

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 source 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.

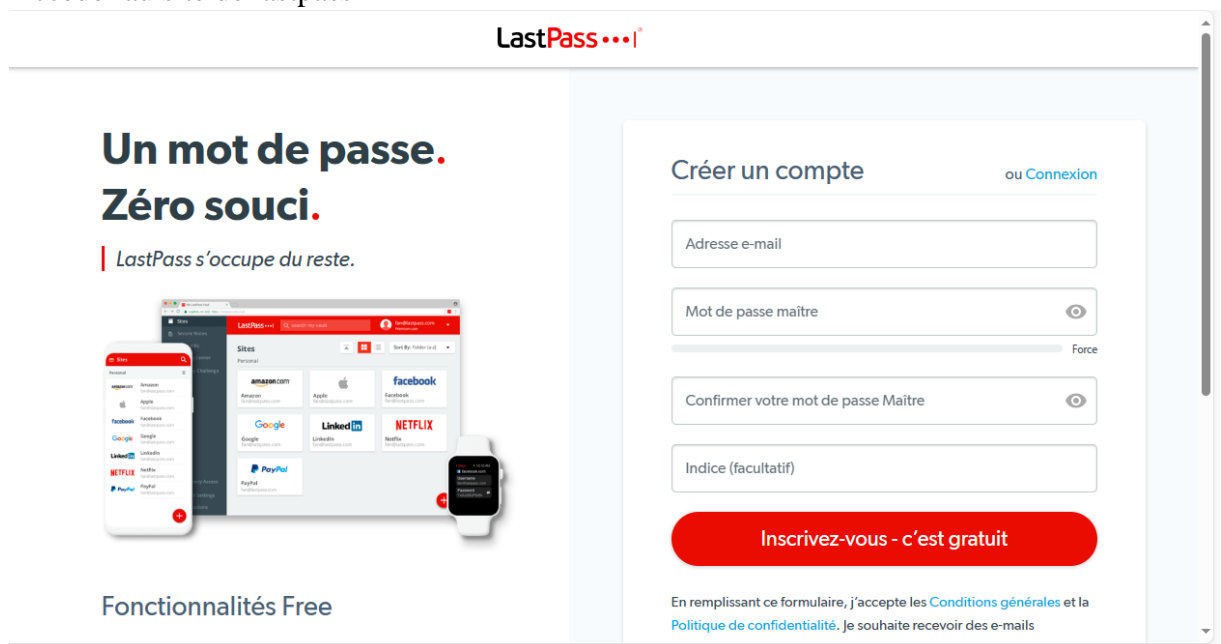
- Article 1 = DESSI – SECURITE INFORMATIQUE
- Article 2 = REDHAT – COMPRENDRE LA SECURITE INFORMATIQUE
- Article 3 = HPE- QU'EST-CE QUE LA SECURITE INFORMATIQUE ?

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)

- ❖ Accéder au site de lastpass



The screenshot shows the LastPass website interface. At the top, the LastPass logo is visible. Below it, a promotional banner reads "Un mot de passe. Zéro souci." followed by "LastPass s'occupe du reste." and "Fonctionnalités Free". The main content area features a "Créer un compte" (Create an account) form with the following fields: "Adresse e-mail", "Mot de passe maître" (Master password) with a strength indicator, "Confirmer votre mot de passe Maître" (Confirm your master password), and "Indice (facultatif)" (Optional hint). A red button labeled "Inscrivez-vous - c'est gratuit" (Sign up - it's free) is at the bottom of the form. Below the button, there is a line of text: "En remplissant ce formulaire, j'accepte les Conditions générales et la Politique de confidentialité. Je souhaite recevoir des e-mails". A "ou Connexion" (or Login) link is located next to the "Créer un compte" header.

