

Mon courrier sécurisé ? – C'est dans la boîte !

Ne plus dépendre de Gmail, Yahoo ou Outlook.com, ne plus avoir toutes ses conversations stockées et centralisées sur les serveurs des géants du web étasunien... C'est un peu le Graal des Dupuis-Morizeau.

Mais comment faire, lorsqu'on a peu de connaissances en informatique, pour avoir une boîte email vraiment indépendante et pouvoir chiffrer ses échanges ?

Les barbu-e-s du logiciel libre le savent, la solution la plus sensée réside dans l'auto-hébergement, et c'est souvent complexe à mettre en place.

Mais des solutions innovantes, à base de logiciel et de matériel libre, naissent pour aider notre famille témoin à reprendre le contrôle de leurs emails sans se fouler le clavier.

Aujourd'hui, nous interrogeons Pierre Parent, co fondateur de [Own-Mailbox](#) : un petit boîtier qui pourrait bien être une solution simple, respectueuse et efficace pour tous les Dupuis-Morizeau qui nous entourent.



Découvrez la Own-Mailbox en cliquant sur l'image

Salut, tu peux expliquer d'où vient le projet, tout ça ? Les membres sont, cocorico, français ?

Salut,

Donc tout d'abord, je me présente : Pierre Parent, cofondateur de [Own-Mailbox](#).

Le projet a pour origine tout d'abord mon engagement et mon attachement au logiciel libre et à la vie privée sur Internet. J'ai découvert les logiciels libres en 2007 grâce à un professeur de l'Insa de Rouen où j'ai fait mes études.

Le projet a aussi pour origine ma volonté de me libérer du travail subordonné et donc salarié. J'ai cette pulsion de liberté qui me pousse à rêver de pouvoir travailler librement sur des choses que je juge moi-même bonnes pour le monde et pour les autres ; ou à défaut, a minima obéir à des décisions collectives et démocratiques auxquelles j'aurai moi-même pris

part.

Dès lors, de nombreuses idées de produit pouvant permettre le lancement d'une création d'entreprise me sont venues. Own-Mailbox a été la plus consistante. J'ai donc continué dans cette cette voie pour améliorer l'idée et aller plus loin.

Romain Kornig, un ami de l'Insa de Rouen, a tout de suite été très enthousiaste quand je lui ai parlé de l'idée de Own-Mailbox,

Un peu plus tard quand le projet a commencé à prendre forme et que j'ai senti que cela pouvait déboucher sur quelque chose de sérieux, je me suis rendu compte que je ne pouvais faire ce projet tout seul. J'ai proposé à Romain de me rejoindre, et il a tout de suite dit oui !

Nous avons fondé tous les deux la boîte (sans jeux de mots !) à Rennes.

Own-Mailbox, c'est un boîtier qu'on met entre Internet et sa machine ?

Non. Own-Mailbox, c'est un tout petit serveur mail que l'on branche chez soi, qui se configure automatiquement, et qui devient alors accessible depuis partout dans le monde. On peut alors y accéder via un webmail (HTTPS) ou en IMAPS, depuis chez soi, mais aussi depuis partout dans le monde. Le serveur permet de chiffrer les emails de manière très simple, afin d'éviter d'être espionné.

Own-Mailbox remplace un peu les serveurs de Gmail, mais en tout petit, chez soi, et hors de portée de la NSA.

Et comment ça se branche, ce boîtier, il faut une prise spéciale ? Et une fois le truc branché, mon ordinateur va le reconnaître tout de suite ou bien il y a un logiciel à installer, des paramètres à régler, une authentification à opérer, etc. ?

C'est très simple. On branche un câble Ethernet entre la Own-Mailbox et sa box internet, et on la relie au secteur via le transformateur fourni. Voilà.

