

# 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 internet

Objectif : à la découverte de la sécurité sur internet

Trois articles parlant de la sécurité sur internet :

- Article 1 : [Mozilla Développer - La sécurité d'un site Web - Apprendre le développement web](#)
- Article 2 : [Kaspersky - 6 conseils pour renforcer votre sécurité en ligne en 2023](#)
- Article 3 : [Les numériques - quels dangers en 2023 ? Comment protéger ses appareils...](#)

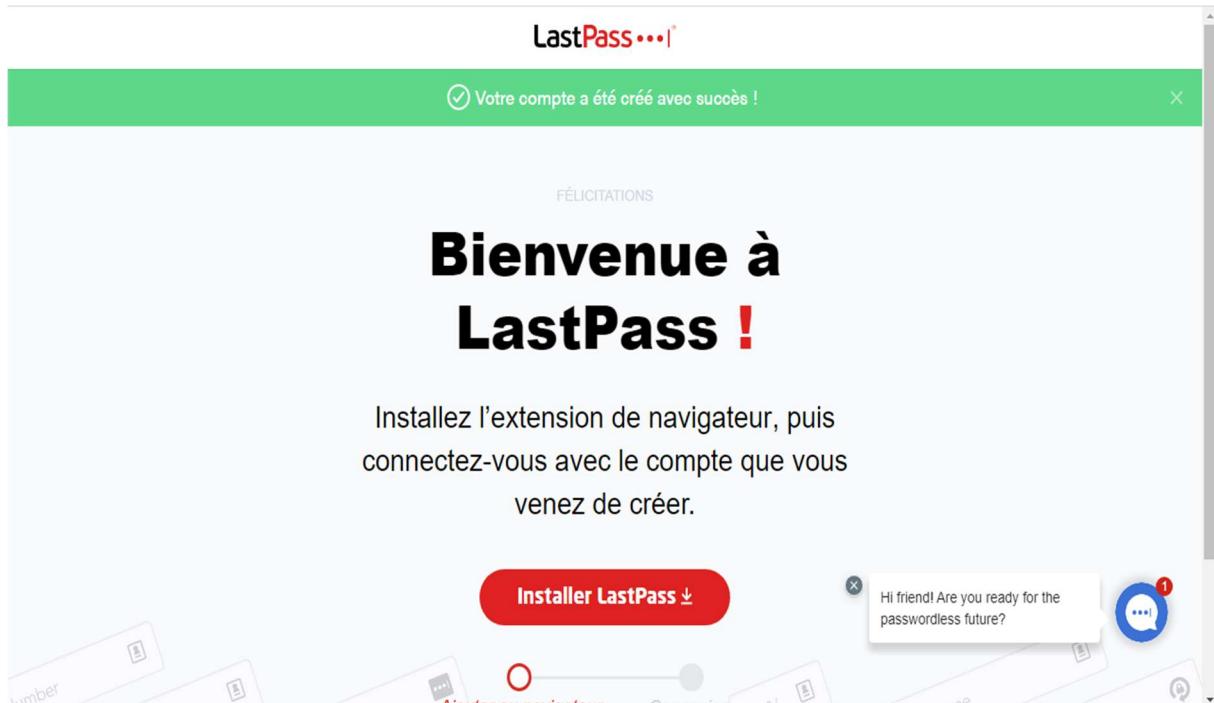
## 2. Créer des mots de passe forts

Objectif : utiliser un gestionnaire de mot de passe LastPass

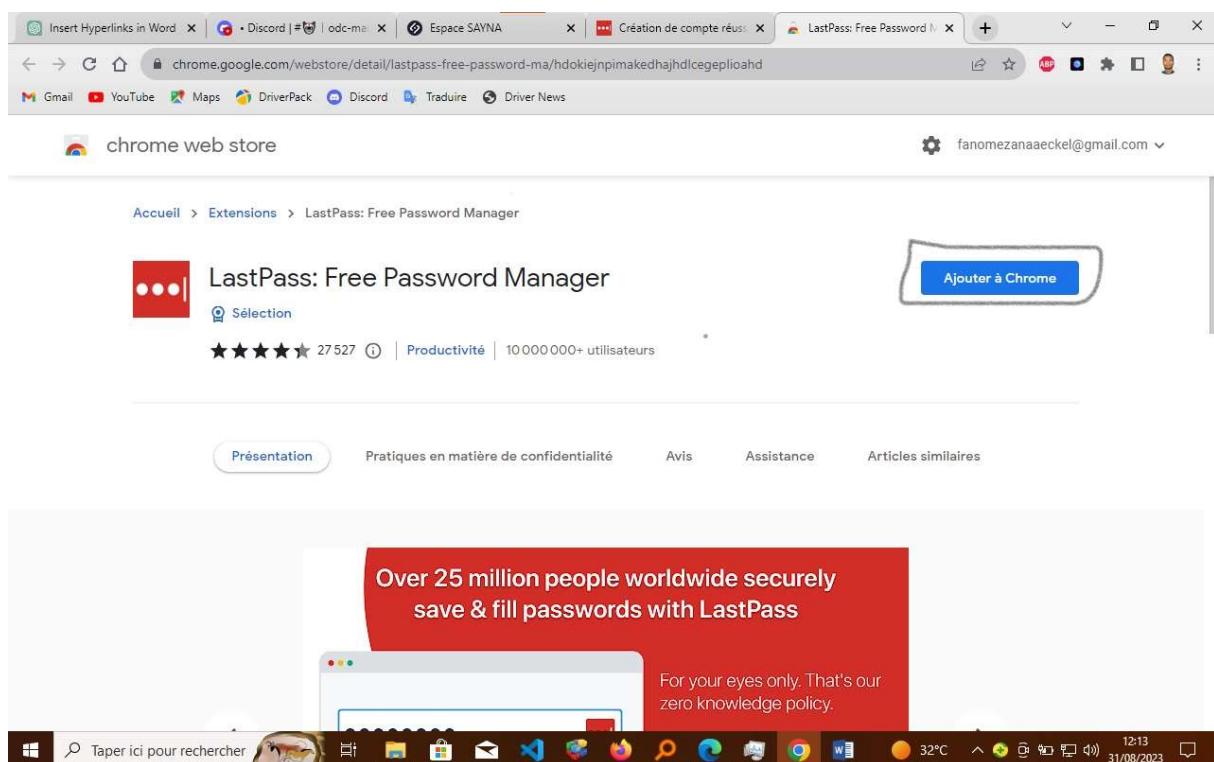
- Accéder au site Lastpass et faire l'inscription

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab is 'Créer un compte | LastPass'. The URL in the address bar is 'lastpass.com/create-account.php'. The page content includes a large 'LastPass....' logo at the top, followed by the text 'Un mot de passe. Zéro souci.' and 'LastPass s'occupe du reste.' Below this, there's a visual of a smartphone, a laptop displaying the LastPass interface, and a smartwatch. A sidebar on the right lists 'Exigences minimales:' with several items checked, such as 'Indicateur de force au maximum', 'Au moins 12 caractères', and 'Pas votre e-mail'. At the bottom of the browser window, the Windows taskbar is visible with various icons.