- ❖ Si on a déjà un compte il suffit de se connecter

3. Fonctionnalité de sécurité de votre navigateur

Objectif : identifier les éléments à observer pour naviguer sur le web en toute sécurité

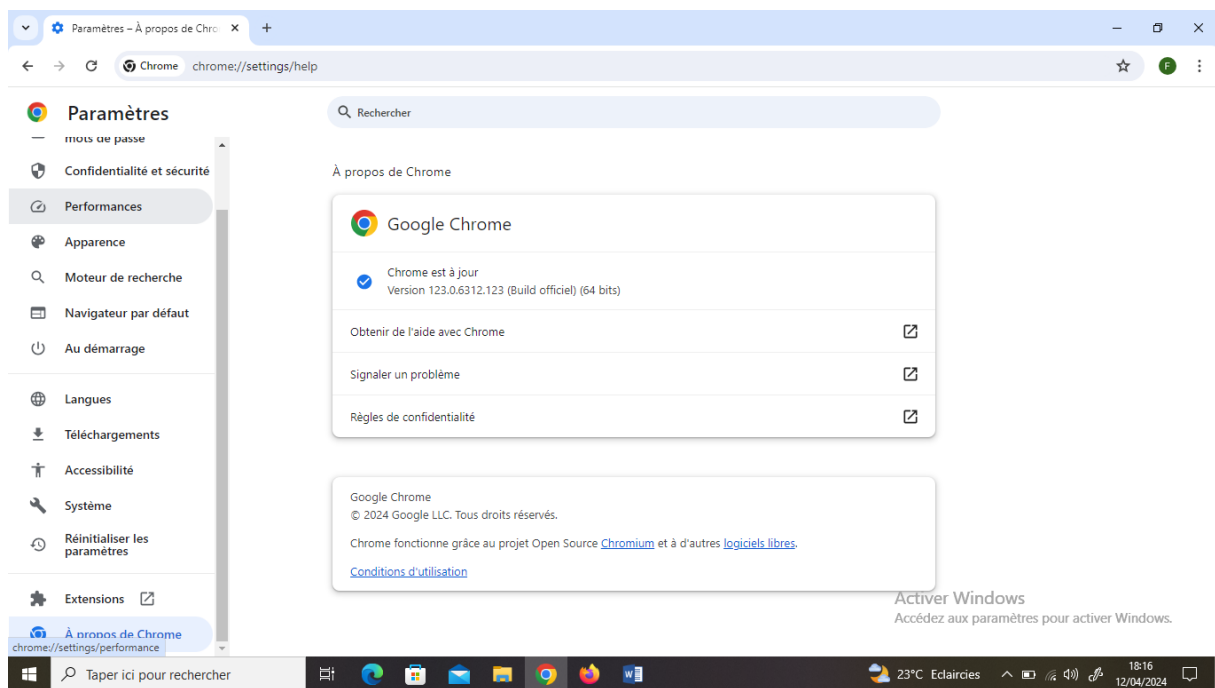
1/ Identifie les adresses internet qui te semblent provenir de sites web malveillants.

(Case à cocher)

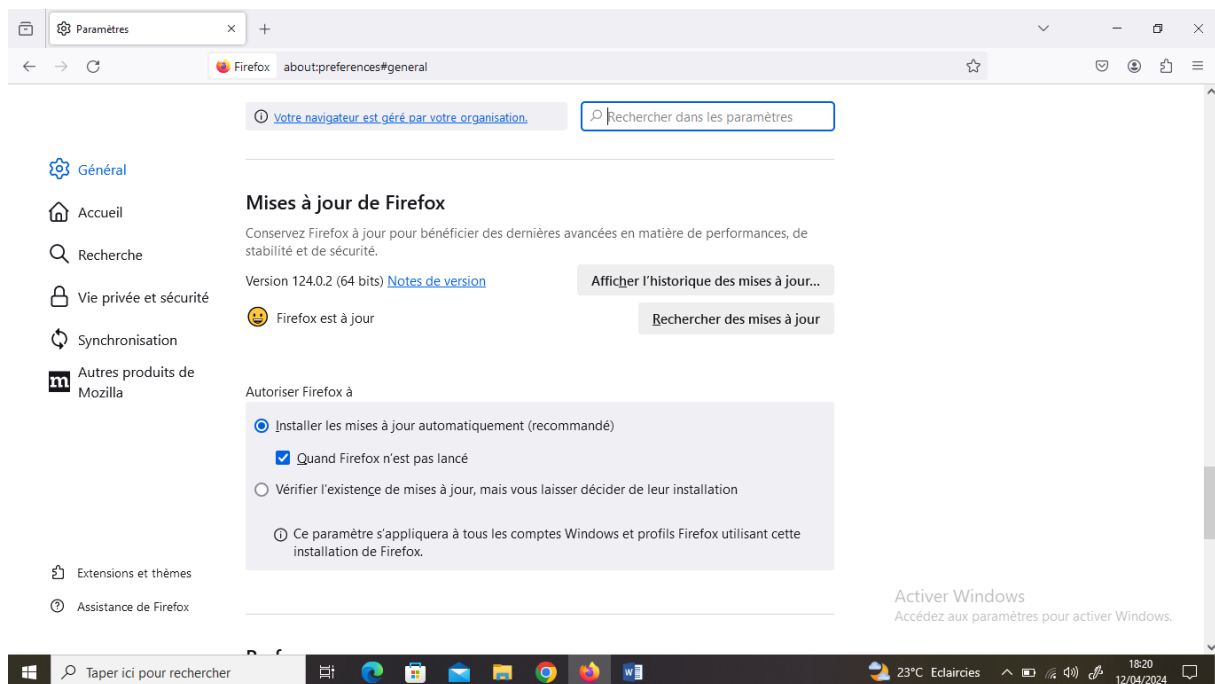
- www.morvel.com
- www.dccomics.com
- www.ironman.com
- www.fessebook.com
- www.instagam.com