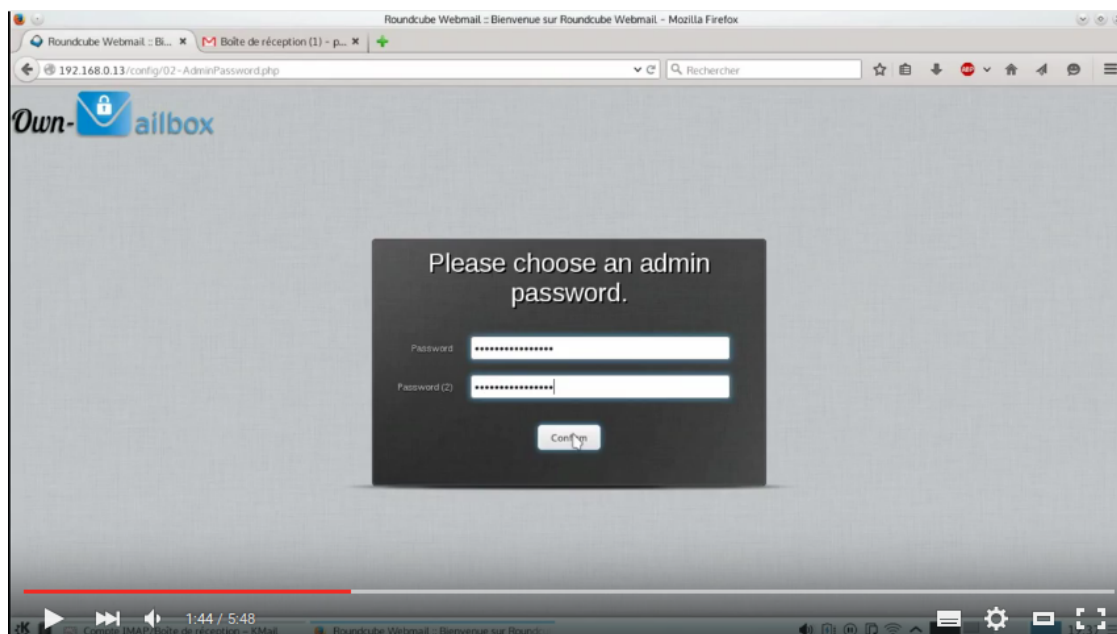
Aucun logiciel supplémentaire n'est nécessaire, on accède à la Own-Mailbox via un navigateur web (comme Firefox) ou un client mail (comme Thunderbird)

Ça veut dire qu'il faut se promener partout avec ?

Non, la Own-Mailbox doit rester chez vous.

Je te préviens, s'il faut que je me mette à Linux et à la ligne de commande, compte pas sur moi.

Pas du tout, c'est très simple, comme tu peux le voir notre vidéo de démonstration (en anglais) :



Par les temps qui courent, on comprend bien l'intérêt de protéger sa correspondance, mais ça ne rend pas les choses un peu compliquées ? Notre famille-test, les Dupuis-Morizeau, ils vont s'en sortir ?

Own-Mailbox est précisément conçue pour rendre le chiffrement et l'auto-hébergement accessibles à tous. Nous nous assurons

qu'à aucun moment l'utilisation d'une Own-Mailbox ne demande une quelconque compétence technique.

En revanche la question serait plutôt : est-ce que notre famille-test va accorder assez d'importance à la vie privée pour investir le minimum (temps et argent) nécessaire à sa défense ? Je ne connais pas encore la réponse...

Pourquoi les gens qui s'y connaissent me cassent les pieds avec la différence entre « chiffrer » et « crypter ». Ça ne veut pas dire « rendre illisible » dans les deux cas ?

Ha ha! Il y a quelques années je disais tous le temps « encrypter » jusqu'à ce que l'on me reproche tellement, et que l'on me dise que ça n'est pas français, que j'ai commencé à dire « chiffrer ».

Explique plus doucement, je n'y comprends rien. Ces histoires de clé privée / clé publique. Je ne sais jamais si je publie la bonne... Et si je l'efface par mégarde, ma clé, je ne pourrai plus lire mes vieux mails ?

Bon à mon avis il faut publier la clef... publique ! Après je ne suis pas sûr sûr... ☐

Plus sérieusement Own-Mailbox publiera pour toi la clef publique donc pas besoin de t'embêter avec ça !

Avec Own-Mailbox tu ne pourras pas effacer ta clef par erreur, à moins d'avoir les compétences techniques nécessaires (console linux, ssh, etc.)

Si ça n'est pas le cas, ou si tu ne bidouilles pas ta Own-Mailbox, tu n'as rien à craindre ! ☐

C'est vraiment sûr et garanti, le chiffrage ? Nan, passque quitte à se faire suer, autant que ça marche, hein... La NSA, elle peut peut-être lire quand même ? On peut le pirater, ce boîtier ?

