# PGP GUIDE

This guide has been created to help you get PGP set up on your laptop or desktop computer.

Thunderbird is, in my opinion, the easiest and the best way to handle PGP encrypted emails on both Apple OS's and Windows OS's. With that in mind, this guide will center on using Thunderbird to handle your personal / work emails, and using a Thunderbird extension called Enigmail to handle your PGP encryption.

Please note that "PGP" (which stands for Pretty Good Privacy) and "GPG" (GNU Privacy Guard) can be used interchangeably. They both essentially refer to the same thing within the scope of this guide.

This guide does not cover PGP on mobile devices, and I will not be creating a guide for mobile devices at this time. Allowing your PGP private key on to your mobile device is a very bad idea, especially if you do not use a very strong passphrase to protect your private key. People often store their passwords on their phone or tablet and these devices are often lost, stolen or perhaps even seized by the authorities.

If a person has access to your private key and password they can decrypt all encrypted emails that are sent to you. An even bigger risk arising from this is the ability of somebody with access to your private key and passphrase to PGP-sign a message with your PGP Private Key enabling that person to pretend very convincingly that they are you.

You can set up your personal / work email account on your phone like any regular Gmail account if you wish in order to receive notifications of new emails, or to write and respond to unencrypted emails. However, you will only be able to decrypt and encrypt emails on your computer using Thunderbird with Enigmail.

# Windows Users:

*Step 1:*
Download Thunderbird from the following link:
 https://www.mozilla.org/en-US/thunderbird/

*Step 2:*
Double click the Thunderbird Setup 45.7.0 file that you downloaded and install Thunderbird.

*Step 3:*
Launch Thunderbird. If you see a 'System Integration' pop-up feel free to click 'Skip integration' if you do not understand any of the options you can choose.

*Step 4:*
You will see the 'Welcome to Thunderbird' screen asking you if you want to create a new email address:
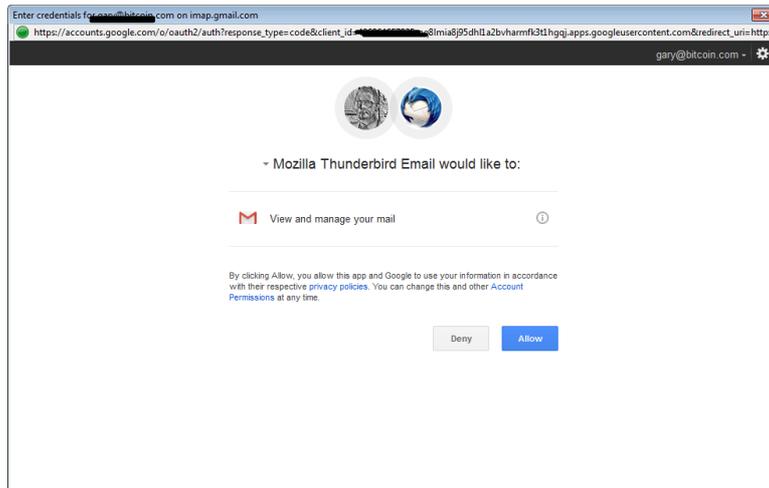


Click 'Skip this and use my existing email'.

*Step 5:*
On the 'Mail Account Setup' screen, enter your name, your 'personal / work' email address and your password in the required fields. I would recommend allowing Thunderbird to store your password; otherwise you will need to enter it every time you open Thunderbird. Once you have entered all required fields, click the 'Continue' button. Depending on your preference you can either select IMAP or POP3. The difference between these is that IMAP *does not* store the emails from your account on your computer, whereas POP3 *does* store the emails from your account on your computer. IMAP is the default selection and should be sufficient for most people. Click 'Done'.

*Step 6:*

Clicking 'Done' will bring you to your Google login page. Here you will need to enter your email account login credentials as normal – your email address, password and two-factor authentication (if already set up on your account).

After entering your login credentials click the blue 'Allow' button to allow Thunderbird to view and manage your mail:



Thunderbird will now begin to sync the emails from your 'personal / work' account and they will appear when you click the 'Inbox' folder on the left.

