



Parcours : DISCOVERY

Module : Naviguer en toute Sécurité

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

Réalisé par : RAILALA Mahalahatse

SOMMAIRE

1 - Introduction à la sécurité sur Internet

1/ trois articles qui parlent de sécurité sur internet.

2- Créer des mots de passe forts

3 - Fonctionnalité de sécurité de votre navigateur

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

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.

4 - Éviter le spam et le phishing

1/ déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.

5 - Comment éviter les logiciels malveillants

6 - Achats en ligne sécurisés :

1/ Dans cet exercice, on va t'aider à créer un registre des achats. 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.

7 - Comprendre le suivi du navigateur

8 - Principes de base de la confidentialité des médias sociaux

1/ Dans cet exercice on va te montrer le réglage des paramètres de confidentialité pour Facebook. Suis les étapes suivantes. (case à cocher)

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

1/ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé
??????? Comment faire ????????

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

1 - Introduction à la sécurité sur Internet

Objectif : à la découverte de la sécurité sur internet

1/ trois articles qui parlent de sécurité sur internet.

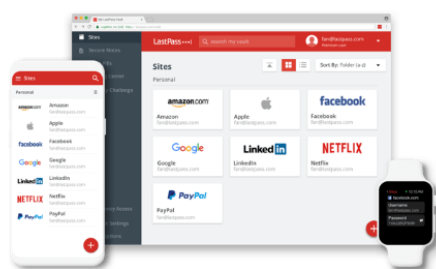
- Article 1 = Avira - Sécurité sur Internet : 10 conseils pour protéger votre ordinateur personnel
- Article 2 = Kaspersky - Confidentialité et sécurité sur Internet : 5 conseils de sécurité
- Article 3 = CYBERMALVEILLANCE.GOUV - Les 10 règles de base pour la sécurité numérique

2- Créer des mots de passe forts



- Accède au site de LastPass ☒

**Un mot de passe.
Zéro souci.**

| LastPass s'occupe du reste.



Fonctionnalités Free

 Coffre-fort de mots de passe sécurisé 

Créer un compte

ou [Connexion](#)

Adresse e-mail

Mot de passe maître



Confirmer votre mot de passe Maître



Indice (facultatif)

Inscrivez-vous - c'est gratuit

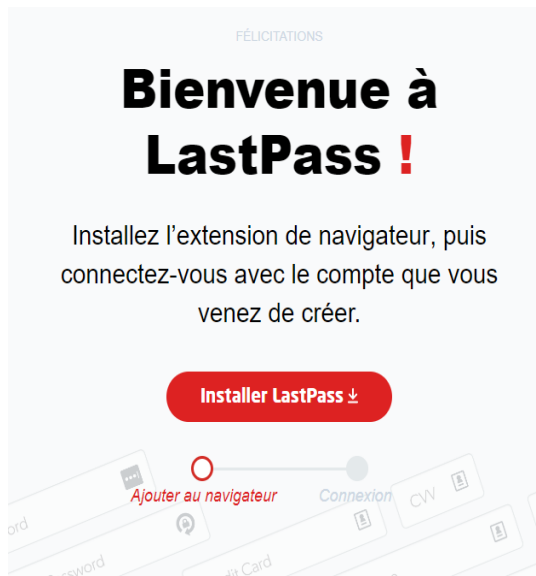
En remplissant ce formulaire, j'accepte les [Conditions générales](#) et la [Politique de confidentialité](#). Je souhaite recevoir des e-mails promotionnels, sauf si [je me désinscris](#).

- Crée un compte en remplissant le formulaire. ☒

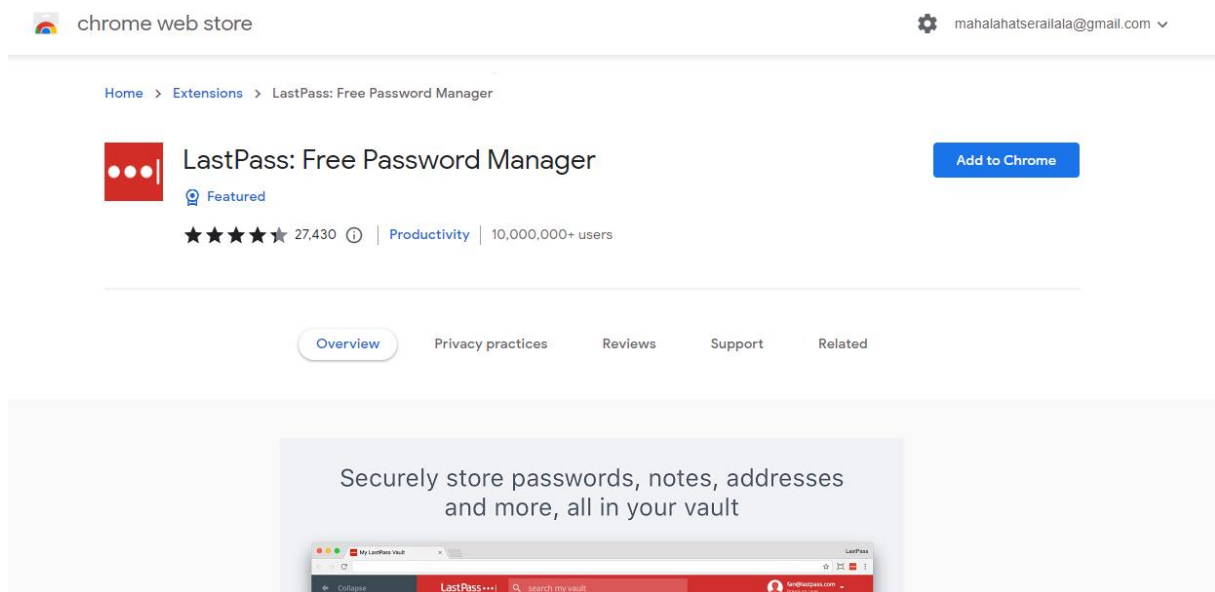
Un conseil, on te demande de choisir un mot de passe maître.

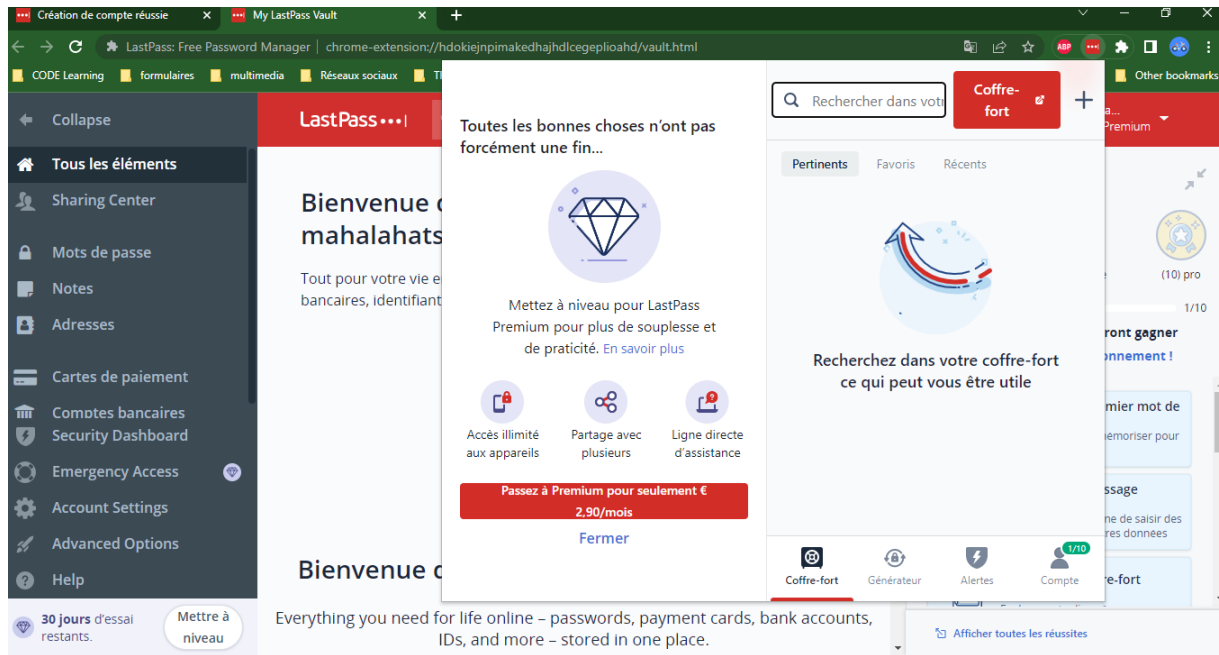
o Exemple de mot de passe maître : c3c!3s!l3M0!2P@SS3 (Ceci est le mot de passe, en remplaçant le "e" par "3" le "i", "t" par "!", "a" par "@" et les premières lettres en minuscules puis majuscules à partir de "mot").

o 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





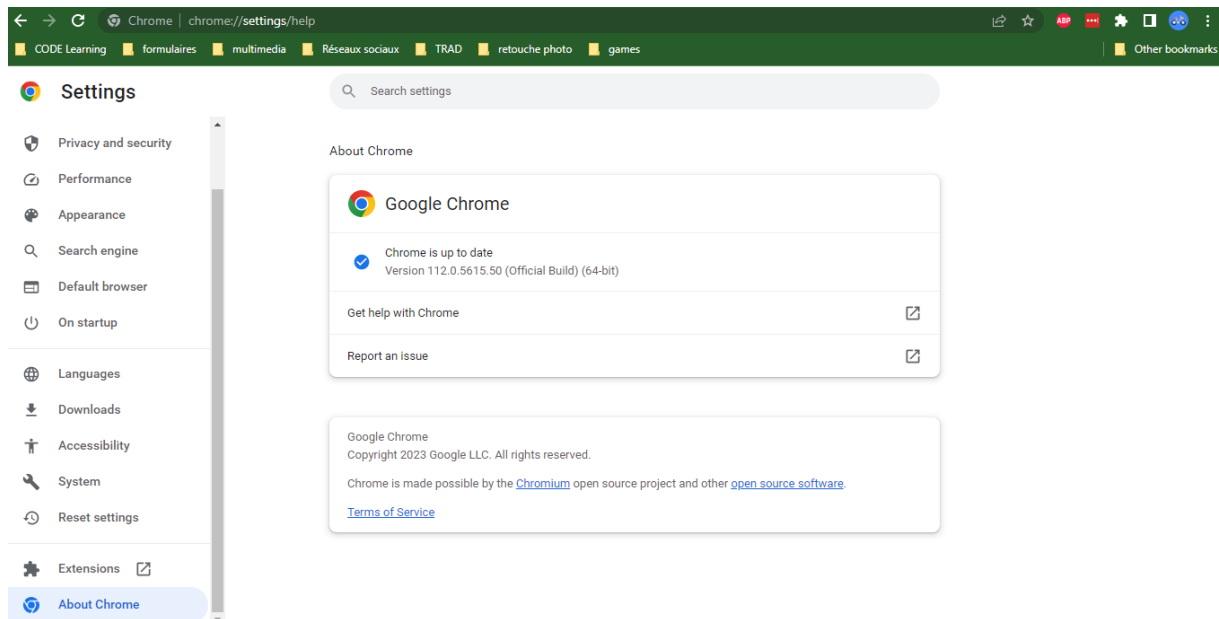
3 - Fonctionnalité de sécurité de votre navigateur

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.instagram.com ☒

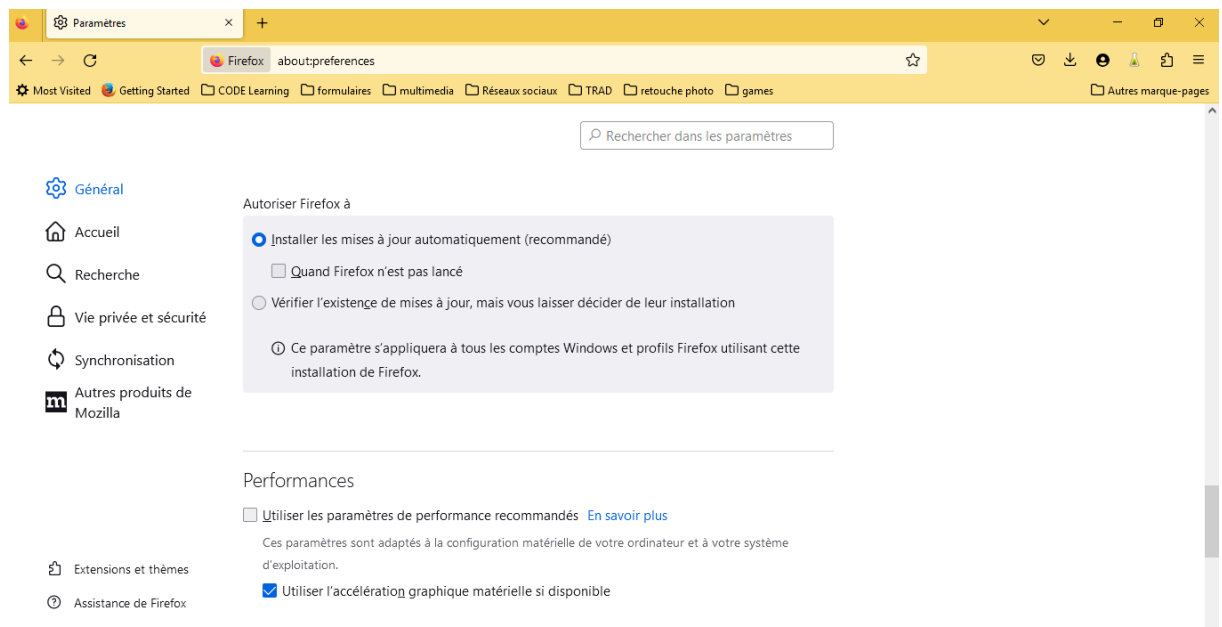
2/ Dans cet exercice, nous allons vérifier si les navigateurs utilisés, Chrome et Firefox dans notre exemple, sont à jour. Pour ce faire, suis les étapes suivantes.

- 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) ✓
- Vérifie que les paramètres sélectionnés sont identiques que sur la photo ✓

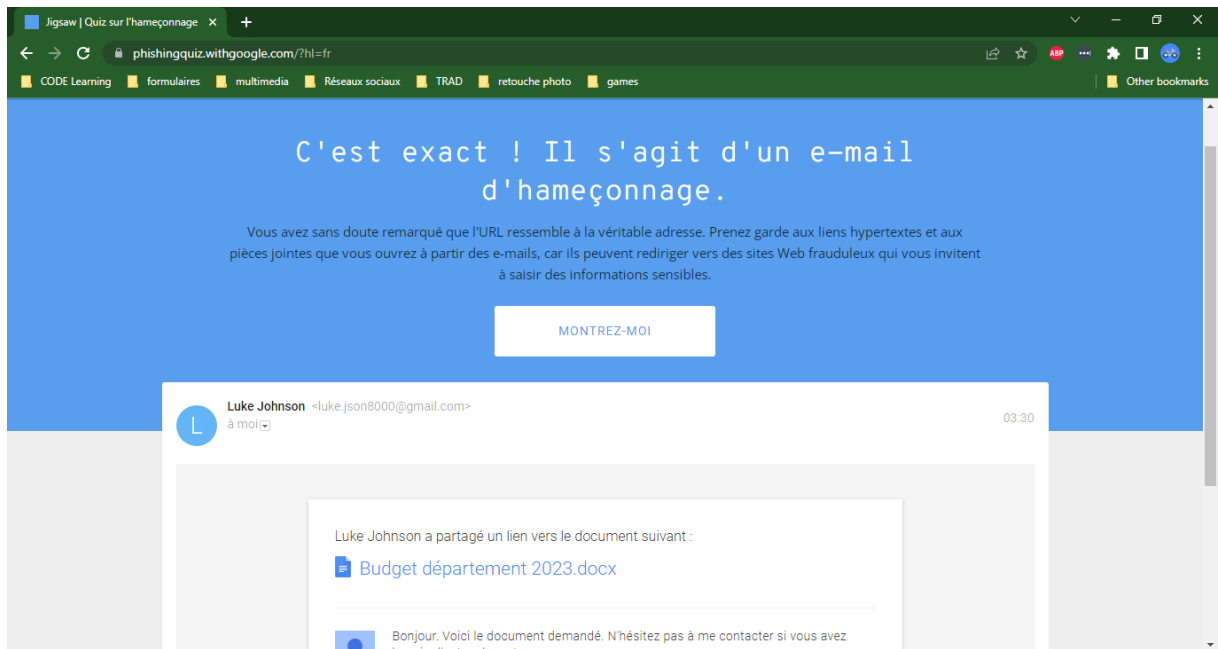
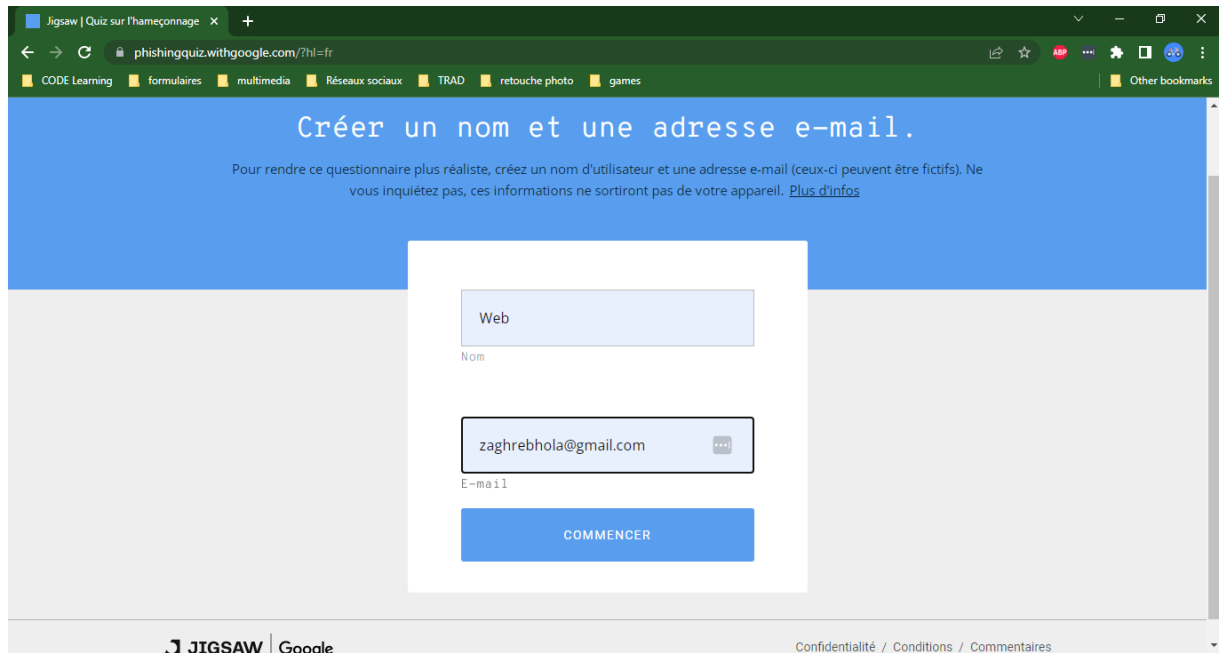


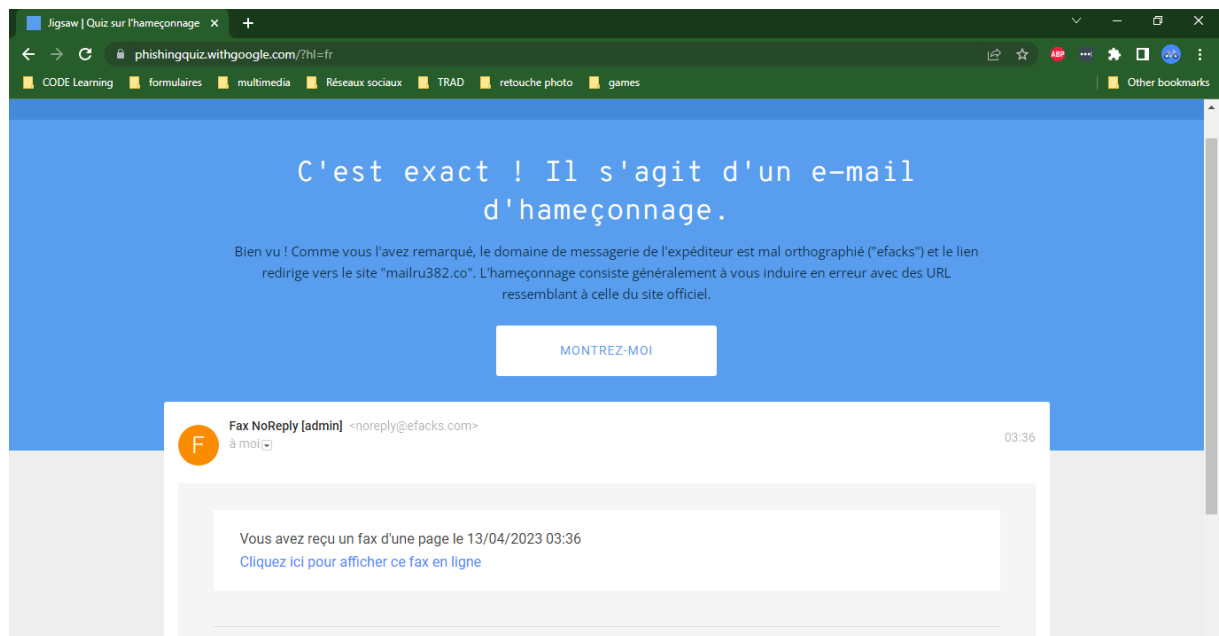
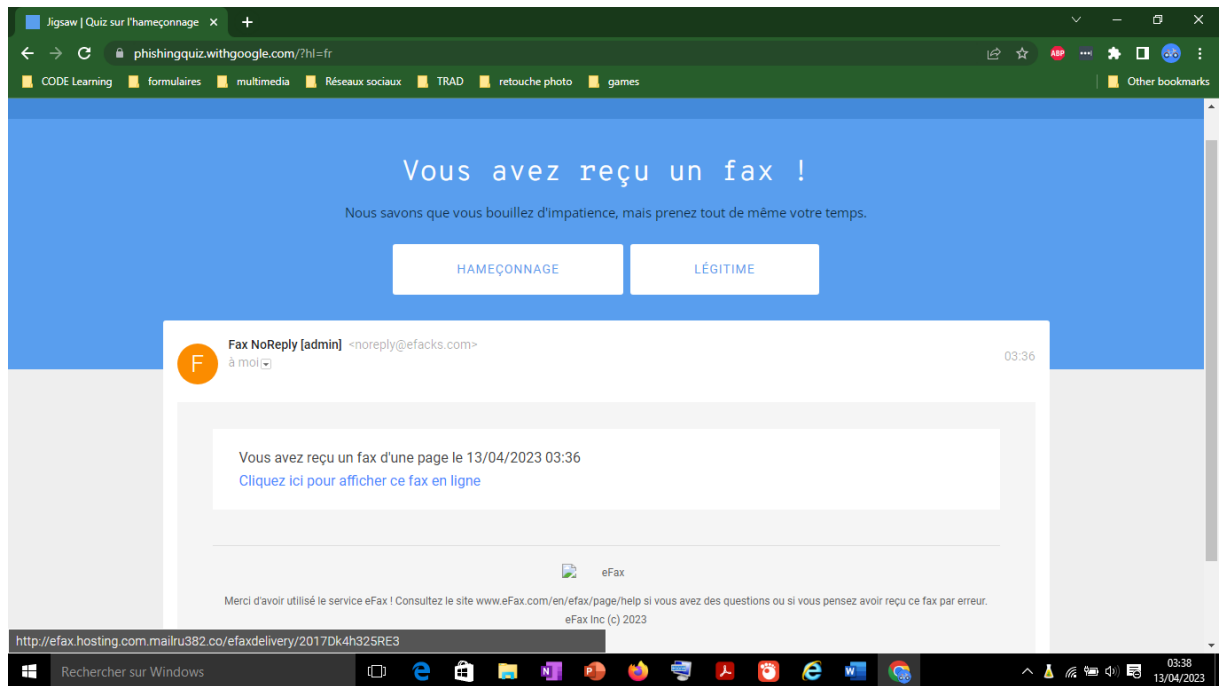
4 - Éviter le spam et le phishing