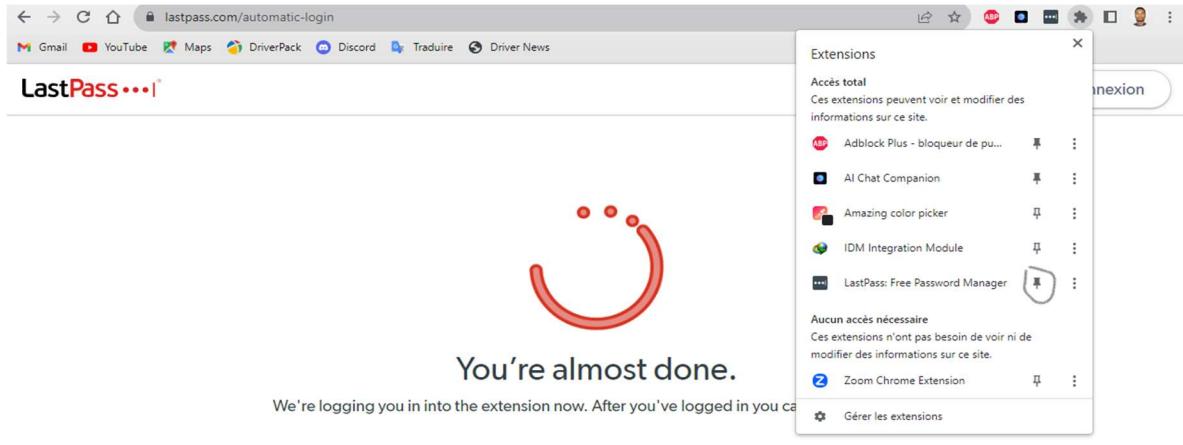
- Voici la page demandant l'installation de l'extension Lastpass sur le navigateur



- Ensuite il ne reste plus que d'installer l'extension sur le navigateur



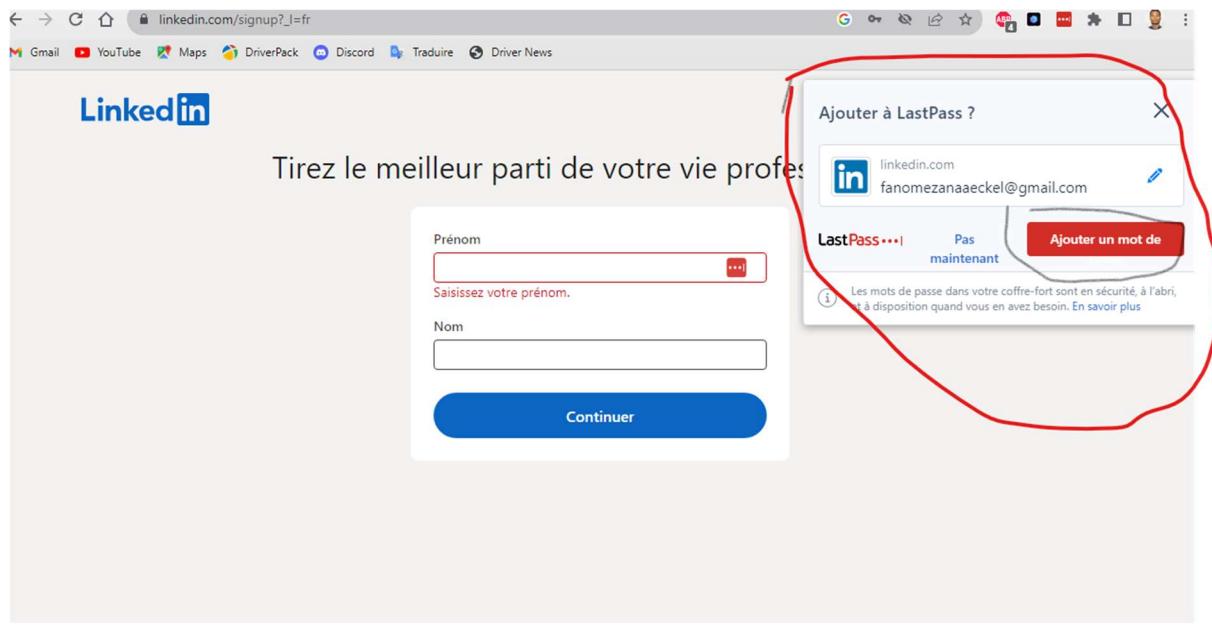
- On épingle l'extension à la barre des extensions



- Ainsi il ne reste plus qu'à se connecter avec l'icône de l'extension en saisissant l'identifiant et le mot de passe

The screenshot shows a browser window with the URL [sayna.space/parcours/course/50?parcours=Discovery](https://sayna.space/parcours/course/50?parcours=Discovery). The main content area displays a course dashboard for "Chapitre 3 - Créer des mots de passe". On the right side, a modal dialog box for "CONNEXION" is open, prompting for "Adresse e-mail" and "Mot de passe maître". Below the modal, there are links for "MOT DE PASSE OUBLIÉ ?" and "Options avancées". The SAYNA platform interface includes a sidebar with chapters and sections, and a top navigation bar with links like "Tableau de bord", "Apprendre", "Français", and "Conditions générales".