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



❖ Pour Firefox



4. Éviter le spam et le phishing

Objectif : Reconnaître plus facilement les messages frauduleux

5. Comment éviter les logiciels malveillants

Objectif : sécuriser votre ordinateur et identifier les liens suspects

1° 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)

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)

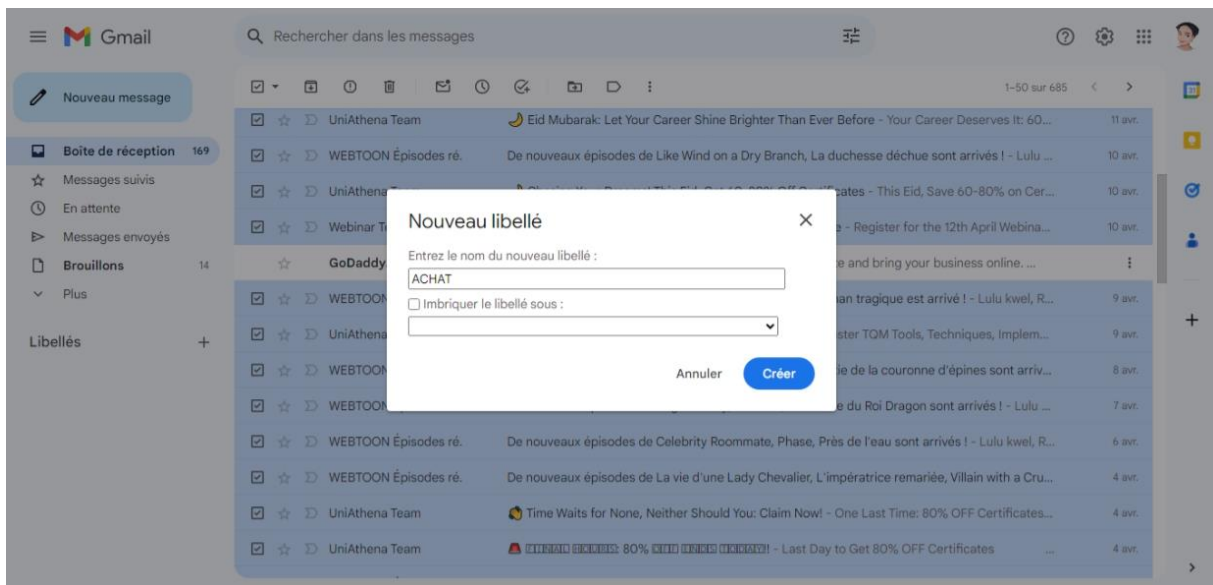
6. Achats en ligne sécurisés

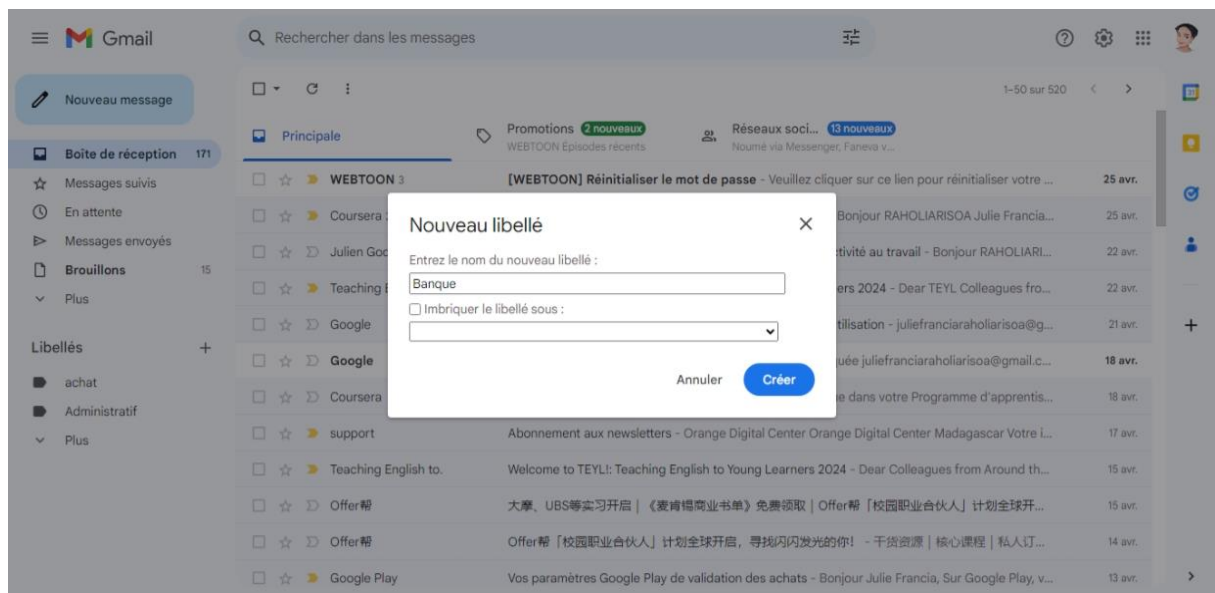
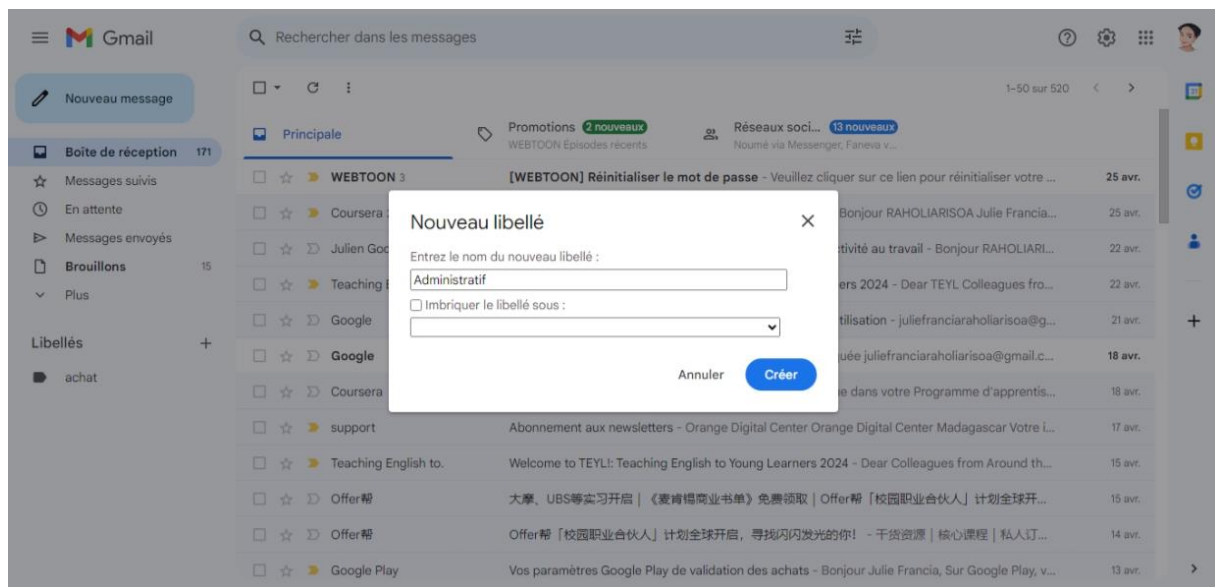
Objectif : créer un registre des achats effectués sur internet

