

# Parcours : DISCOVERY

Module : Naviguer en toute sécurité

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

*Tous vos travaux devront être déposés sur votre compte Github*

**Sommaire**

1 - Introduction à la sécurité sur Internet

2 - Créer des mots de passe forts

3 - Fonctionnalité de sécurité de votre

navigateur 4 - Éviter le spam et le phishing

5 - Comment éviter les logiciels malveillants

6 - Achats en ligne sécurisés

7 - Comprendre le suivi du navigateur

8 - Principes de base de la confidentialité des médias

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

virus

# 1 - Introduction à la sécurité sur Internet

Objectif : à la découverte de la sécurité sur internet

**1/ En naviguant sur le web, consultez trois articles qui parlent de sécurité sur internet. Pense à vérifier la source des informations et essayez de consulter des articles récents pour que les informations soient à jour. Saisissez le nom du site et de l'article. •**

## Réponse 1

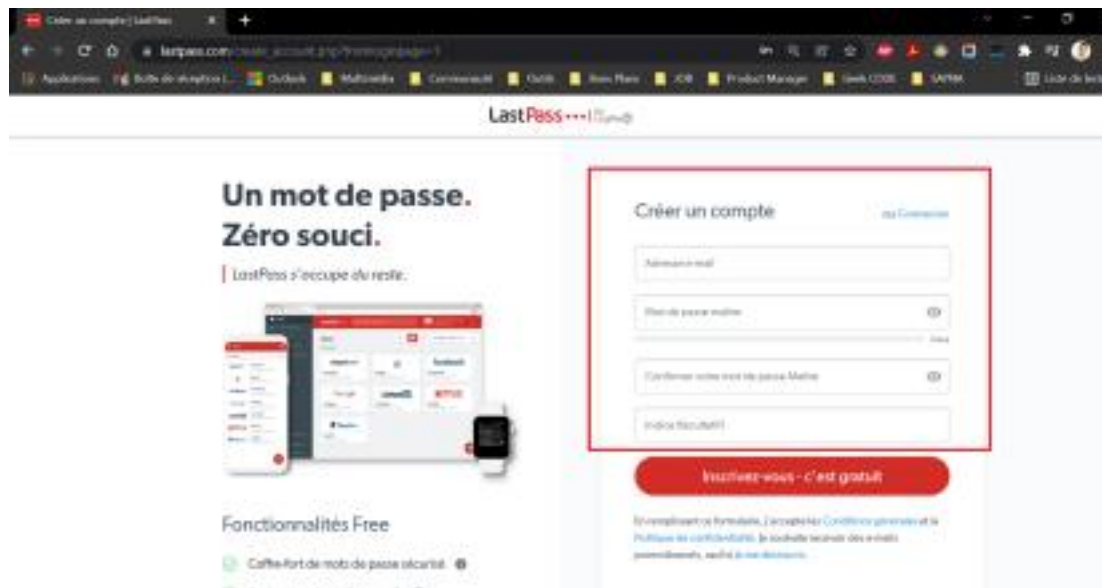
- Article 1 = [www.techradar.com](http://www.techradar.com) - "5 conseils pour protéger votre vie privée en ligne"
- Article 2 = [www.wired.com](http://www.wired.com) - "L'importance de la sécurité des mots de passe"
- Article 3 = <https://www.pcmag.com/how-to/how-to-secure-your-home-wi-fi-network> - nom de l'article - "Comment sécuriser votre réseau domestique"