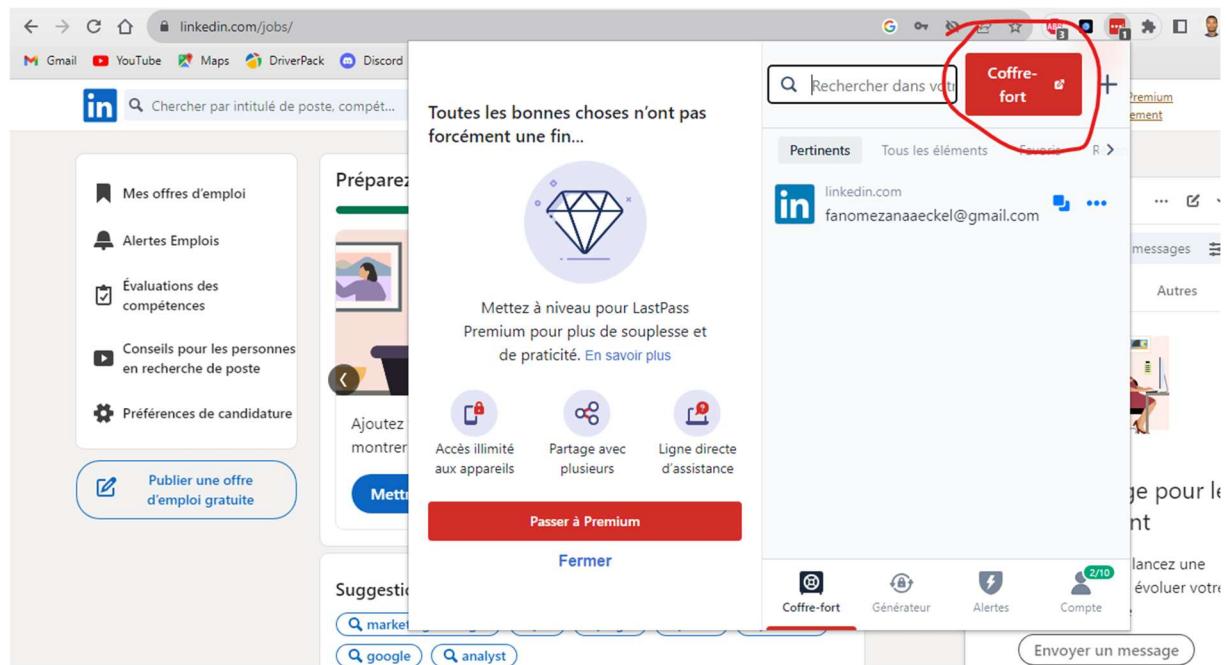
- Désormais, lorsque tu te connectes à tes comptes, tu peux enregistrer le mot de passe grâce à LastPass.



LinkedIn © 2023 À propos Accessibilité Conditions générales d'utilisation de LinkedIn Politique de confidentialité Politique relative aux cookies Politique de copyright

Politique de la marque Réclames invitées Directives de la communauté Langue

- On peut aussi ajouter un compte manuellement en cliquant sur le coffre-fort.



- Puis arriver sur le site de gestion de mot de passe, il ne reste plus qu'à ouvrir l'onglet mot de passe et cliquer sur ajouter

Bienvenue dans LastPass,  
fanomezanaaeckel !

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

**Mots de passe**

rechercher dans mon coffre-fort

Kit de démarrage

(1) novice    (5) expérimenté    (10) pro

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

Essayer le remplissage automatique  
Visitez votre coffre-fort LastPass  
Restez connecté partout

Ajouter toutes les réussites

- La dernière tâche est d'entrer l'url pour se connecter, l'identifiant et le mot de passe.

On peut aussi mettre un commentaire dans la case notes

TOUS LES ÉLÉMENTS Ajouter un mot de passe

URL: https://accounts.google.com/v3/signin/challenge/pwd?TL=AGEVcSS7tOrZSCbPYU7dUnLFjkZSdFE

Nom.: Google Dossier:

Nom d'utilisateur: fanomezanaaeckel@gmail.com Mot de passe du site: .....

Notes:

Paramètres avancés:

Annuler Enregistrer

Voici une liste des meilleurs gestionnaires de mot de passe le plus récent :

- NordPass
- Dashlane
- 1Password
- Lastpass
- Bitwarden
- KeePass

- RoboForm
- Enpass
- Proton Pass
- Dropbox Passwords

### 3. Fonctionnalité de sécurité de votre navigateur

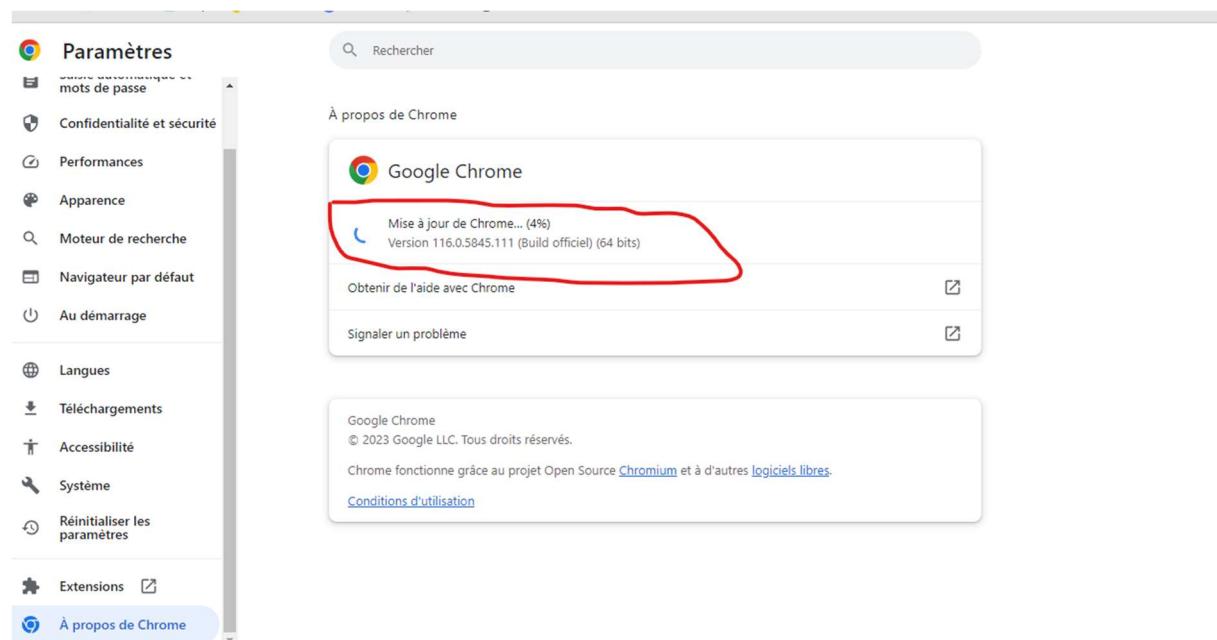
Objectif : identifier les éléments à observer pour naviguer sur le web en toute sécurité

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

- [www.morvel.com](http://www.morvel.com)
- [www.instagram.com](http://www.instagram.com)
- [www.fessebook.com](http://www.fessebook.com)

2. Nous allons vérifier si Chrome et Firefox sont à jour

Pour chrome :



Pour Firefox :

Résultats de la recherche

Mises à jour de Firefox

Conservez Firefox à jour pour bénéficier des dernières avancées en matière de performances, de stabilité et de sécurité.