*Step 7:*

Press the 'alt' key on your keyboard to show the 'File', 'Edit', 'View', etc. menus at the top of your screen. Click 'Tools', then 'Account Settings'. This will bring up the Account Settings menu:
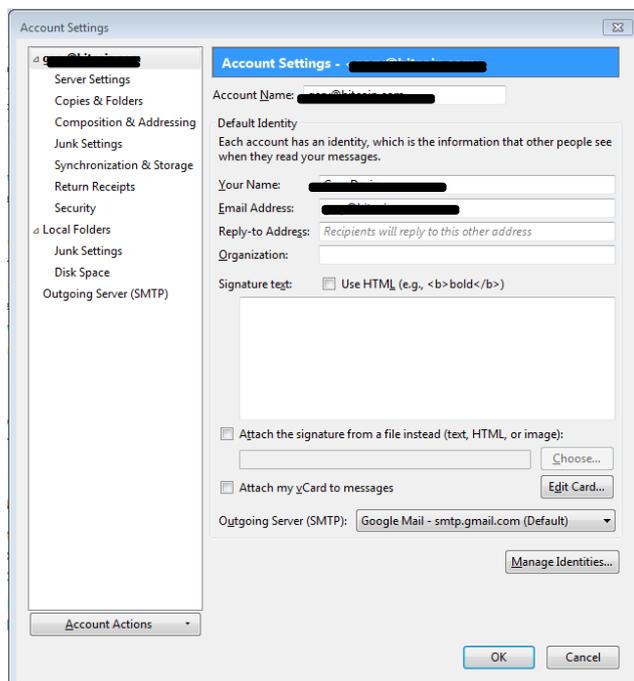
Click 'Server Settings' in the menu on the left, and in the 'Server Settings' section change the 'Check for new messages every' number to '3' minutes. This will ensure that Thunderbird will check for and download any new emails every 3 minutes. Do not change any other settings in this section.

Click 'OK'. If you get a warning about Junk Mail folders, just click 'OK', and click 'OK' again on the Junk Mail screen that appears.
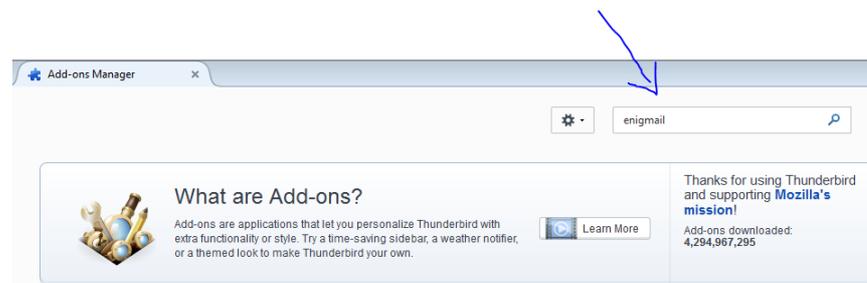
You are now finished setting up Thunderbird! Next we will set up Enigmail:
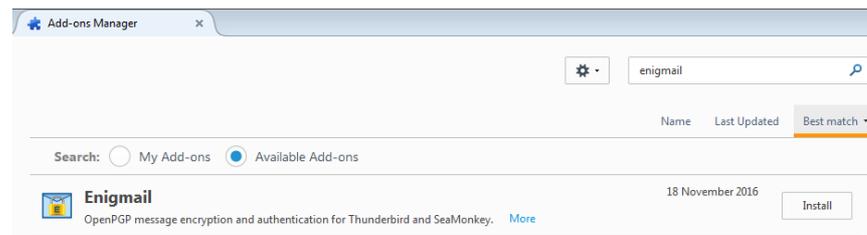
*Step 8:*
Press the 'alt' key on your keyboard again to show the 'File', 'Edit', 'View', etc. menus at the top of your screen. Click 'Tools', then 'Add-ons'. This will take you to the 'Add-ons Manager' screen.