## 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. Suivez les étapes suivantes. (case à cocher)**

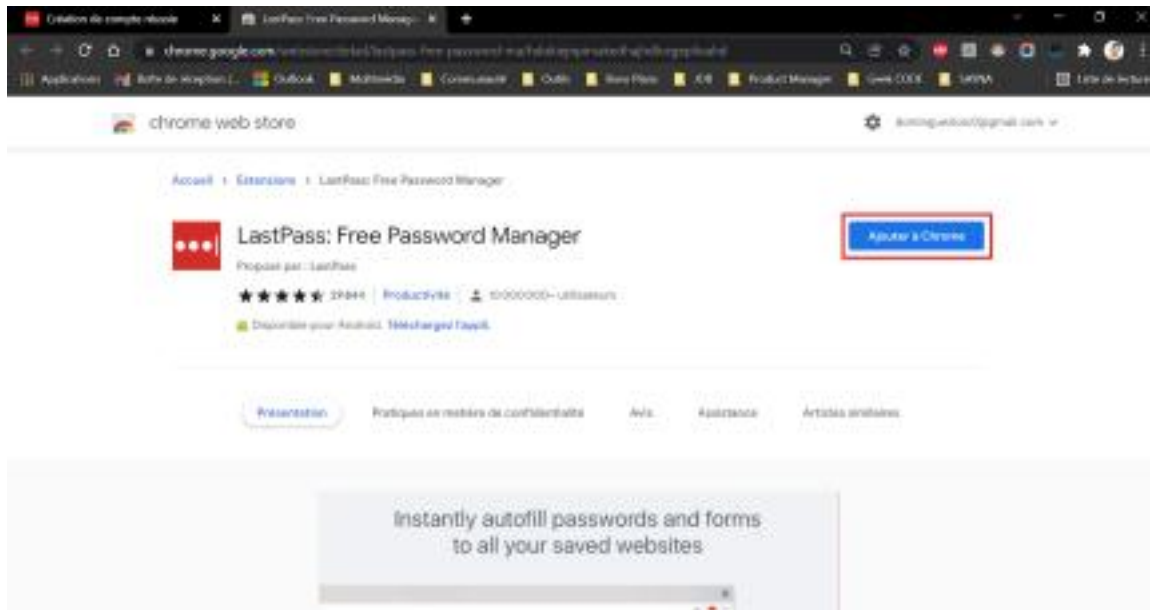
- ✓ • Accédez au site de LastPass avec ce lien : <https://lastpass.com/create-account.php>





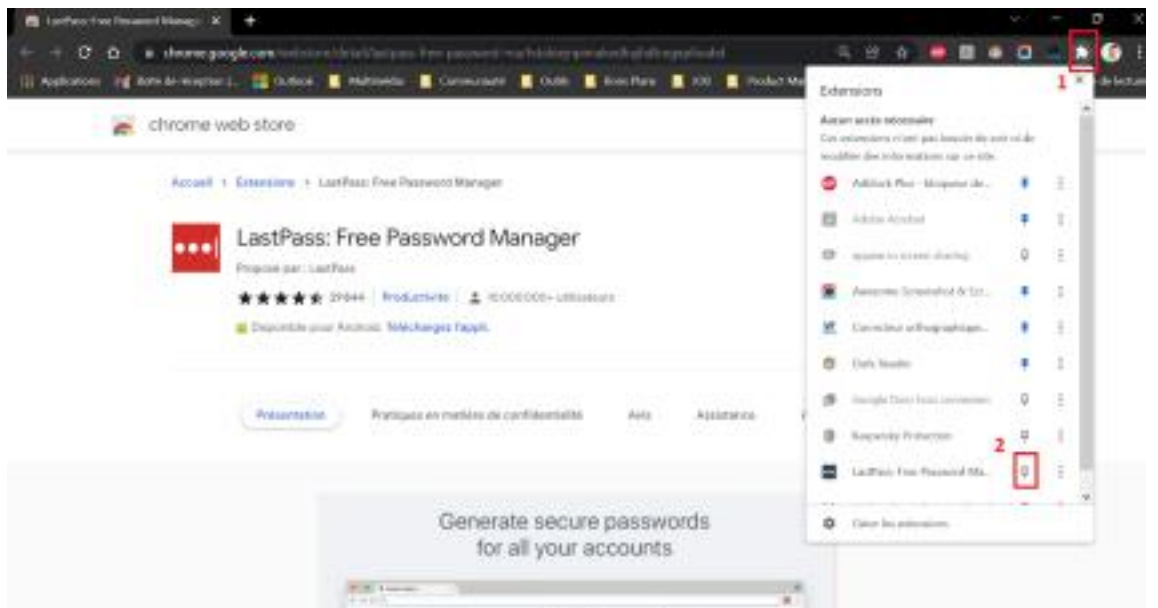
- ✓ • Crée un compte en remplissant le formulaire. Un conseil, on te demande de choisir un mot de passe maître. Pour rappel, ce mot de passe sera unique et te permettra d'accéder à tous tes comptes. Choisis donc un mot de passe avec un niveau de sécurité élevé et assure-toi de pouvoir le retrouver
- 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