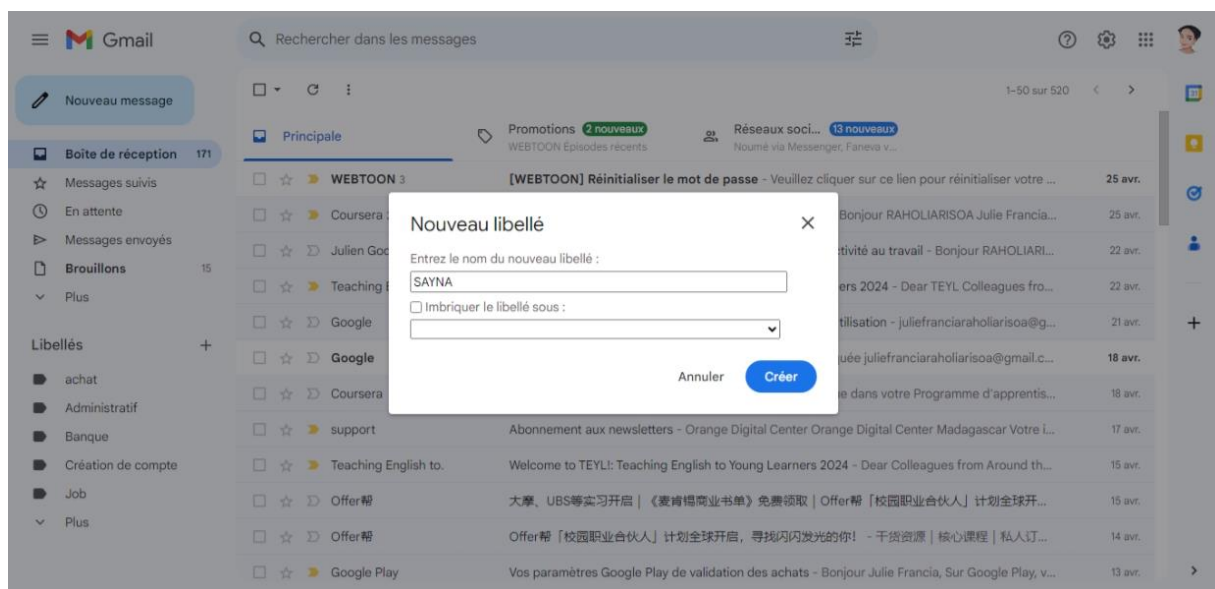
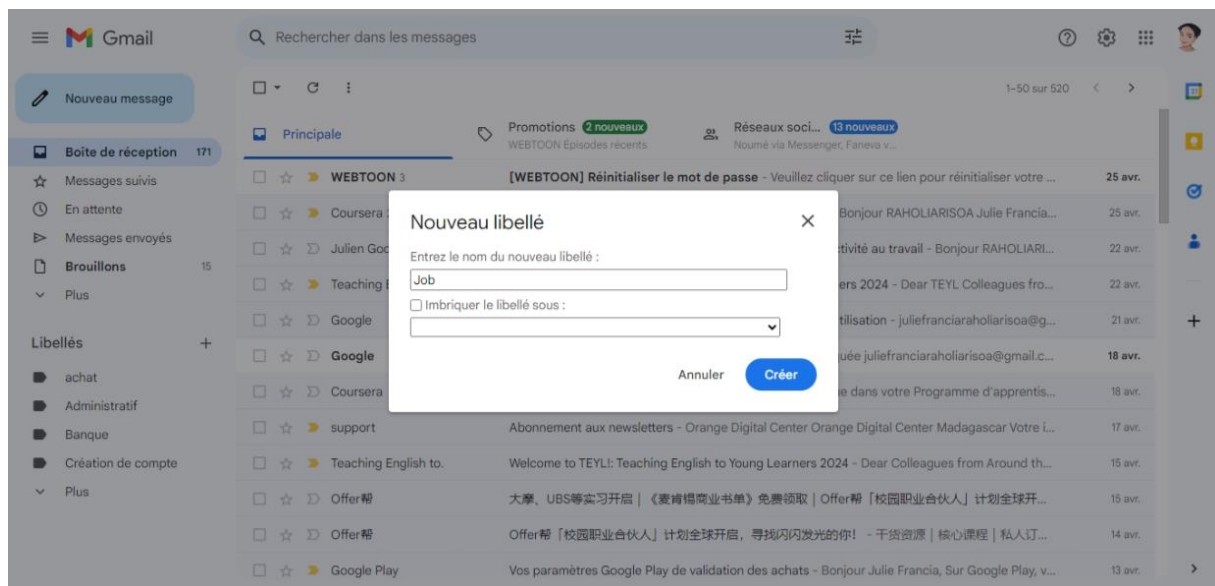
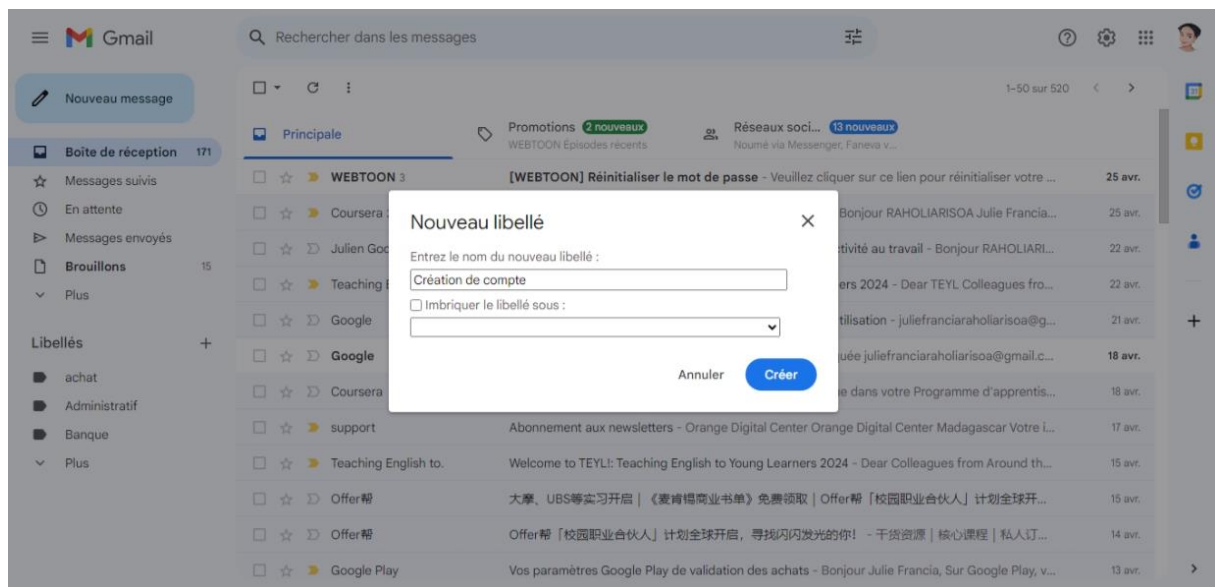
1/ Dans cet exercice, on va t'aider à créer un registre des achats. Comme tu as pu le voir dans le cours, ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le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

