# What is PGP?

If your threat model includes a government or law enforcement, or you have some other reason for wanting to make sure that your email provider is not able to turn over the contents of your email communications to a third party, you may want to consider using end-to-end encryption for your email communications. End-to-End Encryption is uninterrupted protection of data traveling between two communicating parties.

PGP is the standard for end-to-end encryption of your email. PGP stands for Pretty Good Privacy. It's actually very good privacy. If used correctly, it can protect the contents of your messages, text, and even files from being understood even by well-funded government surveillance programs.

PGP is built upon the concept of Public Key Encryption. This is a cryptographic system that uses two keys - a public key known to everyone and a private key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it.

* So public key encryption lets you encrypt and send messages safely to anyone whose public key you know.
* If others know your public key, they can send you messages, which only you can decode.
* And if people know your public key, you can sign messages so that those people will know they could only have come from you.
* And if you know someone else's public key, you can decode a message signed by them, and know that it only came from them.

You should keep your private key stored somewhere safe, and protected with a long password. (If someone else gets a copy of your private key, they can pretend to be you, and sign messages claiming that they were written by you.) You can give your public key to anyone you want to communicate with you, or who wants to learn whether a message truly came from you.

Unfortunately, PGP has a reputation for being difficult to understand, or use. The good news is that there are many programs available now which can hide the ancient design of PGP and make it somewhat easier to use, especially when it comes to encrypting and authenticating email?the main use of PGP.

For detailed instructions on how to install and use PGP encryption for your email, see:

* [How to: Use PGP for Mac OS X](umbrella://lesson/pgp-for-mac-os-x)
* [How to: Use PGP for Windows](umbrella://lesson/pgp-for-windows)
* [How to: Use PGP for Linux](umbrella://lesson/pgp-for-linux) Storing your private encryption key on your mobile device may seem risky. But the benefit of being able to send and store emails securely encrypted on the mobile device might outweigh the risks. Learn how to install and use encryption for email on your smartphone in the [K9 and APG Guide](umbrella://lesson/k9-&-apg).

# What PGP Can?t Do: Metadata

PGP is all about making sure the contents of a message are secret, genuine, and untampered with. But that's not the only privacy concern you might have. PGP does not protect your metadata?which is everything else, including the subject line of your email, or who you are communicating with and when. Metadata can provide extremely revealing information about you even when the content of your communication remains secret.

If you're exchanging PGP messages with a known dissident in your country, you may be in danger for simply communicating with them, even without those messages being decoded. Indeed, in some countries you can face imprisonment simply for refusing to decode encrypted messages.

Protecting your metadata will require you to use other tools, such as Tor, at the same time as end-to-end encryption. You can learn how to do this in the [Internet lesson](umbrella://lesson/the-internet).

The tool guides for PGP will explain in detail about how to create your public PGP key and how you might want to share it. In general, it?s good to keep in mind that if you are working in a dangerous environment and if would use a pseudonym generally, use that pseudonym (and alternative email) when labelling your key.

Disguising that you are communicating with a particular person is more difficult. One way to do this is for both of you to use anonymous email accounts, and access them using Tor. If you do this, PGP will still be useful, both for keeping your email messages private from others, and proving to each other that the messages have not been tampered with.

Swipe right for this lesson's checklist

Go to the Beginner lesson for advice on how to improve basic email security and know if my email has been hacked.

[Go to Beginner Lesson](umbrella://lesson/email/0)

### RELATED LESSONS/TOOLS

* [Internet lesson](umbrella://lesson/the-internet)
* [PGP for Mac OSX tool](umbrella://lesson/pgp-for-mac-os-x)
* [PGP for Windows tool](umbrella://lesson/pgp-for-windows)
* [PGP for Linux tool](umbrella://lesson/pgp-for-linux)
* [K9 & APG tool](umbrella://lesson/k9-&-apg)

### FURTHER READING

* [EFF - Public key cryptography and PGP](https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp)