CRYPTER
SES COURRIELS
Gmail

1,4 milliards

d'utilisateurs par jour

Pourquoi devrais-je chiffrer mes courriels?

Je ne fais rien d'illégal!

- Vous devriez chiffrer votre courrier pour la même raison que vous ne le faites pas:
  - Comme écrire toute votre correspondance au verso d'une carte postale.
- Un courriel est effectivement beaucoup moins sécurisé que le système postal.
- Avec la poste, vous mettez au moins votre lettre dans une enveloppe pour la dissimuler des regards malveillants.

- Jetez un coup d’œil à la zone d’en-tête de tout message électronique, vous verrez qu'il a traversé un certain nombre de *nœuds* (réseaux)* sur son chemin vers vous.
- Chacun de ces *nœuds* (réseaux)* présente le possibilité de fouiner.
- Le cryptage ne doit en aucun cas impliquer une activité illégale.
- Il est simplement destiné à garder vos courriels personnels… personnel.

*Nœuds : « nodes » en anglais

La criminalité?

Si vous n'êtes pas un politicien, chercheur scientifique, investisseur, PDG,

Avocat, célébrité, libertaire dans une société répressive, investisseur

Ou une personne qui s'amuse trop et vous n'envoyez pas de courrier électronique à propos de votre vie sexuelle privée,

Plans financiers / politiques / juridiques / scientifiques, ou potins…

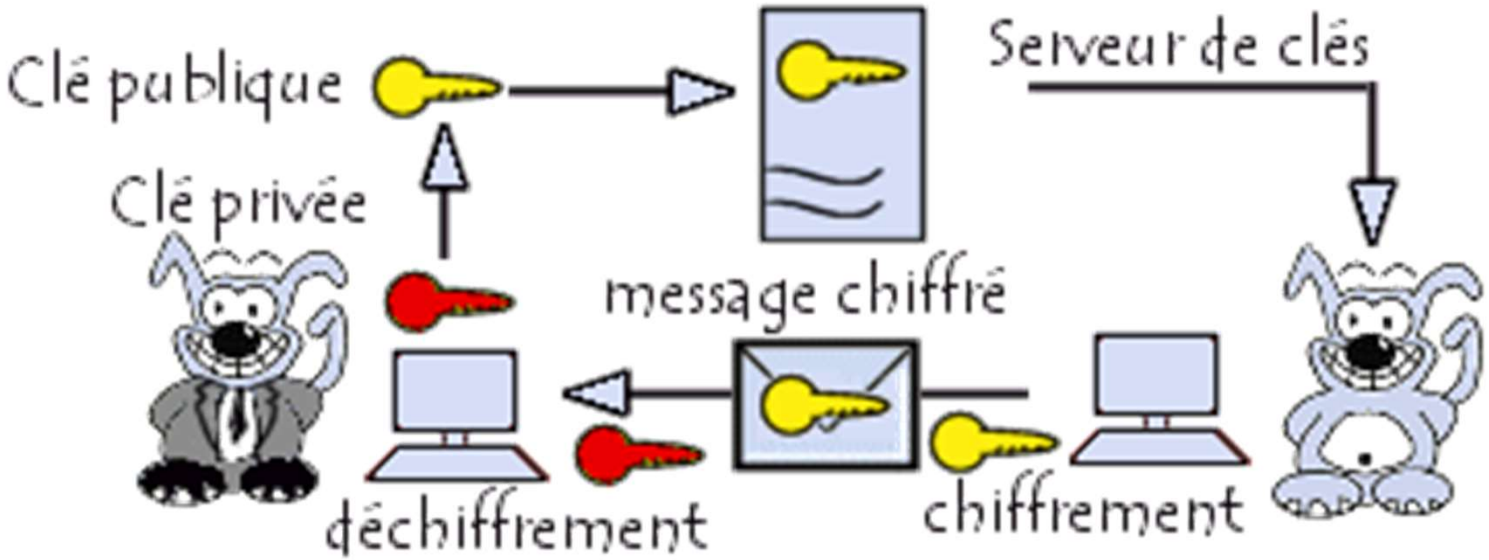
…mais au moins se rendre compte
que
la vie privée n'a rien à voir avec le
crime.

Le cryptage est-il légal?

- Dans une grande partie du monde civilisé, le chiffrement est soit légal, soit du moins toléré.
- Cependant, dans certains pays, de telles activités peuvent vous mettre en contact avec un peloton d'exécution.
- Vérifiez les lois en vigueur dans votre pays avant d'utiliser PGP ou tout autre produit de chiffrement .
- Parmi les pays où le cryptage est illégal, on trouve la…
- …France, l'Iran et l'Irak.

Pour ce faire, des clés de cryptage sont nécessaires

- Avec les schémas de cryptage conventionnels, les clés doivent être échangées avec toutes les personnes avec lesquelles vous souhaitez « *courielliser* » par une autre méthode sécurisée.
- Le problème est que vous avez besoin d'un canal sécurisé avant de pouvoir établir un canal sécurisé!
- Avec le cryptage conventionnel, la même clé est utilisée à la fois pour le cryptage et le décryptage ou il est facile de convertir l'une ou l'autre des clés.


Clé publique
Serveur de clés
Clé privée
message chiffré
déchiffrement
chiffrement

Chiffrement asymétrique

Système de chiffrement symétrique ou asymétrique

- Chiffrement symétrique quand il utilise la même clé pour chiffrer et déchiffrer.
- Chiffrement asymétrique quand il utilise des clés différentes:
  - une paire composée d'une clé publique, servant au chiffrement, et d'une clé privée, servant à déchiffrer.
- Le point fondamental soutenant cette décomposition publique/privée est l'impossibilité calculatoire de déduire la clé privée de la clé publique.

Le programme de cryptage « Pretty Good Privacy » (PGP)

- Écrit par Phillip Zimmermann, un scientifique américain, créateur du:
  - Pretty Good Privacy (PGP)
- Le logiciel de chiffrement de courrier électronique le plus utilisé au monde.

