Comment envoyer un courriel anonyme Cybernews

NDLR: prix annoncés dans le texte sont en devise USD

Paulius Masiliauskas Responsable du contenu ⋮

Nous utilisons le courrier électronique pour beaucoup de choses qui nécessitent l'anonymat.
Qu'il s'agisse de lettres d'amour ou de confirmations de compte, nos boîtes aux lettres abritent des choses épicées !

Il n'y a qu'un seul problème : les courriel**s fournissent une communication bidirectionnelle identifiable** de par leur conception.
Outre l'adresse de l'expéditeur, le couriel contient beaucoup plus de choses qui pourraient vous identifier.
Par exemple, si vous regardez l'en-tête complet d'un courriel, vous pouvez trouver des informations de routage.
Cela pourrait suffire à vous identifier et à causer divers problèmes.

Pourtant, tout n'est pas perdu !
Dans cet article, **je vais vous montrer la bonne façon d'envoyer un courriel anonyme**.

Comment envoyer un courriel anonyme sans être suivi

1. Choisissez un **fournisseur de messagerie sécurisé**. **ProtonMail** est l'une des meilleures options
2. Inscrivez-vous au service pour obtenir **votre boîte aux lettres**
3. Connectez-vous à votre compte
4. Profitez de vos nouvelles communications par e-mail **plus sûres** !

L'envoi d'e-mails privés signifie **cacher votre véritable adresse IP** et **utiliser un fournisseur de services de messagerie sécurisé**.
Les plates-formes de messagerie les plus populaires comme Google ou Yahoo sont excellentes dans leur simplicité et leur stockage, mais manquent de confidentialité.

Si vous prévoyez d'entamer une conversation privée par courriel, vous pouvez faire certaines choses.
Gardez à l'esprit que la plupart du temps, il n'y a pas de solution unique.
Vous obtiendrez la meilleure combinaison de confidentialité et de sécurité si vous essayez de combiner plusieurs méthodes.
Non seulement cela vous aidera à rester en sécurité lorsque vous rédigez des courriels privés, mais aussi lorsque vous recherchez des points faibles dans votre navigation quotidienne.

1. Utilisez un service de messagerie crypté et anonyme

Le courrier électronique chiffré fonctionnera comme un service ordinaire, avec l'avantage que le chiffrement de bout en bout le rend beaucoup plus sûr.
Ce cryptage couvre vos **courriels, votre boîte de réception et votre liste de contacts**. Personne n'espionnant votre trafic ne pourra lire vos courriels, y compris même le fournisseur de services (dans certains cas).
Différents fournisseurs offrent des fonctionnalités différentes, mais ProtonMail, Tutanota, StartMail et Guerilla Mail sont garantis d'être plus privés que Gmail ou Yahoo.

Les comptes de messagerie les plus anonymes :

1. ProtonMail – le meilleur fournisseur de messagerie sécurisée
2. **StartMail** – le meilleur fournisseur de messagerie facile à utiliser
3. **Tutanota** – le fournisseur de messagerie le plus anonyme

4. Guerilla Mail – le meilleur e-mail temporaire contre le spam

2. Utilisez un courriel « brûleur »

De la même manière que les téléphones prépayés bon marché sont utilisés dans des émissions comme *The Wire* et *Breaking Bad*, les courriels brûleurs sont temporairement utilisés, puis éliminés.
Ils **expirent après une période déterminée** ou vous **permettront d'envoyer un message sans enregistrer** de compte qui pourrait être retracé jusqu'à vous.
Vous pouvez utiliser leur compte temporaire « envoyer uniquement » sur AnonymouseMail.