*Step 9:*
Type "Enigmail" into the search bar in the top right corner and click the magnifying glass to search:



Click the 'Install' button on the first result that comes up, titled 'Enigmail':



Once it has finished downloading click the blue 'Restart now' link. This will restart Thunderbird and install Enigmail, opening the 'Enigmail Setup Wizard' automatically. You will most likely see the following alert:
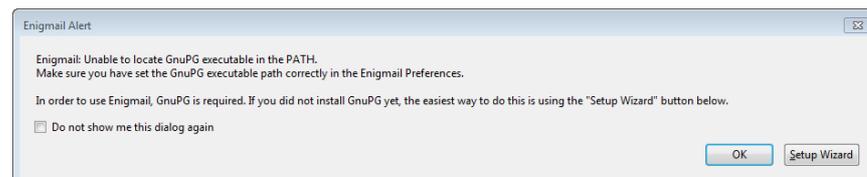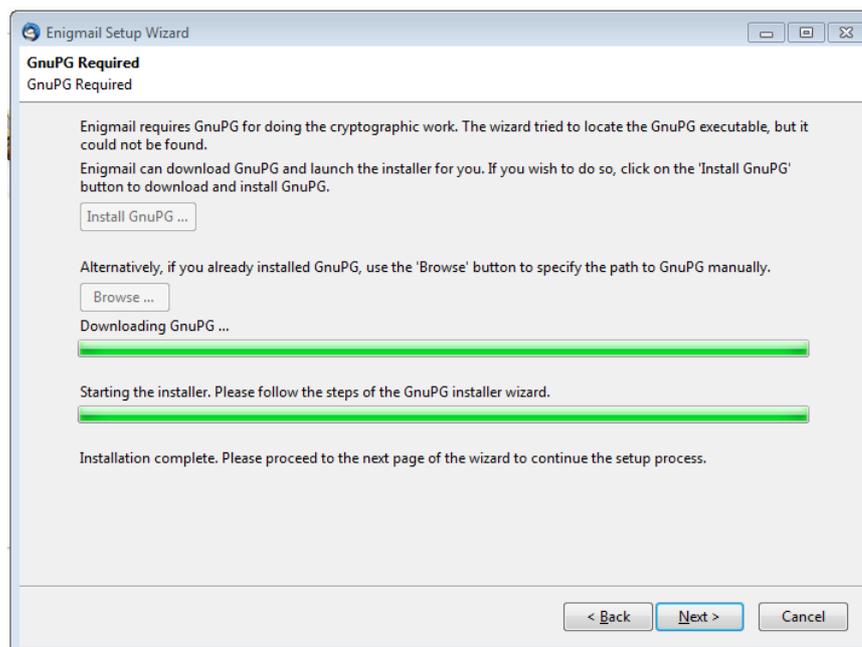
*Step 10:*
Click the 'Setup Wizard' button, ensure 'Start setup now' is selected then click 'Next'. Ensure 'I prefer a standard configuration (recommended for beginners)' is selected and click 'Next'.

Click the 'Install GnuPG' button and it will begin downloading GnuPG. Depending on the speed of your Internet connection this can take a few minutes. Once it is completed, click 'Next'.

(If downloading GnuPG stalls or fails, click the 'Cancel' button. Then press the 'alt' key on your keyboard, click 'Enigmail' in the menu at the top of the screen and click 'Setup wizard' then start Step 10 again.)

Install Gpg4win. On the 'Choose Components' screen, select 'GPA' and 'GpgEX', then click 'Next'. Click 'Next' all the way until you see the 'Install' button, then click 'Install'. Once installation has completed, click 'Next' again and 'Finish'.
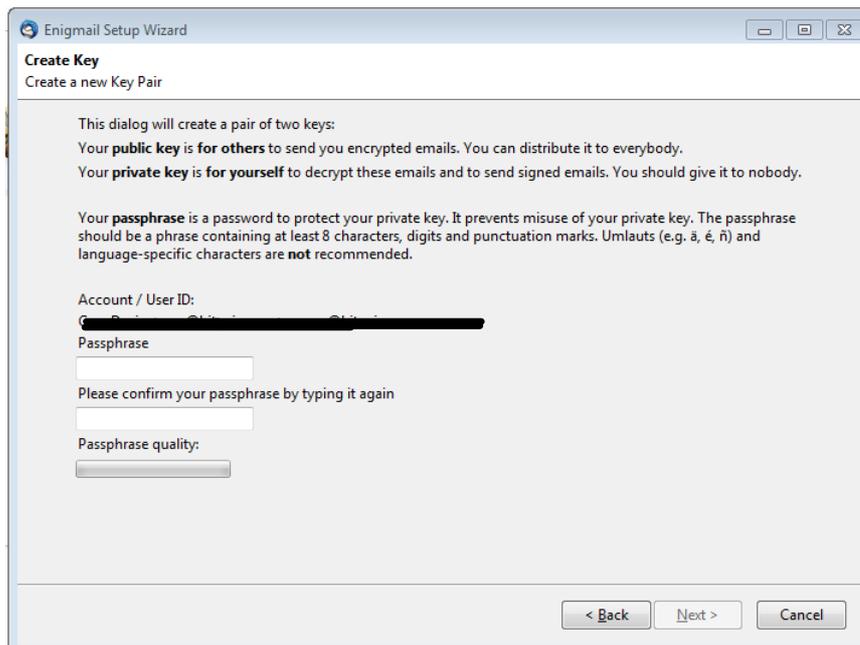
This will take you back to the Enigmail Setup Wizard:

