

SAYNA

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- D'après la recherche que j'ai effectuée, voici les résultats que j'ai trouvés.

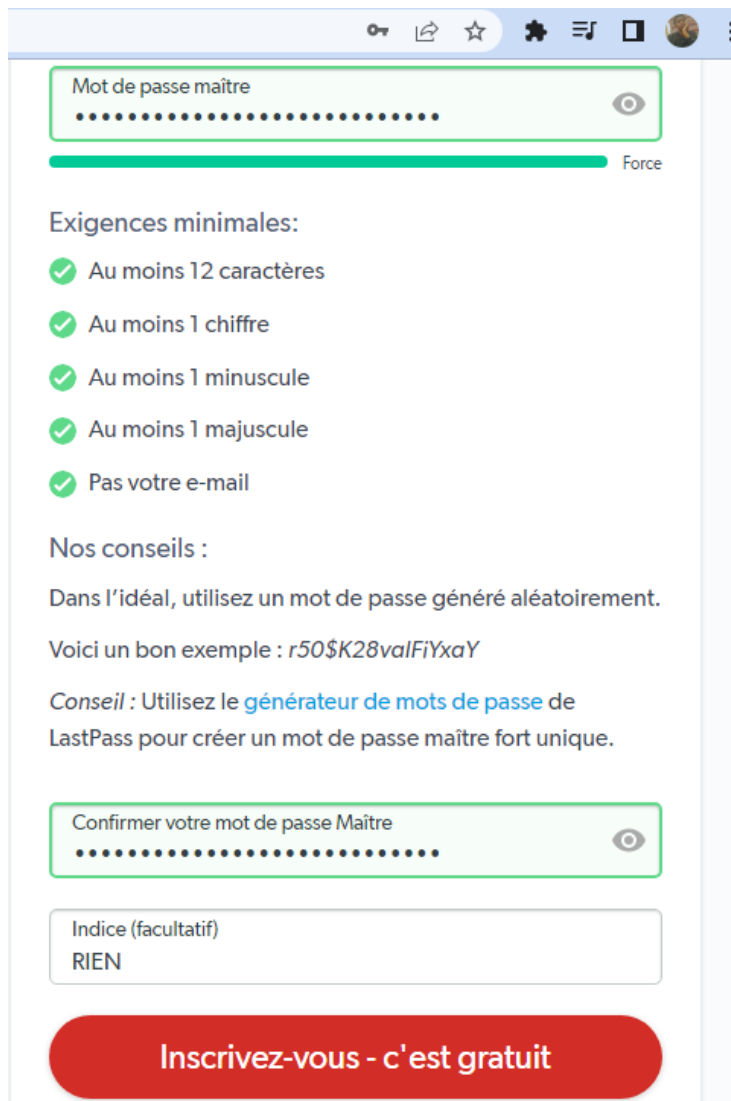
- **Articles 1** = Lemondeinformatique.fr - Cybersécurité : 5 outils pour prendre le pouls des menaces
- **Articles 2** = cybermalveillance.gouv.fr- Comment se protéger sur internet ?
- **Articles 3** = cnil.fr - 10 conseils pour rester net sur le web

2 - Créer des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass

1- Grâce aux étapes pour créer un compte LastPass, j'ai maintenant réussi. Voici le résultat.

Pour la création :



The image shows a web browser window with the LastPass master password creation interface. At the top, there's a browser toolbar with icons for back, forward, star, and others. Below the toolbar is a green-bordered input field labeled "Mot de passe maître" containing a series of dots and an eye icon to toggle visibility. A green progress bar is positioned below this field, with the word "Force" at its right end. Underneath the progress bar, the text "Exigences minimales:" is followed by a list of five requirements, each preceded by a green checkmark: "Au moins 12 caractères", "Au moins 1 chiffre", "Au moins 1 minuscule", "Au moins 1 majuscule", and "Pas votre e-mail". Below this list, the text "Nos conseils :" is followed by two paragraphs: "Dans l'idéal, utilisez un mot de passe généré aléatoirement." and "Voici un bon exemple : r50\$K28valFiYxaY". A blue link "générateur de mots de passe" is included in the second paragraph. Below the advice, there's another green-bordered input field labeled "Confirmer votre mot de passe Maître" with dots and an eye icon. Underneath that is a white-bordered input field labeled "Indice (facultatif)" with the text "RIEN" inside. At the bottom of the form is a large red button with the white text "Inscrivez-vous - c'est gratuit".

Mot de passe maître

Force

Exigences minimales:

- ✓ Au moins 12 caractères
- ✓ Au moins 1 chiffre
- ✓ Au moins 1 minuscule
- ✓ Au moins 1 majuscule
- ✓ Pas votre e-mail

Nos conseils :

Dans l'idéal, utilisez un mot de passe généré aléatoirement.

