Autodefensa de tu correo electrónico contra la vigilancia

¡La vigilancia masiva viola nuestros derechos fundamentales y es una amenaza para la libertad de expresión!
Pero podemos defendernos.

El Problema

La contraseña que protege tu correo electrónico es insuficiente para proteger tus mensajes de la tecnología de vigilancia masiva empleada por los servicios secretos.

Cada mensaje enviado por internet atraviesa muchos ordenadores hasta llegar a su destino. Los servicios secretos y las agencias de vigilancia se aprovechan de ello para leer millones y millones de correos electrónicos cada día.

Aunque pienses que no tienes nada que esconder. Todos con los que te comunicas mediante correos electrónicos desprotegidos, también están expuestos.

Cifrado

¡Recupera tu privacidad con el programa GnuPG! Cifra tus correos electrónicos antes de enviarlos, para que sólo los destinatarios de tu elección puedan leerlos.

GnuPG es independiente de la plataforma. Esto significa que funciona con todas las direcciones de correo electrónico y con cualquier ordenador o teléfono móvil actual. GnuPG es libre y gratuito.

Miles de personas ya están utilizando GnuPG, para uso profesional y privado. ¡Únete a nosotros! Cada persona adicional fortalece nuestra comunidad y demuestra que estamos preparados para defendernos.

La Solución

Cuando un correo electrónico cifrado con GnuPG cae en las manos equivocadas o es interceptado, es inservible; sin la correspondiente llave privada no puede ser leído por nadie. Pero para el destinatario deseado —y sólo para él o ella— se abre como un correo electrónico normal.

Ahora tanto el destinatario como el remitente están seguros. Incluso si el correo electrónico no contiene información privada, el empleo adecuado del cifrado nos protege a todos de la vigilancia masiva injustificada.

Comunicación privada por correo electrónico

¡Recupera tu privacidad!

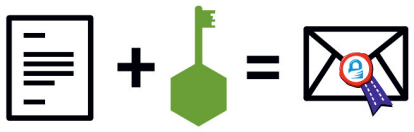
¡Usa GnuPG!

- Software Libre
- Para todas las cuentas de correo electrónico
- Para GNU/Linux, Windows, Mac, Android...
- Sin necesidad de una cuenta o registro
- Gratuito

¿Cómo funciona GnuPG?

Para usar el cifrado GnuPG, creas una pareja única de llave pública y llave privada.
Estas llaves se usan como sigue:

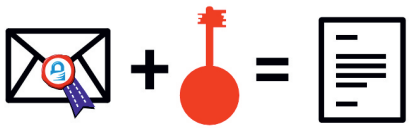
Llave pública



cifrar

Cuando alguien desea enviarte un correo electrónico cifrado, necesita usar tu «llave pública». Por lo tanto, cuanto más divulgues tu llave pública, mejor.
No te preocupes: Tu llave pública sólo puede usarse para cifrar correos electrónicos que te envíen, no para descifrarlos.

Llave privada



descifrar

Tu «llave privada» es como la llave de la puerta principal de tu casa, que guardas segura (y privada) en tu ordenador.
¡Asegúrate de que sólo tú tienes acceso!
Utilizas GnuPG y tu llave privada para descifrar y leer todos los mensajes de correo electrónico cifrados que te han enviado.

¿Qué hace seguro a GnuPG?

GnuPG es **Software Libre** y usa **Estándares Abiertos**: esto es esencial para estar seguros de que el software realmente puede protegernos de la vigilancia. Porque con el software privativo y los formatos propietarios puede suceder algo fuera de nuestro control.

Si nadie está autorizado a ver el código fuente de un programa, nadie puede tampoco asegurar que no contiene programas espías no deseados, también llamados «puertas traseras». Si el software no revela cómo funciona, tan sólo podemos confiar en él a ciegas.
A diferencia de esto, una condición básica del Software Libre es la publicación del código fuente; el Software Libre permite y promueve un control independiente y la revisión pública del código del programa por cualquiera. Con esta trasparencia, las puertas traseras pueden ser detectadas y eliminadas.