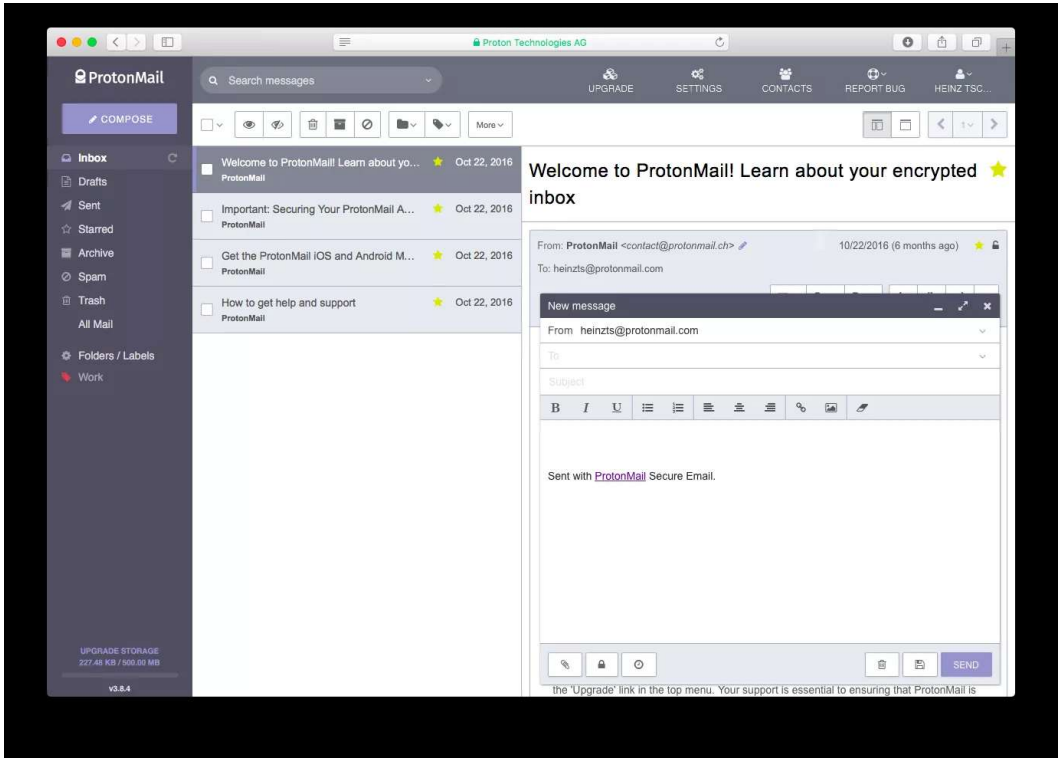
Applications gratuites connues de cryptage de courriels pour Gmail

- **Mailvelope**
  - Proposé par : www.mailvelope.com
  - Extension de Chrome: https://chrome.google.com/webstore/detail/mailvelope/kajibbejlbohfaggdiogboambcijhkke?hl=fr

Les 5 meilleurs services de messagerie sécurisés pour 2018

- Les services de messagerie cryptés préservent la confidentialité de vos messages.
- Un service de messagerie sécurisé est le moyen le plus simple de garder vos emails privés.
- Non seulement ils garantissent un courrier électronique sécurisé et crypté, mais ils protègent également l'anonymat.
- La plupart des comptes de messagerie gratuits conviennent parfaitement à l'utilisateur moyen.

ProtonMail


Proton Technologies AG
ProtonMail
Search messages
UPGRADE
SETTINGS
CONTACTS
REPORT BUG
HEINZ TSC...
COMPOSE
Inbox
Drafts
Sent
Starred
Archive
Spam
Trash
All Mail
Folders / Labels
Work
More
Welcome to ProtonMail! Learn about yo... Oct 22, 2016
ProtonMail
Important: Securing Your ProtonMail A... Oct 22, 2016
ProtonMail
Get the ProtonMail iOS and Android M... Oct 22, 2016
ProtonMail
How to get help and support Oct 22, 2016
ProtonMail
Welcome to ProtonMail! Learn about your encrypted inbox
From: ProtonMail <contact@protonmail.ch>
10/22/2016 (6 months ago)
To: heinzts@protonmail.com
New message
From heinzts@protonmail.com
To
Subject
Sent with ProtonMail Secure Email.
SEND
UPGRADE STORAGE
227.48 KB / 500.00 MB
v3.8.4
the 'Upgrade' link in the top menu. Your support is essential to ensuring that ProtonMail is

ProtonMail suite...

- **Ce qu'on aime:**
  - Authentification à deux facteurs
  - Envoyer des messages cryptés protégés par mot de passe à quiconque
  - Les importations de contacts CSV sont prises en charge

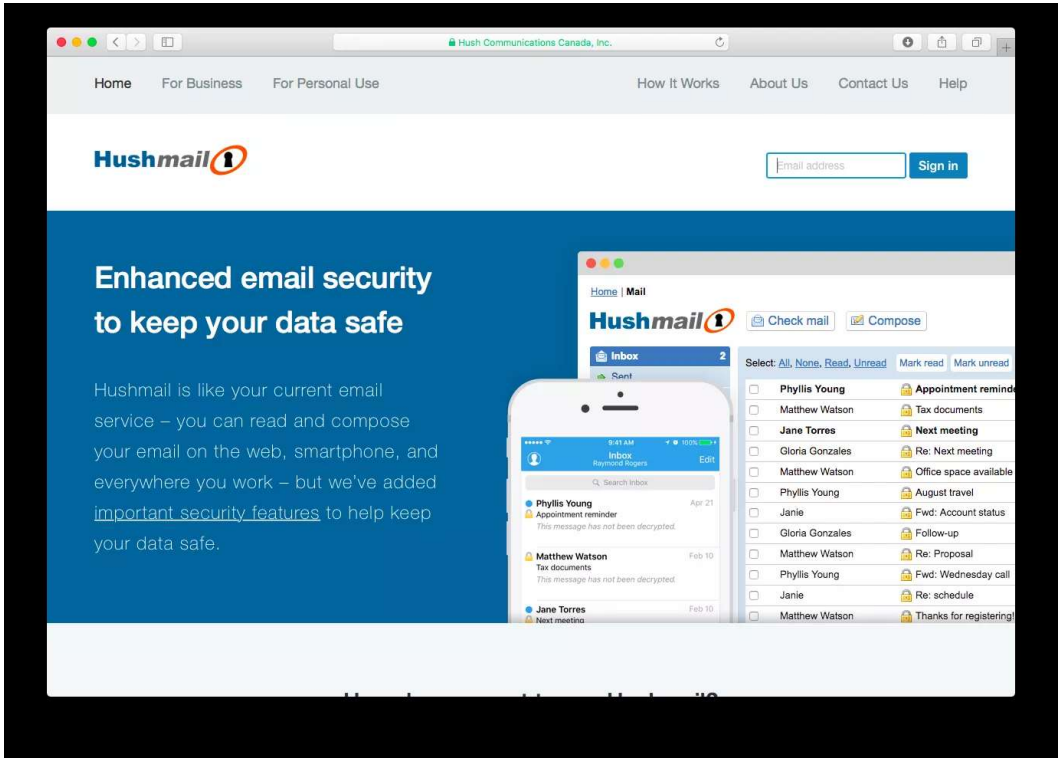
- **Ce que nous n'aimons pas:**
  - Impossible de changer la signature par défaut sur un compte gratuit
  - Ne prend pas en charge IMAP, SMTP ou POP3

CounterMail

CounterMail suite...