Version 117.0 (64 bits) [Notes de version](#)

Afficher l'historique des mises à jour...

Firefox est à jour

Rechercher des mises à jour

Autoriser Firefox à

Installer les mises à jour automatiquement (recommandé)

Quand Firefox n'est pas lancé

Vérifier l'existence de mises à jour, mais vous laisser décider de leur installation

① Ce paramètre s'appliquera à tous les comptes Windows et profils Firefox utilisant cette installation de Firefox.

Utiliser un service en arrière-plan pour installer les mises à jour

## 4. Eviter le spam et le phishing

Objectif : Reconnaître plus facilement les messages frauduleux

- Voici un questionnaire pour reconnaître le phishing

French

Savez-vous reconnaître une tentative d'hameçonnage ?

Il peut être plus difficile qu'il n'y paraît de repérer une tentative d'hameçonnage. Lors d'une tentative d'hameçonnage, une personne malveillante essaye de vous amener à communiquer des informations personnelles se faisant passer pour quelqu'un que vous connaissez. Arrivez-vous à distinguer le vrai du faux ?

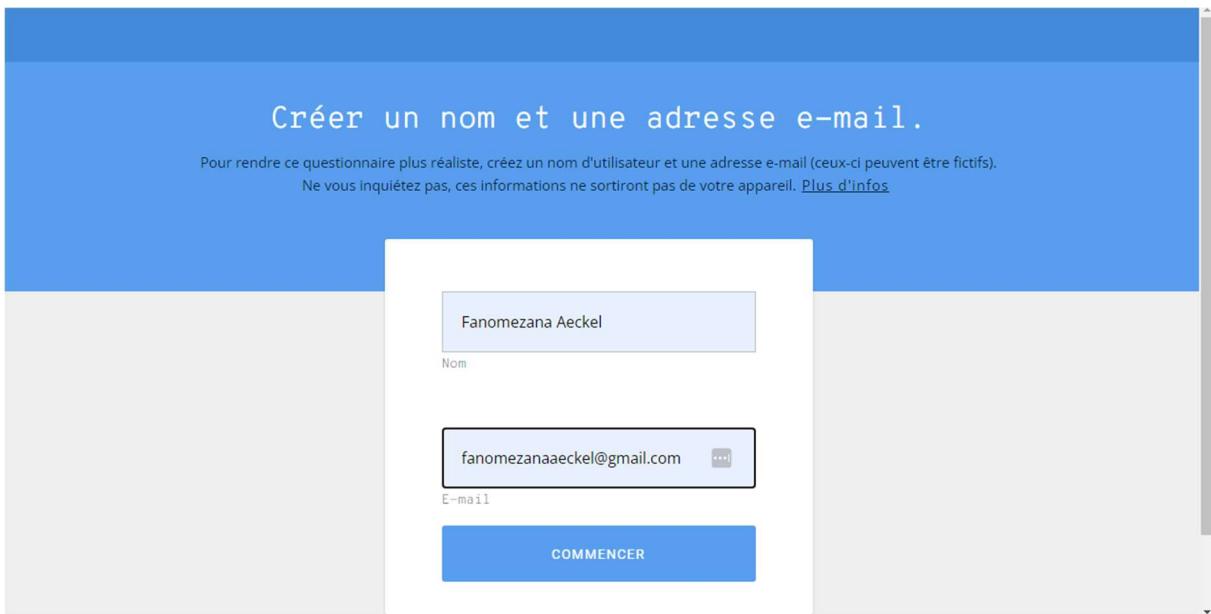
RÉPONDRE AU QUESTIONNAIRE



JIGSAW | Google

Confidentialité / Conditions / Commentaires

- Ensuite on entre le nom d'utilisateur et l'e-mail



- Puis on répond par l'une des deux choix : hameçonnage ou légitime

phishingquiz.withgoogle.com/?hl=fr

Gmail YouTube Maps DriverPack Discord Traduire Driver News

Commençons par cet e-mail Google Docs. 1

Vérifiez bien les URL des liens en passant la souris ou en appuyant de manière prolongée dessus, et examinez les adresses e-mail. Ne vous inquiétez pas, aucun des liens ne fonctionne... Nous ne voudrions pas vous rediriger vers des pages louche !

HAMEÇONNAGE LÉGITIME

Luke Johnson <luke.json8000@gmail.com>  
à moi 10:46

Luke Johnson a partagé un lien vers le document suivant :

Budget département 2023.docx

Bonjour. Voici le document demandé. N'hésitez pas à me contacter si vous avez besoin d'autre chose !

http://drive-google.com/luke.johnson

- A la fin, on note ceux qui sont vrai

8 / 8

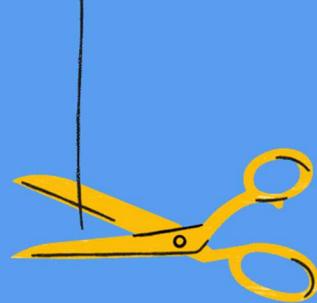
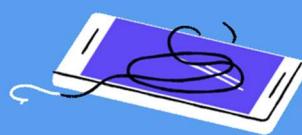
**Bravo, Fanomezana Aeckel !**  
Vous avez obtenu un score de 8/8.

Plus vous vous entraînerez, 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](http://g.co/2SV).

Partager le questionnaire :

[RECOMMENCER LE QUESTIONNAIRE](#)

 JIGSAW | Google Confidentialité / Conditions / Commentaires

## 5. Comment éviter les logiciels malveillants

Objectif : sécuriser votre ordinateur et identifier les liens suspects

Site 1 :

- Indicateur de sécurité
  - Not secure
- Analyse google
  - No available data

Site 2 :

- Indicateur de sécurité
  - HTTPS
- Analyse google
  - No unsafe content found

Site 3 :

- Indicateur de sécurité
  - Not secure
- Analyse google
  - Check a specific URL