Voici un bon exemple : r50\$K28valFiYxaY

Conseil : Utilisez le [générateur de mots de passe](#) de LastPass pour créer un mot de passe maître fort unique.

Confirmer votre mot de passe Maître

Indice (facultatif)
RIEN

Inscrivez-vous - c'est gratuit

Si le compte a été créé. :

← → ↻ LastPass: Free Password Manager | chrome-extension://hdokiejnpimakedhajhdcegeplioahd/vault.html ☆ ⚙ ⌵ 🔍

← Réduire

LastPass... | 🔍 rechercher dans mon coffre | walkerlemec@... Utilisateur d'essai Premium


Tous les éléments

- 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
- Aide

30 jours d'essai restants. Mettre à niveau

Bienvenue dans LastPass, walkerlemec !

Tout pour votre vie en ligne – mots de passe, cartes de paiement, comptes bancaires, identifiants et bien plus encore – au même endroit.



Bienvenue dans LastPass, walkerlemec

Tout pour votre vie en ligne – mots de passe, cartes de paiement, comptes bancaires, identifiants et bien plus encore

Kit de démarrage

(1) novice (5) expérimenté (10) pro

1/10

Ces 10 réussites vous feront gagner 10 % sur le prix de l'abonnement !

- Ajoutez votre premier mot de passe**
Laissez LastPass le mémoriser pour vous
- Essayez le remplissage automatique**
Épargnez-vous la peine de saisir des mots de passe et autres données
- Visitez votre coffre-fort LastPass**
Explorez votre lieu sûr
- Restez connecté partout**

Afficher toutes les réussites

Je vais ajouter mon premier mot de passe.



GitLab.com

Nom d'utilisateur ou adresse de courriel principale

patrice.ndri@gs2e.ci

Mot de passe

.....



[Mot de passe oublié ?](#)

☐ Se souvenir de moi

Connexion

En vous connectant, vous acceptez les [Conditions d'utilisation](#) et reconnaissez avoir pris connaissance de la [Politique de confidentialité](#) et de la [Politique en matière de cookies](#).

Vous n'avez pas encore de compte ? [Inscrivez-vous maintenant](#)