- **Ce qu'on aime**
  - Prend en charge IMAP
  - Ne conserve pas les journaux d'adresses IP
  - Inclut un gestionnaire de mot de passe intégré (appelé Safebox)
- **Ce que nous n'aimons pas**
  - Impossible d'envoyer des courriels cryptés à des non-utilisateurs
  - Espace de stockage limité
  - Essai gratuit d'une durée limitée (une semaine)

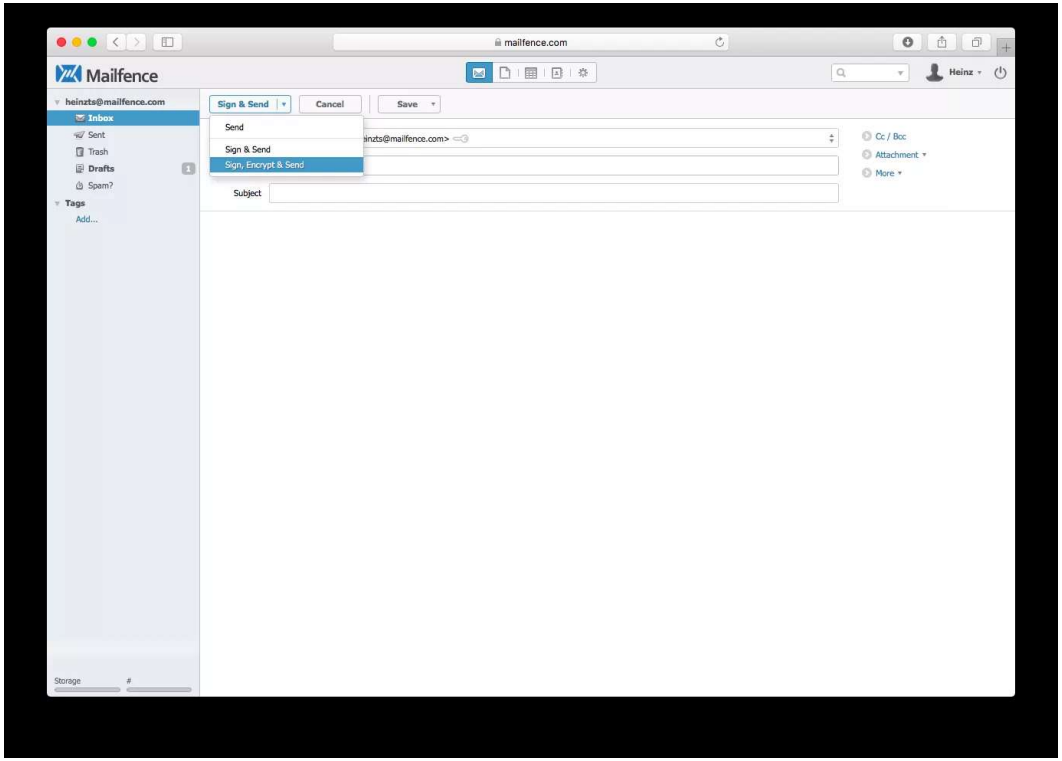
Hushmail


Hush Communications Canada, Inc.
Home
For Business
For Personal Use
How It Works
About Us
Contact Us
Help
Hushmail
Email address
Sign in
Enhanced email security to keep your data safe
Hushmail is like your current email service – you can read and compose your email on the web, smartphone, and everywhere you work – but we've added important security features to help keep your data safe.
Home | Mail
Hushmail
Check mail
Compose
Inbox 2
Sent
Select: All, None, Read, Unread
Mark read
Mark unread
Phyllis Young
Appointment reminder
Matthew Watson
Tax documents
Jane Torres
Next meeting
Gloria Gonzales
Re: Next meeting
Matthew Watson
Office space available
Phyllis Young
August travel
Janie
Fwd: Account status
Gloria Gonzales
Follow-up
Matthew Watson
Re: Proposal
Phyllis Young
Fwd: Wednesday call
Janie
Re: schedule
Matthew Watson
Thanks for registering!

Hushmail suite...

- **Ce qu'on aime**
  - Prend en charge IMAP et POP
  - Vérification facultative en deux étapes
  - Les contacts peuvent être importés à l'aide d'un fichier CSV
  - Comprend un filtre anti-spam et un répondeur automatique
  - Comprend 10 Go de stockage
- **Ce que nous n'aimons pas**
  - Compte gratuit comprend peu de stockage
  - Utiliser une adresse électronique et un numéro de téléphone différents lors de l'inscription et de la vérification

