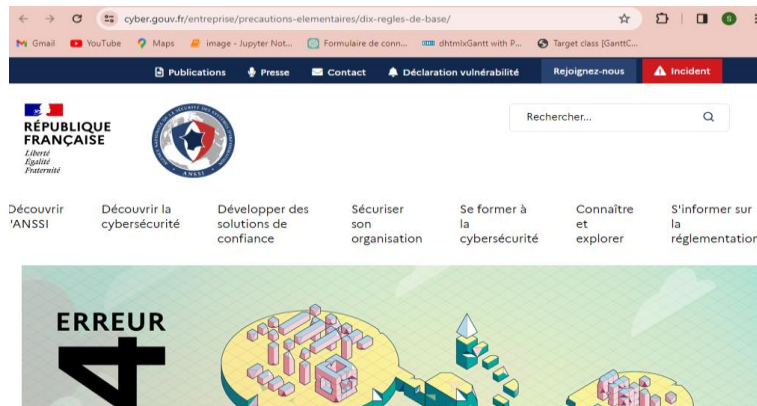


## NAVIGUER EN TOUTE SECURITE SUR INTERNET

### Introduction à la sécurité sur internet

Les trois articles qui parlent de sécurité sur internet :



#### Article 1 = ANSSI – Dix règles de base




#### Article 2 = Economie gouv – Comment assurer votre sécurité numérique



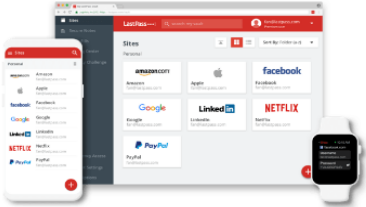
#### Article 3 = Site W- naviguer en toute sécurité sur internet

## Créer des mots de passe forts



**Un mot de passe.  
Zéro souci.**

| LastPass s'occupe du reste.




**Fonctionnalités Free**


Coffre fort de mots de passe

**Créer un compte** ou [Connexion](#)

Adresse e-mail

Mot de passe maître 

Force

Confirmer votre mot de passe Maître 

Indice (facultatif)

**Inscrivez-vous - c'est gratuit**



✓ Votre compte a été créé avec succès !

FÉLICITATIONS

# Bienvenue à LastPass !


Installez l'extension de navigateur, puis connectez-vous avec le compte que vous venez de créer.