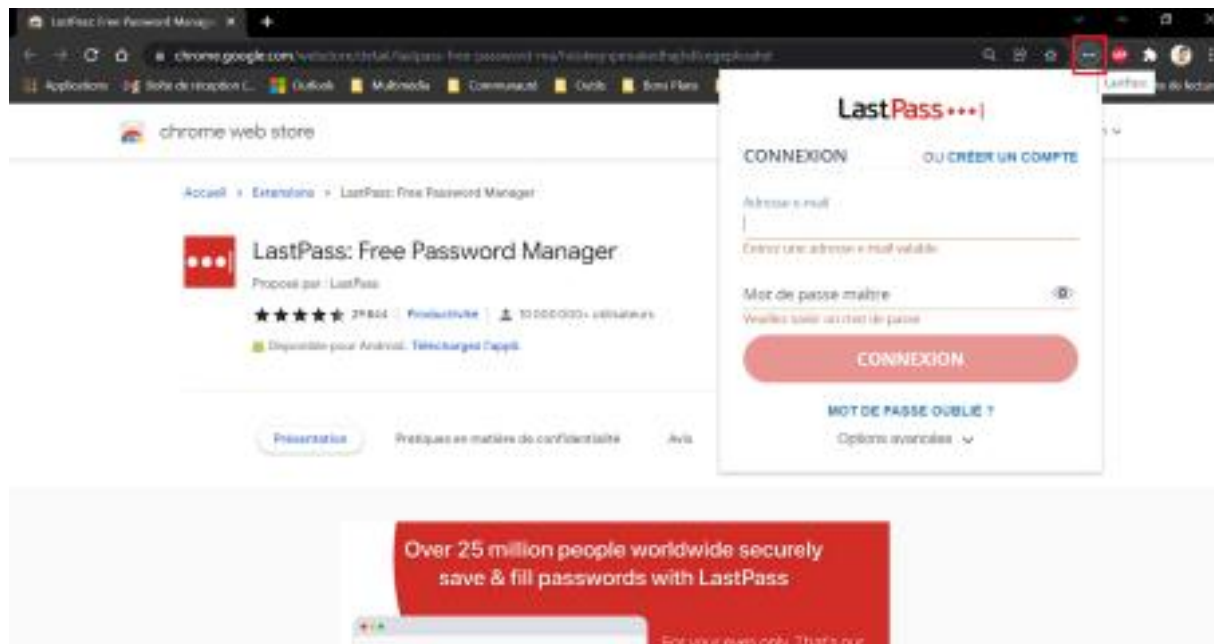
Il te suffit de valider l'opération sur le Chrome Web Store en effectuant un clic sur le bouton "Ajouter à Chrome"



- ✓
  - 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" 
    - (2) Épingler l'extension de LastPass avec l'icône 