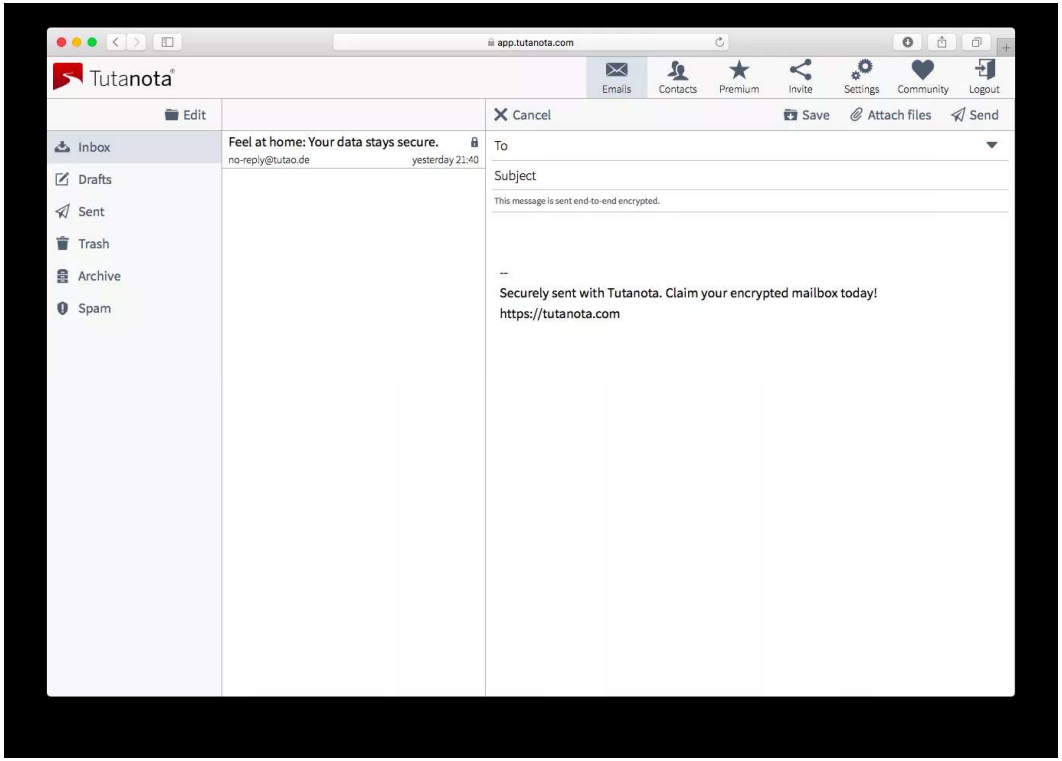
Mailfence


mailfence.com
Mailfence
Heinz
heinzts@mailfence.com
Inbox
Sent
Trash
Drafts
Spam?
Tags
Add...
Storage
Sign & Send
Cancel
Save
Send
Sign & Send
Sign, Encrypt & Send
Subject
Cc / Bcc
Attachment
More

Mailfence suite...

- **Ce qu'on aime**
  - Les signatures électroniques numériques prouvent la qualité d'auteur
  - Prend en charge l'authentification à deux facteurs
  - Comprend le bloqueur de spam
  - Les contacts peuvent être importés depuis Outlook, un fichier CSV, vCard, LDIF ou Gmail
  - Inclut le calendrier et le stockage de fichiers pour les documents
- **Ce que nous n'aimons pas**
  - Stockage en ligne limité
  - Nécessite une adresse électronique alternative pour recevoir la clé d'activation
  - Clés privées conservées sur les serveurs Mailfence
  - Les courriers électroniques cryptés ne peuvent être envoyés qu'aux utilisateurs de Mailfence ou OpenPGP
  - Le code de chiffrement du courrier électronique est disponible pour inspection

Tutanota


app.tutanota.com
Tutanota
Emails
Contacts
Premium
Invite
Settings
Community
Logout
Edit
Inbox
Drafts
Sent
Trash
Archive
Spam
Feel at home: Your data stays secure.
no-reply@tutao.de
yesterday 21:40
Cancel
Save
Attach files
Send
To
Subject
This message is sent end-to-end encrypted.
--
Securely sent with Tutanota. Claim your encrypted mailbox today!
https://tutanota.com

Tutanota suite...

- **Ce qu'on aime**
  - Applications pour iOS et Android
  - Comprend 1 Go d'espace de stockage
  - Open source
  - Prend en charge le filtrage anti-spam
- **Ce que nous n'aimons pas**
  - Prend en charge uniquement les e-mails en texte brut
  - Des fonctionnalités telles que les alias et les règles de messagerie disponibles uniquement pour les comptes payés
  - Ne supporte pas IMA
  - Impossible d'importer des contacts en vrac

Étapes supplémentaires pour garder le courrier électronique sécurisé et privé

- Si vous utilisez un service de messagerie sécurisé offrant un cryptage de bout en bout, vous avez franchi une étape importante pour rendre votre messagerie véritablement sécurisée et privée.

- Pour rendre la vie difficile même aux pirates les plus passionnés, vous pouvez prendre quelques précautions supplémentaires:

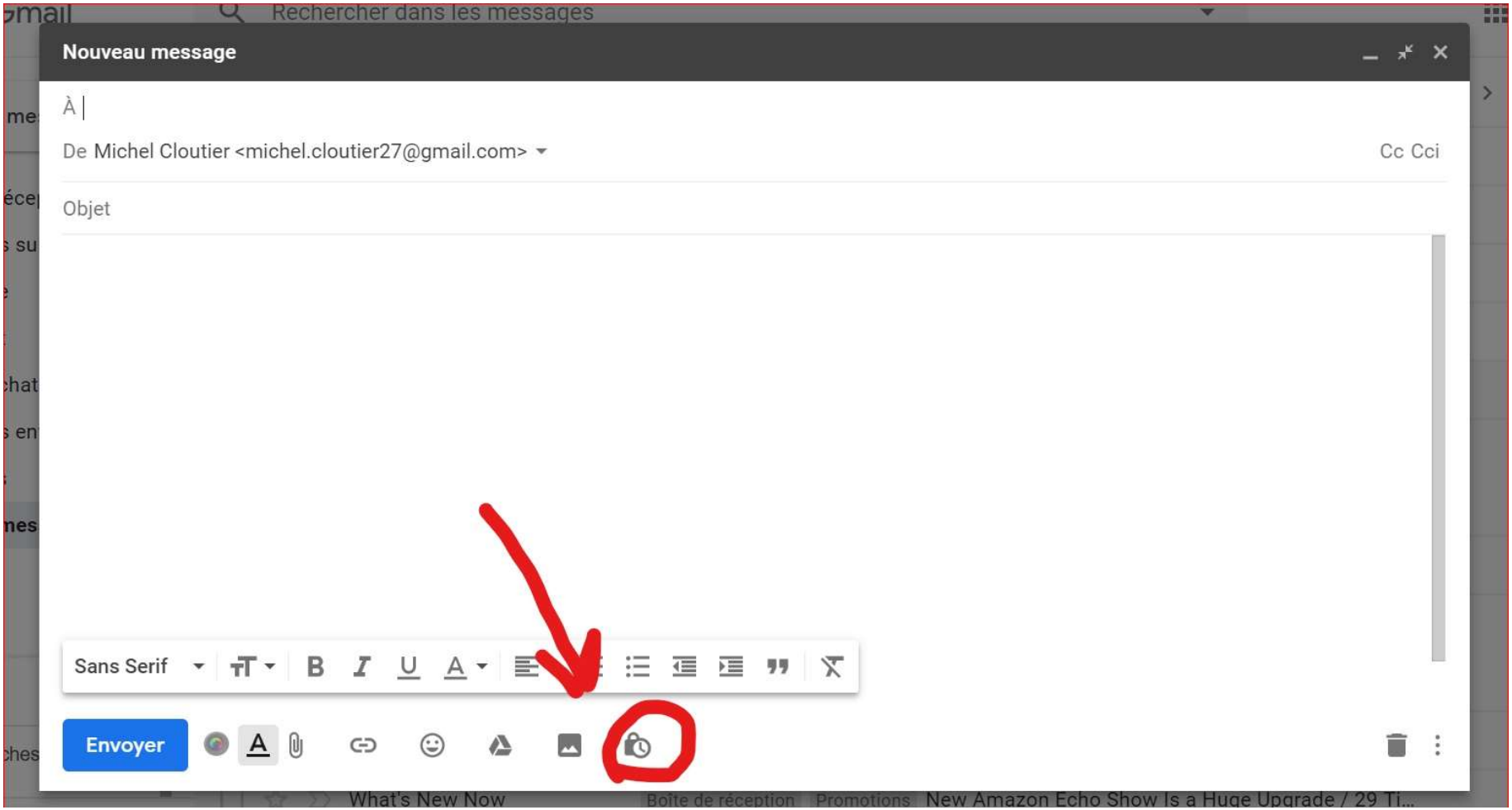
- Méfiez-vous des logiciels d'enregistrement au clavier qui saisissent ce que vous tapez directement à partir de votre clavier. Ceux-ci peuvent complètement déjouer le cryptage si le mot de passe est tout ce dont le pirate a besoin pour accéder à votre compte.
- Ne laissez pas vos appareils mobiles et vos ordinateurs sans surveillance. Assurez-vous également que vos *appareils sont protégés par des mots de passe forts ou des données biométriques* et ne permettent pas de comptes invités ni d'accès similaire non protégé.

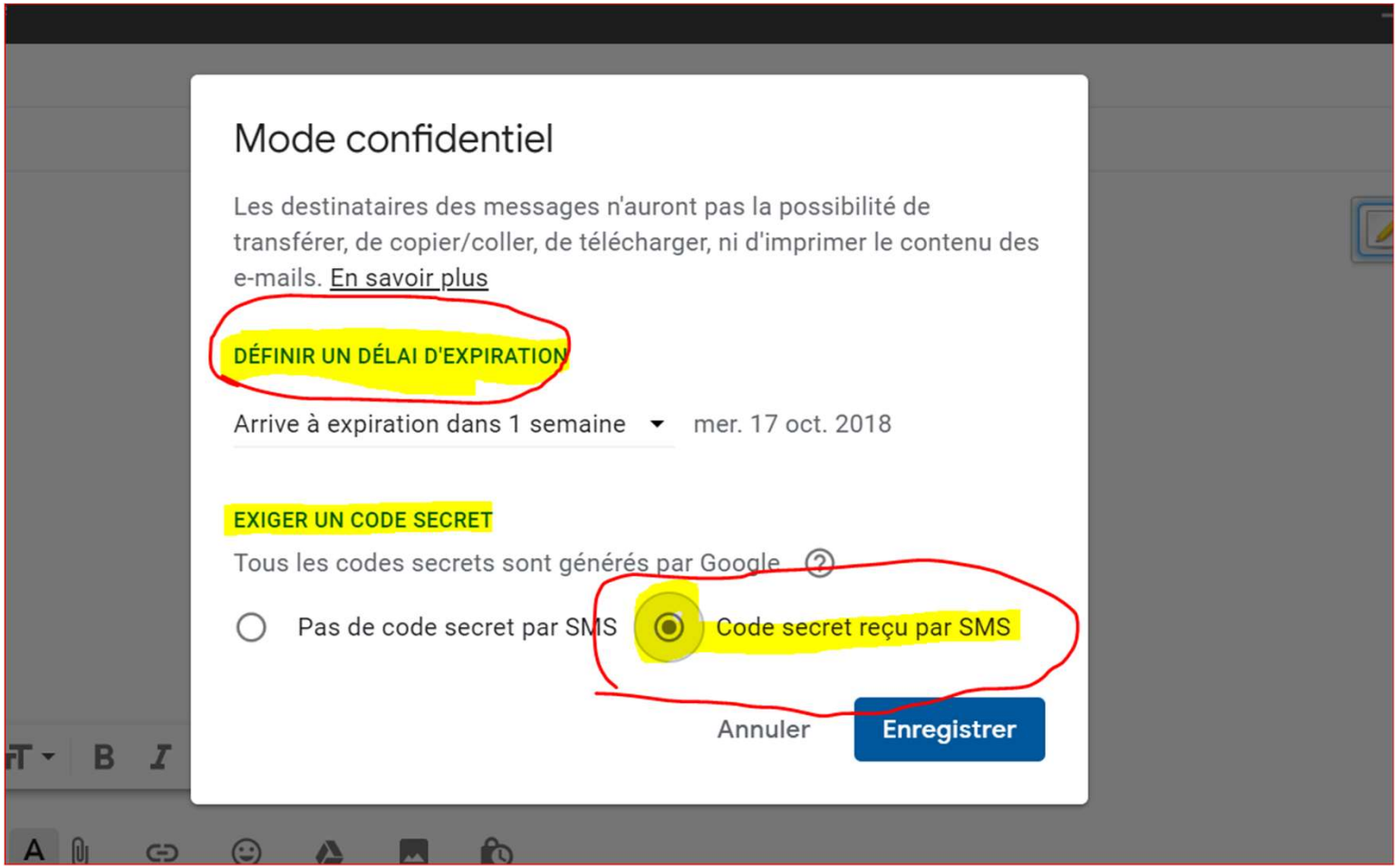
- Soyez vigilant de l'ingénierie sociale.
- Les tentatives de phishing se produisent souvent par courriel, messagerie instantanée, VoIP ou sur les réseaux sociaux.
- Elles peuvent être conçues avec soin ou adaptées à votre cas.
- Ce sont des astuces qui vous permettent de donner des informations personnelles telles que les mots de passe et les informations bancaires.
- N'écrivez ou ne partagez aucun mot de passe.
- Ne notez jamais le mot de passe qui vous permet de déchiffrer des courriels sécurisés.
- C'est à moins que vous le stockiez dans un gestionnaire de mot de passe sécurisé .