ou connectez-vous avec

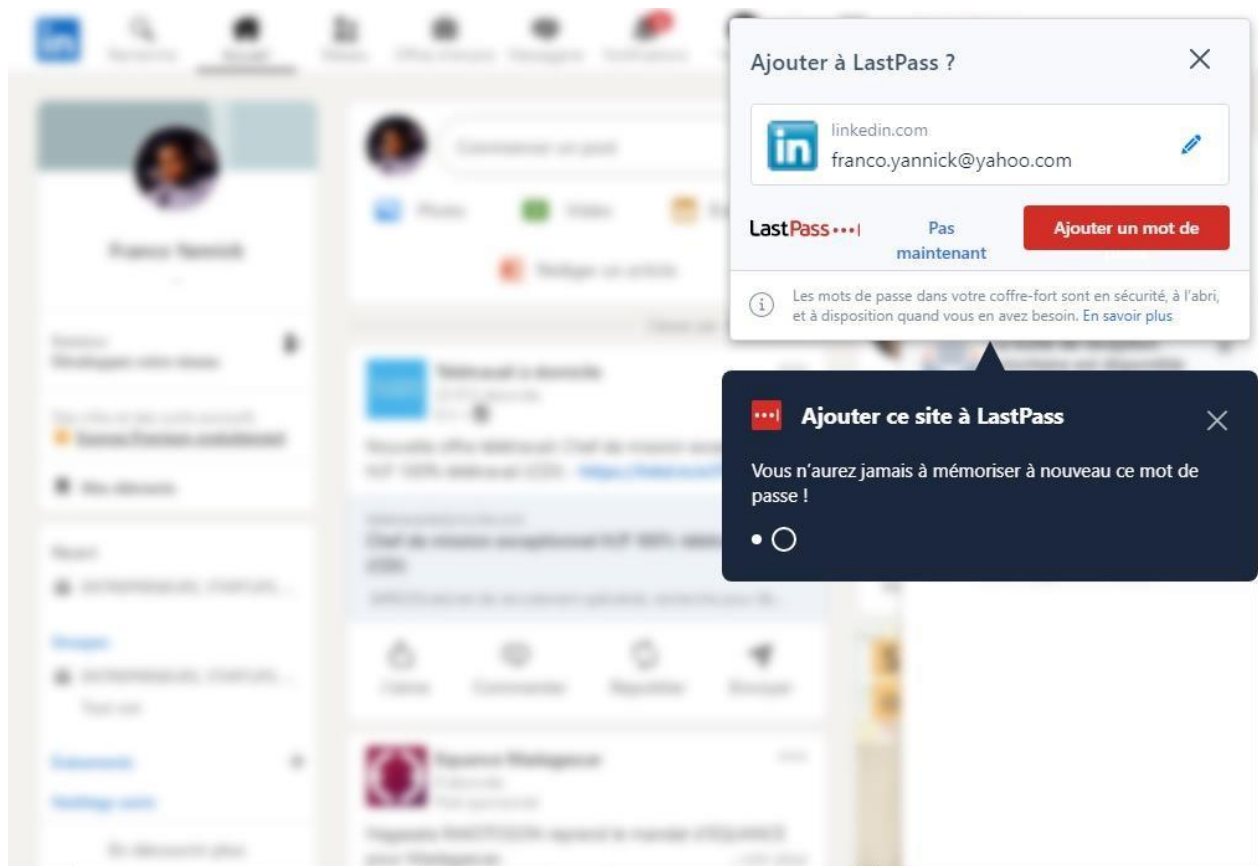
 Google

 GitHub

 Bitbucket

Salesforce

☐ Se souvenir de moi



3 - Fonctionnalité de sécurité de votre navigateur

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

1 Les sites web qui semblent être malveillants sont :

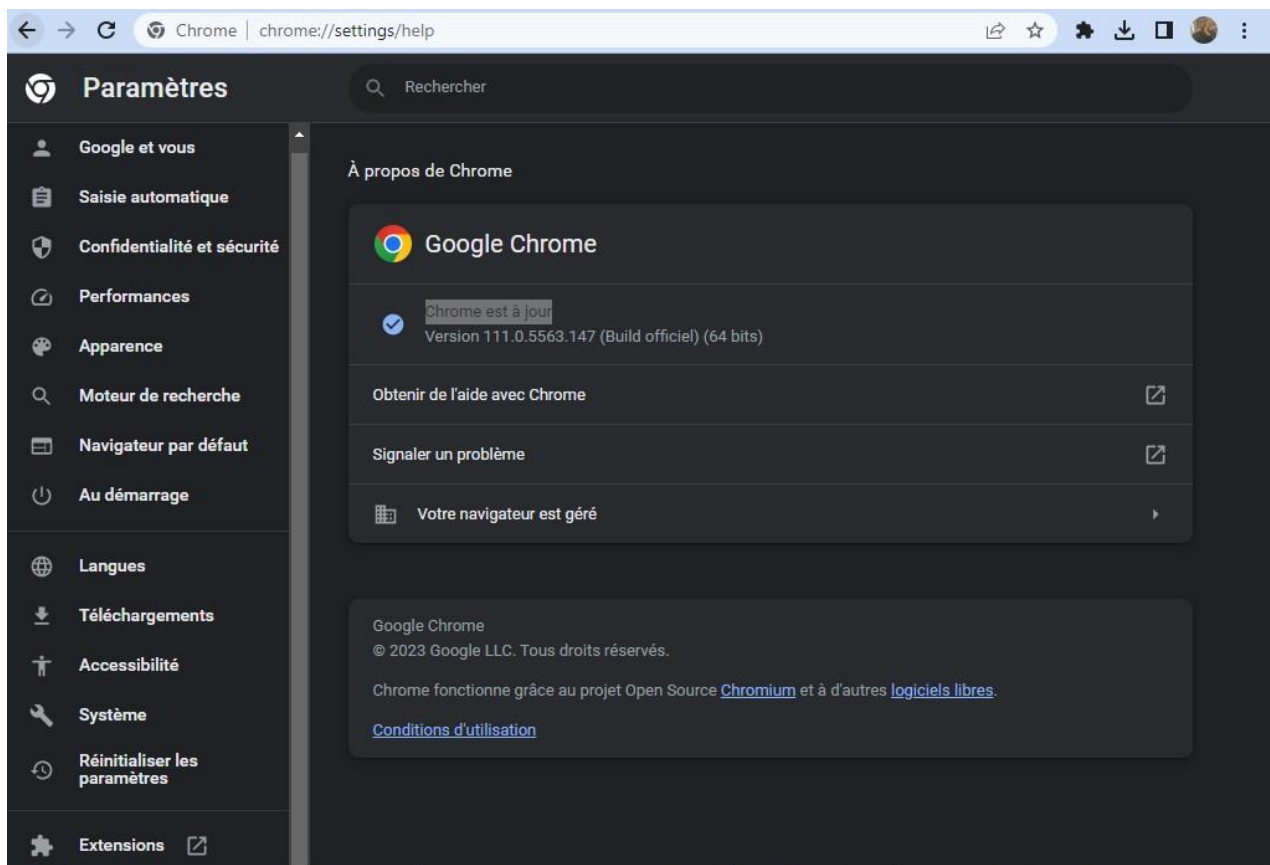
- www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel
- www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde
- www.instagramam.com, un dérivé de www.instagram.com, un autre réseau Social très utilisé

Les seuls sites qui semblaient être cohérents sont donc :