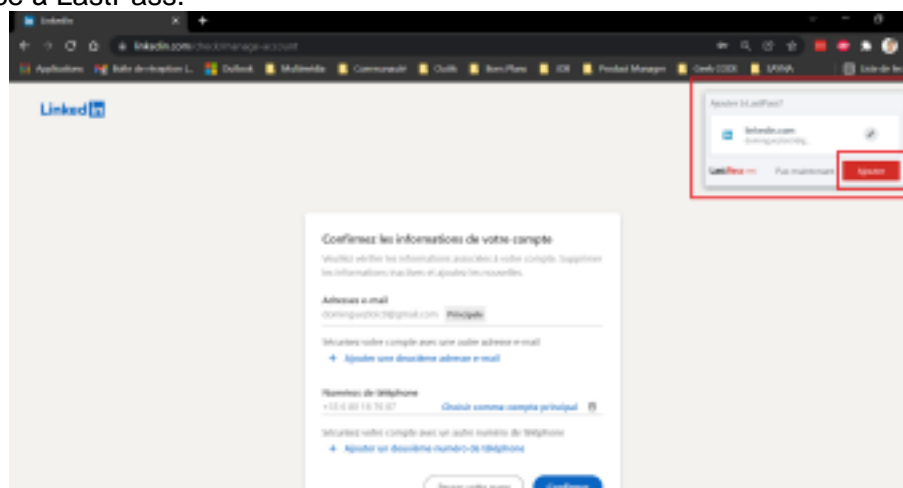


- ✓
  - Il ne te reste plus qu'à te connecter en effectuant un clic sur l'icône de l'extension et en saisissant ton identifiant et mot de passe