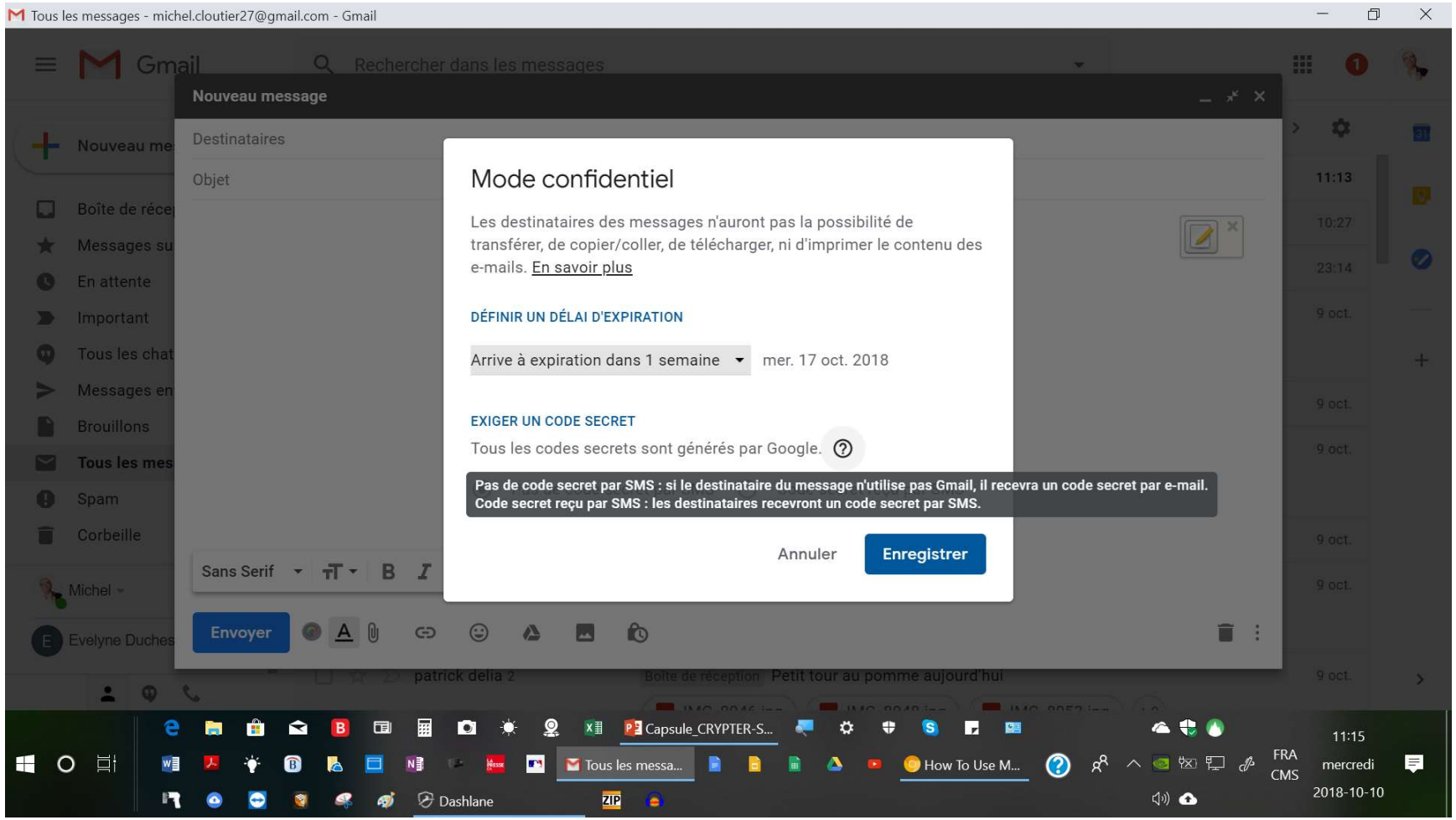
MODE CONFIDENTIEL GMAIL

Bon pour les « petits secrets »

Mauvais pour les « gros secrets »


Rechercher dans les messages
Nouveau message
À
De Michel Cloutier <michel.cloutier27@gmail.com>
Cc Cci
Objet
Sans Serif
Envoyer
What's New Now
Boîte de réception
Promotions
New Amazon Echo Show Is a Huge Upgrade / 29 Ti...


Mode confidentiel
Les destinataires des messages n'auront pas la possibilité de transférer, de copier/coller, de télécharger, ni d'imprimer le contenu des e-mails. En savoir plus
DÉFINIR UN DÉLAI D'EXPIRATION
Arrive à expiration dans 1 semaine
mer. 17 oct. 2018
EXIGER UN CODE SECRET
Tous les codes secrets sont générés par Google
Pas de code secret par SMS
Code secret reçu par SMS
Annuler
Enregistrer


Tous les messages - michel.cloutier27@gmail.com - Gmail
Gmail
Rechercher dans les messages
Nouveau message
Destinataires
Objet
Mode confidentiel
Les destinataires des messages n'auront pas la possibilité de transférer, de copier/coller, de télécharger, ni d'imprimer le contenu des e-mails. En savoir plus
DÉFINIR UN DÉLAI D'EXPIRATION
Arrive à expiration dans 1 semaine
mer. 17 oct. 2018
EXIGER UN CODE SECRET
Tous les codes secrets sont générés par Google.
Pas de code secret par SMS : si le destinataire du message n'utilise pas Gmail, il recevra un code secret par e-mail.
Code secret reçu par SMS : les destinataires recevront un code secret par SMS.
Annuler
Enregistrer
Sans Serif
Envoyer
Boîte de réception
Messages su
En attente
Important
Tous les chat
Messages en
Brouillons
Tous les mes
Spam
Corbeille
Michel
Evelyne Duches
patrick delia 2
Petit tour au pomme aujourd'hui
11:13
10:27
23:14
9 oct.
Capsule_CRYPTER-S...
Tous les messa...
How To Use M...
Dashlane
FRA
CMS
11:15
mercredi
2018-10-10