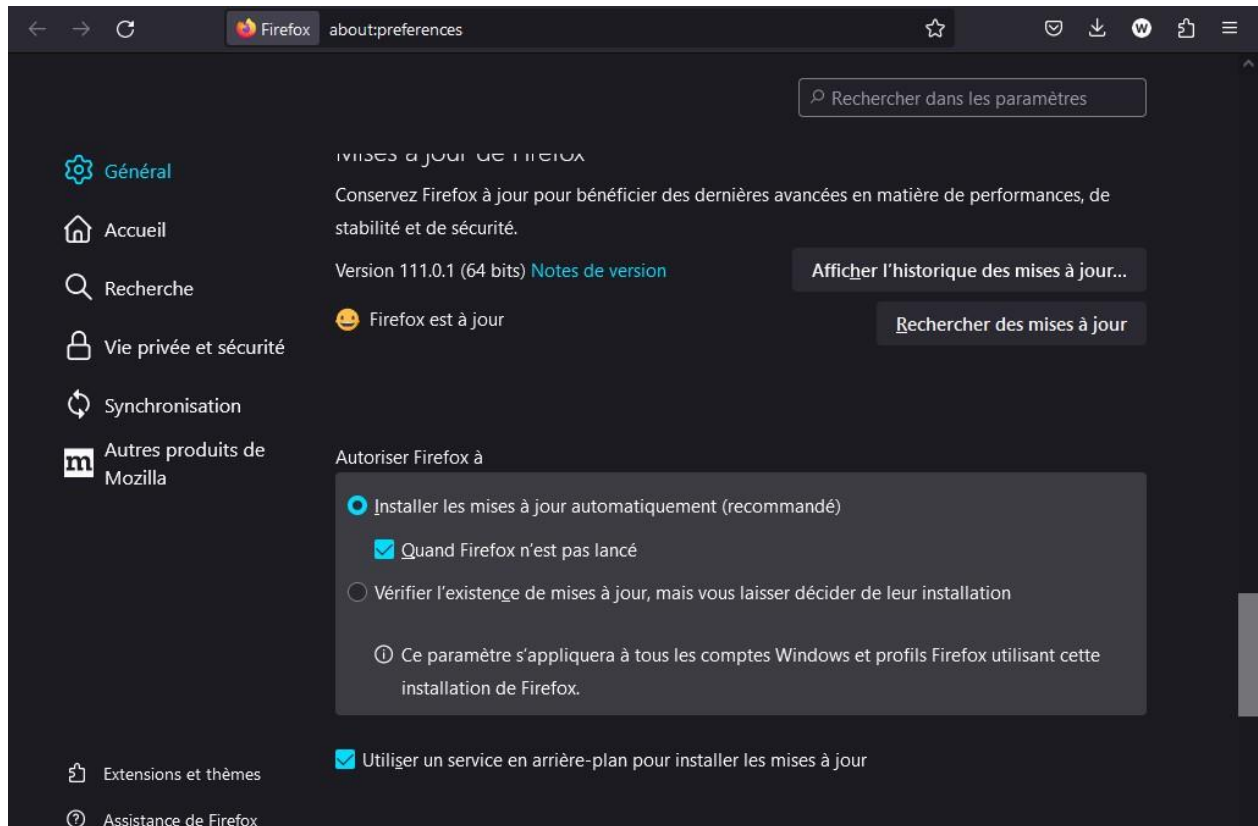
- www.dccomics.com, le site officiel de l'univers DC Comics
- www.ironman.com, le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

2 D'après la vérification du navigateur utilisé, voici le résultat de chacun.

- Pour le navigateur chrome :
Il n'y a pas de mise à jour disponible pour le moment, mais il fonctionne correctement. Lorsqu'une mise à jour sera disponible, elle sera installée automatiquement.



- Pour le navigateur Firefox :
Nous n'avons pas de mise à jour disponible pour le moment. Si une mise à jour est disponible, elle sera installée automatiquement.



4 - Éviter le spam et le phishing

Objectif : Reconnaître plus facilement les messages frauduleux

J'ai terminé l'exercice sur le spam et le phishing. Voici le résultat du quiz que j'ai obtenu.

Bon travail, Patrice
Achille Kouassi !
Vous avez obtenu un
score de 5/8.

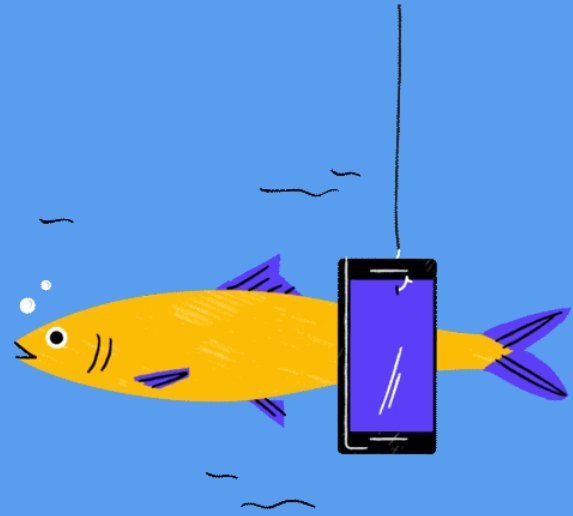
Plus vous vous entraînez, mieux vous saurez identifier les
pièges et vous protéger des tentatives d'hameçonnage.