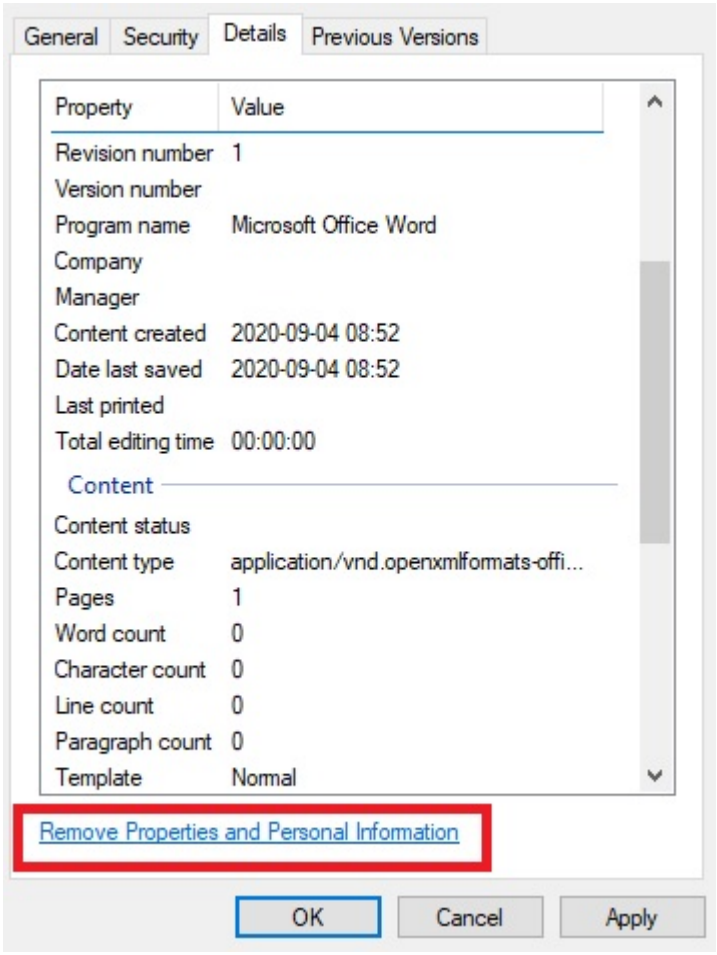
Les e-mails brûleurs peuvent vous aider à lutter contre le spam lorsque vous vous inscrivez sur des sites Web louches.
Le seul inconvénient est qu'il peut être très délicat de réinitialiser votre compte enregistré sur un courriel brûleur dans les cas où vous oubliez votre mot de passe.
Le meilleur plan d'action serait d'utiliser des courriels brûleurs lorsque vous savez qu'il y a peu de chances que vous ayez besoin de les utiliser à l'avenir.

3. Cachez votre adresse IP

Quelle que soit la méthode que vous choisissez pour envoyer un courriel anonyme, votre adresse IP peut toujours être un handicap.
Pour masquer votre adresse IP, vous devez utiliser un VPN ou un **navigateur Tor** sans journaux.
Un VPN cryptera votre connexion et l'acheminera via un serveur intermédiaire, masquant ainsi votre adresse IP réelle.
Tor fera passer votre connexion à travers plusieurs nœuds de réseau, ce qui vous rendra intraçable.
Il existe même des VPN qui utilisent ces technologies en conjonction, comme Onion over VPN de NordVPN.

4. Supprimez les métadonnées des fichiers

Si vous envoyez un document Word, les métadonnées contenues dans les fichiers pourraient vous révéler.
Il peut contenir votre nom complet et d'autres informations personnelles que vous ne souhaitez pas partager.
S'il s'agit simplement de documents que vous souhaitez envoyer sans être tracé, vous devez prendre une capture d'écran et **en supprimer toutes les données EXIF**.



Sous Windows, il existe également un outil intégré de suppression des métadonnées appelé Inspecteur de document.
Cela vous aidera à analyser ce que vous incluez, ce qui vous donnera la possibilité de supprimer toutes les informations d'un fichier que vous ne souhaitez pas partager.

5. Créez un nouveau compte de messagerie

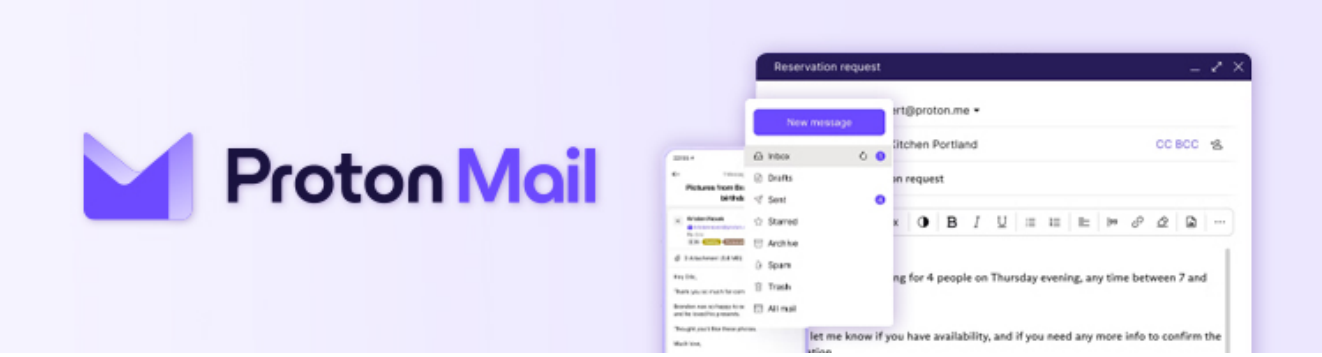
Le moyen le plus simple d'envoyer des courriels de manière anonyme est de créer un nouveau compte de messagerie.
Si vous devez utiliser les services Gmail ou Yahoo, vous pouvez créer un courriel en utilisant de **fausses informations**.
Choisissez un faux nom, une fausse adresse, une fausse date de naissance et ne fournissez pas de numéro de téléphone.
Gardez à l'esprit, cependant, que même avec ces précautions, ces services suivront toujours vos cybermouvements.
Ils sont également tenus de fournir ces informations aux organismes d'application de la loi.