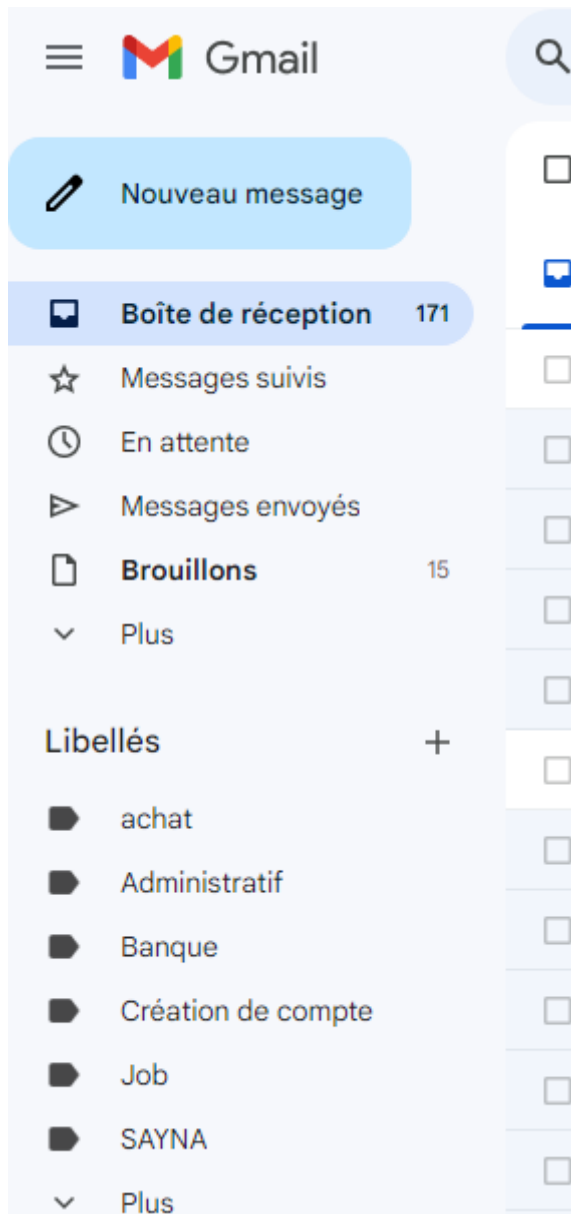
Deux possibilités s'offrent à toi pour organiser ce registre :