Click the 'Next' button, and this will take you to the 'Create Key' window:
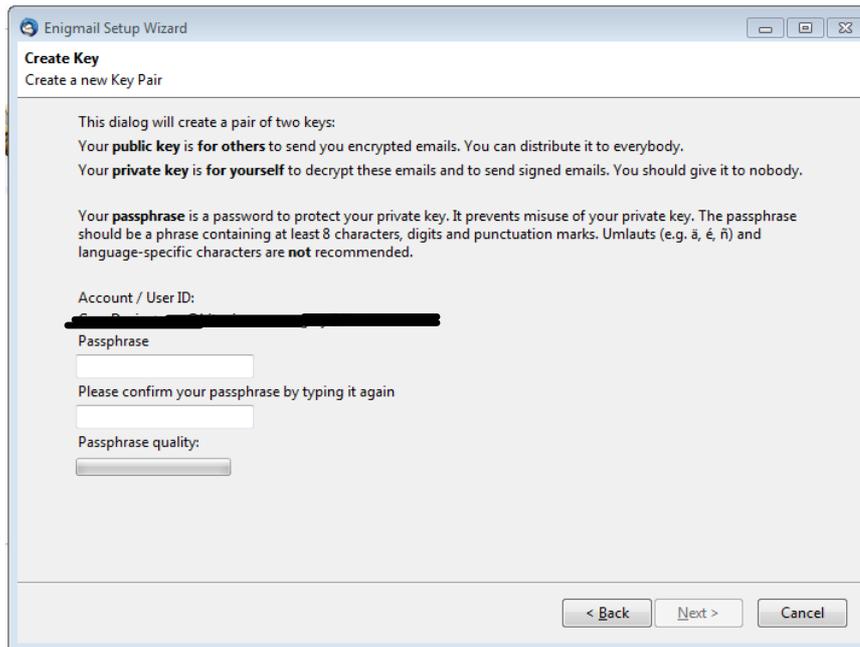


*Step 11:*



Here you will need to set a strong passphrase. This passphrase will be used to protect your private key, and it is **highly recommended** that you pick a phrase containing at least 8 characters, digits and punctuation marks at minimum – a 16 – 24 character passphrase would be preferable.

DO NOT FORGET THIS PASSPHRASE. Without it you will be unable to decrypt emails that are encrypted to your public key.

Once you have entered your desired passphrase (and written it down somewhere safe) click the 'Next' button.

<u>Step 12:</u>
Once your key has been created you will need to create a revocation certificate. Click the 'Create Revocation Certificate' button and you will be prompted for your passphrase. Enter your passphrase and click 'OK'. Save the revocation certificate file somewhere very safe, and then click the 'Next' button. Click 'Finish'.

<u>Step 13:</u>
Press the 'alt' key on your keyboard one more time. In the 'Enigmail' menu at the top of the screen, click 'Key Management'. Right-click on your name and click 'Upload Public Keys to Keyserver'. This will ensure that other people are able to find your public key with ease in order to encrypt emails to you.