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



5 - Comment éviter les logiciels malveillants

Objectif : sécuriser votre ordinateur et identifier les liens suspects

1) Voici les résultats de l'analyse des listes que j'ai effectuée pour les tester en termes de sécurité sur Google Transparency Report.

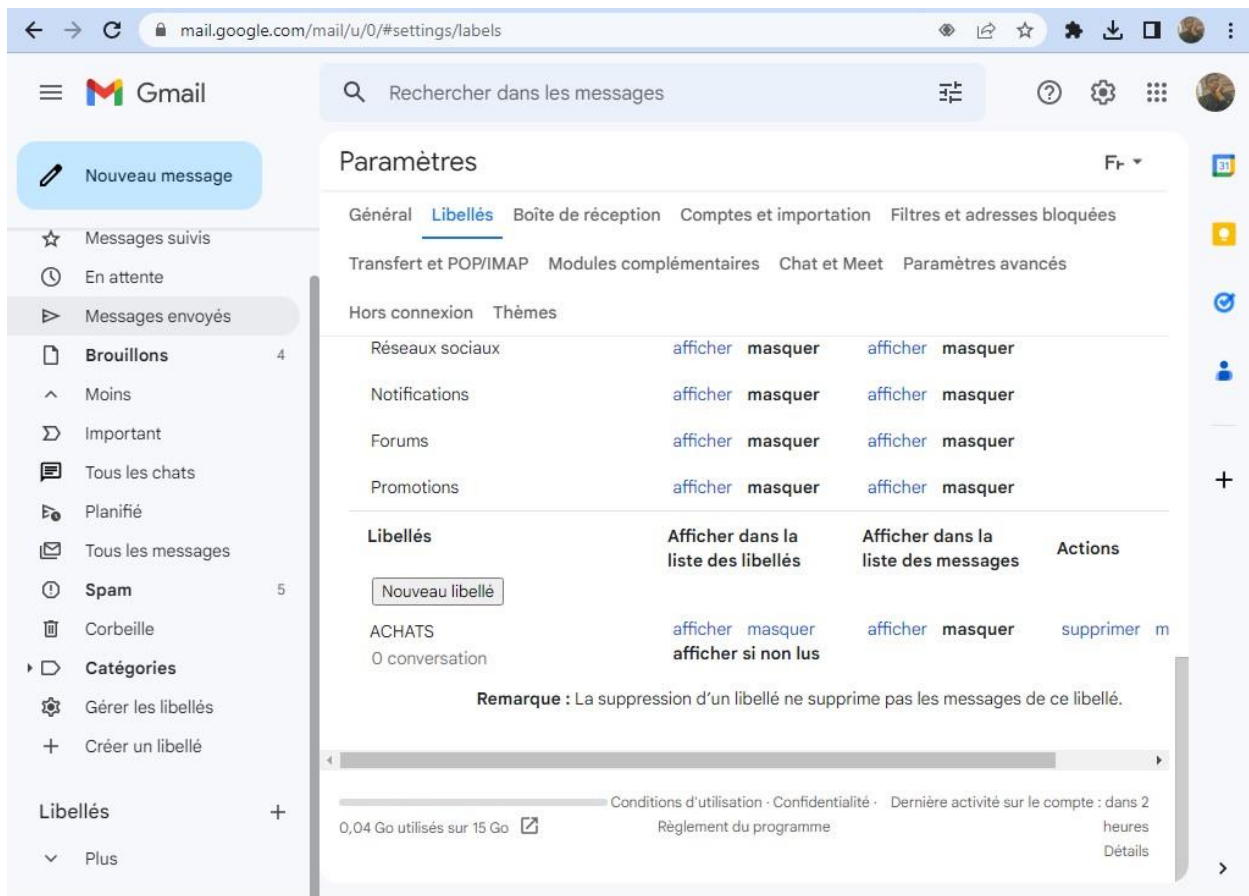
- <https://apache.org/>
 - Indicateur de sécurité
 - HTTPS
 - Analyse Google
 - Aucun contenu suspect détecté
- <https://etherscan.io/>
 - Indicateur de sécurité
 - HTTPS
 - Analyse Google
 - Aucun contenu suspect détecté

- <https://11st.co.kr/>
 - Indicateur de sécurité
 - HTTPS Not secure
 - Analyse Google
 - Aucun contenu suspect détecté