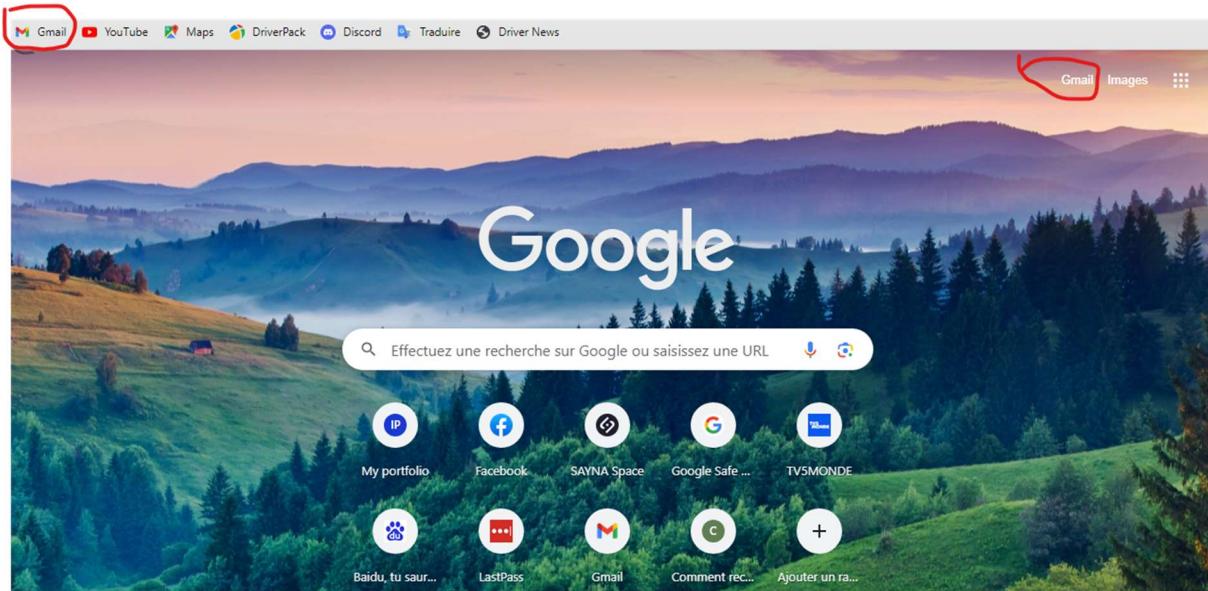
Site 4 (non sécurisé)

## 6. Achats en ligne sécurisés

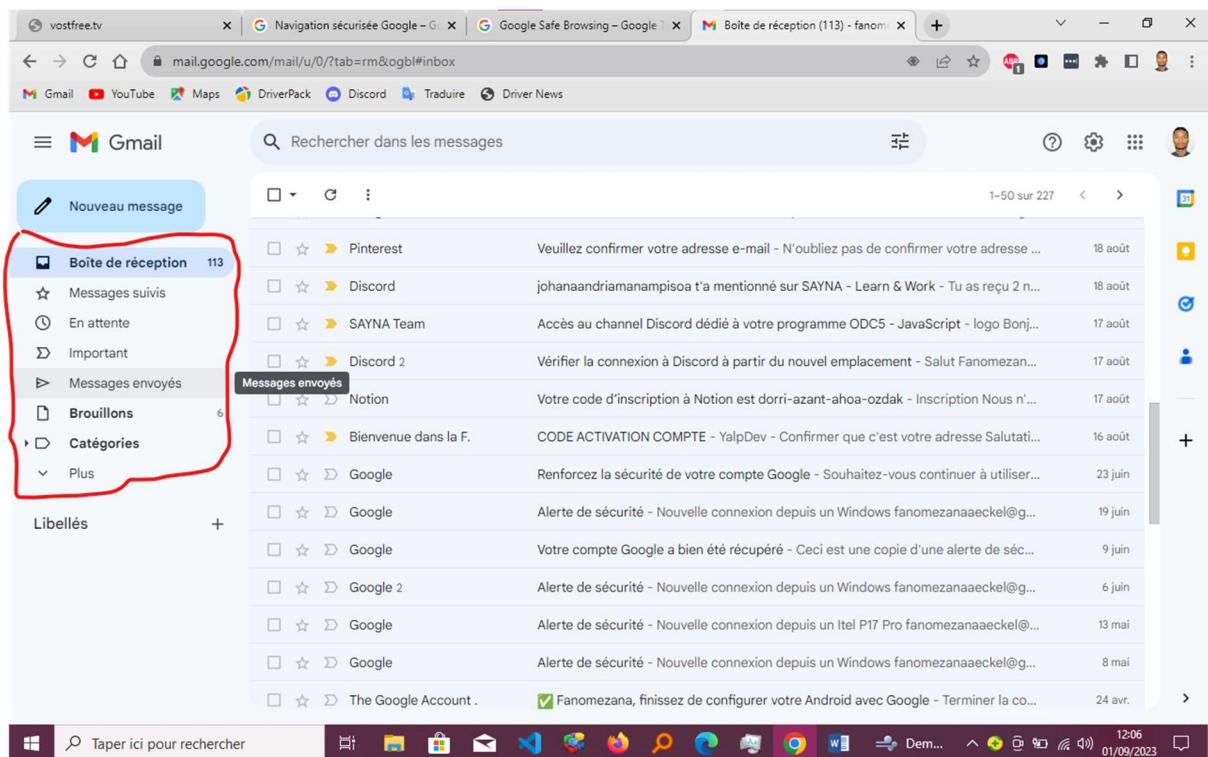
Objectif : créer un registre des achats effectués sur internet

On va créer un registre pour conserver les informations relatives aux des achats en ligne.

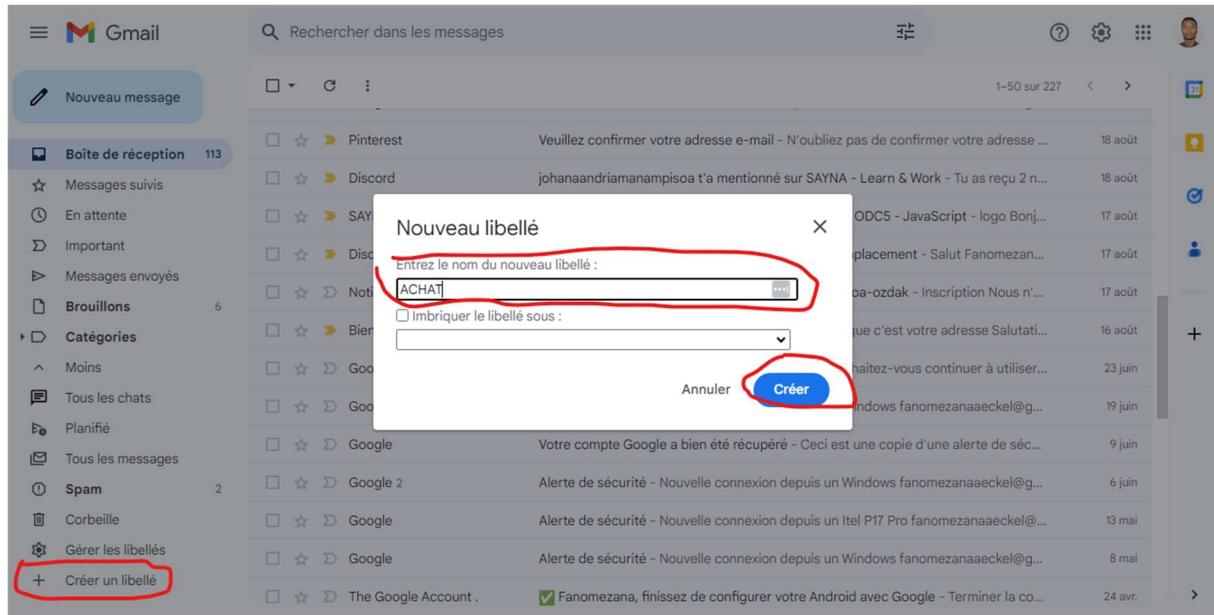
- Tout d'abord en ouvre la messagerie instantanée



