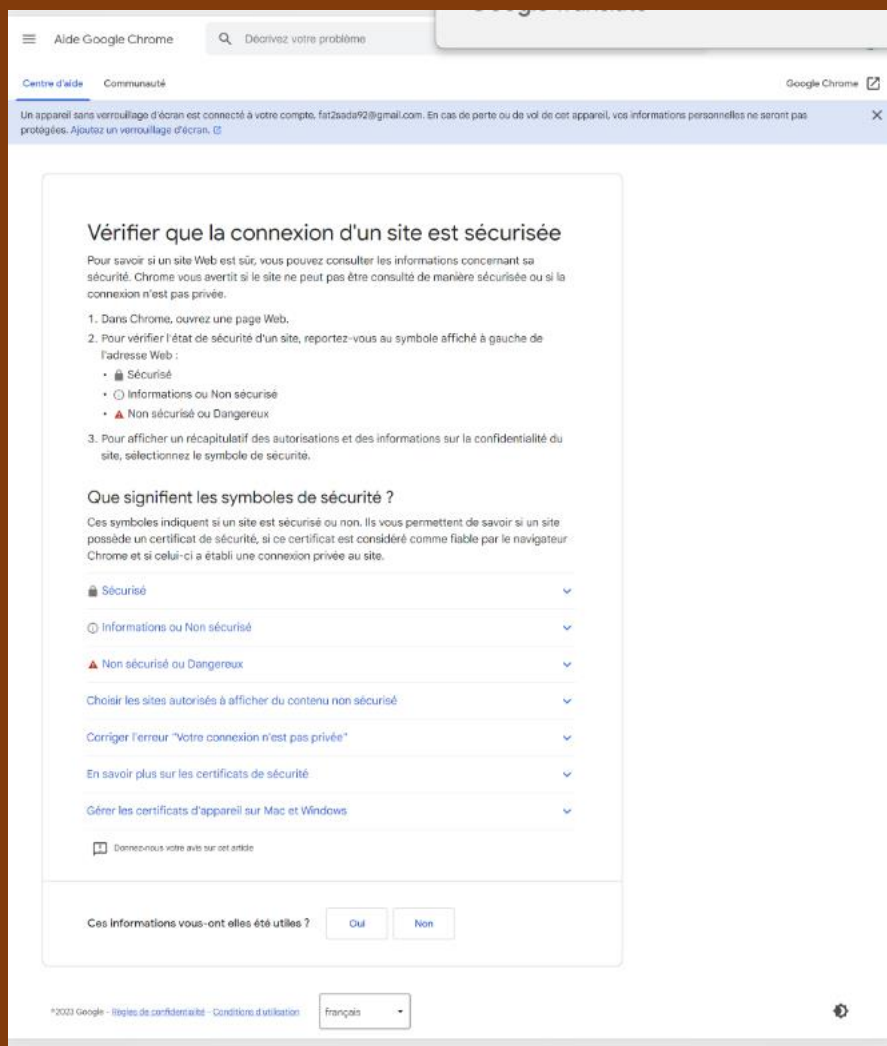
- Site du gouvernement [cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr)  
<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage>

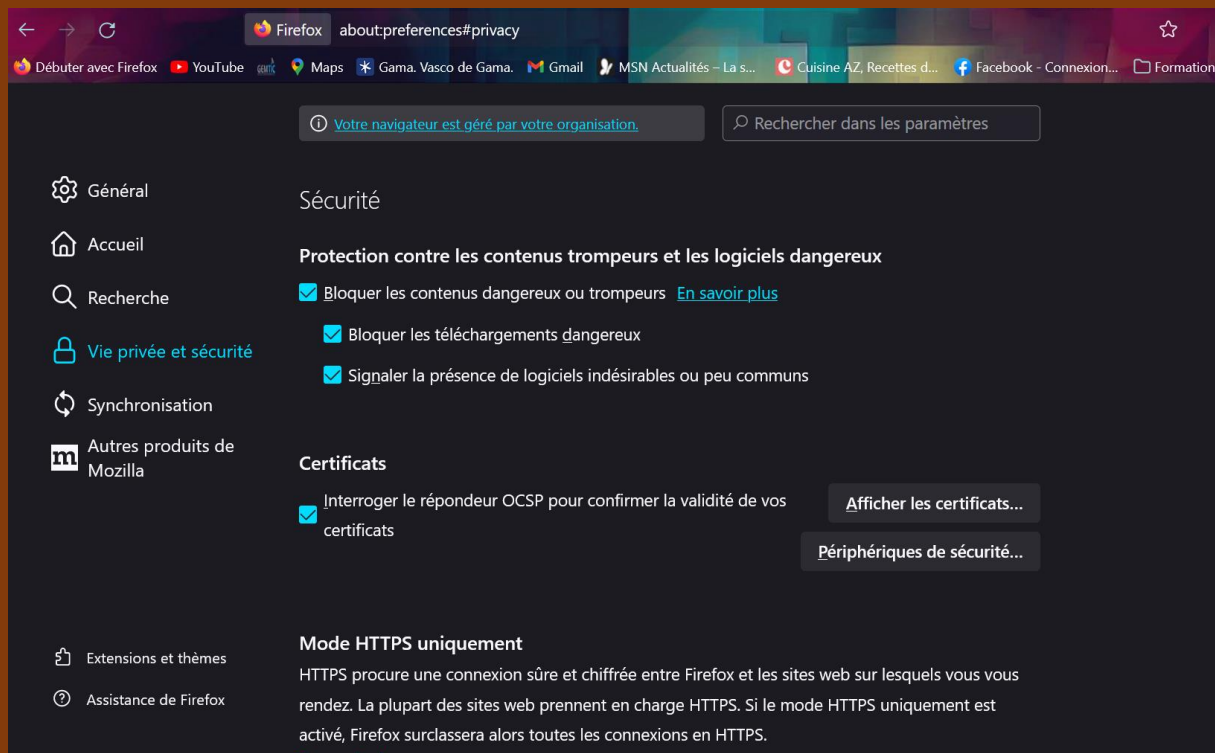
## 5- Comment éviter les logiciels malveillants