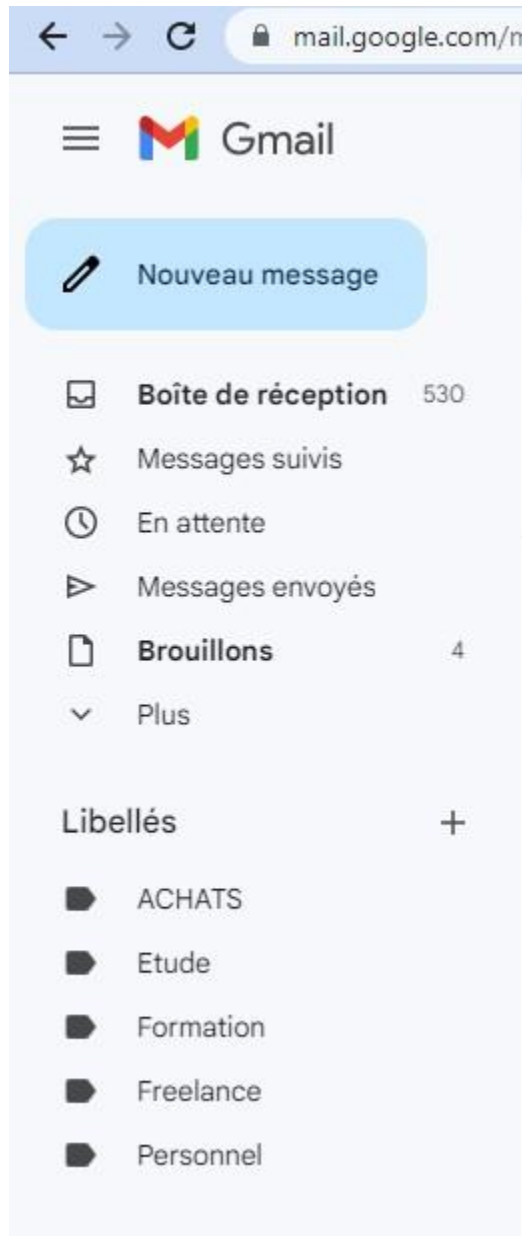
6 - Achats en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

1. Je peux créer une libellé appelée "Achats" pour stocker toutes les informations sur mes achats passés, y compris les détails tels que la date d'achat, le montant dépensé et les produits achetés



Ensuite, je créerai d'autres libellés pour faciliter la recherche de toutes les informations importantes ou nécessaires dont j'aurai besoin



- Pour l'étude : Je vais utiliser des libellés pour organiser mes cours en ligne, mes lectures obligatoires, mes projets en cours, mes devoirs à rendre.
- Pour la formation : Je vais utiliser des libellés pour suivre mes sessions de formation, organiser mon matériel de formation, évaluer mes performances, définir mes objectifs de formation et mes programmes de certification

- Pour freelance : Je vais créer des libellés pour gérer mes clients actuels, mes prospects, ma facturation, mes tâches à effectuer, mon budget et mes collaborateurs en tant que travailleur indépendant.
- Pour les informations personnelles : Je vais créer des libellés pour gérer ma liste de tout le message personnel.

7 - Comprendre le suivi du navigateur

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

- Voici quelques instructions pour comparer votre navigateur web préféré et un navigateur privé.
 - Ouvrez votre navigateur web préféré et accédez à un site web de votre choix.
 - Utilisez l'option "Inspecter l'élément" (en général, il suffit de cliquer sur le bouton droit de la souris et de sélectionner l'option "Inspecter l'élément") pour accéder aux outils de développement du navigateur.
 - Sélectionnez l'onglet "Stockage" dans les outils de développement. Explorez les différentes options disponibles pour les cookies.
 - Regardez les différents types de cookies présents et notez les informations qu'ils contiennent.
 - Activez la navigation privée dans votre navigateur.
 - Accédez au même site web que précédemment et naviguez sur le site pendant quelques minutes.
 - Utilisez à nouveau les outils de développement pour vérifier si des cookies ont été stockés pendant votre session de navigation privée.
 - Comparez les résultats obtenus lors de la navigation normale et de la navigation privée.

1) Comment fonctionnent les cookies et de quelle manière sont-ils employés pour suivre la navigation sur un site web ?

- Les cookies sont des fichiers de données stockés sur votre ordinateur lors de la visite d'un site web.
- Les cookies sont utilisés pour stocker des informations telles que les préférences de navigation, les noms d'utilisateur et les mots de passe.
- Les cookies sont également utilisés pour suivre l'activité des utilisateurs sur un site web. Les cookies peuvent améliorer l'expérience utilisateur en permettant aux utilisateurs de rester connectés à leur compte ou en personnalisant le contenu en fonction de leurs préférences.
- Les cookies peuvent également être utilisés pour suivre l'activité en ligne, collecter des informations sur les habitudes de navigation et les partager avec des tiers.
- Les navigateurs proposent des options de navigation privée pour supprimer automatiquement les cookies et bloquer les cookies tiers.
- Les options de navigation privée protègent la vie privée des utilisateurs en empêchant les sites web et les annonceurs de suivre leur activité en ligne.