Le chiffrement de Own-Mailbox se base sur des logiciels libres reconnus, testés et éprouvés depuis des années ([la technologie GPG](#)).

Eux-mêmes reposent sur des algorithmes mathématiques qui rendent le déchiffrement par des tiers tellement coûteux en temps de calcul qu'il paraît impossible.

Edward Snowden a fait confiance à ces logiciels à des moments où sa vie était en jeu.

Après, un bug est toujours possible, mais le code des logiciels de chiffrement étant ouvert il est constamment relu par de nombreuses personnes ce qui réduit le risque de bug, et le cas échéant réduit le délai avant qu'il ne soit corrigé.



Soutenez Own-Mailbox et précommandez la vôtre en cliquant sur l'image

Il va falloir que je retienne un mot de passe de vingt caractères, avec des chiffres et des caractères spéciaux ? Pfou !

Non, avec la Own-Mailbox un mot de passe de 10 caractères est sûr.

Des mesures sont prises de manière à ce que l'interface de connexion ne puisse être piratée avec un mot de passe de 10 caractères

(Empêcher le brute force, voir notre FAQ).

Comment dialoguer avec un-e correspondant-e qui ne chiffre pas ses mails ? Comment ille fait pour lire ce que je lui écris ?

Alors soit ce que tu veux lui envoyer n'est pas confidentiel, et tu as toujours la possibilité de le lui envoyer en clair. Soit tu veux lui envoyer un message confidentiel, eh bien nous avons conçu un système basé sur un lien HTTPS, en le cliquant la personne destinataire du message pourra le visualiser ton message sans risque d'être espionnée.

Une dernière solution est aussi de la convaincre de commencer à chiffrer ses emails et/ou utiliser une Own-Mailbox !

Et si j'écris à quelqu'un-e qui utilise une boîte mail fournie par Google ou Microsoft, ça sert à quelque chose de chiffrer ?

Oui, le principe du chiffrement est justement que les intermédiaires (Google ou Microsoft), ne peuvent pas déchiffrer le contenu, seul le destinataire le peut.

Je vois dans la partie « Fonctionnalités » du site web l'annonce suivante : « *Integrated Framasoft services, to provide you with private large file sharing, event scheduling, shared spreadsheet and documents.* », ça veut dire quoi ?

Cela veut dire que l'on planifie d'ajouter de manière pré-installé sur notre boîtier, une partie des services proposées par Framasoft pour « dégoogliser » Internet(<http://degooglisons-internet.org/liste/>) afin de fournir des services connexes aux mails tel que le partage de gros fichier, les tableurs partagés, l'organisation de réunions, le tout de manière totalement confidentielle.

Vous aussi, vous vous lancez dans le crowdfunding ? Forcément, on vous imagine mal demander des subventions au Ministère de l'Intérieur. □

Pour que Own-Mailbox puisse être utilisable par tous il faut qu'elle soit « All-In-The-Box » et « Plug-And-Play ». Cela

implique que nous
produisons des boîtiers physiques pré-configurées.

Nous ne pouvons évidemment pas financer de notre poche les premières séries de production, et les banques et autres investisseurs traditionnels ont du mal à se projeter dans ce type de projet un peu hors-système.

Le crowdfunding paraît donc la solution optimale pour ce type de projet, et vous retrouverez [notre campagne ici, sur kickstarter.](#)

N'hésitez pas à participer, la campagne ne dure que jusqu'au 5 Octobre 2015.

L'étape d'après, c'est quoi ?

Alors tout d'abord l'étape la plus importante, c'est de livrer les Own-Mailbox aux contributeurs sur Kickstarter, puis aux clients qui suivront !

Lorsque la Own-Mailbox sera bien lancée nous allons sortir une version PME de Own-Mailbox. Car l'espionnage industriel implique de grosses pertes pour les entreprises française comme l'a révélé Wikileaks il y a quelques mois (à hauteur de 200 millions par an).

Par la suite nous avons beaucoup d'autres projets de produits dans les cartons, mais pour l'instant nous gardons cela pour nous !

—

Pour soutenir ce projet et avoir votre Own-Mailbox avant tout le monde, [allez sur leur page Kickstarter.](#)