Les fournisseurs de messagerie les plus anonymes

Si vous souhaitez envoyer des e-mails de manière anonyme, il s'agit toujours de choisir un fournisseur de messagerie sécurisé.

Ils peuvent toujours tenir un journal avec votre nom, votre adresse IP ou votre emplacement, vous devez donc en choisir un qui respectera votre anonymat et ne collectera pas vos données.

1. ProtonMail - le meilleur fournisseur de messagerie sécurisée



Version gratuite : Oui, 500 Mo de stockage
Plates-formes: iOS, Android
Stockage: 5 à 20 Go
Offre actuelle : **Obtenez jusqu'à 33 % de réduction sur Proton Mail !**

Rendez-vous sur ProtonMail

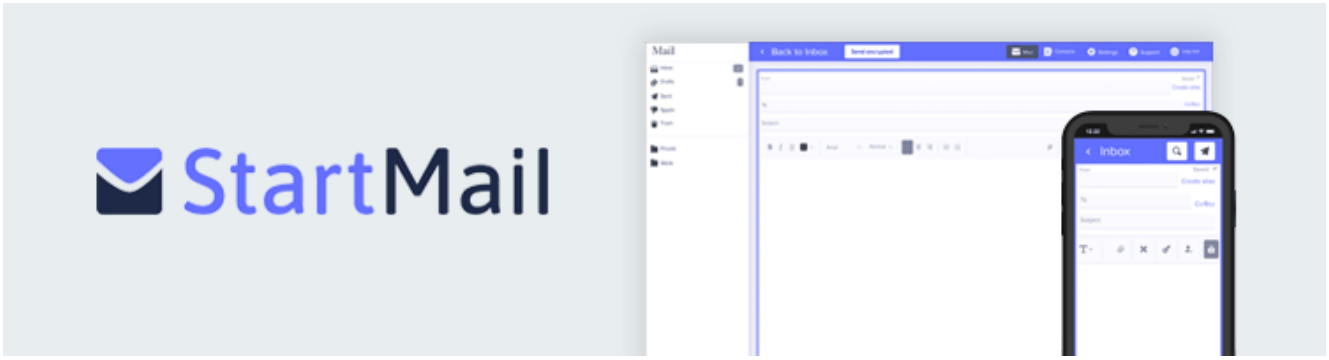
ProtonMail utilise le chiffrement PGP pour vos courriels avant qu'ils ne quittent votre appareil.
Il garantit une politique de non-enregistrement, de sorte que même si les forces de l'ordre venaient frapper à la porte du fournisseur, elles n'auraient rien à leur montrer.

Gardez à l'esprit qu'une fois le courriel envoyé, il ne chiffrera pas les métadonnées, les en-têtes ou les lignes d'objet.
Il existe un plan gratuit et payant (à partir de 3,49 $ par mois) qui augmente le nombre maximum de messages que vous pouvez envoyer par jour.
Le seul inconvénient est qu'ils vous demanderont probablement de fournir un numéro de téléphone pour confirmer votre compte.

ProtonMail offre également la fonctionnalité d'autodestruction des messages.
Tout ce que vous avez à faire est de définir votre heure d'expiration préférée et, le moment venu, ProtonMail supprimera les messages de la boîte de réception du destinataire.

En dehors de cela, ce service de messagerie vous offre un VPN gratuit, des applications pour iOS et Android, et un calendrier crypté.

