Email self-defense against surveillance

Mass surveillance violates our fundamental rights and is a menace to the freedom of speech!
But: we can defend ourselves.

The Problem

The password that protects your email is not sufficient to protect your mails against the mass surveillance technologies used by secret services.

Each email sent over the internet passes through many computer systems on the way to its destination. Secret services and surveillance agencies take advantage of this to read millions and millions of emails each day.

Even if you think you have nothing to hide: Everyone else that you communicate with via unprotected emails is being exposed as well.

Encryption

Take back your privacy by using GnuPG! It encrypts your emails before they are sent, so only the recipients of your choice can read them.

GnuPG is platform independent. That means it works with every email address and runs on pretty much any computer or recent mobile phone. GnuPG is free and available at no charge.

Thousands of people already use GnuPG, for professional and private use. Come and join us! Each person makes our community stronger and proves that we are ready to fight back.

The Solution

Whenever an email that is encrypted with GnuPG is intercepted or ends up in the wrong hands, it is useless: Without the appropriate private key it cannot be read by anyone. But, for the intended recipient—and only for her—it opens like a totally normal email.

Sender and recipient are both safer now. Even if some of your emails contain no private information, consistent use of encryption protects us all from unjustified mass surveillance.

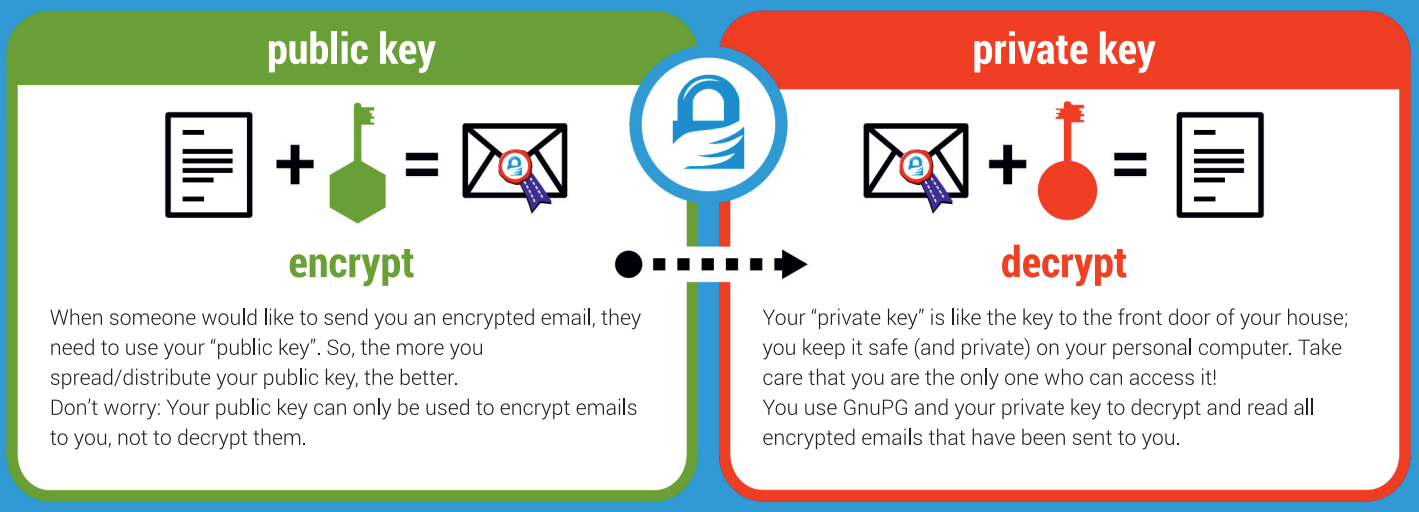
Private email communication

Take back your privacy!
Use GnuPG!

- Free Software
- for all email addresses
- for GNU/Linux, Windows, Mac, Android, ...
- no account or registration needed
- free of charge

How GnuPG works

To use GnuPG encryption you create a unique pair of a public and a private "key".
These keys are used as follows



What makes GnuPG secure?

GnuPG is **Free Software** and uses **Open Standards**. That is essential to be sure that software can really protect us from surveillance. Because in proprietary software and formats, things might happen beyond your control.

If no one is allowed to see the source code of a program, nobody can be sure that it does not contain undesirable spy programs—so-called "backdoors". If software does not reveal how it works, we can merely trust it blindly.
In contrast, a fundamental condition of Free Software is to publish its source code: Free Software allows and supports independent checking and public review of the applied source code by everyone. Given this transparency, backdoors can be detected and removed.

Most Free Software lies in the hands of a community that works together to build secure software for everyone. If you want to protect yourself from surveillance you can only trust Free Software.

What is Free Software?

Free Software can be used by everyone for any purpose. That includes free copying, reading the source code and the possibility to improve or adapt it to your own needs (the so-called "four freedoms").

Even if you "only want to use" the program, you still benefit from these freedoms. Because they guarantee that Free Software remains in the hands of our society and that its further development is not controlled by the interests of private companies or governments.

Find out more about this and how Free Software can lead us into a Free Society:

fsfe.org/freesoftware

Practical advice

The technology behind GnuPG provides first-class protection. The following guidelines will help you to ensure that your encrypted communication is not compromised for other reasons:

To decrypt your emails you need your private key and your **passphrase**. This passphrase should be at least 8 characters long and contain digits, special characters as well as upper and lower case letters. Furthermore, no one with background knowledge about you should be able to guess your passphrase.

Backup your private key! If your harddisk breaks you don't need to create a new one and you don't lose your data.

Encrypt as much as you can! By doing so, you prevent others from realising when and with whom you exchange sensitive information. Thus, the more often you encrypt your messages, the less suspicious encrypted messages will be.

Be aware that the **subject is transmitted unencrypted!**

Tutorial

You can find a simple tutorial for email self-defense with GnuPG encryption here:

EmailSelfDefense.FSF.org

Or you watch out for so-called **"Cryptoparties"** in your area. These are events where you can meet people that would be happy to help you in setting up and using GnuPG as well as other encryption tools at no charge.

2016-04-04

About the FSFE

This leaflet was created by the Free Software Foundation Europe (FSFE), a non-profit organisation dedicated to promoting Free Software and working to build a free digital society.

Access to software determines how we can take part in our society. Therefore, FSFE strives for fair access and participation for everyone in the information age by fighting for digital freedom.

Nobody should ever be forced to use software that does not grant the freedoms to **use, study, share and improve the software**. We need the right to shape technology to fit our needs.

The work of FSFE is backed by a community of people committed to these goals. If you would like to join us and/or help us to reach our goals, there are many ways to contribute. No matter what your background is. You can learn more about this and how you can support our work under:

fsfe.org/contribute

Become a sustaining member!

Donations are critical for us to continue our work and to guarantee our independence. You can support our work best by becoming a sustaining member of the FSFE, a "Fellow". By doing so, you directly help us to continue the fight for Free Software wherever needed.

fsfe.org/join

You can order this and other leaflets at no charge:

fsfe.org/promo

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