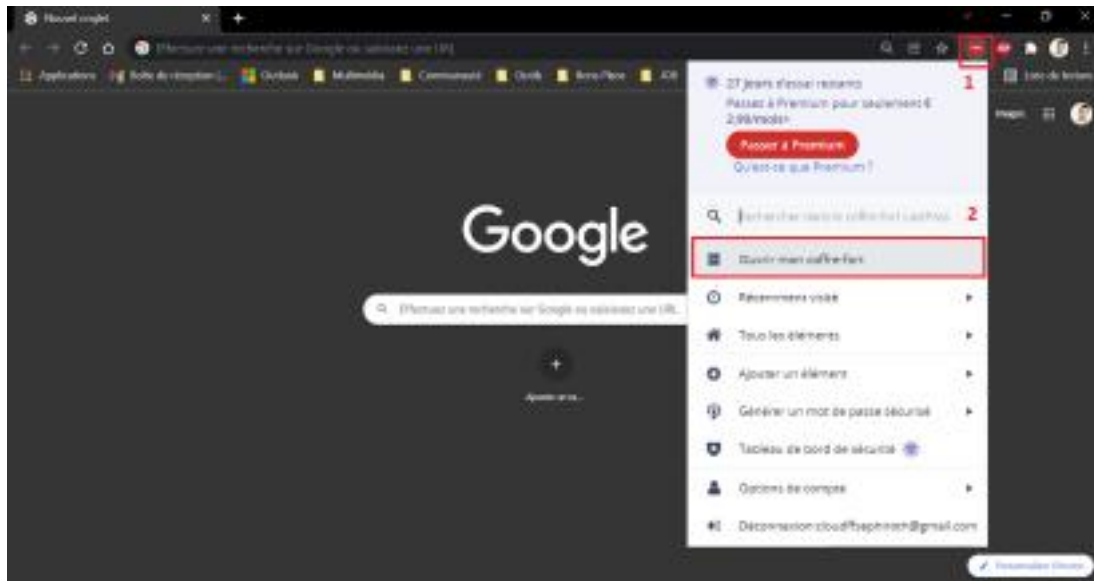


## Réponse 1

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



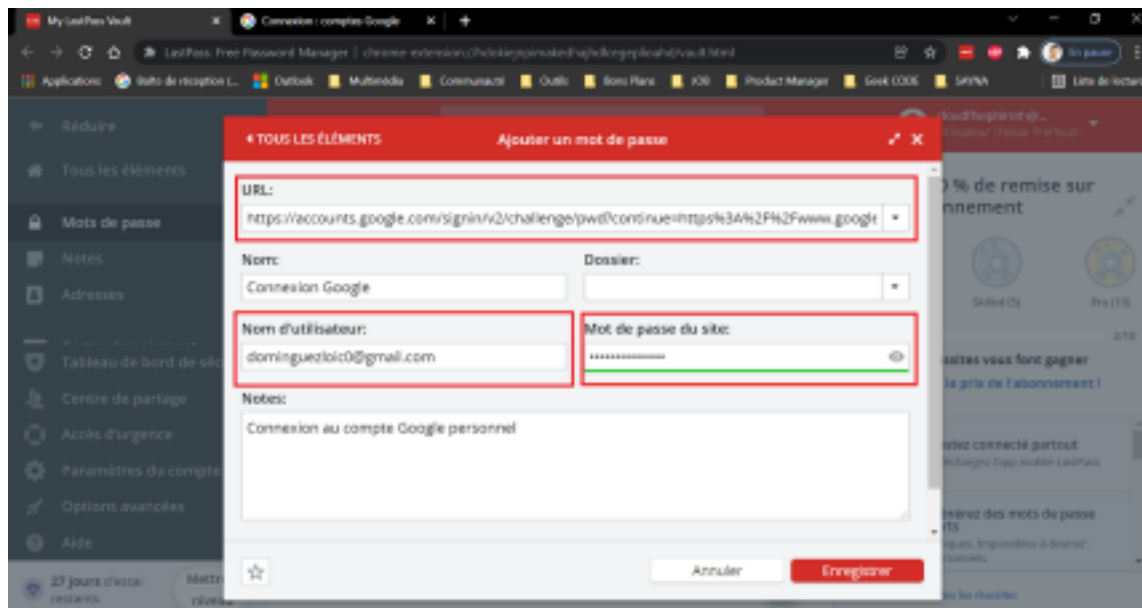
Tu peux également ajouter des comptes manuellement en accédant au coffre-fort, espace de stockage de tous tes mots de passe. Pour y accéder, clic sur l'icône de l'extension puis sur "Ouvrir mon coffre-fort".



- ✓ 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.

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](http://www.morvel.com)
- ✓ • [www.dccomics.com](http://www.dccomics.com)
- ✓ • [www.ironman.com](http://www.ironman.com)
- ✓ • [www.fessebook.com](http://www.fessebook.com)
- ✓ • [www.instagram.com](http://www.instagram.com)


#### Réponse 1

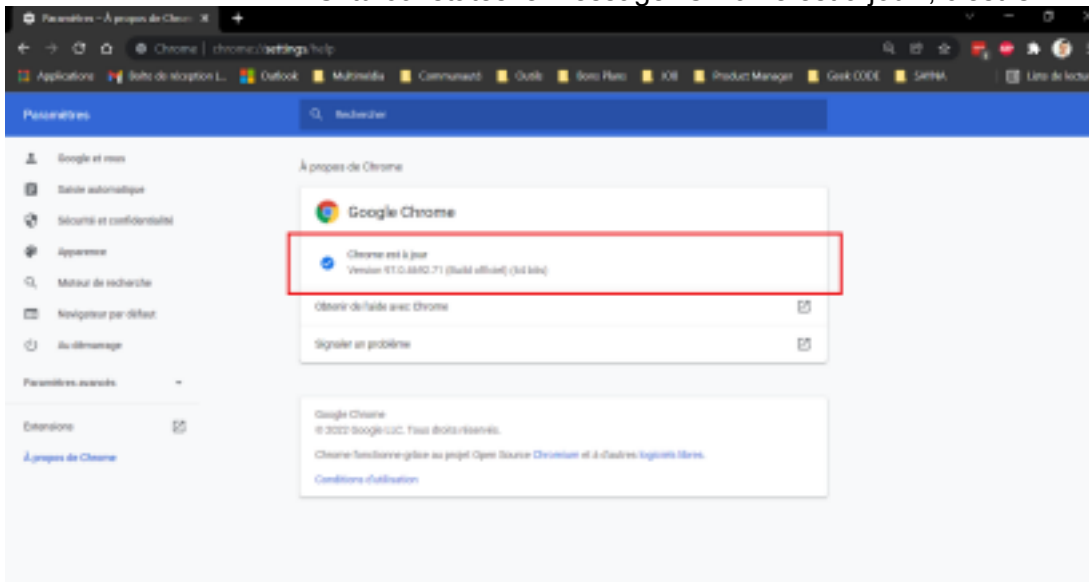
Les sites web qui semblent être malveillants sont :