*Congratulations! You're now set up for secure PGP encrypted communication!*

# Mac Users:

*Step 1:*
Download Thunderbird from the following link:
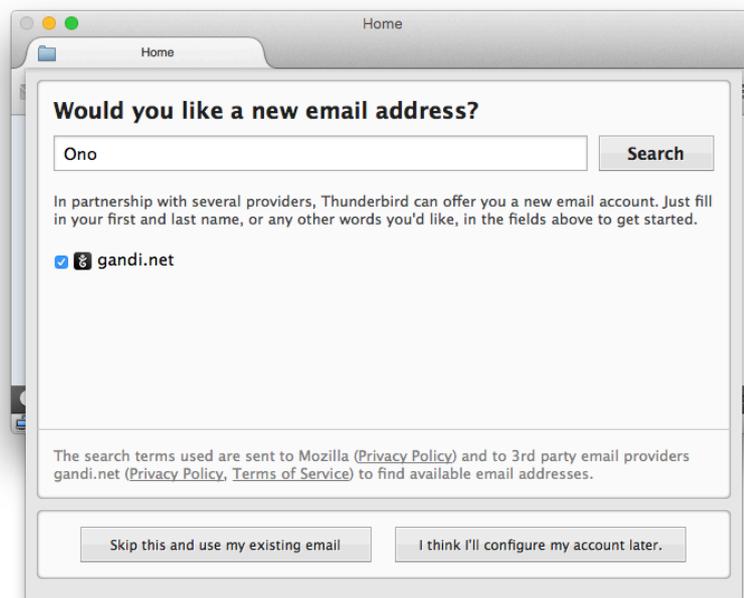 https://www.mozilla.org/en-US/thunderbird/

*Step 2:*
Mount the downloaded .dmg file (at the time of writing the current version of Thunderbird is 45.7.0, so the file you need to mount is called **Thunderbird 45.7.0.dmg**) and install Thunderbird.

*Step 3:*
Launch Thunderbird. If you see a 'System Integration' pop-up feel free to click 'Skip integration' if you do not understand any of the options you can choose. Also click 'Skip integration' if you use Apple Mail for your regular emails on your Mac.

*Step 4:*
You will see the 'Welcome to Thunderbird' screen asking you if you want to create a new email address:



*Step 5:*
On the 'Mail Account Setup' screen, enter your name, your 'personal / work' email address and your password in the required fields. I would recommend allowing Thunderbird to store your password; otherwise you will need to enter it every time you open Thunderbird.
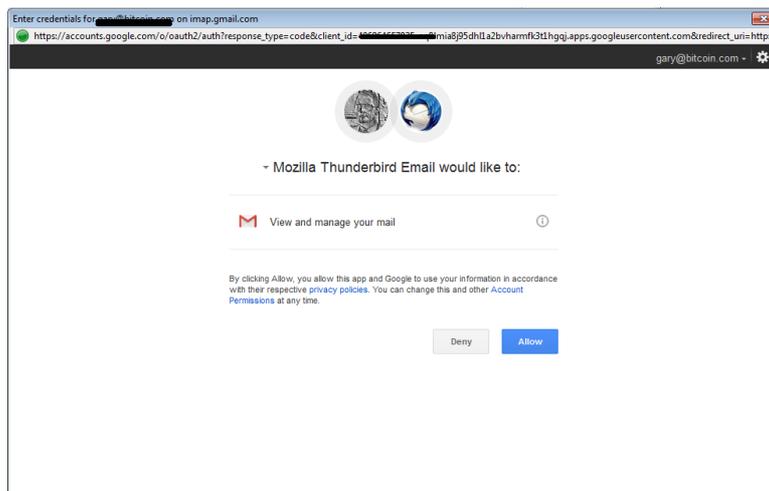
Once you have entered all required fields, click the 'Continue' button. Depending on your preference you can either select IMAP or POP3. The difference between these is that IMAP *does not* store the emails from your account on your

computer, whereas POP3 *does* store the emails from your account on your computer. IMAP is the default selection and should be sufficient for most people. Click 'Done'.

*Step 6:*
Clicking 'Done' will bring you to your Google login page. Here you will need to enter your email account login credentials as normal – your email address, password and two-factor authentication (if already set up on your account).

After entering your login credentials click the blue 'Allow' button to allow Thunderbird to view and manage your mail:



Thunderbird will now begin to sync the emails from your 'personal / work' account and they will appear when you click the 'Inbox' folder on the left.