2. StartMail - le meilleur fournisseur de messagerie facile à utiliser



Version gratuite : Non
Plates-formes: Web uniquement
Stockage: 10 Go
Offre actuelle : **Obtenez Startmail, maintenant 50% de réduction!**

Visitez StartMail

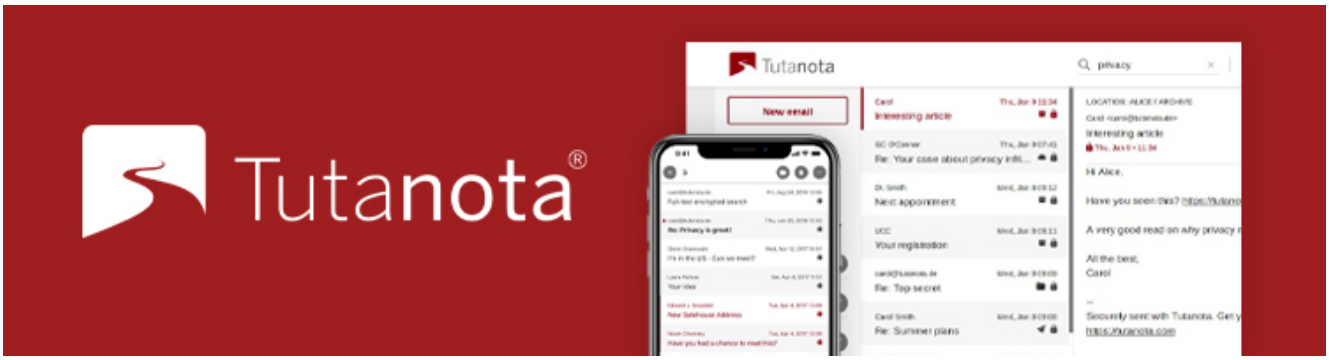
StartMail est ce que Gmail pourrait être si son entreprise se concentrait davantage sur la confidentialité plutôt que sur la façon de placer des annonces.
Leur **société mère gère même Startpage**, qui est l'un des rares moteurs de recherche respectueux de la vie privée.

En suivant cet exemple, StartMail est l'une des boîtes de courriel les plus privées que vous puissiez obtenir.
Il **prend en charge les courriels brûleurs**, ce qui vous permet d'ajouter des barrières à votre boîte aux lettres.
Même si un tel courriel apparaît dans une liste de diffusion de spam, vous pouvez rapidement vous en débarrasser et en créer un autre.

Comme la plupart des services de messagerie axés sur la confidentialité, StartMail **crypte les messages localement et les** envoie via HTTPS.
Il existe également un support PGP, mais votre contact devra également utiliser une configuration correspondante.
Sinon, cela ne fonctionnera pas.

En termes de prix, les plans de StartMail commencent à 2,50 $/mois.
Vous pouvez également utiliser un **essai gratuit de 7 jours** pour essayer d'abord toutes les fonctionnalités premium.

3. Tutanota - le fournisseur de messagerie le plus anonyme



Version gratuite : Oui, 1 Go

Plates-formes: Windows, macOS, iOS, Android

Stockage: 1 à 10 Go

Offre actuelle : Obtenez jusqu'à 20% de réduction sur Tutanota!

Visiter Tutanota

Tutanota peut vous fournir un cryptage de bout en bout.
Si vous en avez besoin, vous pourrez envoyer des messages cryptés même à des utilisateurs non-Tutanota.
Le chiffrement inclut non seulement la boîte de réception, mais aussi vos contacts.
Vous n'aurez pas besoin de fournir d'informations identifiables lors de l'enregistrement d'un compte.
De plus, il supprimera votre adresse IP de vos courriels.
Leur code est open source afin que tout le monde puisse l'examiner.

Ce service de messagerie sécurisé est l'une des meilleures options pour ceux qui ne veulent pas dépenser une fortune - ou dépenser de l'argent du tout.
C'est parce qu'il propose une version gratuite qui comprend 1 Go de stockage. Cependant, ce plan ne prend en charge qu'un seul utilisateur et a d'autres limites - par exemple, il ne stocke vos courriels que pendant quatre semaines.
Pour des fonctionnalités supplémentaires, comme la configuration de calendriers cryptés et d'un historique illimité de courriels, vous pouvez payer aussi peu que 1,20 $ par mois.

4. Guerilla Mail - le meilleur courriel temporaire contre le spam

Version gratuite : Oui

Plates-formes: Web

Stockage: N/A

Visitez Guerilla Mail

Guerilla Mail est un fournisseur de messagerie anonyme populaire depuis 2006.
Il diffère des autres fournisseurs de messagerie sécurisée de cette liste, car il fournit une adresse courriel temporelle pour envoyer et recevoir des courriels de manière anonyme. Vous pouvez soit créer l'adresse courriel vous-même, soit laisser Guerilla Mail le faire pour vous si vous êtes pressé.
Vous n'avez même pas besoin d'avoir un compte pour envoyer des messages, ce qui rend les choses encore plus confortables.