Objectif : *sécuriser votre ordinateur et identifier les liens suspects*

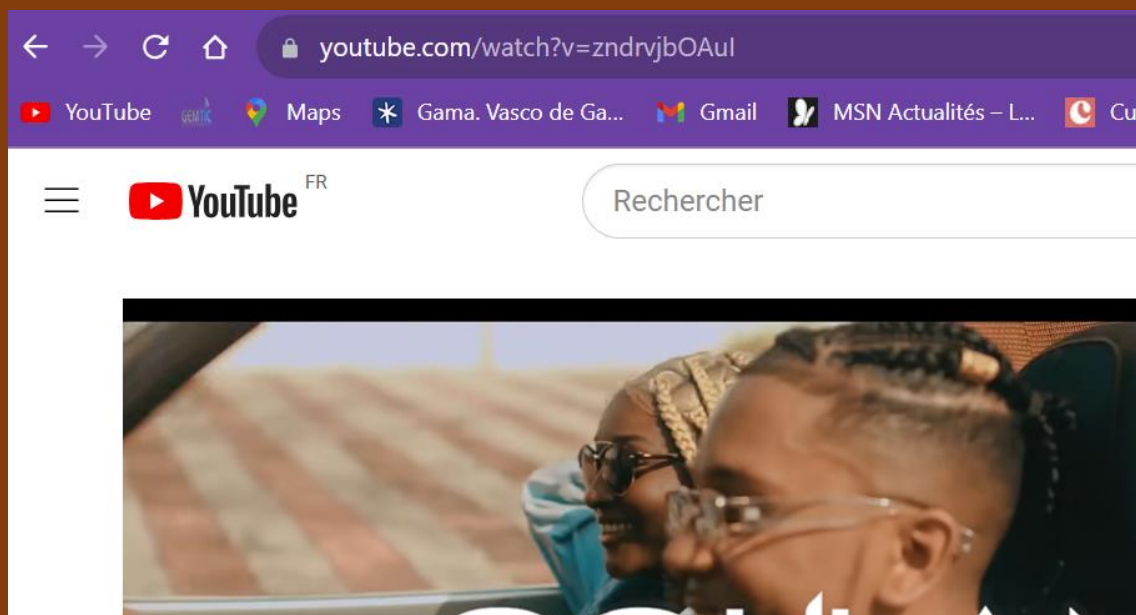
**3/ Lors de la navigation sur le web, il arrive d'avoir des doutes sur la sécurité de certains sites. Comme tu as pu le voir précédemment, le premier de niveau de vigilance à avoir se trouve dans la barre d'adresse des navigateurs web. La plupart affichent des indicateurs de sécurité pour donner une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



### ○ Indicateur de sécurité

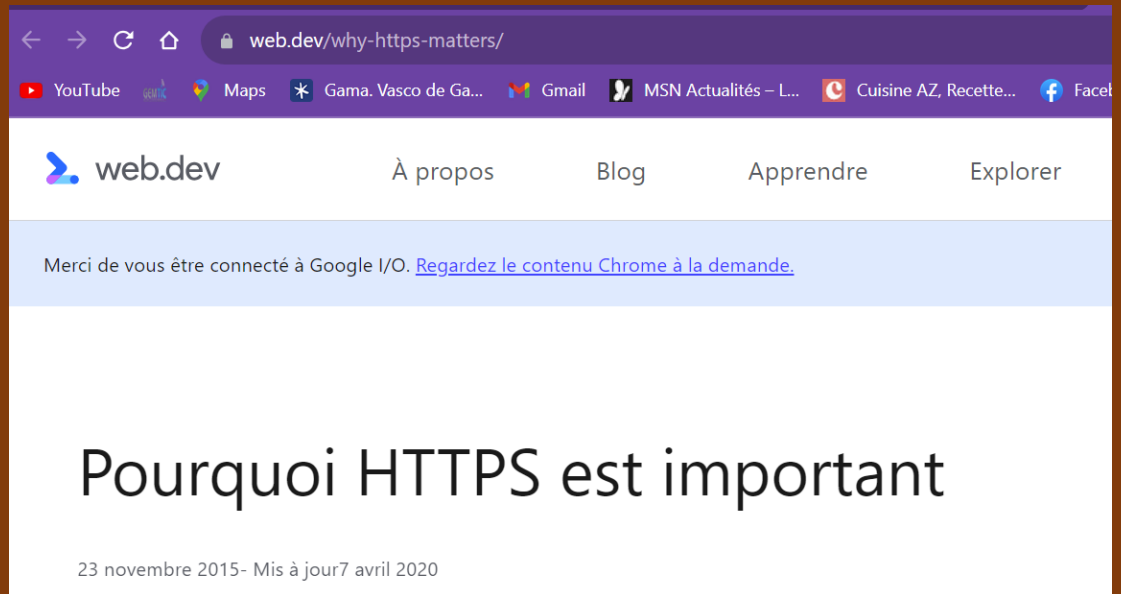
- HTTPS 

### Analyse Google

- Aucun contenu suspect
- Vérifier un URL en particulier ●




Site n°2 : **Web.Dev**



- **Indicateur de sécurité**
  - HTTPS 
- **Analyse Google**
  - Aucun contenu suspect
  - Vérifier un URL en particulier •

Site n°3 : **Git**



- **Indicateur de sécurité**
  - HTTPS 
- **Analyse Google**
  - Aucun contenu suspect
  - Vérifier un URL en particulier •