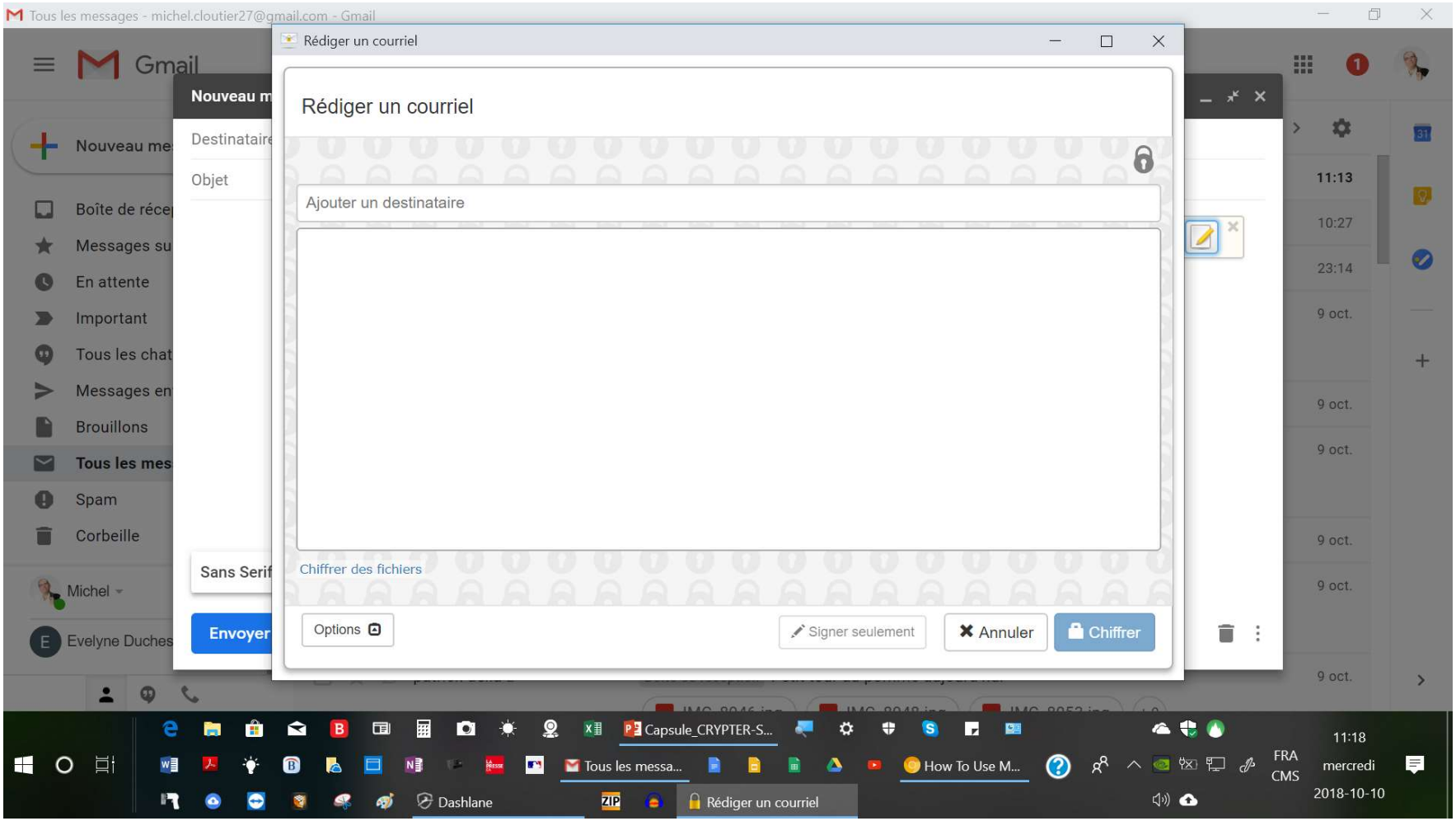
chrome web store

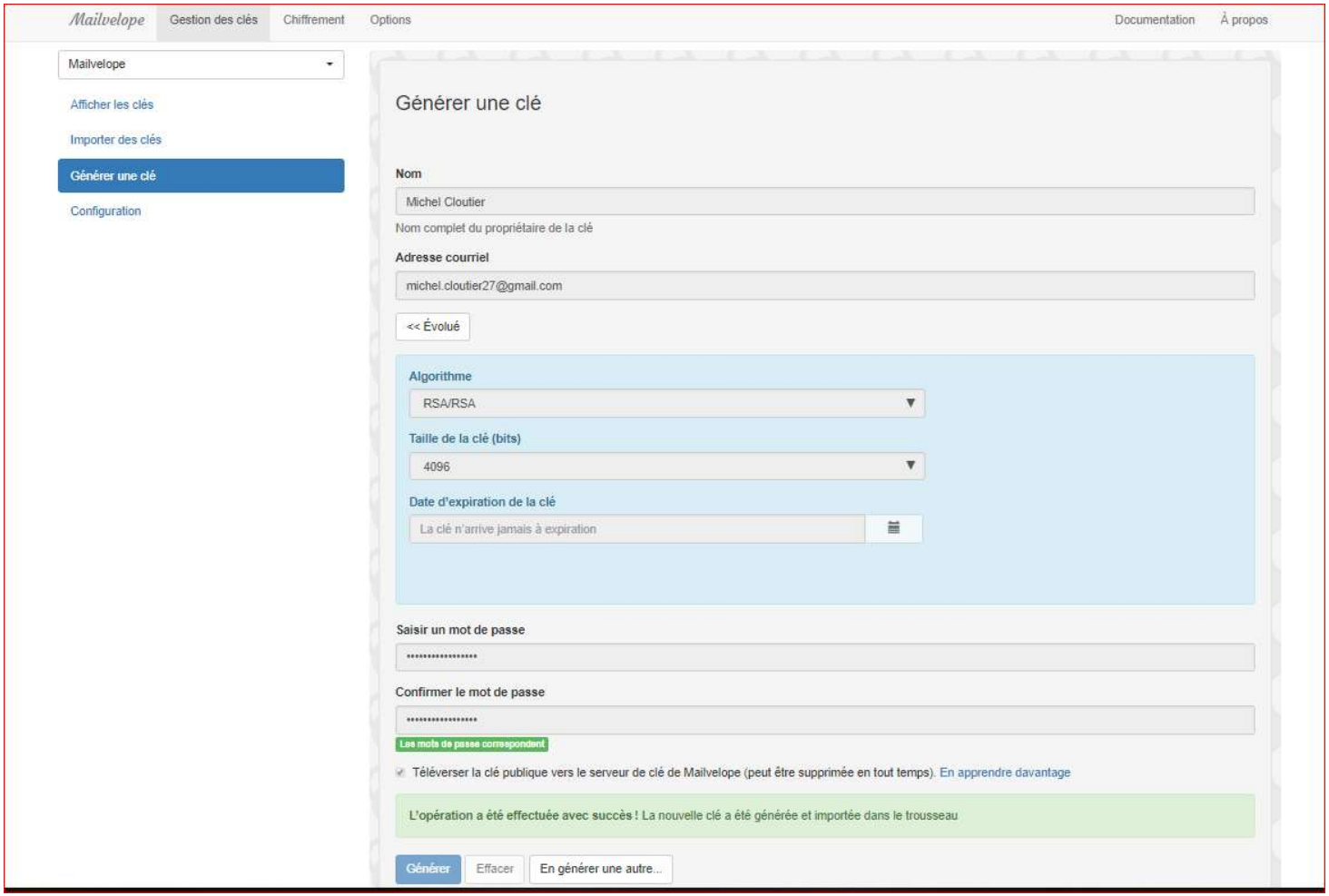
Mailvelope

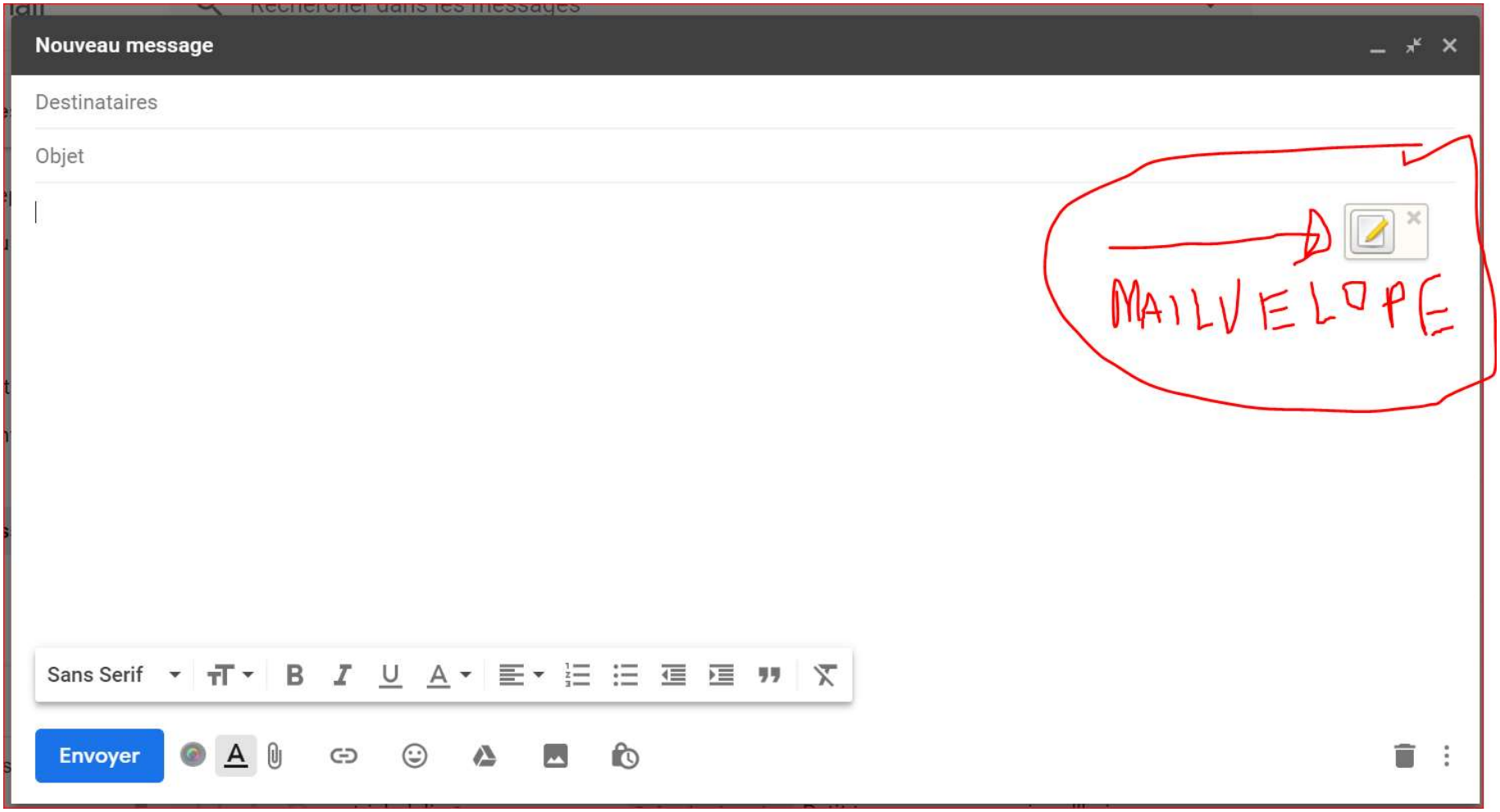
Proposé par : www.mailvelope.com

4.5 427 | Réseaux sociaux et communication | 206 562 utilisateurs

Présentation Avis Assistance Articles Similaires


Tous les messages - michel.cloutier27@gmail.com - Gmail
Rédiger un courriel
Rédiger un courriel
Ajouter un destinataire
Chiffrer des fichiers
Options
Signer seulement
Annuler
Chiffrer
Gmail
Nouveau message
Boîte de réception
Messages suivis
En attente
Important
Tous les chats
Messages envoyés
Brouillons
Tous les messages
Spam
Corbeille
Michel
Evelyne Duches
Destinataire
Objet
Sans Serif
Envoyer
11:13
10:27
23:14
9 oct.
9 oct.
9 oct.
9 oct.
9 oct.
9 oct.
Capsule_CRYPTER-S...
Tous les messa...
How To Use M...
Dashlane
Rédiger un courriel
FRA
CMS
11:18
mercredi
2018-10-10


Mailvelope
Gestion des clés
Chiffrement
Options
Documentation
À propos
Mailvelope
Afficher les clés
Importer des clés
Générer une clé
Configuration
Générer une clé
Nom
Michel Cloutier
Nom complet du propriétaire de la clé
Adresse courriel
michel.cloutier27@gmail.com
<< Évolué
Algorithme
RSA/RSA
Taille de la clé (bits)
4096
Date d'expiration de la clé
La clé n'arrive jamais à expiration
Saisir un mot de passe
Confirmer le mot de passe
