L'autodéfense de l'email contre la surveillance

La surveillance de masse viole nos droits fondamentaux et constitue une menace pour la liberté d'expression !
Mais, nous pouvons nous en protéger

Le problème

Le mot de passe qui protège l'accès à votre compte email ne suffit pas pour protéger vos messages contre la surveillance de masse.

Le chemin parcouru par chaque email envoyé passe par de nombreux systèmes informatiques avant d'arriver à destination. Les agences de surveillance en profitent pour lire plusieurs millions d'emails quotidiennement.

Même si vous pensez n'avoir rien à cacher : tous ceux avec qui vous communiquez par email non chiffré sont également exposés.

Chiffrement

Récupérez votre vie privée en utilisant GnuPG ! Il chiffre vos messages avant qu'ils ne soient envoyés, de façon que seuls les destinataires que vous avez choisis puissent les lire.

GnuPG ne dépend d'aucune plateforme. Cela signifie qu'il fonctionne avec toutes les adresses électroniques et tourne sur presque tout ordinateur ou téléphone récent. GnuPG est libre et gratuit.

Des milliers de personnes utilisent déjà GnuPG, pour leurs usages professionnel et personnel. Rejoignez-nous ! Chaque personne renforce notre communauté et montre que nous sommes prêts à résister.

La solution

Si un message chiffré avec GnuPG est intercepté ou termine dans de mauvaises mains, il est inutilisable. Sans la clé privée adéquate, personne ne peut le lire. Mais le destinataire initial – et seulement lui – peut le lire comme n'importe quel autre message.

L'émetteur et le destinataire sont tous les deux protégés. Même si quelques-uns de vos messages ne contiennent aucune information privée, l'utilisation massive du chiffrement nous protége tous d'une surveillance de masse injustifiée.

Communication privée par email

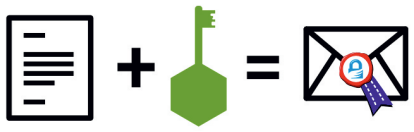
Reprenez en main votre vie privée !
Utilisez GnuPG !

- Logiciel Libre
- pour toutes les adresses électroniques
- pour GNU/Linux, Windows, Mac, Android…
- ni compte ni enregistrement requis
- gratuit

Comment GnuPG fonctionne

Pour utiliser le chiffrement de GnuPG, vous créez une paire de clés uniques privée et publique.
Ces clés ont les fonctions suivantes :

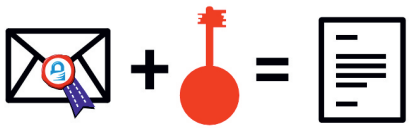
clé publique



chiffrement

Lorsque quelqu'un désire vous envoyer un email chiffré, il a besoin de votre « clé publique ». Par conséquent, plus vous diffusez votre clé publique, mieux c'est.
Cependant, ne vous inquiétez pas : votre clé publique ne peut être utilisée que pour chiffrer des messages, pas pour les déchiffrer.

clé privée



déchiffrement

Votre « clé privée » est comme la clé de la porte d'entrée de votre maison, vous la gardez en sûreté (et de manière privée) sur votre ordinateur. Prenez garde à être le seul et uniquement le seul à pouvoir y accéder.
Vous utilisez GnuPG et votre clé privée pour déchiffrer et lire tous les messages chiffrés qui vous sont envoyés.

En quoi GnuPG est-il sécurisé ?

GnuPG est un **Logiciel Libre** et utilise des **standards ouverts**. C'est un point essentiel pour être sûr que ce logiciel nous protège vraiment de la surveillance. En effet, les logiciels non-libres peuvent masquer des procédés indésirables.

Si personne n'est autorisé à voir le code source d'un programme, personne ne peut être sûr qu'il ne contient pas de programme espion ou indésirable, couramment appelés « portes dérobées ». Si le logiciel ne révèle pas son fonctionnement, alors l'utiliser revient à lui faire une confiance aveugle.