2) Découvrir comment utiliser la navigation privée afin de prévenir la surveillance de votre navigation.

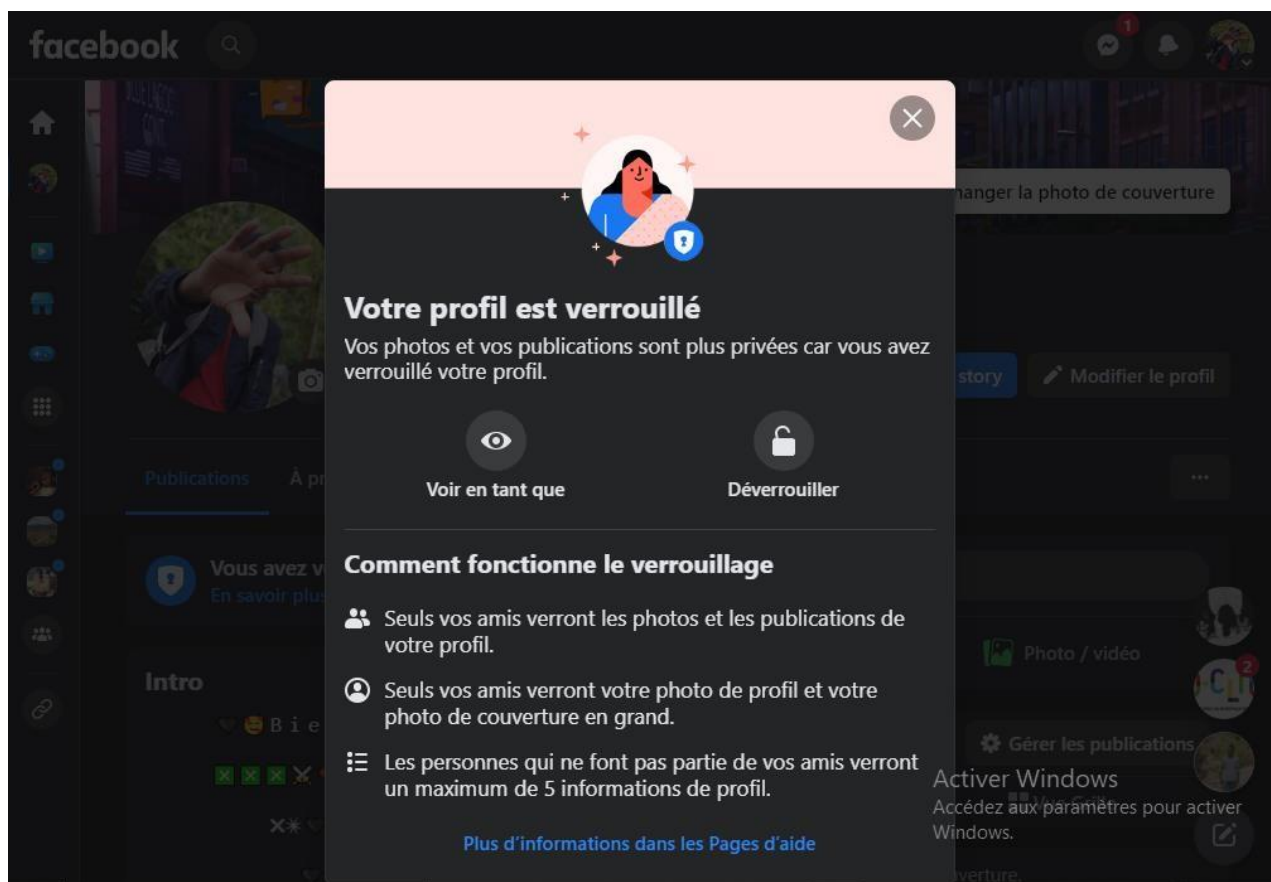
- Ouvrez votre navigateur web préféré, tel que Google Chrome, Mozilla Firefox ou Safari.
- Trouvez l'option pour activer la navigation privée. Dans Google Chrome, vous pouvez cliquer sur les trois points en haut à droite de la fenêtre du navigateur, puis sélectionner "Nouvelle fenêtre de navigation privée". Dans Mozilla Firefox, vous pouvez cliquer sur les trois traits en haut à droite, puis sélectionner "Nouvelle fenêtre privée". Dans Safari, vous pouvez cliquer sur "Fichier" dans la barre de menu, puis sélectionner "Nouvelle fenêtre privée".