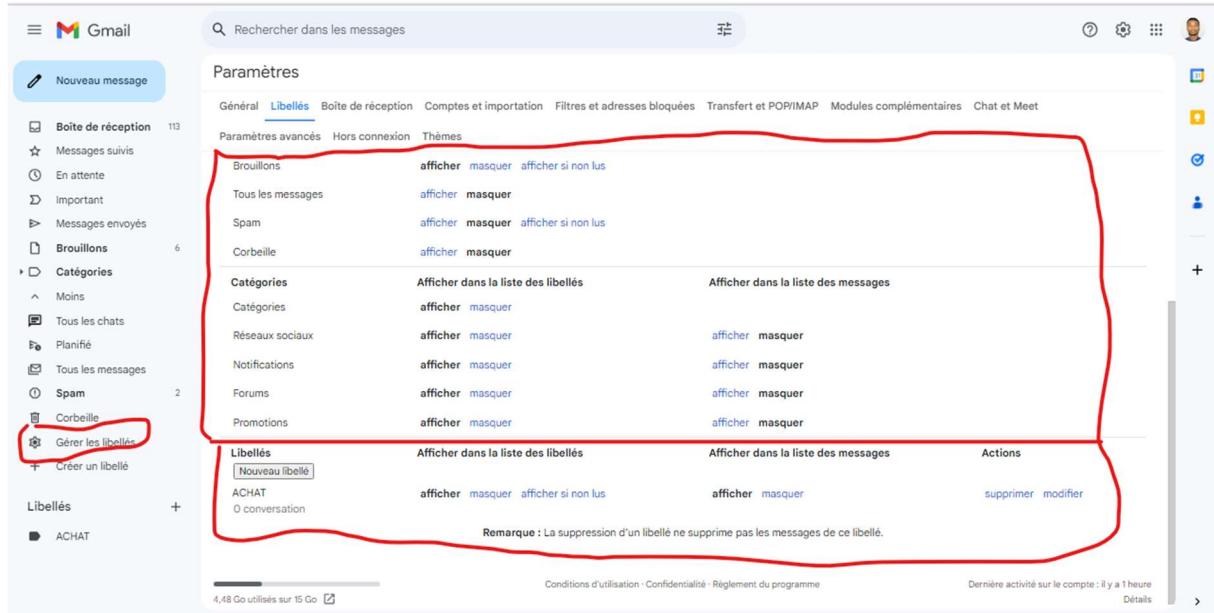
- Cliquer sur 'plus' dans la barre à gauche



- Créer le libellé ACHAT ;



- On peut aussi gérer les libellés :



- Créer quelques libellés pour mieux gérer la messagerie électronique

The screenshot shows a list of categories in a mobile application. At the top, there is a header 'Libellés' with a '+' icon. Below it is a list of items, each with a small icon and text: 'ACHAT', 'Administratif', 'Banque', 'Création de compte 1', 'Google 1', 'JOB', and 'SAYNA'. To the right of each item is a vertical ellipsis (...).

## 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

Ici on va paramétriser la confidentialité sur Facebook.

- Tout d'abord, on se connecte sur Facebook, on recherche l'onglet paramètre

The screenshot shows the Facebook homepage. On the left, there is a sidebar with links: 'Fanomezana Aeckel', 'Ami(e)s', 'Enregistrements', 'Souvenirs', 'Groupes', 'Vidéo', and 'Voir plus'. Below this is a section for 'Vos raccourcis' with links to 'CV (curriculum vitae) en ligne', 'WEBTOON-CJP HIGH LEVEL', 'IUGM - 19ème promotion', and 'Scan Up To Down [Mada]'. At the bottom of the sidebar is the URL 'https://web.facebook.com/settings/A'. On the right side of the screen, there is a sidebar titled 'Paramètres et confidentialité' with a red box around the 'Paramètres' option. Other options in this sidebar include 'Langue', 'Assistance confidentialité', 'Centre de confidentialité', 'Historique d'activité', and 'Préférences du Fil'. Below this sidebar, there is a list of friends: 'Aina Anaïs', 'Rakotoarison Sylvain Desire', 'Kanto Dia Arimanana', and 'Sitrak'ny Aina Fan'ouella'.

- On ouvre l'onglet confidentialité

**Paramètres**

- Général
- Sécurité et connexion
- Vos informations Facebook
- Confidentialité**
- Profil et identification
- Publications publiques**
- Blocage
- Langue et région
- Stories
- Notifications
- Mobile

**Paramètres et outils de confidentialité**

**Raccourcis de confidentialité**

Vérifiez certains paramètres importants  
Passez en revue rapidement quelques paramètres importants pour vous assurer que vous partagez bien avec les personnes souhaitées.

**Gérez votre profil**

Accédez à votre profil pour modifier vos informations de confidentialité, par exemple qui peut voir votre date d'anniversaire ou vos relations.

**En savoir plus sur le Centre de confidentialité**

Gérez votre confidentialité sur Facebook, Instagram et Messenger, et d'autres produits Meta.

**Votre activité**

Qui peut voir vos futures publications ?	Ami(e)s	Modifier
Examinez toutes les publications et tous les contenus dans lesquels vous êtes identifié(e)		Utiliser l'historique d'activité
Limit the audience for posts you've shared with Ami(e)s et leurs ami(e)s or Public?		Limiter l'audience des anciennes publications

- Enfin on clique sur le raccourcis de confidentialité

**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

You can discover more privacy settings on Facebook in [Parameters](#).