Vous pouvez utiliser Guerilla Mail lorsque vous souhaitez vous inscrire sur un site mais que vous n'êtes pas à l'aise avec l'utilisation de votre véritable adresse courriel.
En d'autres termes, vous pouvez utiliser ce fournisseur de messagerie comme une benne à ordures pour les spams indésirables, ou lorsque vous ne faites pas confiance à l'expéditeur.

La meilleure chose à propos de Guerilla Mail est le fait qu'il est absolument gratuit - il vous suffit d'aller sur leur site et d'utiliser le service.
Jusqu'à présent, Guerilla a traité plus de 13 milliards de courriels - et ce nombre ne cesse d'augmenter.

Importance de la sécurité et de l'anonymat des courriels

En utilisant un fournisseur de messagerie standard, dans la plupart des cas, vous obtiendrez un service décent, mais votre vie privée peut être en danger.
Ces services génèrent des revenus grâce aux publicités, et ils ont besoin de connaître vos habitudes de navigation pour adapter ces publicités à vos besoins.
De plus, les métadonnées des courriels exposeront votre adresse IP privée à toute personne désireuse de consulter les lignes **X-Originating-IP** ou **Original-IP**.
Cela permettra aux pirates (ou au destinataire) de trouver votre ville, votre état, votre code postal, votre fournisseur d'accès à Internet, etc.

Capture d'écran, pour visionner la vidéo, cliquer le lien YouTube suivant:

ProtonMail, Tutanota and others - How to Send an Anonymous Email tutorial - YouTube

FAQ

Gmail révèle-t-il votre adresse IP ?

Si vous utilisez Gmail en tant que service de messagerie Web, votre adresse IP externe et votre nom d'hôte ne seront pas divulgués.
Cependant, si vous utilisez Thunderbird ou le client Outlook pour envoyer des courriels Gmail à l'aide de SMTP, votre adresse IP et votre nom d'hôte seront envoyés avec votre courriel.
Gardez à l'esprit que lors d'une enquête policière, Gmail serait obligé de révéler votre adresse IP et votre emplacement.

Comment masquer votre adresse courriel lors de l'envoi d'un courriel

Il est **impossible de masquer les adresses « De » lors de** l'envoi de courriels. Cependant, vous pouvez **utiliser une fausse adresse pour faire croire à** quelqu'un qu'il s'agit de quelqu'un d'autre.
Vous devrez toujours utiliser un vrai nom de domaine, car les noms de domaine inexistants seront pris dans les filtres anti-spam.

Pouvez-vous envoyer un e-mail anonyme dans Outlook?

De par sa conception, Outlook utilise toujours un compte de messagerie associé à l'expéditeur.
Cela signifie qu'il est **impossible d'indiquer d'autres « De »** que votre compte de messagerie utilisé.
S'ils ne correspondent pas, Outlook renverra une erreur et il sera impossible d'envoyer un courriel.

Gmail est-il anonyme ?

Gmail **n'est pas anonyme** car Google a tendance à collecter vos données et à vous proposer des annonces.
Cependant, il est possible de conserver un certain degré de confidentialité avec le compte Gmail en utilisant un faux nom, un faux emplacement, une fausse date de naissance lors de l'inscription et en utilisant toujours un VPN avec celui-ci.

Puis-je masquer mon adresse IP lors de l'envoi d'un courriel ?

Vous pouvez utiliser un VPN ou un TOR pour masquer votre adresse IP d'origine lors de l'envoi d'un courriel afin qu'il affiche l'adresse IP du serveur proxy au lieu de votre adresse IP personnelle réelle.
Cela ne révélera pas votre adresse IP au public lors de l'envoi de courriels.

Qu'est-ce qu'un compte de messagerie graveur ?

Un compte de messagerie brûleur est un **compte de messagerie séparé sans contacts importants** dont son utilisateur peut se débarrasser rapidement après plusieurs utilisations.
Il a l'avantage de ne pas être lié aux noms des utilisateurs réels ou à ses autres comptes.

Outlook est-il plus sécurisé que Gmail ?

Les paramètres de sécurité de Microsoft sont une énigme.
Pendant ce temps, **la politique de confidentialité de Google est beaucoup plus transparente**.
En outre, Google propose la connexion via le matériel 2FA, qui est une méthode d'authentification très sécurisée.
De plus, il existe d'excellents avantages avec Gmail, comme le fait de placer le spam dans un dossier de courrier indésirable séparé plutôt que d'ajouter une icône rouge ou jaune en haut des courriels suspects.
Cela signifie que Gmail est préférable à Outlook en matière de sécurité.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231016
"C'est ensemble qu'on avance"