- [www.morvel.com](http://www.morvel.com), un dérivé de [www.marvel.com](http://www.marvel.com), le site web officiel de l'univers Marvel
  - [www.fessebook.com](http://www.fessebook.com), un dérivé de [www.facebook.com](http://www.facebook.com), le plus grand réseau social du monde
  - [www.instagram.com](http://www.instagram.com), un dérivé de [www.instagram.com](http://www.instagram.com), un autre réseau social très utilisé
- Les seuls sites qui semblaient être cohérents sont donc :
- [www.dccomics.com](http://www.dccomics.com), le site officiel de l'univers DC Comics
  - [www.ironman.com](http://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)**

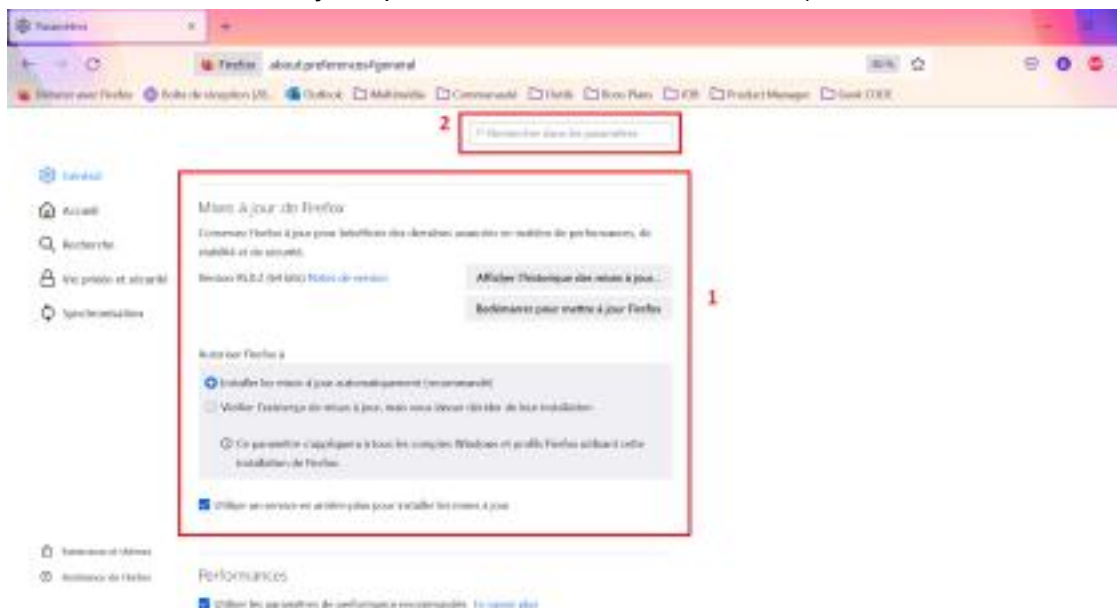
- Pour Chrome

- ✓ ○ 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)



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

**Réponse 2**



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.