- Voici un paramètre de confidentialité

The screenshot shows the Facebook privacy settings interface. On the left, a sidebar lists various privacy options: Général, Sécurité et connexion, Vos informations Facebook, Confidentialité (selected), Profil et identification, Publications publiques, Blocage, Langue et région, Stories, Notifications, Mobile, Applications et sites web, Intégrations professionnelles, and Publicités. The main content area is titled 'Gérez votre confidentialité sur Facebook, Instagram et Messenger, et d'autres produits Meta.' It shows the 'Votre activité' section with a table:

Votre activité	Qui peut voir vos futures publications ?	Public	Modifier
Examinez toutes les publications et tous les contenus dans lesquels vous êtes identifié(e)	Utiliser l'historique d'activité		
Limit the audience for posts you've shared with Ami(e)s et leurs ami(e)s or Public	Limiter l'audience des anciennes publications		
Qui peut voir les personnes, Pages et listes que vous suivez ?	Public	Modifier	
Comment les autres peuvent vous trouver et vous contacter	Qui peut vous envoyer des invitations ?	Tout le monde	Modifier
	Qui peut voir votre liste d'amis ?	Ami(e)s	Modifier
	Qui peut vous trouver à l'aide de l'adresse e-mail que vous avez fournie ?	Tout le monde	Modifier
	Qui peut vous trouver à l'aide du numéro de téléphone que vous avez fourni ?	Fermer	
	Ceci concerne les personnes qui ne peuvent pas voir votre numéro de téléphone sur votre profil.		
	<input checked="" type="checkbox"/> Tout le monde		
	Voulez-vous que les moteurs de recherche en dehors de Facebook affichent un lien vers votre profil ?	Oui	Modifier

- o Et un paramètre pour les publications publiques

The screenshot shows the 'Publications publiques' section of the Facebook privacy settings. The sidebar remains the same. The main content area is titled 'Filtres et outils des publications publiques'. It contains several sections with explanatory text and buttons:

- Qui peut me suivre**: Descriptions of who can follow your public posts (real and stories) in the filter. Buttons: **Publique**.
- Commentaires des publications publiques**: Descriptions of who is allowed to comment on your public posts. Buttons: **Publique**.
- Notifications de publications publiques**: Descriptions of notifications received when people not part of your friends list interact with your public posts. Buttons: **Publique**.
- Informations de profil publiques**: Descriptions of profile information being public. Buttons: **Ami(e)s**.

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

Objectif :

- a. Un ou plusieurs exercices pour vérifier la sécurité en fonction de l'appareil utilisé

La sécurité des appareils dépend souvent de leur utilisation et de la manière dont ils sont configurés. Voici quelques exercices que vous pouvez effectuer pour vérifier la sécurité en fonction de l'appareil utilisé :

### Personnel informatique :

- Exercice : Mettez à jour votre système d'exploitation et tous les logiciels installés pour garantir que vous disposez des derniers correctifs de sécurité.

- Exercice : Installez un logiciel antivirus et effectuez une analyse complète de votre système pour détecter et supprimer les logiciels malveillants.
- Exercice : Configurez un pare-feu pour bloquer les connexions non autorisées à votre ordinateur.

**Smartphone :**

- Exercice : Mettez à jour le système d'exploitation de votre smartphone ainsi que toutes les applications installées.
- Exercice : Activez le verrouillage par mot de passe, empreinte numérique ou reconnaissance faciale pour sécuriser l'accès à votre appareil.
- Exercice : Examinez les autorisations d'application et révoquez celles qui semblent excessives ou non nécessaires.

**Routeur Wi-Fi :**

- Exercice : Changez le mot de passe par défaut de votre routeur pour empêcher les accès non autorisés à votre réseau.
- Exercice : Activez le chiffre WPA3 ou WPA2 sur votre réseau Wi-Fi pour protéger vos communications sans fil.
- Exercice : Désactivez le WPS (Wi-Fi Protected Setup) si vous ne l'utilisez pas, car il peut présenter des vulnérabilités de sécurité.

**Télévision intelligente :**

- Exercice : Mettez à jour le micrologiciel (firmware) de votre télévision intelligente pour corriger les failles de sécurité connues.
- Exercice : Désactivez les fonctionnalités de suivi et de collecte de données si elles ne sont pas nécessaires.
- Exercice : Utilisez un réseau Wi-Fi distinct pour votre téléviseur intelligent afin de réduire le risque d'accès non autorisé à d'autres appareils sur votre réseau domestique.

**Dispositifs IoT (Internet des objets) :**

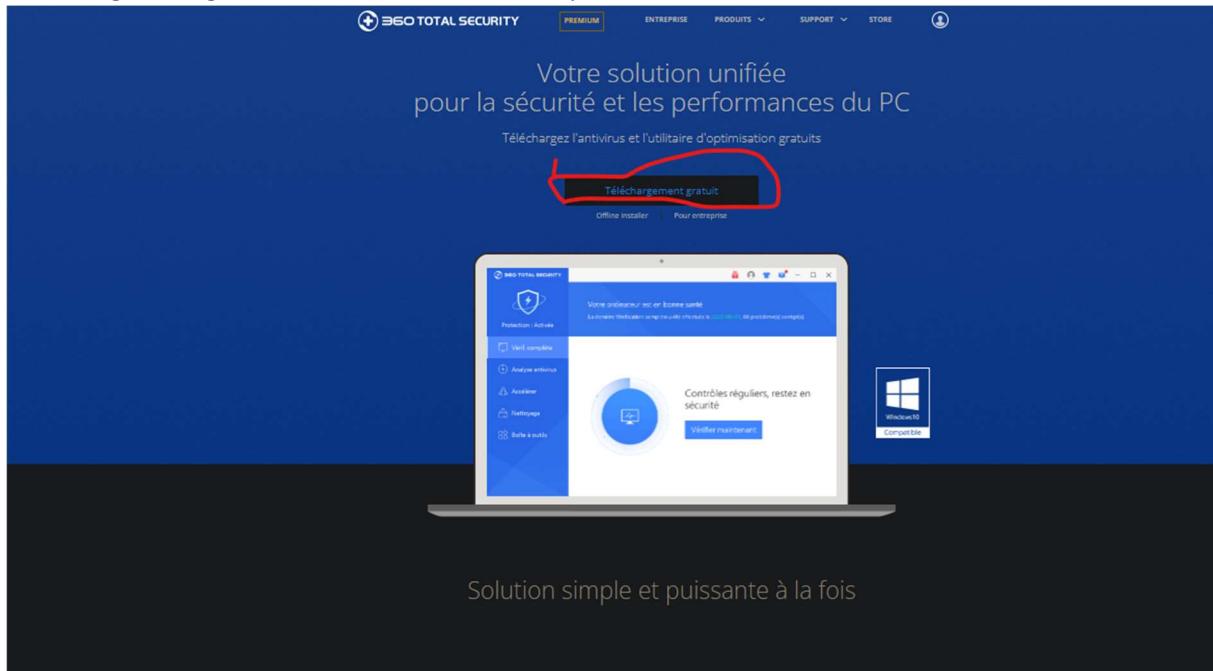
- Exercice : Changez les mots de passe par défaut sur les appareils IoT et mettez à jour leur firmware régulièrement.
- Exercice : Créez un réseau IoT distinct, isolé du réseau principal, pour minimiser les risques en cas de compromission d'un dispositif.
- Exercice : Limitez l'accès à distance aux dispositifs IoT autant que possible.