**Installer LastPass** ↓


chrome web store

Rechercher des extensions et des thèmes

ivrir Extensions Thèmes

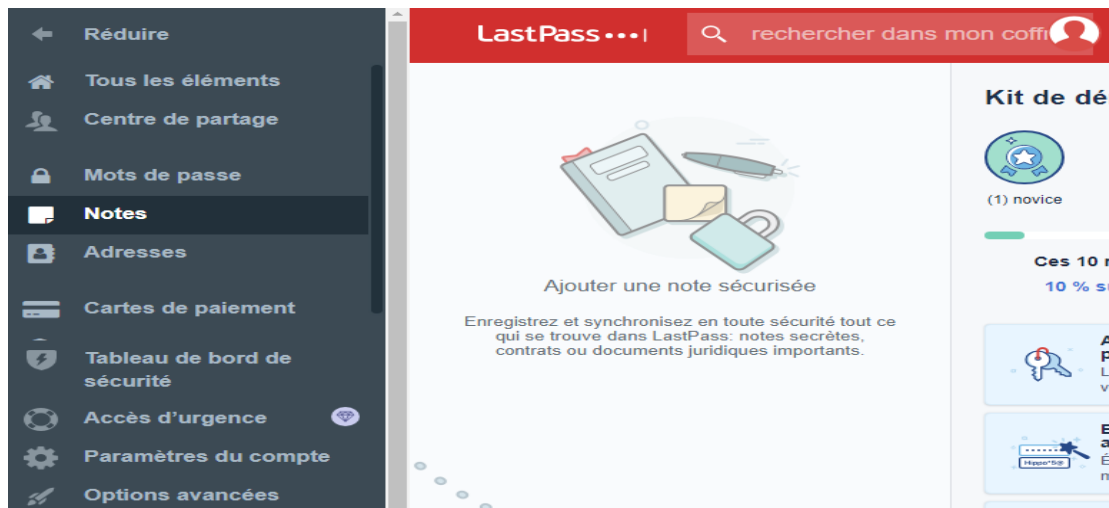


## LastPass: Free Password Manager

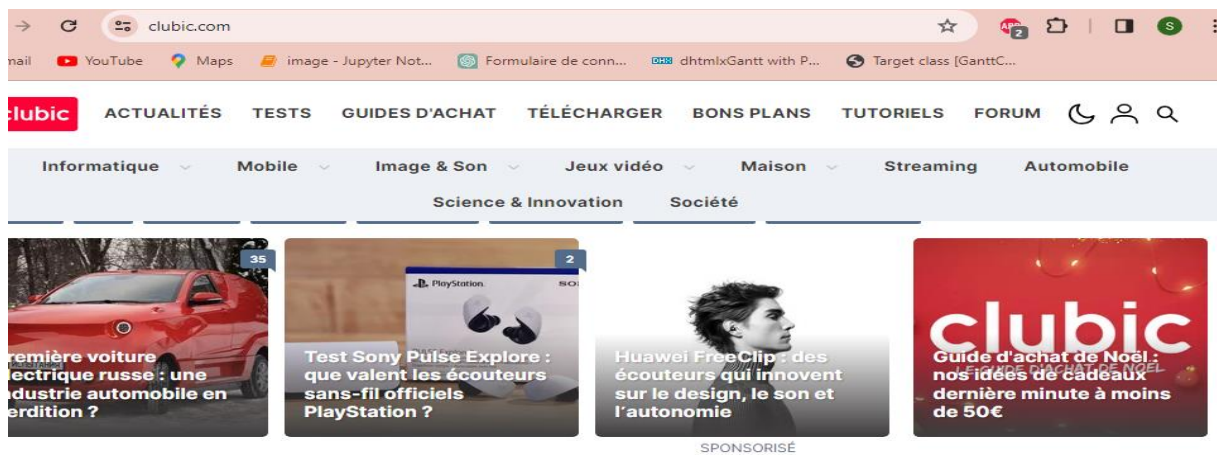
 Sélection 4,4 ★ (27,6 k avis)

Extension Workflows/planification 10 000 000 utilisateurs

**Ajouter à Google**



NB : Le lien concernant les comparatifs des gestionnaires de mot de passe a affiché la page ci-dessous



## Fonctionnalité de sécurité de votre navigateur

Les adresses internet provenant de site web malveillants sont :

[www.morvel.com](http://www.morvel.com)

[www.fessebook.com](http://www.fessebook.com)

[www.instagramm.com](http://www.instagramm.com)

## À propos de Chrome

 **Google Chrome**



Presque à jour ! Relancez Chrome pour terminer la mise à jour.  
Version 120.0.6099.111 (Build officiel) (64 bits)

[Relancer](#)

Obtenir de l'aide avec Chrome



Signaler un problème



Règles de confidentialité



## Mise à jour de chrome

### Général

#### Accueil

#### Recherche

#### Vie privée et sécurité

#### Synchronisation

#### Autres produits de Mozilla

### Mises à jour de Firefox

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

Version 121.0 (32 bits) [Notes de version](#)

 Firefox est à jour

[Afficher l'historique des mises à jour...](#)

[Rechercher des mises à jour](#)

## Mise à jour de firefox


## Eviter le spam et le pishing

3 / 8

### C'est exact ! Il s'agit d'un e-mail d'hameçonnage.

Vous avez correctement identifié l'URL trompeuse. Le véritable domaine est "sytez.net", que l'on a camouflé pour le faire passer pour un lien Google Drive. Soyez particulièrement vigilant si vous n'êtes pas sûr de connaître l'expéditeur.

[MONTREZ-MOI](#)