## 6- Achats en ligne sécurisés

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

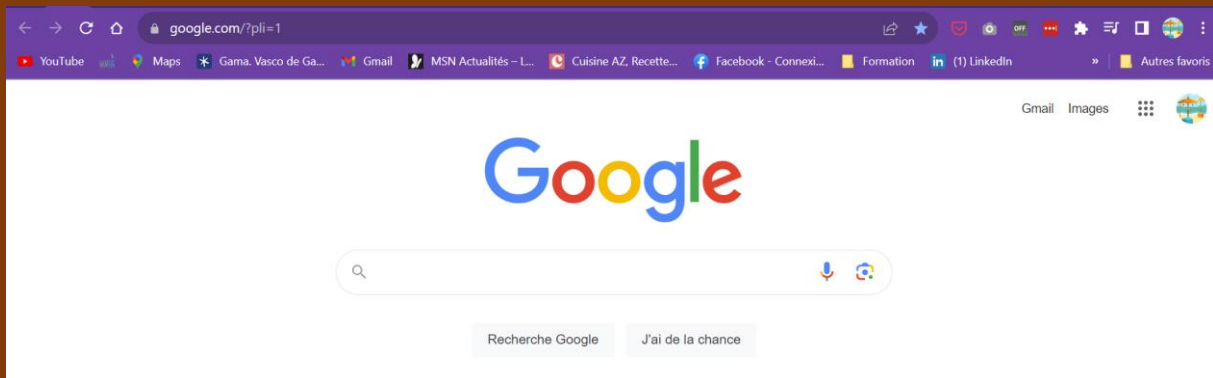
**1 / Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le bilan de tes dépenses du mois.**

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

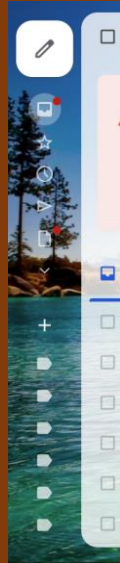
- 1. Créer un dossier sur ta messagerie électronique**
- 2. Créer un dossier sur ton espace de stockage personnel (en local ou sur le cloud)**

**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)**

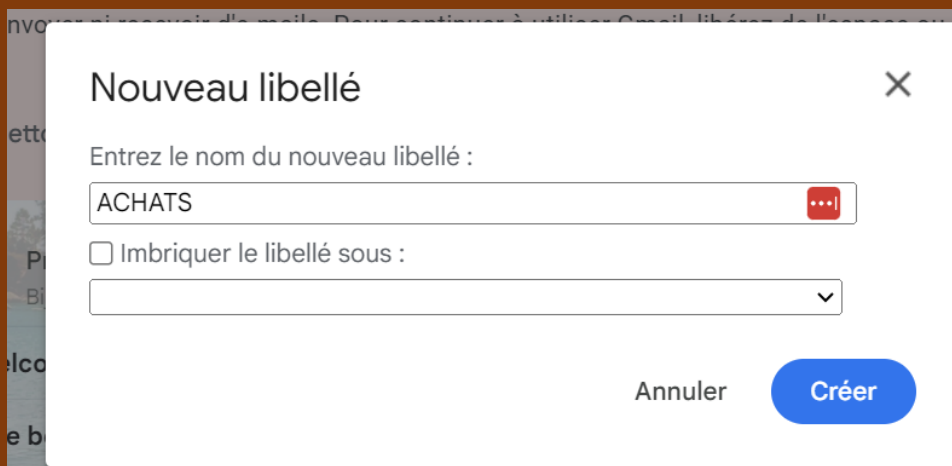
- Pour commencer, accède à ta messagerie électronique. Pour rappel, tu peux y accéder rapidement en ouvrant un nouvel onglet (dans la barre des favoris ou via le raccourci)



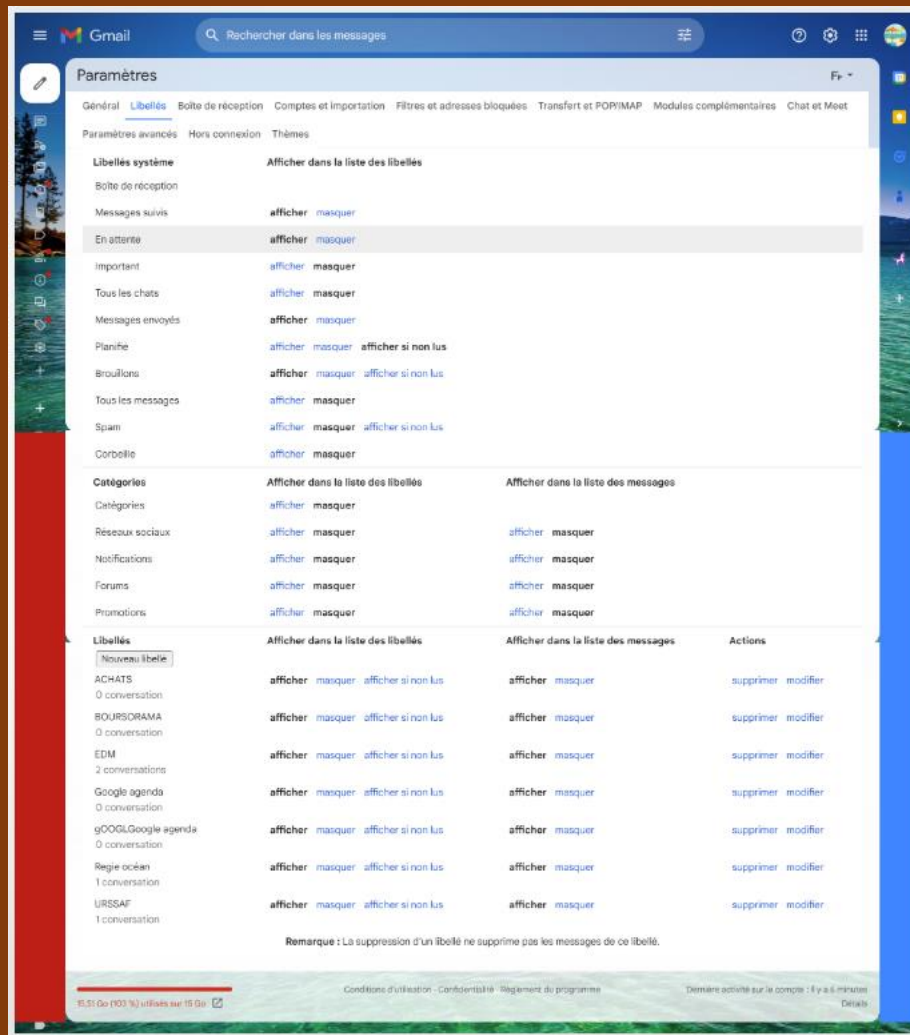
- Sur la page d'accueil de ta messagerie, tu trouveras sur la gauche les libellés initialement prévus (boîte de réception, messages envoyés, etc.)



- 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.