- Utilisez la fenêtre de navigation privée pour naviguer sur Internet. Les cookies et les informations de navigation ne seront pas enregistrés sur votre ordinateur, ce qui peut aider à prévenir le suivi de la navigation.
- Fermez la fenêtre de navigation privée lorsque vous avez terminé de naviguer. Les informations de navigation ne seront pas enregistrées, ce qui peut aider à protéger la vie privée en ligne.

8 - Principes de base de la confidentialité des médias sociaux

Objectif : Régler les paramètres de confidentialité de Facebook

1) Je choisis de verrouiller mon profil pour sécuriser les informations confidentielles de mon compte.



Pour amie seulement :

tous vos logiciels sont à jour avec les dernières mises à jour de sécurité pour éviter les failles connues.

- Test de votre antivirus : Utilisez un outil en ligne pour tester votre antivirus et vous assurer de son bon fonctionnement.
- Vérification des paramètres de sécurité de votre navigateur : Utilisez un outil en ligne pour examiner les paramètres de sécurité de votre navigateur et vous assurer qu'ils sont correctement configurés.
- Analyse complète de votre ordinateur : Utilisez un logiciel antivirus pour exécuter une analyse approfondie de votre ordinateur afin de détecter et de supprimer tout programme malveillant.
- Vérification des paramètres de votre pare-feu : Vérifiez que votre pare-feu est activé et configuré pour bloquer les connexions entrantes non autorisées.
- Utilisation d'un VPN : Employez un réseau privé virtuel (VPN) pour sécuriser votre connexion Internet et chiffrer toutes les données que vous transmettez et recevez.
- Vérification des paramètres de votre compte utilisateur : Assurez-vous que votre compte utilisateur est configuré avec un mot de passe solide et que les paramètres de sécurité sont adéquats. Sauvegarde régulière de vos données : Effectuez régulièrement des sauvegardes de vos données importantes sur un disque dur externe ou dans le cloud pour éviter de perdre des données en cas de problème de sécurité ou de défaillance de disque dur.

2) Pour la sécurité de votre téléphone :

- Mettez à jour votre téléphone : Installez les mises à jour de sécurité pour votre téléphone dès qu'elles sont disponibles pour maintenir votre appareil protégé contre les menaces en ligne.
- Sécurisez votre téléphone avec un code ou une empreinte digitale : Protégez votre téléphone en le sécurisant avec un code ou une empreinte digitale pour prévenir tout accès non autorisé.
- Sélectionnez des sources d'application fiables : Choisissez des sources d'application fiables, telles que le Google Play Store ou l'App Store, pour éviter les applications malveillantes.

- Utilisez une application antivirus : Installez une application antivirus pour détecter et supprimer les menaces potentielles, telles que les logiciels malveillants et les virus.
- Contrôlez les autorisations des applications : Avant d'installer une application, vérifiez les autorisations qu'elle demande pour s'assurer qu'elle n'a pas accès à des informations sensibles sans votre consentement.
- Activez la localisation sélective : Activez la localisation sélective pour éviter de partager votre position avec des applications ou des services non fiables.
- Sécurisez votre connexion en évitant les réseaux Wi-Fi publics non fiables ou en utilisant un VPN pour protéger votre trafic.
- Effectuez des sauvegardes fréquentes de vos données : Enregistrez régulièrement vos données importantes sur un ordinateur ou un service de stockage en ligne pour éviter de les perdre en cas de vol ou de perte de votre téléphone.
- Effectuez des vérifications périodiques sur votre téléphone : Examinez régulièrement les applications installées, les paramètres de sécurité et l'historique de navigation pour déceler toute activité anormale.

b. Je propose un exercice pour installer et utiliser un antivirus et un antimalware adapté à l'appareil utilisé.

- Alors je choisis McAfee pour faire un exemple :
 - Tout d'abord, rendez-vous sur le site officiel de McAfee pour télécharger le logiciel d'installation : <https://www.mcafee.com/en-us/downloads/>. Assurez-vous de télécharger la version compatible avec votre système d'exploitation.
 - Une fois le téléchargement terminé, double-cliquez sur le fichier d'installation pour lancer le processus d'installation. Suivez les instructions à l'écran pour installer le logiciel.

- Une fois l'installation terminée, ouvrez McAfee et suivez les instructions pour configurer le programme. Vous pouvez choisir les paramètres de numérisation et les options de sécurité en fonction de vos préférences.
- Pour lancer une numérisation, cliquez sur le bouton "Analyser" dans l'interface de McAfee. Vous pouvez choisir de numériser tout votre système ou des fichiers spécifiques.
- En cas de détection de menaces, McAfee vous avertira et vous proposera des options pour supprimer ou mettre en quarantaine les fichiers infectés.
- Vous pouvez également configurer des paramètres de planification pour que McAfee effectue des numérisations régulières de votre système, ou exécuter manuellement une numérisation à tout moment.
- Enfin, il est important de garder McAfee à jour en téléchargeant les dernières mises à jour de sécurité pour vous protéger contre les nouvelles menaces.