*Step 7:*
Click 'Tools' at the top of your screen, then 'Account Settings'. This will bring up the Account Settings menu:
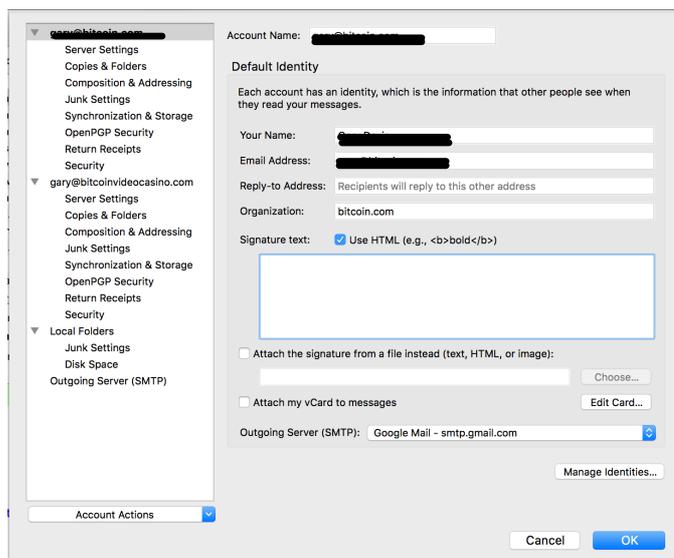
Click 'Server Settings' in the menu on the left, and in the 'Server Settings' section change the 'Check for new messages every' number to '3' minutes. This will ensure that Thunderbird will check for and download any new emails every 3 minutes. Do not change any other settings in this section.
Click 'OK'. If you get a warning about Junk Mail folders, just click 'OK', and click 'OK' again on the Junk Mail screen that appears.

You are now finished setting up Thunderbird! Next you will set up GPG Suite, then Enigmail.

To install GPG Suite, follow the steps below - you can also visit this page to see pictures of GPG Suite setup:
https://securityinabox.org/en/guide/thunderbird/mac/#install-gpg-suite-and-enigmail

*Step 1:*
Browse to the GPG Suite download page at https://gpgtools.org/gpgsuite.html

*Step 2:*
Click [Download GPG Suite] to download the installer disk image.

*Step 3:*
Make sure DiskImageMounter (default) is selected next to Open with and click [OK].

After your browser has downloaded the disk image, Finder will mount it so you can install GPG Suite.

*Step 4:*
Double-click the Install icon on the left to begin the process of installing GPG Suite.

*Step 5:*
Click [Continue] to choose a location for the installation.

*Step 6:*
Click [Install] to install to enter your login passphrase.

*Step 7:*
Type the passphrase you use to log in to your computer.

*Step 8:*
Click [Install Software] to install GPG Suite.

When the installer is done, it will launch the GPG Keychain application so that you can generate your GnuPG public and private key pair.

Now you can quit GPG Keychain by following the steps below.

*Step 9:*
Click [Cancel] to close the key generation screen

*Step 10:*
To quit GPG Keychain, press Command-Q.

Next, you should quit the installer and dismount the installation disk image by following the steps below:

*Step 11*:
Switch back to the Install GPG Suite installer application

*Step 12:*
Click [Close] to quit the installer

*Step 13:*
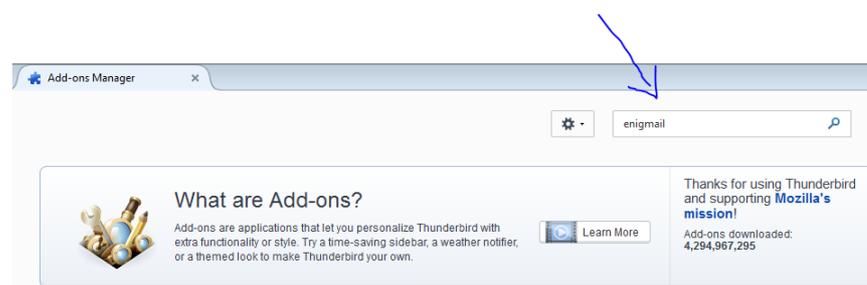Switch back to Finder

*Step 14:*
Dismount the GPG Suite installer disk image by pressing Command-E while the disk image window is active
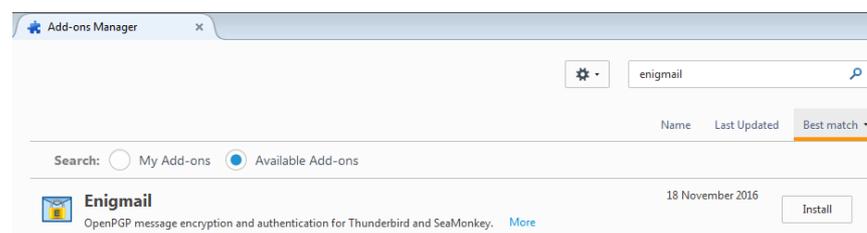
*Step 15:*
Click the 'Tools' menu at the top of your screen, then 'Add-ons'. This will take you to the 'Add-ons Manager' screen.

*Step 16:*
Type "Enigmail" into the search bar in the top right corner and click the magnifying glass to search:



Click the 'Install' button on the first result that comes up, titled 'Enigmail':

Once it has finished downloading click the blue 'Restart now' link. This will restart Thunderbird and install Enigmail, opening the 'Enigmail Setup Wizard' automatically.

If it does appear automatically click the 'Setup Wizard' button, ensure 'Start setup now' is selected then click 'Continue'. If it does not appear automatically click the 'Enigmail' file menu at the top of the screen and click 'Setup Wizard'. Ensure 'I prefer a standard configuration (recommended for beginners)' is selected and click 'Continue'.

You may see a warning about your GnuPG version, as shown below:
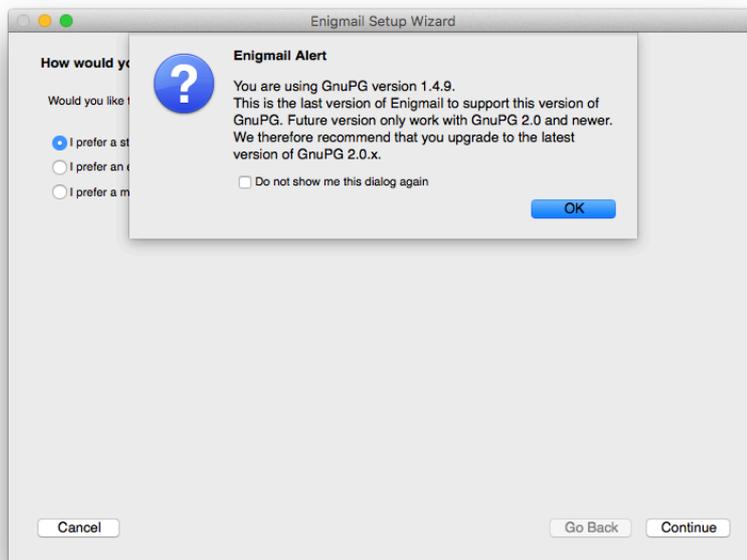


If you do, click 'OK'. Otherwise, simply continue on to the 'Create Key' window:
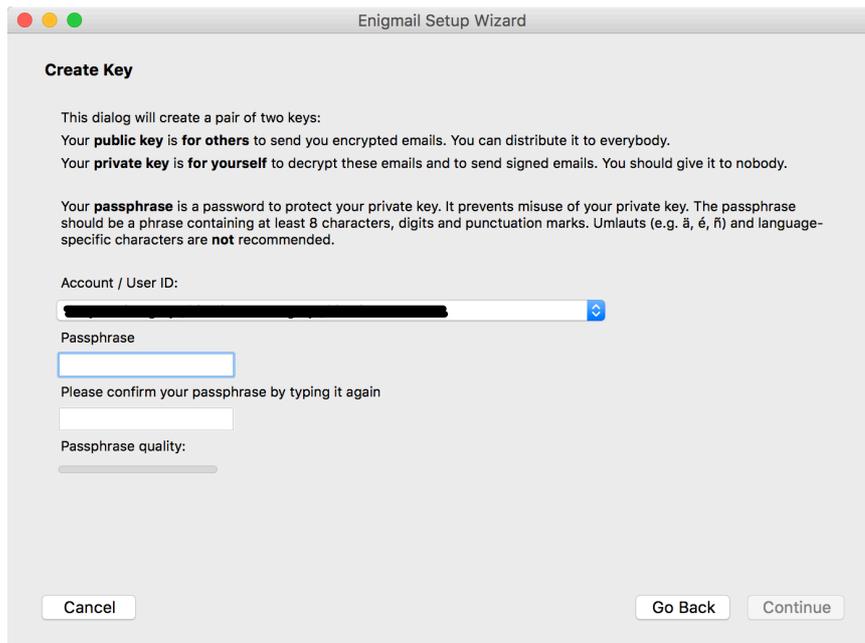
**Step 18:**
Here you will need to set a strong passphrase. This passphrase will be used to protect your private key, and it is **highly recommended** that you pick a phrase containing at least 8 characters, digits and punctuation marks at minimum – a 16 – 24 character passphrase would be preferable.