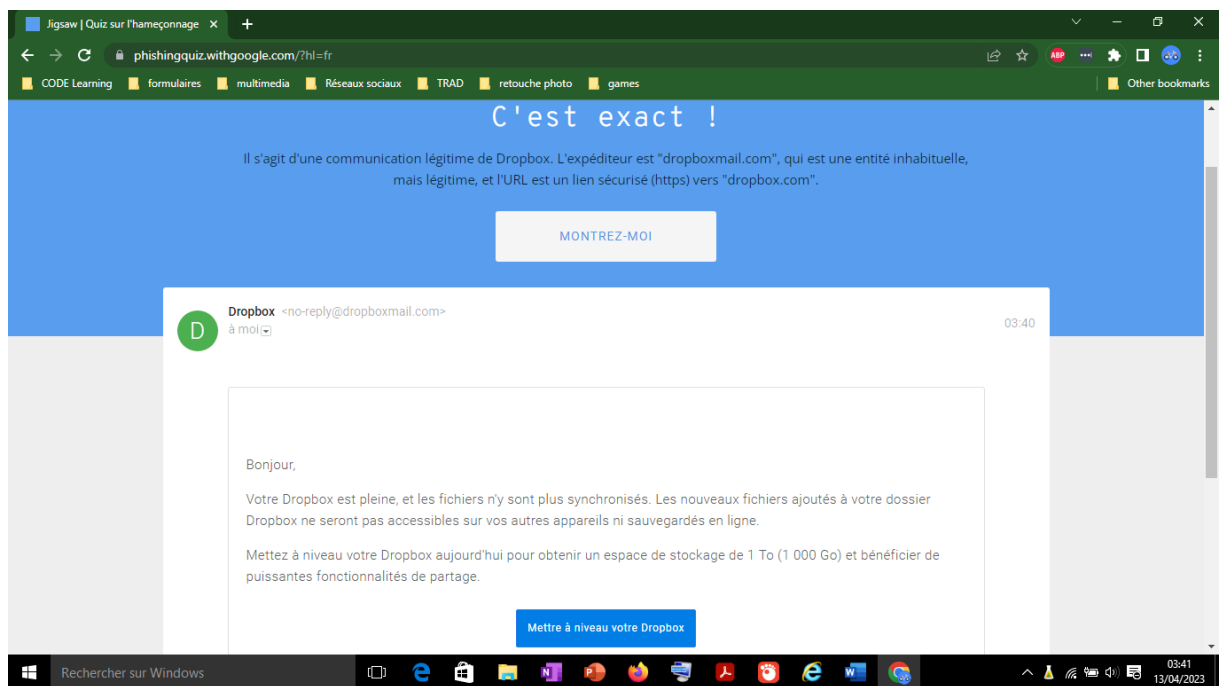
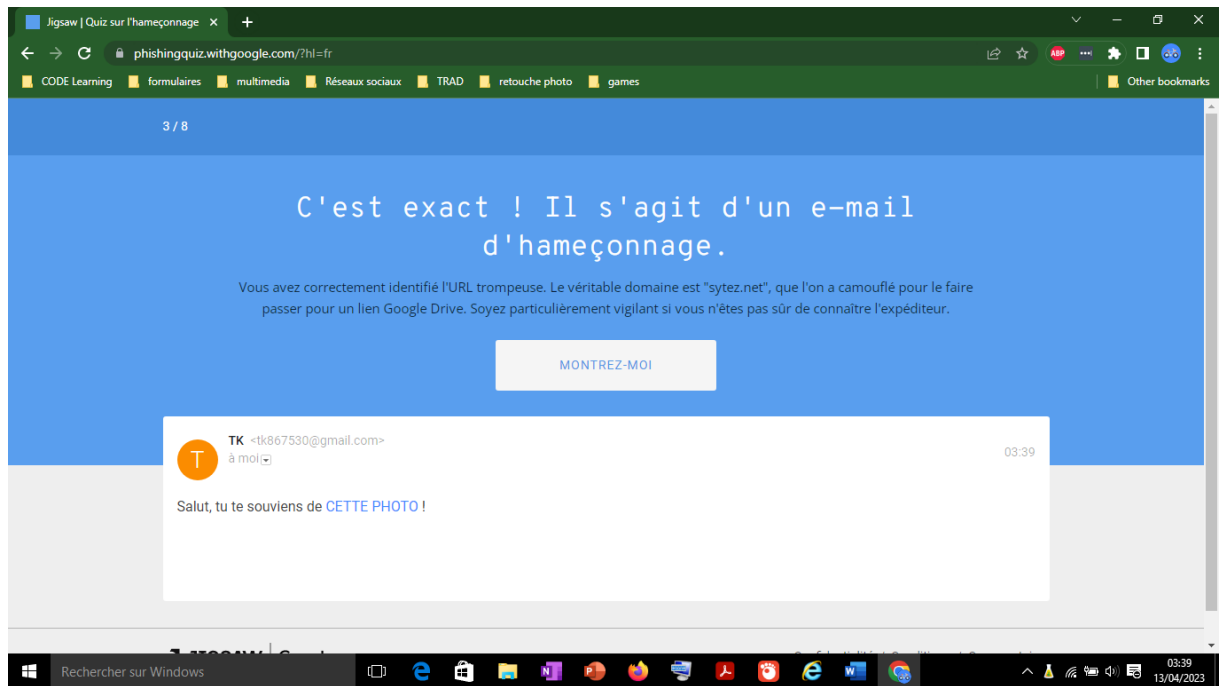
1/ déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.

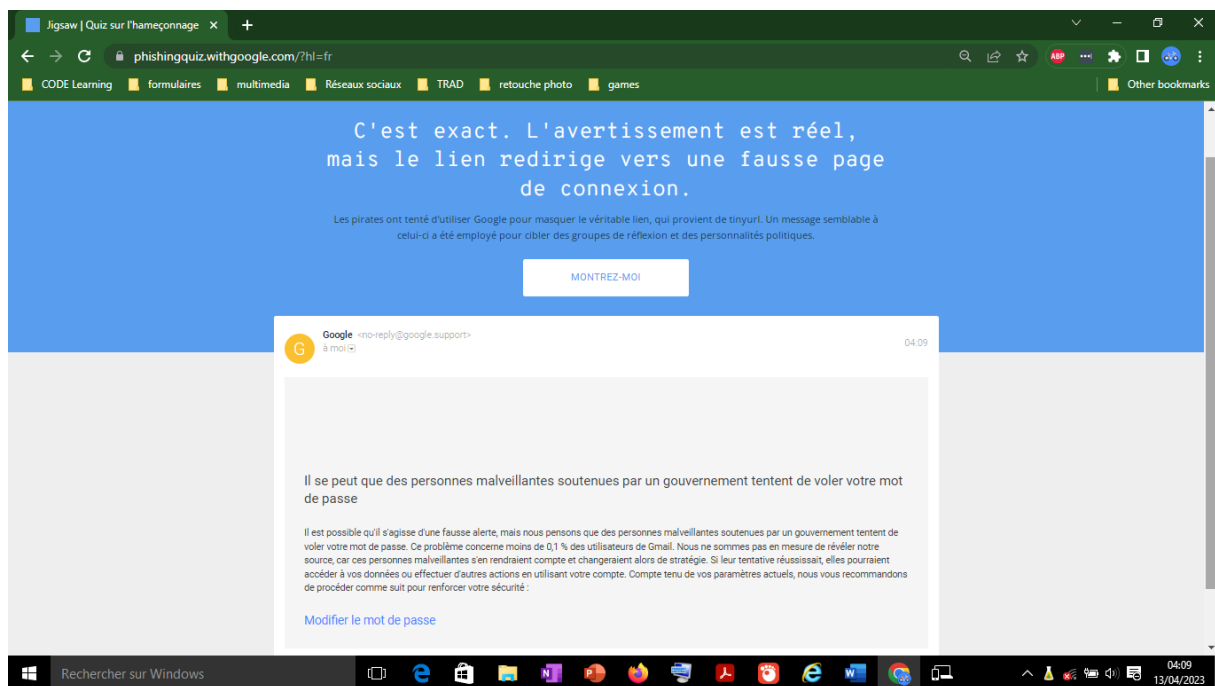
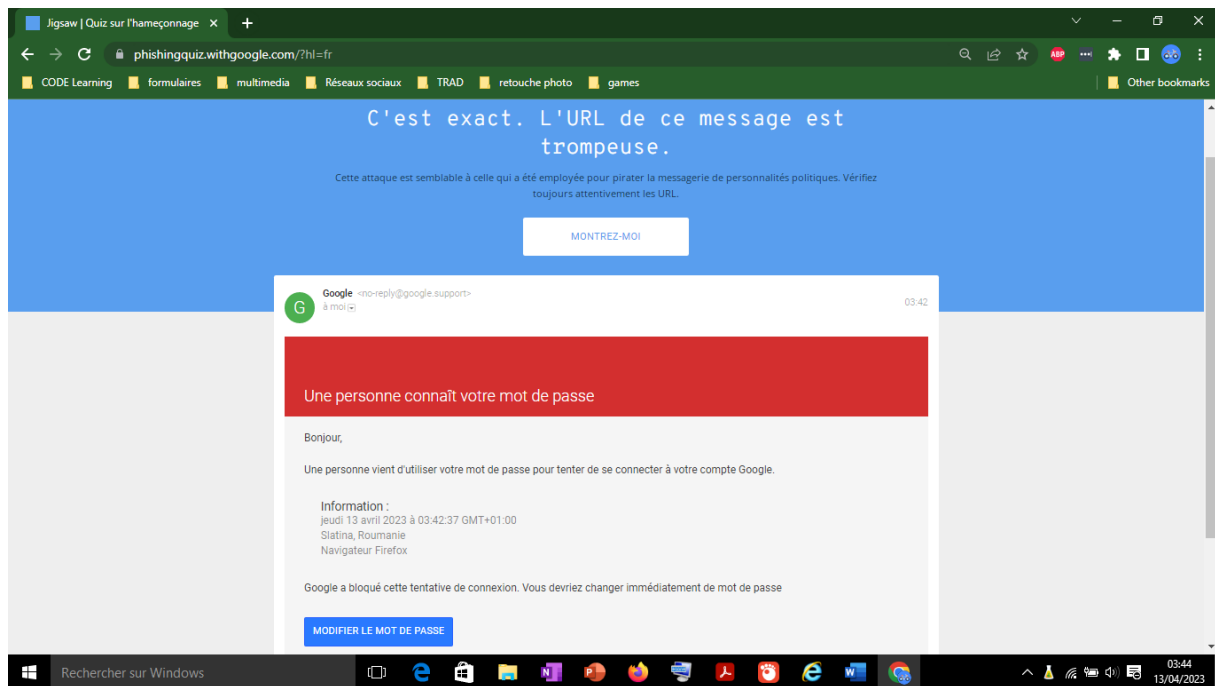
Pour ce faire accède au lien suivant et suis les étapes qui y sont décrites :