## 7 - Comprendre le suivi du navigateur

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

### Libellés

[Nouveau libellé](#)

ACHATS

0 conversation

BOURSORAMA

0 conversation

EDM

2 conversations

Google agenda

0 conversation

gOOGLEGoogle agenda

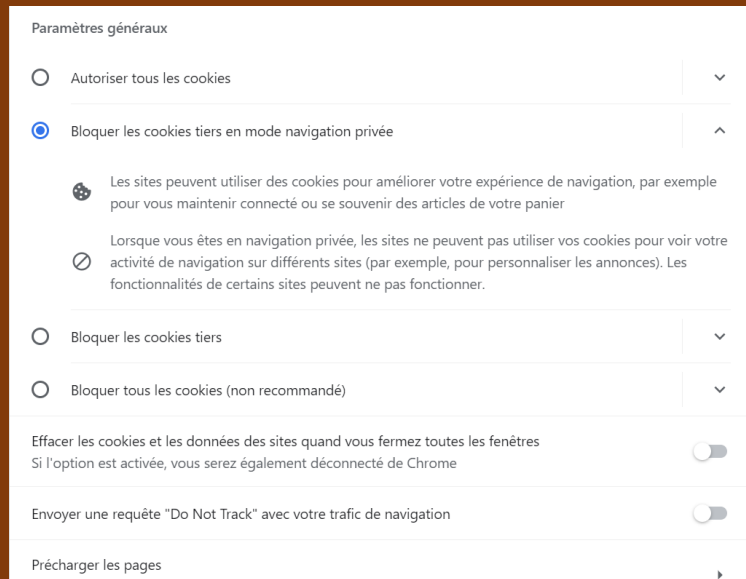
0 conversation

Regie océan

1 conversation

URSSAF




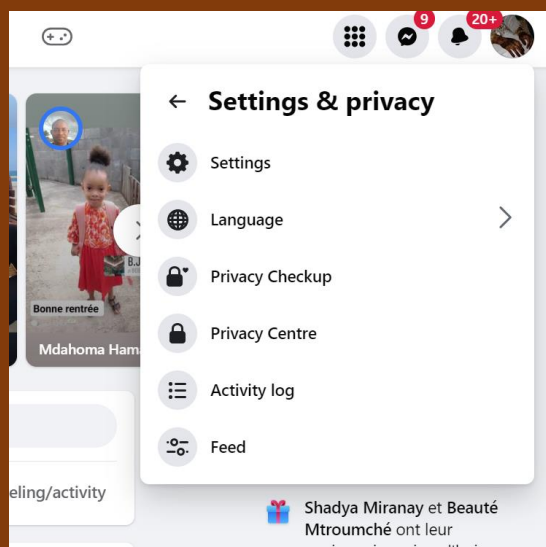


## 8- Principes de base de la confidentialité des médias sociaux

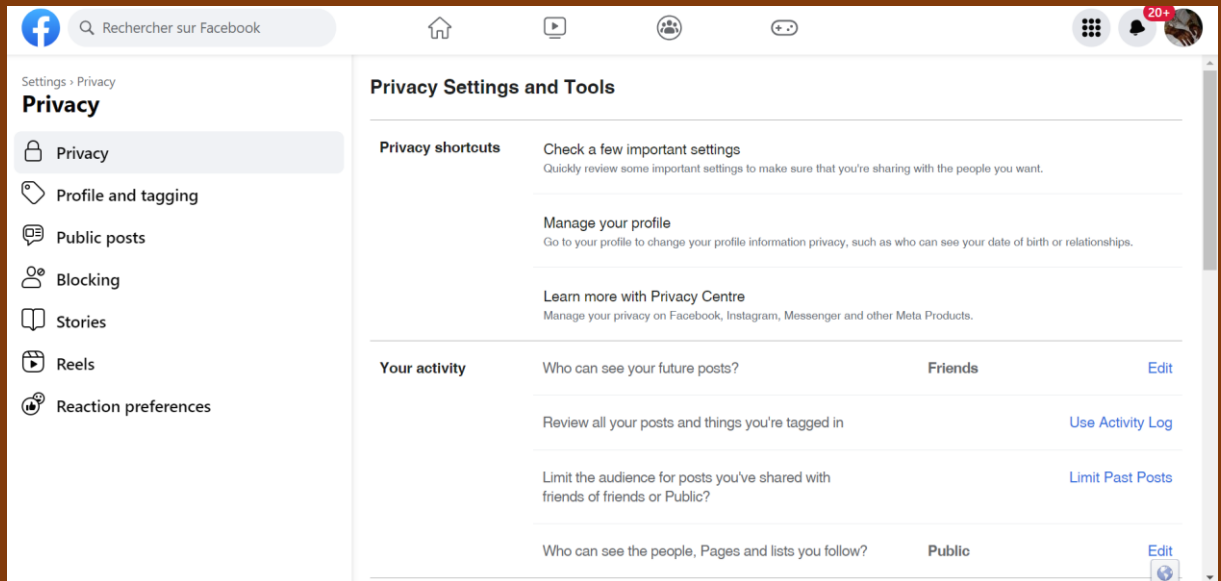
Objectif : Régler les paramètres de confidentialité de Facebook

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)

