Why encrypt?

Maybe you're an activist, maybe you're a lawyer, maybe you just want to opt-out of surveillance imposed by government agencies. In any case, if you're not currently using strong encryption your correspondance is travelling across the internet in plain text. This sucks, but anyone can learn to use software to prevent that!

How does it work?

We're going to set-up a piece of software called Gnu Privacy Guard (GPG), which can encrypt emails so that they are unreadable by anyone except the intended recipient. GPG works with a 'key pair', a set of two cryptographic keys (one public and one private) which are paired. The private key stays on one device, and the public key is shared widely. An email encrypted with a user's public key can only be decrypted (for reading) by the corresponding private key. This sounds complicated, but it works and is simple in practice!

See https://en.wikipedia.org/wiki/GNU_Privacy_Guard for more details on how GPG encryption works.

What you need:

- An email account! One with IMAP access is preferable (for gmail users: Settings -> Forwarding and POP/IMAP -> Enable IMAP)
- A computer (Mac OS, Windows, or any version of Linux)
- An internet connection
- An hour or so!

Ok let's go!

1. Visit https://getthunderbird.com or install with your package manager (Linux)

Thunderbird is a local mail client, so it runs on your computer as a separate application instead of in a web browser (as Gmail does). We need a local mail client so that we have access to the GPG private key we'll store on your computer.

Set up your email account

Thunderbird should pop-up a 'new account' wizard when you first run it. This will ask for your name, email address, and the password you use to log-in. On the next screen you'll see options for POP or IMAP (IMAP is recommended) and Thunderbird will try to guess the server settings to download and send email using your address. It usually gets this right (it will for Gmail, Riseup, and most common email providers). If all goes well you should be presented with your email! Thunderbird is a powerful, but simple to use program, so you may want to check out the documentation at https://support.mozilla.org/en-US/products/thunderbird for more details.

Click on this button in the upper right corner: and then find 'Add-ons'. Now we want to:

find a plugin called Enigmail. You should find version 1.8.2. Install it!

Enigmail is a plugin that will allow Thunderbird to send and decrypt emails encrypted with GPG. It will automate installing the other software (GnuPG) that we need to do this, and provide tools for managing, signing, and importing public keys, as well as making your own keypair. It's super handy!

Set-up Enigmail:

When you first open Thunderbird after installing Enigmail a set-up wizard should pop-up. For most folks the 'standard' configuration will be totally fine, so click 'Start setup now', and then on the next screen select 'I prefer a standard configuration'.

Create a Key Pair

On the next screen we'll create a 'key pair': as we said earlier, this is a 'private' key (which stays on your computer), and a 'public' key, which we'll share with folks to exchange secure email (we'll get to the sharing part in a bit).

Choose a secure password for your keypair (make sure it's different from your email and computer password, at the least). This is an extra layer of protection for your email - in order to read email encrypted with your unique public key you'll also need to enter this passphrase. Key generation might take a minute or two, depending on how fast your machine is. Get a cup of coffee or tea! Yum.

Enigmail will ask about a 'revocation certificate'. Save it in a safe place.

Sharing your public key:

In order for someone to write an encrypted email to you, they need to have a copy of your public key on their computer. You can share your key in a variety of ways, but the easiest ways are probably over email, and by uploading to a keyserver.

Click the hamburger:

Find Enigmail -> Key Management. This will show you the public keys saved on your machine, and let you do various things with them.

Right click on your key!

it will look something like this!

If you click 'Send Public Keys by Email' you can share your key with anyone whom you trust. Make sure you get their key too, and then all of your correspondance will be safe!

If you click 'Upload Public Keys to Keyserver' your public key will be uploaded to a server. This means that other people will be able to find your public key, simply by looking for a key associated with your email address. Neat!

Sending Encrypted Mail:

OK, so we've made a key, we've shared it with our trusted friends, and maybe they've shared their keys back. How do we actually write an encrypted email to someone?

Well, it's pretty easy! Enigmail takes care of almost all of the work. If you write an email to a friend (say her email is sarah@example.com), and you have Sarah's public key on your computer, Enigmail will automatically encrypt your mail message with Sarah's key, so only she can read it. Nice!

You can be sure an email is going to be encrypted when the following appears in the 'compose' window:

Note: signing is different than encryption. Signing uses your private key to digitally sign the message - because of the pairing between your public and private keys, a recipient who has your public key can verify that the message came from you.

That's the basics! For more:

- https://emailselfdefense.fsf.org/en/
- https://www.cryptoparty.in/brief#email
- https://ssd.eff.org/en
- https://tech.safehubcollective.org/cybersecurity/

All files related to this zine can be found here:
https://github.com/aliceriot/PocketGuide
Improvements, suggestions, and corrections are most welcome!
Contact info for the author at
https://aliceriot.github.io/contact

♥ Please print and share! ♥
Encryption works!

the pocket guide to EMAIL ENCRYPTION

protect yourself!
communicate securely!
resist the surveillance state!