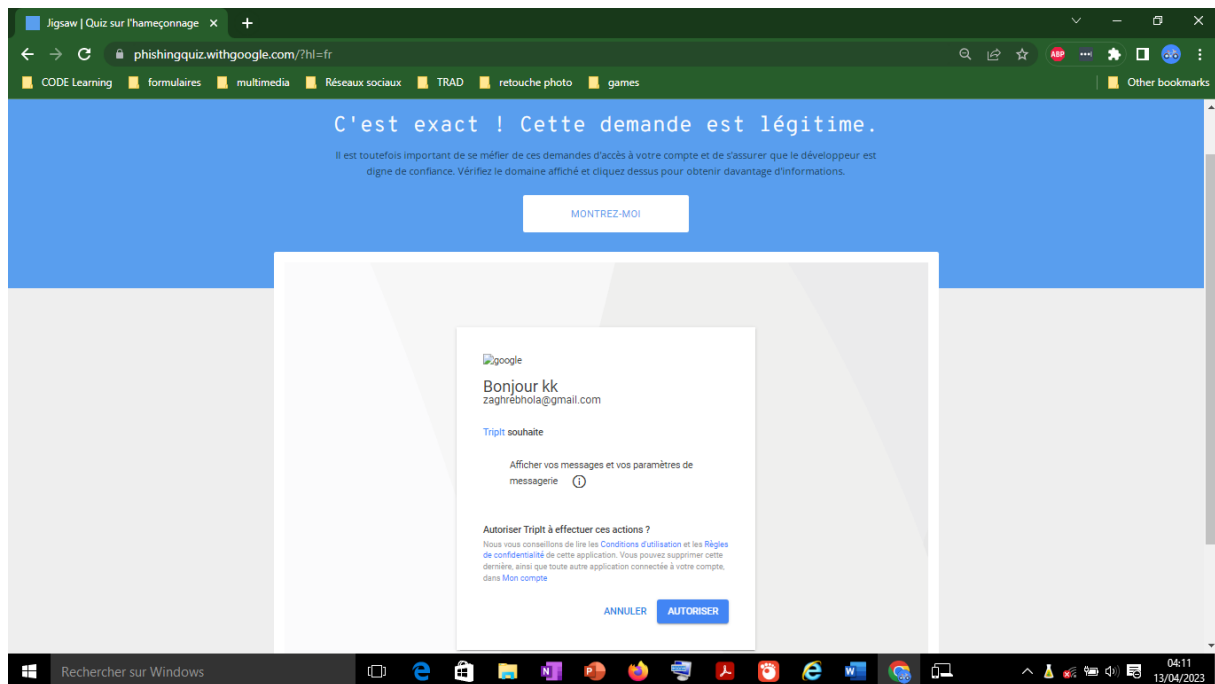
<https://phishingquiz.withgoogle.com/?hl=fr>











5 - Comment éviter les logiciels malveillants

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 (<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 (<http://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
 - 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) ☒

6 - Achats en ligne sécurisés :

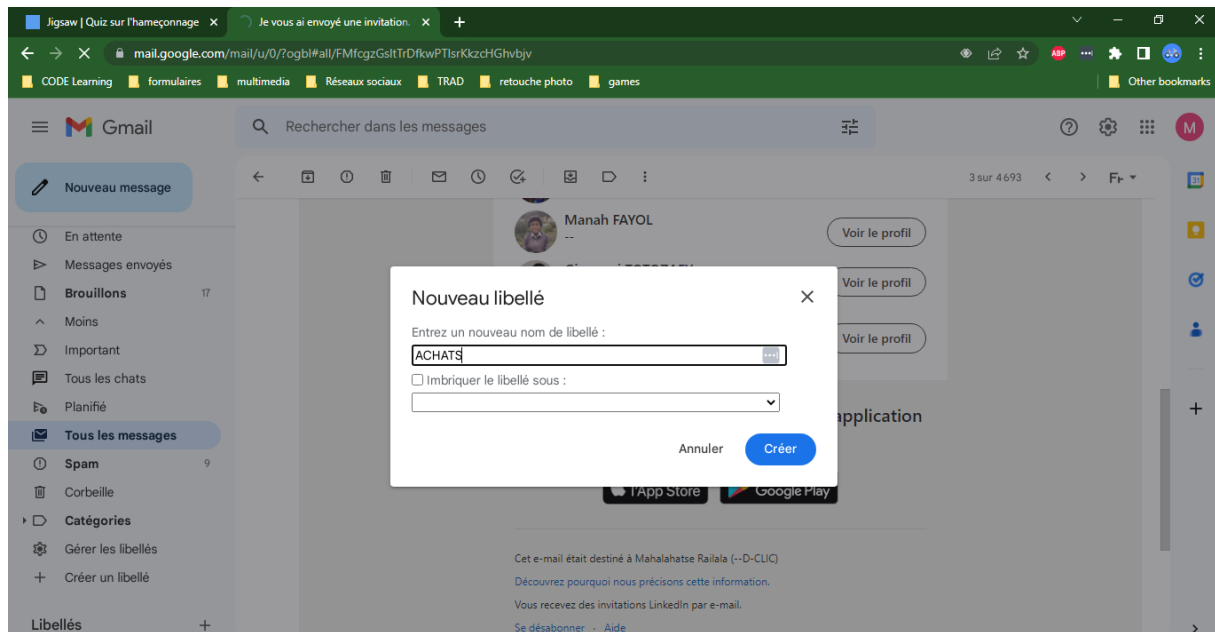
1/ Dans cet exercice, on va t'aider à créer un registre des achats. Ce registre a pour but de conserver les informations relatives à tes achats en ligne. Très pratique lorsque tu fais face à un litige, un problème sur ta commande ou tout simplement pour faire le bilan de tes dépenses du mois.

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

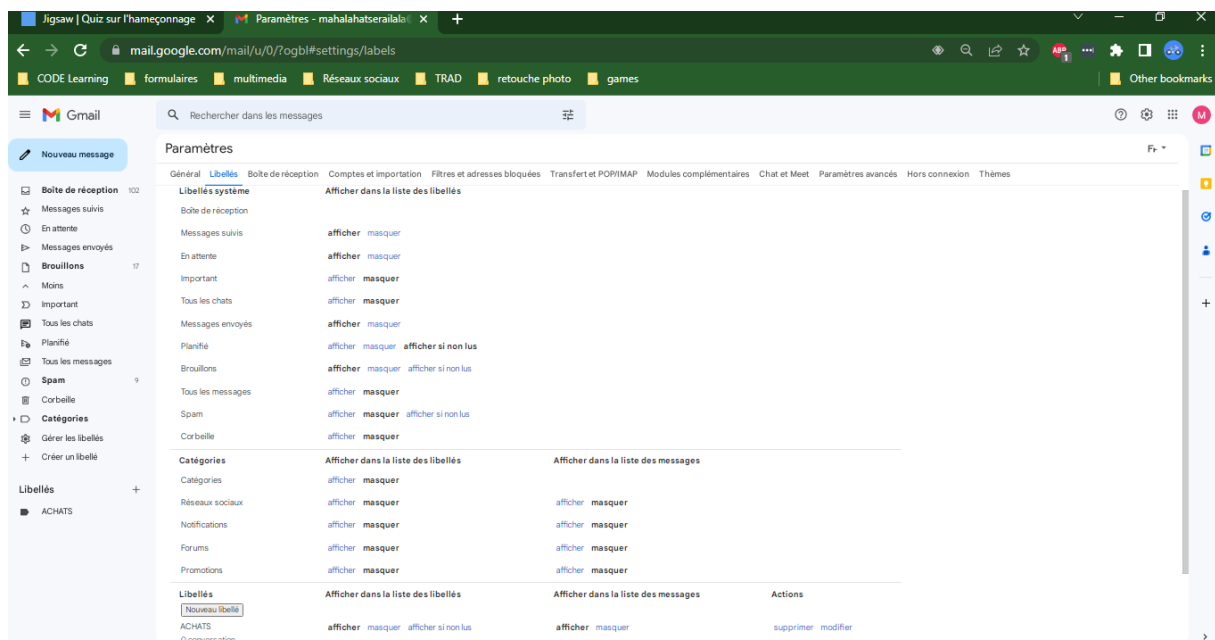
1. Créer un dossier sur ta messagerie électronique
2. Créer un dossier sur ton espace de stockage personnel (en local ou sur le cloud)

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) ☒
- 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) ☒



- 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

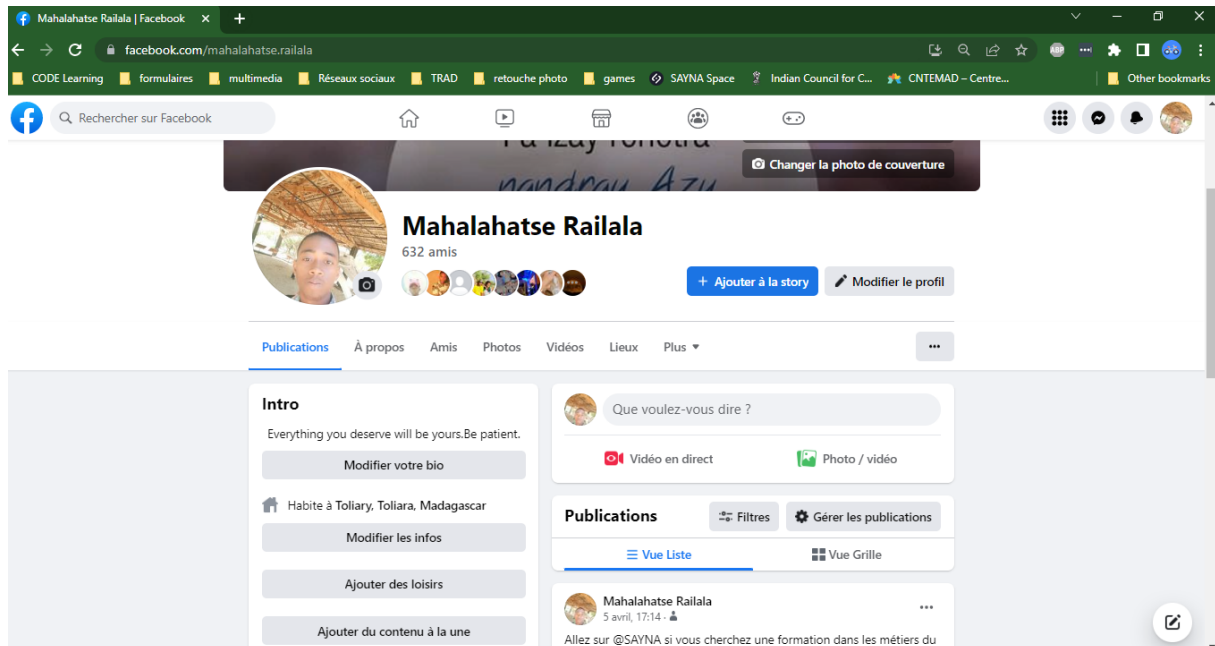
Objectif : exercice présent sur la gestion des cookies et l’utilisation de la navigation privée

8 - Principes de base de la confidentialité des médias sociaux

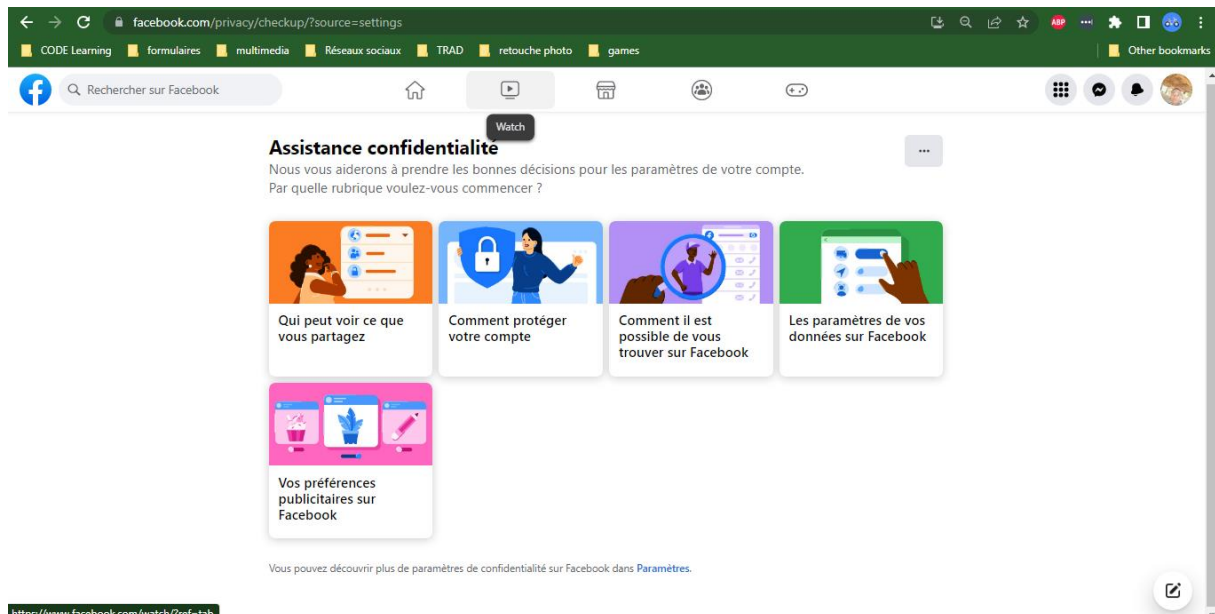
Objectif : Régler les paramètres de confidentialité de Facebook

1/ 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 ☒



La dernière rubrique (rose) permet de gérer les informations récoltées par

- 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/ Proposer un ou plusieurs exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé ?????? Comment faire ??????

Il existe plusieurs façons de vérifier la sécurité d'un appareil en fonction de l'appareil utilisé.

- Pour les ordinateurs :

-exécuter un programme de vérification de sécurité tel que Norton Security ou McAfee Security sur votre ordinateur pour identifier les virus, les logiciels malveillants et les menaces potentielles pour la sécurité de votre ordinateur.

- Pour les smartphones :

-Installer une application de sécurité pour smartphone telle que Norton Mobile Security ou Avast Mobile Security pour vérifier la sécurité de votre smartphone. Ces applications peuvent détecter les virus et les logiciels malveillants, ainsi que protéger votre téléphone contre les attaques de phishing.

-Il est essentiel de maintenir vos appareils à jour avec les derniers correctifs de sécurité et de suivre les meilleures pratiques en matière de sécurité en ligne pour minimiser les risques de violation de sécurité.

-Mettre à jour le téléphone et le nettoyer avec un gestionnaire d'applications préinstallé

- Pour les routeurs :

-Accéder à l'interface de votre routeur et vérifier les paramètres de sécurité tels que les mots de passe, les pare-feux et les paramètres de sécurité sans fil,

-également utiliser un outil de détection de vulnérabilités pour vérifier la sécurité de votre réseau.

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

- Sur un ordinateur Windows

-Recherchez un antivirus + antimalware recommandé pour les ordinateurs Windows. Par exemple : Avast Antivirus, Bitdefender Antivirus, ou Norton Antivirus.

-Téléchargez le logiciel d'installation de l'antivirus + antimalware depuis le site officiel du fournisseur.

-Exécutez le programme d'installation et suivez les instructions à l'écran pour installer le logiciel sur votre ordinateur.

-Une fois l'installation terminée, lancez l'antivirus + antimalware et effectuez une analyse complète du système pour détecter les virus et les logiciels malveillants.

-Configurez le logiciel pour effectuer des analyses régulières du système et pour mettre à jour automatiquement les définitions de virus et de logiciels malveillants.

-Éduquez-vous sur les meilleures pratiques de sécurité en ligne et assurez-vous de maintenir votre logiciel antivirus + antimalware à jour.

-Effectuez des analyses régulières de votre système pour détecter les menaces potentielles et suivez les instructions fournies par le logiciel pour les éliminer.

- Sur un smartphone :

-Télécharger un antivirus et antimalware fiable à partir de Google Play Store ou de l'App Store. Il y a de nombreux choix, tels que Avast Mobile Security, Bitdefender Mobile Security, McAfee Mobile Security et Norton Mobile Security.

- Ouvrir l'application et suivre les instructions pour configurer un compte utilisateur.
- Une fois le compte créé, effectuer une analyse complète du système pour détecter les menaces éventuelles. Les résultats de l'analyse doivent être affichés.
- Si des menaces sont détectées, suivre les instructions fournies par l'application pour les supprimer.
- Configurer des options de protection supplémentaires telles que le blocage d'appels et de messages indésirables, la protection de la vie privée et la sauvegarde de données.
- Activer la fonction de mise à jour automatique pour garantir que l'antivirus et l'antimalware sont toujours à jour.
- Planifier des analyses régulières pour garantir que le téléphone reste protégé contre les menaces potentielles.
- Enfin, sensibiliser l'utilisateur à l'importance d'une navigation sûre sur le Web, des téléchargements d'applications sûrs et de l'ouverture de pièces jointes et de liens provenant de sources connues et fiables.