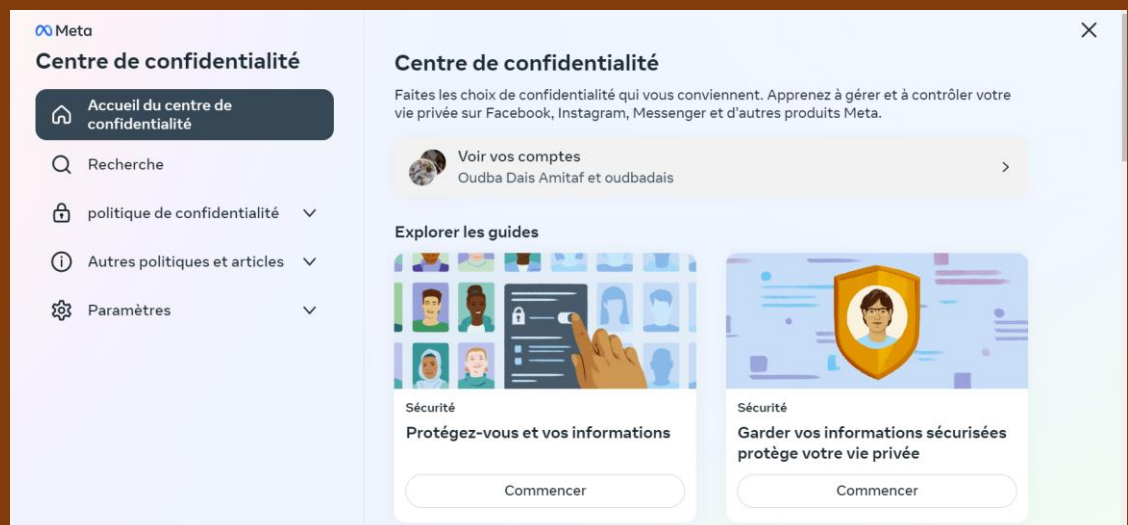
- Connecte-toi à ton compte Facebook ;
- Une fois sur la page d'accueil, ouvre le menu Facebook  , puis effectue un clic sur "Paramètres et confidentialité". Pour finir, clic sur "Paramètres".



- 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 te permettra de régler la visibilité de tes informations personnelles ;
  - La deuxième rubrique te permet de changer ton mot de passe ;
  - La troisième rubrique te permet de gérer la visibilité de ton profil pour la gestion des invitations ;
  - La quatrième rubrique permet de gérer la connexion simplifiée sur des applications ou des sites utilisés qui permettent cela ;
    - La dernière rubrique permet de gérer les informations récoltées par Facebook utiles pour les annonceurs.

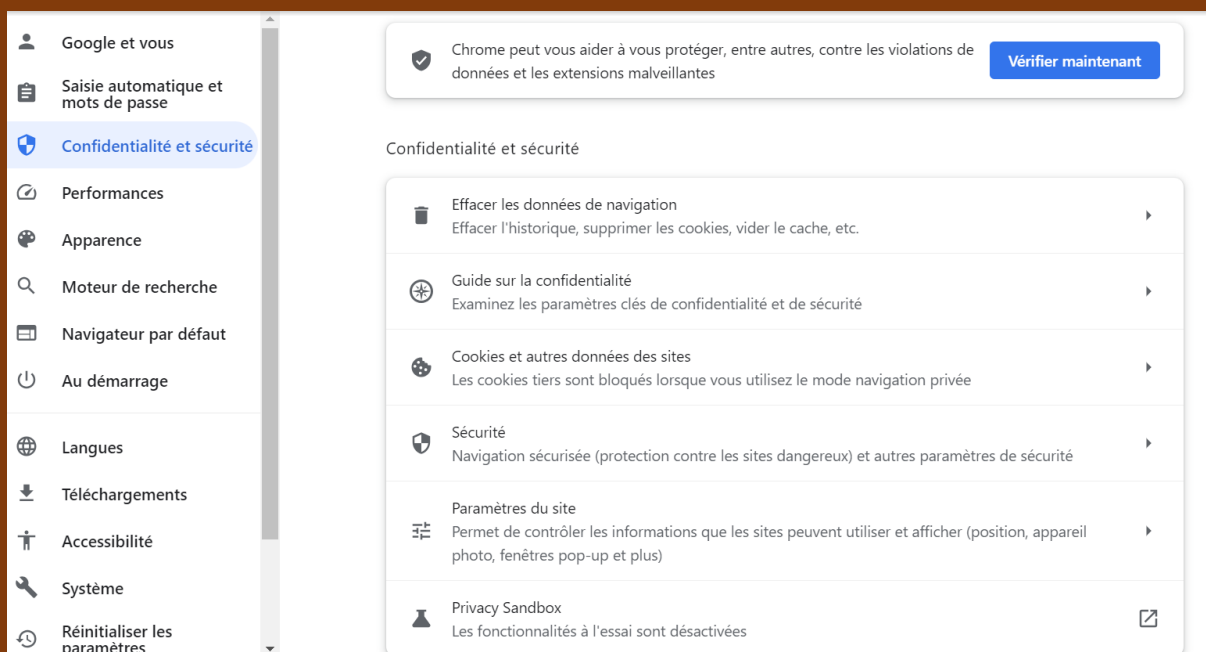
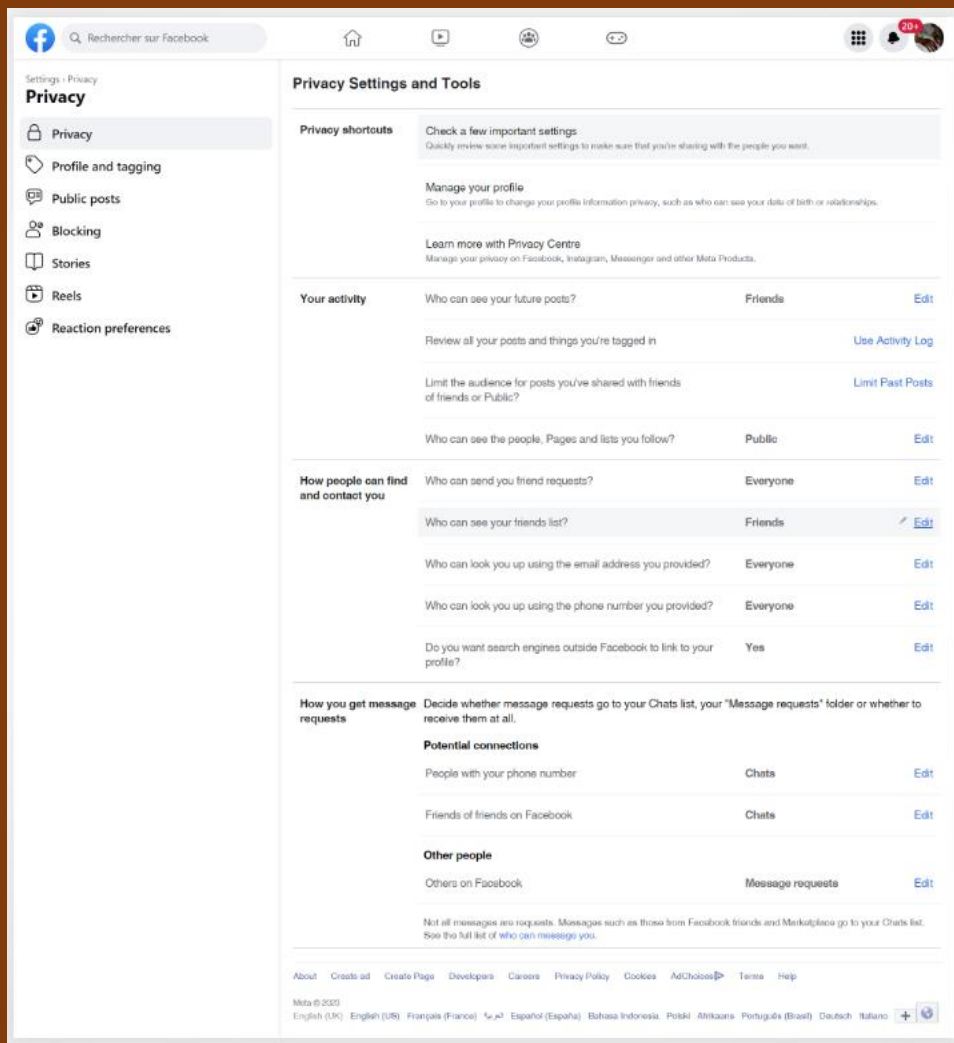


- Retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à gauche. Tu peux continuer à explorer les rubriques pour personnaliser tes paramètres. On ne peut pas te dire ce que tu dois faire. C'est à toi de choisir les informations que tu souhaites partager et celles que tu veux 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.

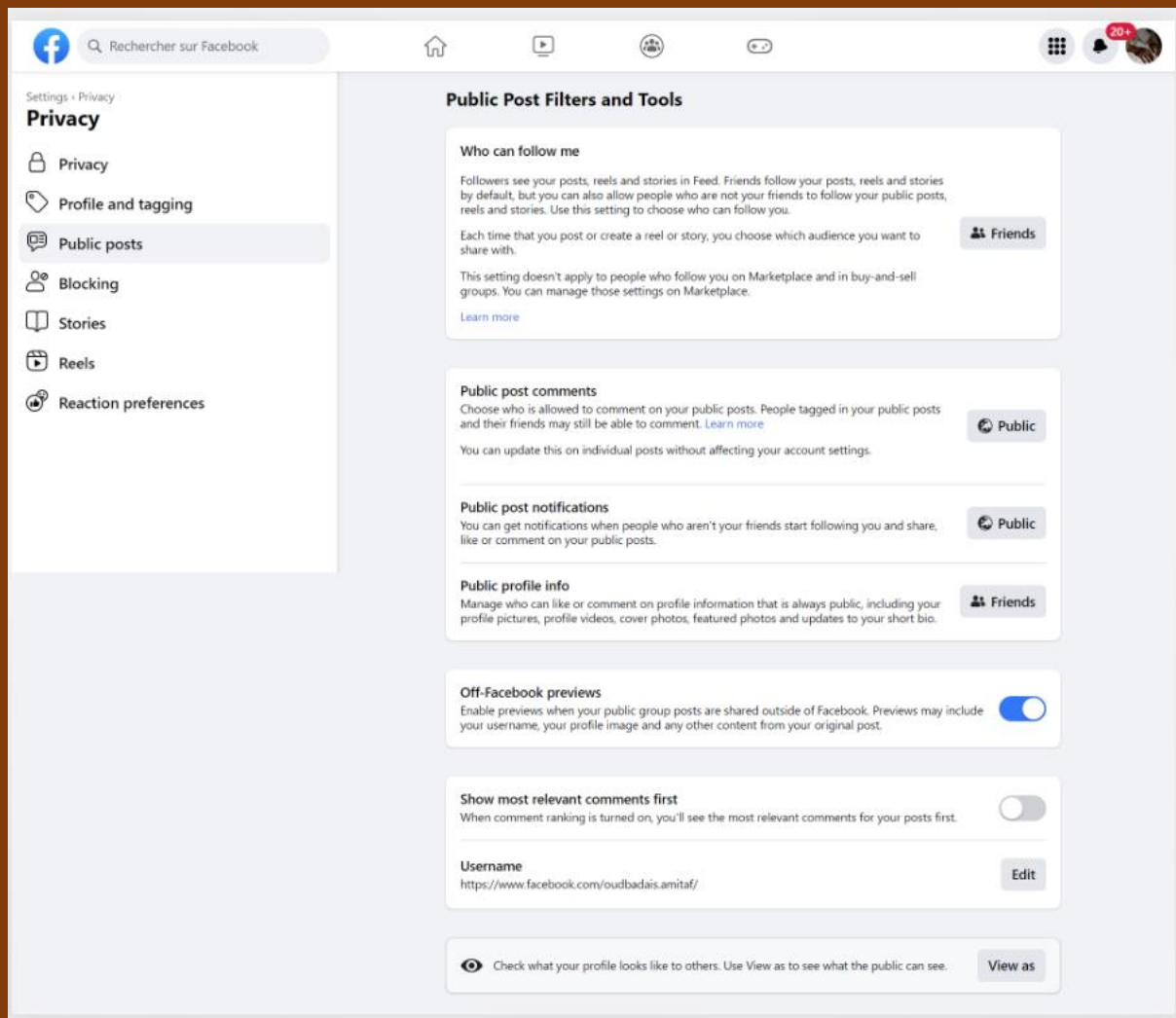
### Réponse 1

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 ????????




## Créer un compte Firefox


Pocket utilise les comptes Firefox pour préserver la confidentialité et la sécurité de vos données. [En savoir plus](#)

Inscription

 Utiliser un compte Firefox existant

OU

 Continuer avec Apple

 Continuer avec Google

Vous avez déjà un compte ? [Connectez-vous](#)

En poursuivant, vous acceptez :  
 Les [Conditions d'utilisation](#) et la [Politique de confidentialité](#) de Pocket  
 Les [Conditions d'utilisation](#) et la [Politique de confidentialité](#) de Firefox

 Avast Antivirus

 Fermer

 **Avast**

GÉRER CES NOTIFICATIONS ✓

### Une petite leçon sur les dangers posés par les RAT

Les RAT (Remote Access Trojans), ou chevaux de Troie d'accès à distance, constituent une menace unique dans le monde de la cybersécurité. Il s'agit d'une menace dangereuse et courante, qu'il est recommandé de surveiller en raison des dommages qu'elle peut causer et de l'ingéniosité dont font preuve les cybercriminels lorsqu'ils tentent d'infecter votre ordinateur.