L'une des conditions fondamentales du Logiciel Libre est la publication du code source. Ainsi, le Logiciel Libre autorise et soutient la vérification publique et le contrôle indépendant du code source. Cela signifie que les portes dérobées peuvent être détectées et retirées.

Le Logiciel Libre est avant tout pris en mains par une communauté qui travaille de concert pour programmer un logiciel sécurisé pour tous. Si vous voulez vous protéger de la surveillance, vous ne pouvez vous fier qu'à du Logiciel Libre.

Qu'est-ce que le Logiciel Libre ?

Un Logiciel Libre peut être utilisé par tout le monde et dans n'importe quel but. Cela inclut la liberté de faire des copies, de lire le code source et la possibilité d'améliorer et d'adapter le code à vos propres besoins (les « quatre libertés »).

Même si vous êtes « simplement utilisateur » du programme, vous êtes toujours bénéficiaire de ces libertés parce qu'elles garantissent que le Logiciel Libre restera dans les mains de notre société et son futur développement ne sera pas monopolisé par des entreprises privées ou des gouvernements.

Apprenez-en davantage sur le Logiciel Libre et comment il peut nous amener à une société libre :

fsfe.org/freesoftware

Conseils pratiques

La technologie derrière GnuPG fournit une protection de première classe. Les conseils suivants vont vous aider à vous assurer que votre communication n'est pas compromise pour d'autres raisons.

Pour déchiffrer vos messages vous avez besoin de votre clé privée et de votre **phrase clé** (mot de passe). Cette phrase clé doit être constituée d'au moins 8 caractères et contenir des chiffres, des caractères spéciaux, des minuscules et des majuscules. De plus, aucune personne ayant des information sur vous ne doit être en mesure de deviner votre phrase clé.

Faite une sauvegarde de votre clé privée ! Si votre disque dur vous lâche, vous ne serez pas obligé d'en créer une nouvelle et vous ne perdrez pas vos données.

Chiffrez autant que vous pouvez ! En procédant de la sorte, vous ne révélez pas de fait le caractère sensible de quelques échanges d'informations. Autrement dit, plus vous chiffrez, moins vos messages chiffrés paraîtront suspects.

Prenez garde : le **sujet est transmis non chiffré !**

Tutoriel

Vous pouvez trouver un tutoriel accessible pour l'autodéfense de l'email à cette adresse :

EmailSelfDefense.FSF.org

Ou vous pouvez participer à des **« Cryptoparties »** ou « cafés vie privée » dans votre région. Vous y rencontrerez des gens qui seront heureux de vous aider à utiliser GnuPG et d'autres outils de chiffrement.

2016-04-04

À propos de la FSFE

Ce tract a été réalisé par la Free Software Foundation Europe (FSFE), organisation à but non lucratif ayant pour but de promouvoir le logiciel libre et de construire une société numérique libre.

L'accès aux logiciels détermine la manière dont nous pouvons prendre part à notre société. La FSFE s'emploie à assurer l'égal accès et la participation de tous à l'âge de l'information, en luttant pour les libertés numériques.

Personne ne devrait être obligé de se servir de logiciels ne pouvant pas être **utilisés, étudiés, partagés et améliorés** librement. Nous devons avoir le droit d'adapter la technologie à nos besoins.

Le travail de la FSFE résulte des efforts d'une communauté de personnes engagées pour ces objectifs. Si vous souhaitez vous joindre à nous, il existe de nombreuses façons de contribuer, quelque soit votre profil. Vous trouverez plus d'informations et saurez comment vous pouvez soutenir notre travail sur :

fsfe.org/contribute

Soutenez notre action

Les dons sont primordiaux pour assurer la continuité de notre travail et notre indépendance. Vous pouvez soutenir notre action en rejoignant la Fellowship et nous permettre ainsi de continuer à lutter pour le logiciel libre tant que nécessaire :

fsfe.org/join

Vous pouvez commander gratuitement nos tracts sur :

fsfe.org/promo

Free Software Foundation Europe e.V.
Schönhauser Allee 6/7
10119 Berlin
Germany
https://fsfe.org