El Software Libre se encuentra la mayoría de las veces en manos de una comunidad que trabaja conjuntamente para programar un Software seguro para todos. Si quieres protegerte de la vigilancia solamente puedes confiar en Software Libre.

¿Qué es el Software Libre?

El Software Libre puede ser usado por cualquier persona para cualquier propósito. Esto incluye la copia libre, la lectura del código fuente así como la posibilidad de mejorarlo o adaptarlo a tus propias necesidades (las denominadas «cuatro libertades»).

Incluso si «sólo quieres utilizar el programa», aún así te beneficias de estas cuatro libertades. Pues éstas garantizan que el Software Libre permanece en manos de nuestra sociedad y que su desarrollo no está controlado por los intereses de empresas privadas o gobiernos.

Amplía información sobre cómo el Software libre nos puede llevar a una sociedad libre:

fsfe.org/freesoftware

Consejos prácticos

GnuPG ofrece técnicas de protección de primera clase. Estos consejos te ayudarán a evitar que tu comunicación cifrada pueda verse comprometida por otras razones:

Para descifrar tus correos electrónicos, necesitas una llave privada y una frase de **contraseña**, que debe tener al menos 8 caracteres de longitud y contener números, caracteres especiales así como letras minúsculas y mayúsculas. Además, nadie con conocimientos sobre ti debería ser capaz de adivinar tu frase de contraseña.

¡Haz una copia de seguridad de tu llave privada! En caso de que tu disco duro se rompa, no tendrás que hacer una nueva ni sufrir ninguna pérdida de datos.

¡Cifra tanto como sea posible! Con eso impides que otros se den cuenta de cuándo y con quién intercambias información confidencial. Cuanto más a menudo cifres, más discretos son tus mensajes cifrados.

¡Ten en cuenta que **«el asunto» del correo se transmite sin cifrar**!

Instrucciones

Una guía sencilla para la autodefensa del correo electrónico con GnuPG se puede encontrar en el enlace:

EmailSelfDefense.FSF.org

O busca las denominadas **«Cryptoparties»** (fiestas de cifrado). Allí encontrarás personas que de forma gratuita te ayudarán con el manejo de GnuPG y otras técnicas de cifrado.

2016-04-04

Acerca de la FSFE

Este folleto fue creado por la Fundación Europea de Software Libre (FSFE), una organización sin ánimo de lucro que se dedica a la difusión del Software Libre y por lo tanto al desarrollo de una sociedad digital libre.

El acceso al software determina la forma en que podemos participar en nuestra sociedad. Es por eso que la FSFE aboga por un correcto acceso y una participación equitativa de todos en la sociedad de la información, luchando por la libertad digital.

Nadie debería nunca verse forzado a usar un software que no garantice las libertades de ser **utilizado, estudiado, compartido y mejorado**. Necesitamos el derecho de adaptar la tecnología para que se ajuste a nuestras necesidades.

El trabajo de FSFE se basa en una comunidad de personas comprometidas con estos objetivos. Si quieres unirte a nosotros y / o ayudar en el logro de nuestros objetivos, hay muchas maneras de contribuir. No importa el conocimiento que traigas. Puedes obtener más información y conocer cómo apoyar nuestro trabajo en:

fsfe.org/contribute

¡Hazte miembro promotor!

Las donaciones son esenciales para continuar con nuestro trabajo y garantizar nuestra independencia. Puedes apoyar mejor nuestro trabajo convertiéndote en un miembro promotor de la FSFE, un «Fellow». Haciéndolo, nos ayudas directamente para continuar la lucha por el Software libre donde quiera que sea necesario:

fsfe.org/join

Puedes pedir éste y otros folletos de forma gratuita en:

fsfe.org/promo

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