DO NOT FORGET THIS PASSPHRASE. Without it you will be unable to decrypt emails that are encrypted to your public key.

Once you have entered your desired passphrase (and written it down somewhere safe) click the 'Continue' button.

**Step 19:**
Once your key has been created you will need to create a revocation certificate. Click the 'Create Revocation Certificate' button and you will be prompted for your passphrase. Enter your passphrase and click 'OK'. Save the revocation certificate file somewhere very safe, and then click the 'Continue' button. Click 'Done / Finish'.

**Step 20:**
In the 'Enigmail' menu at the top of the screen, click 'Key Management'. Right-click on your name and click 'Upload Public Keys to Keyserver'. This will ensure that other people are able to find your public key with ease in order to encrypt emails to you.

*Congratulations! You're now set up for secure PGP encrypted communication!*

## Sending a PGP encrypted email:

To send an encrypted email, click the 'Write' button beside 'Get Messages'. This will open up the compose email screen. Enter the email addresses of whomever you want to send the email to.

In the upper left corner you will see a small padlock icon and a small pencil icon. The padlock icon should be selected automatically, but if it is not then go ahead and select it now. This tells Enigmail to encrypt your email.

You probably won't have the PGP public key of the person you are sending the email to. Remember when you uploaded your Public Key to the keyserver in Step 13? The reason you did that was so that people could download your PGP Public Key in order to be able to encrypt emails to you. With Thunderbird and Enigmail, this is very easy.

Once you have finished writing your email, click the 'Send' button. You will see a pop up that states "Recipients not valid, not trusted or not found". Click the 'Download missing keys' button – this will download the PGP Public Key of the person you are sending the email to.

If that person (or at least one person on your list of recipients) has not yet set up PGP or has not uploaded their PGP Public Key to the keyserver, no key will be found for that recipient and you will not be able to encrypt the email to them. If this occurs – and if the email does not contain sensitive information – clicking the 'Send' button will send the email unencrypted. Advise that person to get their PGP set up and send them this guide!


## Receiving a PGP encrypted email:

In order to be able to read an email from somebody that they have encrypted to your PGP Public Key, just click on the email that they have sent to you. You will be prompted to enter your passphrase to decrypt the email, and you will have the option of letting Thunderbird remember your passphrase. Feel free to select this if you wish.


Welcome to the world of secure communications!

## Extras:

A note about protecting your PGP Private Key and Revocation Certificate:

*Revocation is incredibly useful in case your key gets compromised - it makes it easy for you to let people know that key is no longer in use / no longer safe, so be sure to keep your revocation certificate (that you saved when creating your key) somewhere safe and also keep a backup of it. Never upload your private key or your revocation certificate to any cloud storage or cloud email; treat the private key like a key to a safe - never share it with anyone - and treat the revocation certificate like your insurance to make the safe's contents useless should someone manage to get the key and get into the safe.*


A more detailed, feature rich guide for Windows users can be found here:
https://securityinabox.org/en/guide/thunderbird/windows/


A more detailed, feature rich guide for Mac users can be found here:
https://securityinabox.org/en/guide/thunderbird/mac/


Thunderbird and Enigmail are both highly configurable; you can read more about configuring Enigmail to your own specific requirements here:
https://enigmail.wiki/Configuration