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









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 »




Rechercher sur Facebook







20+





Paramètres et confidentialité


Rechercher dans les paramètres

**Espace Comptes**
Gérez vos expériences partagées et vos paramètres de comptes sur l'ensemble des technologies Meta.

 Informations personnelles

 Mot de passe et sécurité


 Préférences publicitaires


 Vérification

En voir plus dans l'Espace Comptes

Outils et ressources

Nos outils vous aident à contrôler et gérer votre confi...


 Assistance confidentialité


 Supervision parentale


Trouvez le paramètre dont vous avez besoin

Rechercher dans les paramètres






Vous cherchez autre chose ?




**Centre de confidentialité**
Découvrez comment gérer et contrôler votre confidentialité au sein des produits Meta. →

**Pages d'aide Facebook**
Apprenez-en plus sur la version mise à jour de nos paramètres sur Facebook. →




Rechercher sur Facebook






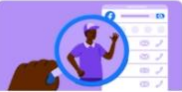
20+





Assistance confidentialité


Nous vous aiderons à prendre les bonnes décisions pour les paramètres de votre compte.
Par quelle rubrique voulez-vous commencer ?

**Qui peut voir ce que vous partagez**

**Comment il est possible de vous trouver sur Facebook**

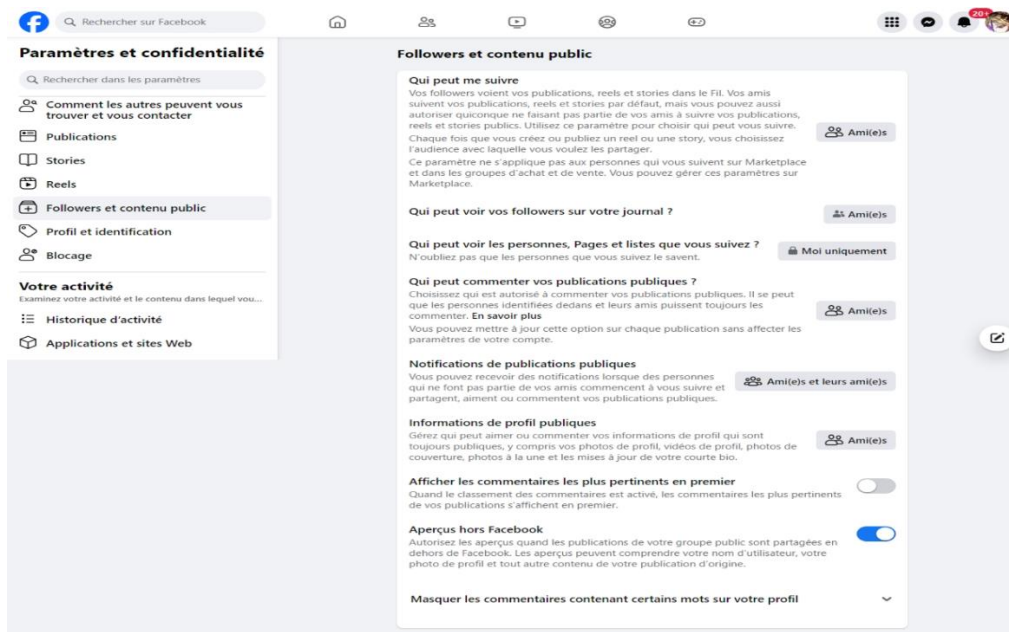
**Comment protéger votre compte**

**Les paramètres de vos données sur Facebook**

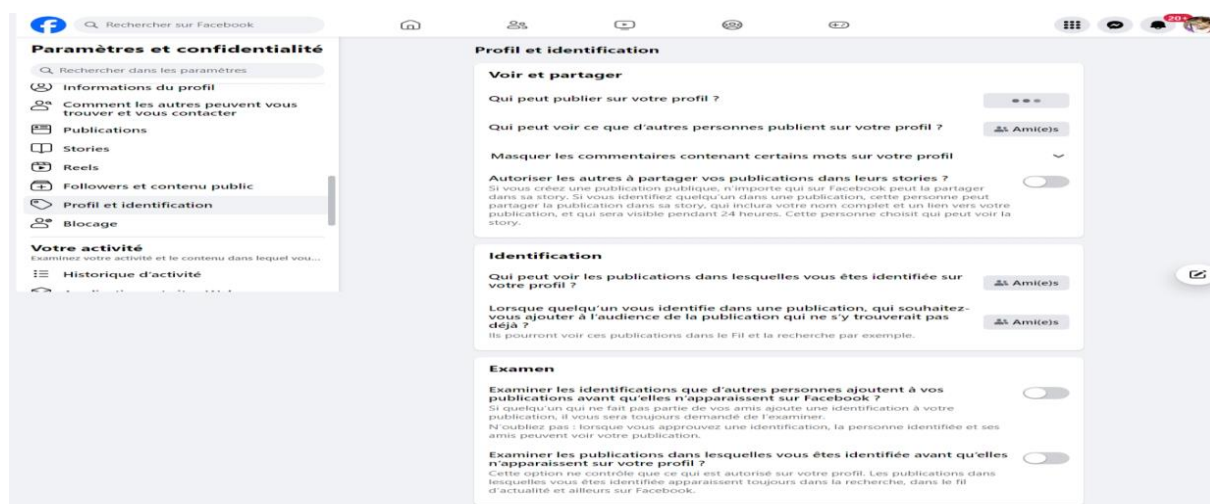
**Vos préférences publicitaires sur Facebook**

Vous pouvez découvrir plus de paramètres de confidentialité sur Facebook dans [Paramètres](#).

❖ Paramètre de contenu public et followers



❖ Paramètre de profil et identification



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

1/

Exercice pour les smartphones/tablettes :

- ✓ Faites une vérification des autorisations des applications installées. Demandez aux utilisateurs de vérifier les autorisations accordées à chaque application et de désactiver celles qui semblent excessives ou non nécessaires.
- ✓ Simuler une tentative de phishing en envoyant un e-mail ou un message texte avec un lien suspect. Les utilisateurs devraient être capables de reconnaître les signes d'une tentative de phishing et de ne pas cliquer sur le lien.