Ces exercices sont conçus pour aider à améliorer la sécurité de différents types d'appareils. Cependant, la sécurité informatique est un domaine en constante évolution, et il est important de rester informé des dernières menaces et des bonnes pratiques en matière de sécurité pour garantir la protection de vos appareils.

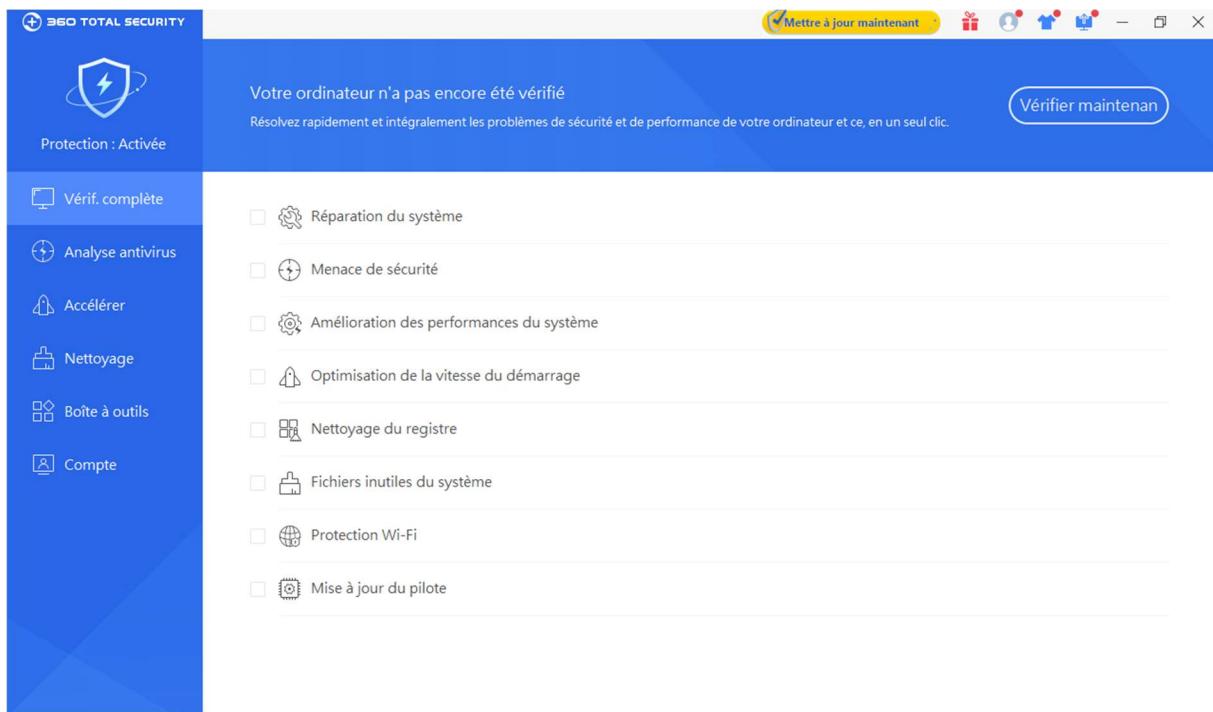
**b. Un exercice pour installer et utiliser un antivirus + malware**

J'utilise 360 Total Security en mode gratuit, donc voici les étapes à suivre :

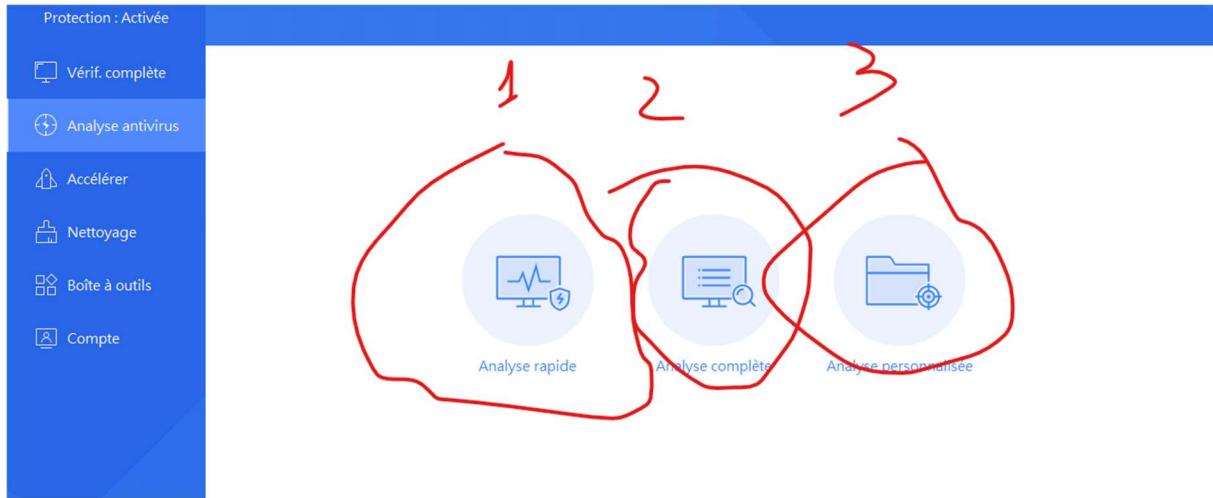
Télécharger le logiciel sur [www.360totalsecurity.com](http://www.360totalsecurity.com)



Ensuite installer le et ouvrir



Tu peux lancer une analyse antivirus général ou avancé selon ton choix



Où faire une vérification complète de l'ordinateur