**En bref**

1. Les RAT sont des outils qui offrent aux cybercriminels un accès complet à l'ordinateur d'une victime, y compris à ses **fichiers et sa webcam**.
2. Les RAT sont parfois vendus en tant que logiciels soi-disant « légitimes », mais ils ne le sont jamais. **Ne faites pas confiance à un RAT !**
3. Les cybercriminels ont tenté de diffuser des RAT par le biais de **logiciels piratés, d'e-mails et de sites web infectés**.
4. Les nombreux **agents de protection d'Avast** vous aideront à vous protéger de cette menace quelque peu intimidante.



Source : Données des laboratoires de menaces Avast

 Ce message vous a-t-il été utile ?
 






COMMENT LES ÉVITER →

✕ Fermer



GÉRER CES NOTIFICATIONS ✓

## Comment éviter les RAT ?

Si les chevaux de Troie d'accès à distance, et en particulier leur capacité à donner à un pirate informatique le contrôle total de votre appareil à distance, sont plus inquiétants que beaucoup d'autres menaces, ils se propagent à peu près de la même manière.



Lorsque vous achetez un logiciel en ligne, assurez-vous qu'il **provient d'une source légitime**. Si cela n'est pas possible, vérifiez le logiciel à l'aide d'un antivirus et exécutez-le tout d'abord dans une instance isolée (mode Sandbox).



Ne naviguez pas sans protection ! **Utilisez l'Agent web Avast** (ou au moins un bloqueur de pub) pour vous protéger des sites web dangereux ou des publicités infectées, également appelées « malvertising ».



Vous avez reçu un e-mail étrange accompagné d'une pièce jointe encore plus étrange ? Ne l'ouvrez pas. Si vous n'êtes pas sûr, vous pouvez l'analyser avec l'outil de sécurité de votre choix **ou utiliser notre Protection e-mail**.



Comme toujours, faites preuve de prudence face aux promesses ou aux menaces que vous recevez de la part d'inconnus en ligne. Les cybercriminels sont prêts à tout pour vous inciter à cliquer sur un lien de téléchargement ou une pièce jointe à un e-mail. **Alors, restez sur vos gardes.**

← RETOUR

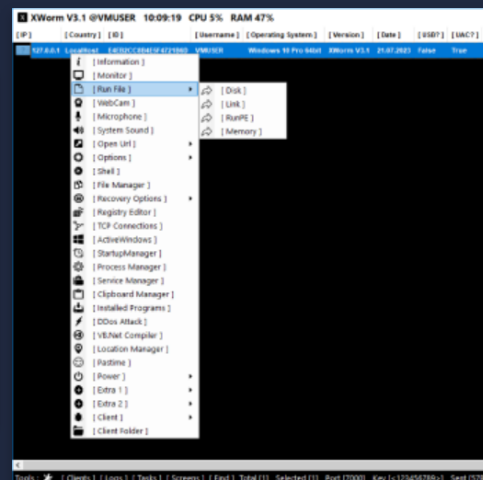
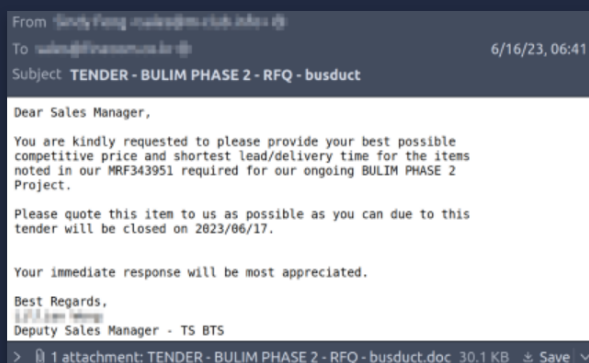
À QUOI RESSEMBLENT-ILS ? →

✕ Fermer



GÉRER CES NOTIFICATIONS ✓

## Un e-mail de RAT et le panneau de contrôle du pirate informatique



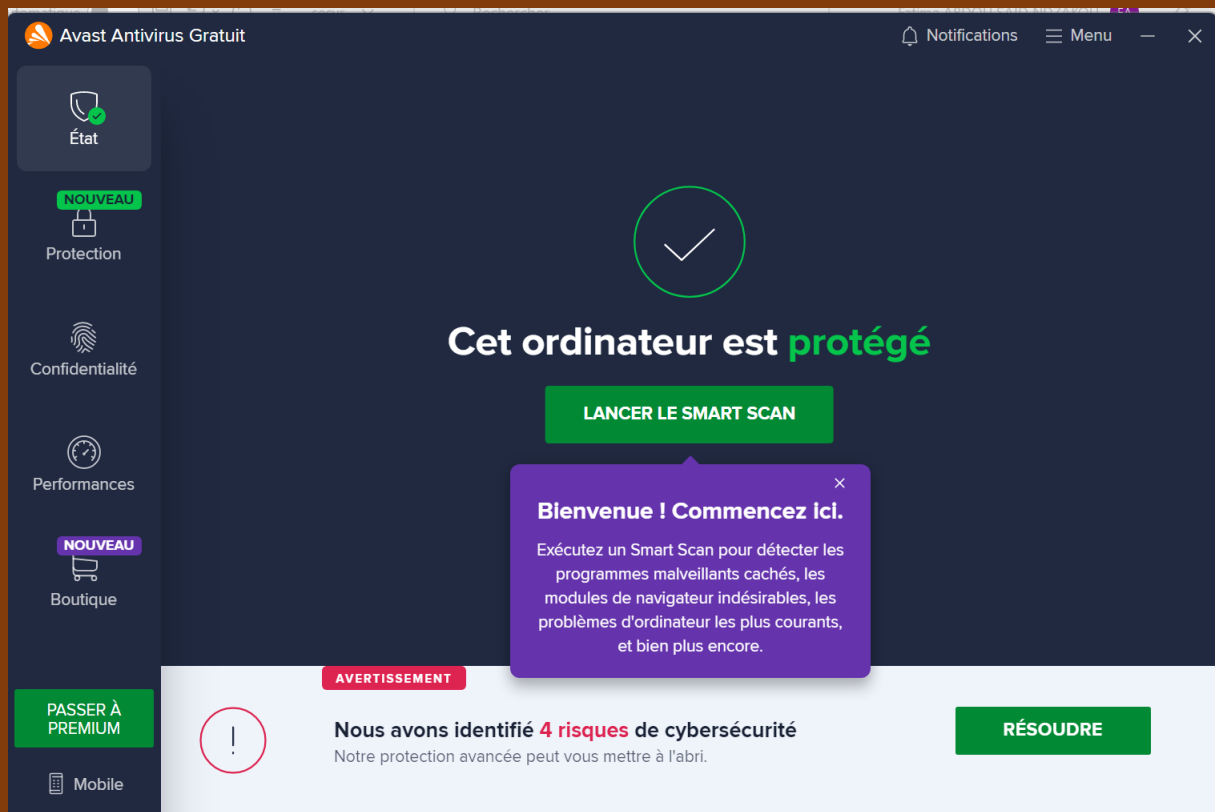
L'image de gauche est un exemple trouvé sur Internet, nous ne l'avons pas générée. L'image de droite a été générée par nos soins, mais elle est authentique. Tous les logos ou marques affichés sont des marques déposées.