Exercice pour les ordinateurs portables/PC :

- ✓ Mettez en place un exercice de sensibilisation à la sécurité des mots de passe. Demandez aux utilisateurs de créer des mots de passe forts pour leurs comptes et de mettre en place l'authentification à deux facteurs lorsque cela est possible.
- ✓ Effectuez une vérification des logiciels malveillants en lançant un scan antivirus sur les ordinateurs et en demandant aux utilisateurs de comprendre comment réagir en cas de détection d'une menace.

Exercice pour les systèmes de vidéosurveillance :

- ✓ Effectuez un test de pénétration en essayant d'accéder aux flux vidéo à partir d'un appareil non autorisé. Les utilisateurs doivent comprendre l'importance de sécuriser les paramètres d'accès à leurs systèmes de vidéosurveillance.
- ✓ Vérifiez les protocoles de stockage des données et assurez-vous que les vidéos sont cryptées et sécurisées contre toute altération ou accès non autorisé.

2/

Smartphones/tablettes :

- ✓ Demandez aux utilisateurs de rechercher et d'installer une application antivirus fiable à partir de leur magasin d'applications respectif (comme Avast, Bitdefender, AVG, etc.).
- ✓ Une fois l'application installée, guidez-les à travers le processus de configuration en leur montrant comment effectuer une analyse complète de leur appareil et comment planifier des analyses régulières.
- ✓ Ensuite, demandez-leur d'installer également une application anti-malware, comme Malwarebytes, et de configurer des analyses régulières avec celle-ci également.

Ordinateurs portables/PC :

- ✓ Dirigez les utilisateurs vers un site Web de confiance où ils peuvent télécharger un logiciel antivirus reconnu comme Avira, Norton, Kaspersky, etc.
- ✓ Une fois le logiciel téléchargé et installé, guidez-les à travers le processus de configuration initiale, en mettant l'accent sur la planification des analyses régulières et la mise à jour des définitions de virus.
- ✓ En complément, demandez-leur d'installer un logiciel anti-malware tel que Malwarebytes et de configurer des analyses régulières avec celui-ci