Les mots de passe correspondent
Téléverser la clé publique vers le serveur de clé de Mailvelope (peut être supprimée en tout temps). En apprendre davantage
L'opération a été effectuée avec succès ! La nouvelle clé a été générée et importée dans le trousseau
Générer
Effacer
En générer une autre...


Nouveau message
Destinataires
Objet
MAILVELOPE
Sans Serif
Envoyer

TOUT CELA POUR VOUS DIRE…

SI VOUS VOULEZ VRAIMENT
PARTAGER UN SECRET « D'ÉTAT »
EH BIEN,
RENCONTRER VOTRE DESTINATAIRE
DANS UN GARAGE EN BÉTON
SANS ÉCLAIRAGE
SITUÉ TRÈS PROFONDÉMENT DANS LE SOL.

Références:

- http://www.faqs.org/faqs/pgp-faq/part1/
  - PGP Foire aux questions avec réponses
- https://fr.wikipedia.org/wiki/Chiffrement#Syst%C3%A8me_sym%C3%A9trique_ou_asym%C3%A9trique
- https://fr.wikipedia.org/wiki/Pretty_Good_Privacy
- https://technologie.toutcomment.com/article/comment-crypter-un-email-sur-gmail-9452.html
- https://www.lifewire.com/best-secure-email-services-4136763

Références YouTube

- https://www.youtube.com/watch?v=aPU_Os3mNtk
  - now How ... 50: Cryptez votre courrier électronique avec PGP
- https://www.youtube.com/watch?v=Ro3MSBS9w-A
- https://www.youtube.com/watch?v=QiI3RiETHmU
- https://www.youtube.com/watch?v=xKDk3l6nRc4
  - Tutoriels sur Mailvelope
- https://www.youtube.com/watch?v=xKDk3l6nRc4&t=20s