Source : Données des laboratoires de menaces Avast

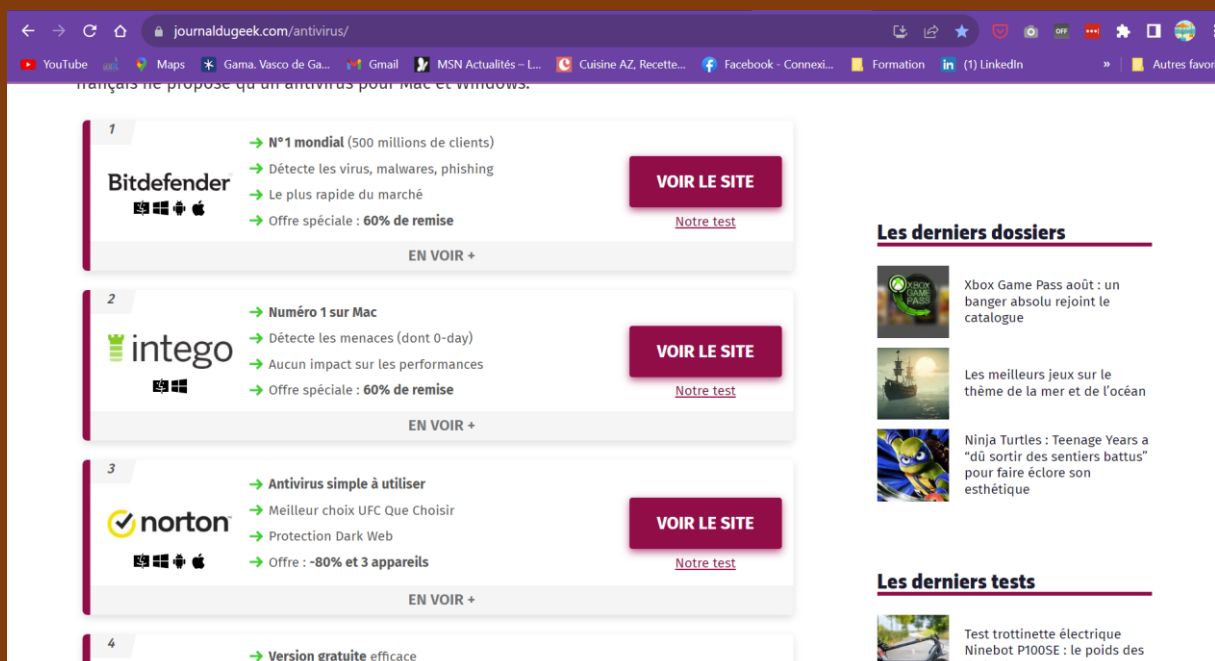
← RETOUR

CONCLUSION →





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






**AVG AntiVirus Free**

PASSER À PREMIUM

2 Notifications
 Menu



## Le Mode passif est activé

Nous avons désactivé la protection en temps réel car un autre antivirus est installé. Mais n'hésitez pas à exécuter vous-même des analyses.

**PROTECTION BASIQUE**



Informatique  
Non protégé



Web et email  
Non protégé  
Bloque les menaces

**PROTECTION COMPLÈTE**



Attaques de pirates  
Non protégé



Données personnelles  
Non protégé

**EXPLORER**



**NEW**  
Boutique  
Acheter


**VOUS ÊTES À JOUR**  
 Dernière mise à jour le : il y a 2 minutes

AFFICHER LES RÉSULTATS


EXÉCUTER D'AUTRES ANALYSES
   
 Dernière analyse antivirus : il y a 2 jours








Vous avez un cadeau de bienvenue de la part d'AVG.  
Déballez-le maintenant et découvrez ce qui vous attend.

DÉBALLER

On peut passer en premium pour avoir plus de fonctionnalité afin de mieux protéger son ordinateur et ses données.


**AVG AntiVirus gratuit**

Réclamez votre cadeau de bienvenue : **81 %** de réduction

	Protection actuelle <b>Antivirus Gratuit</b>	Mise à niveau vers <b>Internet Security</b>
 Bloquez les malwares en temps réel	✓	✓
 Préservez votre PC contre les pirates <small>Empêchez les pirates d'accéder à votre PC grâce à notre Pare-feu amélioré et bloquez les connexions Remote Desktop indésirables grâce à notre Agent contre l'accès à distance.</small>		✓
 Mettez fin à l'espionnage par webcam		✓
 Protégez vos documents personnels		✓
 Sécurisez vos achats en évitant les sites web frauduleux		✓
		<b>1,49 € par mois</b> CONTINUER