## 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/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 : <http://www.baidu.com>
  - Indicateur de sécurité
    - HTTPS Not secure :
  - Analyse Google
    - Verifier un URL en particulier
- Site n°2 : <https://apache.org>
  - Indicateur de sécurité
    - HTTPS
  - Analyse Google
    - Aucun contenu suspect

- Site n°3 : <http://chinadaily.com.cn>
  - **Indicateur de sécurité**
    - HTTPS Not secure
  - **Analyse Google**
    - Vérifier un URL en particulier

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. (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

Voici un exercice pour la gestion des cookies et l'utilisation de la navigation privée :

- Ouvrez votre navigateur web préféré et accédez à un site web de votre choix.
- Vérifiez les paramètres de votre navigateur pour voir si les cookies sont activés. Si les cookies sont activés, les sites web peuvent stocker des informations sur votre ordinateur pour améliorer votre expérience en ligne.
- Désactivez les cookies dans les paramètres de votre navigateur et rechargez le site web. Notez les différences dans les fonctionnalités et les performances du site web.
- Activez la navigation privée dans les paramètres de votre navigateur. Cette fonctionnalité empêche le navigateur de stocker des informations sur votre historique de navigation, vos mots de passe et autres informations personnelles.
- Accédez à un autre site web dans une nouvelle fenêtre de navigation privée et vérifiez si les cookies sont activés. Notez les différences dans les fonctionnalités et les performances du site web.
- Fermez la fenêtre de navigation privée et accédez à nouveau au premier site web. Notez que toutes les informations stockées dans les cookies ont été supprimées.
- On peut gérer les cookies sur votre navigateur et d'utiliser la navigation privée pour protéger votre vie privée en ligne. Vous pouvez également noter les différences de performances entre les différents modes de navigation et choisir celui qui convient le mieux à vos besoins en ligne.

## 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 (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.

### 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 ????????

- Sélectionnez plusieurs appareils différents que vous utilisez couramment, tels que votre ordinateur portable, votre téléphone portable et votre tablette.
- Connectez-vous à votre compte de messagerie, votre compte de réseaux sociaux ou votre compte bancaire en ligne sur chaque appareil.
- Essayez d'accéder à ces comptes en utilisant des mots de passe différents et complexes pour chaque appareil. Vérifiez également que les fonctionnalités de sécurité, telles que l'authentification à deux facteurs, sont activées pour chaque compte.

- Essayez de connecter aux mêmes comptes à partir d'un ordinateur public, tel qu'une bibliothèque ou un cybercafé. Notez les différences dans la sécurité et la facilité d'accès entre les différents appareils.
- Si on trouve des problèmes de sécurité, tels que des informations de connexion stockées sur un appareil public ou une connexion non sécurisée, prenez des mesures pour résoudre ces problèmes, tels que la suppression de l'historique de navigation ou la modification des paramètres de sécurité de votre compte.
- Il faut vérifier la sécurité des appareils et de prendre les mesures nécessaires pour protéger vos informations personnelles et financières en ligne.

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

Voici un exercice pour installer et utiliser un antivirus + antimalware en fonction de l'appareil utilisé :

- Sélectionnez un antivirus + antimalware que vous souhaitez installer sur votre appareil. Il existe de nombreuses options disponibles, telles que Norton, McAfee, Avast, Bitdefender, etc. Recherchez les avis et les recommandations avant de faire votre choix.
- Téléchargez et installez l'antivirus + antimalware sur votre appareil. Les étapes d'installation varieront en fonction du logiciel que vous avez choisi, mais elles sont généralement simples et guidées.
- Après l'installation, ouvrez le logiciel et effectuez une analyse complète de votre appareil. Cette analyse peut prendre un certain temps en fonction de la taille de votre disque dur et de la quantité de données stockées sur votre appareil.
- Si l'antivirus + antimalware détecte des menaces, suivez les instructions pour supprimer les fichiers infectés ou mettre en quarantaine les fichiers suspects.
- Assurez-vous que l'antivirus + antimalware est mis à jour régulièrement pour protéger votre appareil contre les dernières menaces de sécurité. La plupart des logiciels ont une option pour effectuer des mises à jour automatiques.
- Utilisez votre appareil en toute sécurité en sachant que vous êtes protégé contre les menaces de sécurité en ligne.