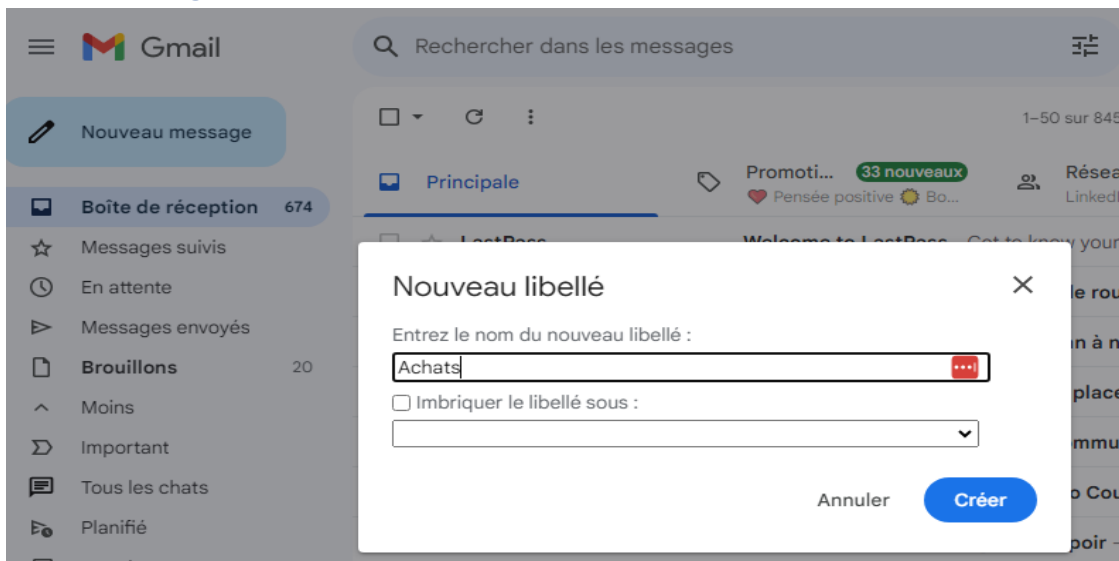
 **TK** <tk867530@gmail.com>  
à moi (🔒)

Salut, tu te souviens de [CETTE PHOTO](#) !

L'URL du lien redirige en réalité vers "sytez.net", et non vers Google Drive.

[Suivant](#)

## Achat en ligne sécurisés



## Comprendre le suivi du navigateur

## Principe de base de la confidentialité des médias sociaux

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

Voici quelques étapes générales que vous pouvez suivre pour vérifier et traiter une infection par un virus sur un ordinateur :

### Exercices de vérification sur un ordinateur (sous Windows)

#### 1. Analyse antivirus :

- Utilisez un logiciel antivirus à jour pour effectuer une analyse complète du système.
- Exercice : Assurez-vous que votre antivirus est activé et planifiez une analyse complète de votre ordinateur.

#### 2. Mises à jour système :

- Assurez-vous que votre système d'exploitation et vos logiciels sont à jour.
- Exercice : Vérifiez les mises à jour disponibles pour Windows et installez-les.

#### 3. Pare-feu :

- Vérifiez que votre pare-feu est activé pour bloquer les connexions non autorisées.
- Exercice : Confirmez que le pare-feu Windows est activé et configurez-le pour bloquer les connexions non désirées.

#### 4. Suppression des logiciels malveillants :

- Utilisez des outils anti-malware spécifiques pour détecter et supprimer les logiciels malveillants.
- Exercice : Téléchargez et exécutez un outil anti-malware comme Malwarebytes.

## 5. Changement de mots de passe :

- Changez tous les mots de passe sensibles après avoir nettoyé votre système.
- Exercice : Changez les mots de passe des comptes en ligne et locaux.

## 6. Sauvegarde des données :

- Sauvegardez vos données importantes sur un support externe.
- Exercice : Créez une sauvegarde de vos fichiers importants sur un disque dur externe.

## 7. Sensibilisation à la sécurité :

- Informez-vous sur les bonnes pratiques de sécurité en ligne pour éviter de nouvelles infections.
- Exercice : Lisez des articles sur la sécurité en ligne et appliquez les conseils.

## Exercice : Installer et utiliser un antivirus + antimalware

### 1. Téléchargement de l'antivirus :

- Utilisez un navigateur web pour accéder au site Web de l'antivirus de votre choix.  
Exemple : Avast, AVG, Bitdefender, etc.
- Exercice : Téléchargez et installez l'antivirus sur votre ordinateur.

### 2. Configuration de l'antivirus :

- Suivez les instructions d'installation et configurez les paramètres de l'antivirus.
- Exercice : Activez la protection en temps réel et planifiez une analyse complète régulière.

### 3. Installation de l'anti-malware :

- Téléchargez un logiciel anti-malware, par exemple, Malwarebytes, sur le site officiel.
- Exercice : Installez l'anti-malware et mettez-le à jour.

### 4. Analyse avec l'anti-malware :

- Lancez une analyse complète de votre système avec l'anti-malware.
- Exercice : Exécutez une analyse complète et notez les éventuels logiciels malveillants détectés.

### 5. Planification des analyses régulières :

- Configurez l'anti-malware pour effectuer des analyses régulières.
- Exercice : Planifiez une analyse hebdomadaire avec l'anti-malware.

