# PGP FOR MAC O SX TOOL GUIDE

PGP for Mac O SX Tool Guide  
Encrypted email for Mac ----------------------------

**Lesson to read:**  
**?** [**Email**](umbrella://lesson/email)  
**Download Location:**  
 ? [GPG Suite](https://gpgtools.org/)   
? [Mozilla Thunderbird](https://www.mozilla.org/thunderbird/)   
? [Enigmail](https://www.enigmail.net/home/index.php)  
**Computer requirements:** An internet connection, a computer running Mac OS X, an email account  
**Version used in this guide:**? GPG Suite Beta 4  
? Mozilla Thunderbird 31.2.0  
? Enigmail 1.7.2  
**License:** Free Software; mix of Free Software licenses  
**Level:** Advanced  
**Other reading:** <http://support.gpgtools.org/>  
**Time required:** 30-60 minutes

**Using PGP will give you:**  
? The ability to protect your email communications from being read by anyone except their intended recipients.  
? The ability to prove that an email came from a particular person, instead of being a fake message sent by another sender (it is otherwise very easy for email to be fabricated). Both of these are important defenses if you're being targeted for surveillance or misinformation.

### 1.0 Before you start

To use Pretty Good Privacy (PGP), you will need to install some extra software that will work with your current email program. You will also need to create a private key, which you will keep private. The private key is what you will use to decrypt emails sent to you, and to digitally sign emails that you send to show they truly came from you. Finally, you'll learn how to distribute your public key?a small chunk of information that others will need to know before they can send you encrypted mail, and that they can use to verify emails you send.

This guide will show you how to use PGP with an Apple Mac (but not iPad or iPhone), with either the Mac's built-in Mail program, or with Mozilla Thunderbird, a popular alternative email program.

You can't currently use PGP directly with a web email service like Gmail, Hotmail, Yahoo! Mail, or Outlook Live. You can still use your webmail address; you?ll just have to configure it with the Thunderbird program on your computer.

**Note that both ends of the email conversation need to be using PGP-compatible software for it to work.**

People will normally use this only on their own personal devices, not on shared devices. Fortunately, PGP is available for most desktop computers and mobile devices, and you can point them to these guides to help them set up their own version. This guide is for Mac users.

### 2.0 Installing GPGTools on your Mac

PGP is an open standard, which means that more than one piece of software can use it. The software we're going to use for PGP is called the GPG Suite, from GPG Tools, because it works on Macs, is free for anyone to use, and it's open source: the underlying source code is available for anyone to check for bugs and backdoors.

Once the GPG Suite is installed, you can set up your keys for the first time, and then enable PGP on Apple Mail and, optionally, Thunderbird.

**Step 1: Install the program.**

First, go to <https://www.gpgtools.org/> in your browser and choose ?Download GPG Suite.

You'll end up with a disk image that you can click on to install the software. If you're not accustomed to installing third-party software on your computer, ask a nearby Mac expert ? this is a step most techies can help you with, even if they don't know PGP or encryption.

Clicking on install will give you a list of tools that will be added to your computer.

***What exactly am I installing here?***

These are tools will mostly work behind the scenes so that more than one program on your Mac can use PGP. Think of them as programs that other programs can use, rather than applications that you will use directly. GPGMail lets Apple Mail send and read PGP emails, GPG Keychain Access lets you keep your private and public keys in the same manner as you can save other passwords on your Mac.

GPGServices optionally adds a feature to OS X to let you use PGP directly in programs other than email (for instance, in a word processor). GPGPreferences is for changing PGP settings in Apple's preferences. Finally, MacGPG2 is the basic tool that any program needs to use to do encryption or signing.

In October 2014, the GPG Tools team announced that they would soon be charging for GPGMail, the part of their package that lets you use GPG with Apple's Mail application. This tutorial is about using GPG with Thunderbird, so it doesn't use that component. You can just use the zero-cost part of the GPG Suite, as outlined here, if you like. This option has the added benefit that all of these tools are "free software" meaning you are still allowed to freely examine, edit and redistribute GPG Mail's underlying source code, so they are even more secure. For more information, see GPG Tools' [own FAQ](https://gpgtools.org/news.html) on their decision.

Click "Continue" to install GPG Suite.

When the installation is complete, open GPG Keychain (found in your applications folder) if it doesn't automatically open and prompt you to generate your PGP keys after installation.  Click "New" to generate your PGP keys.

**Step 2: Create your PGP key**

Sometimes when you install new software, your computer will pester you with questions that have no obvious answer, without actually giving you any advice on how to reply. This is one of those times.

It's important to spend a little time thinking about the answers you'll give here, because changing your PGP key details can be difficult later, and if you?ve chosen to publish your key somewhere, you won?t be able to unpublish it. (There are still thousands of old public keys from the 1990?s floating around, with the names and old email addresses of the people who made them back then.)

PGP keys contain a name and an email address that link the key to you. The email address will be one of the ways others can discover which key to use when they are encrypting a message to you.

***When should I not put my real name or email address on my PGP key? When shouldn't I upload my key?***

For most people, it makes sense to add a real email address to your key, and upload it to the public keyservers ? it's how people will match the right key to you. They can send you an email directly, and know it will be encrypted with the right key, and when they receive a signed email from you, the digital signature will be marked with your name.

For some people, though, it will not make sense to add your real name to your key, for instance if your threat model means that having your identity publicly attached to your key (and the linked email address) is not a good idea. Edward Snowden communicated with journalists using PGP and an anonymous email address before he revealed his identity; his PGP key certainly wasn't marked with his name.

**Uploading your key is normal practice, but it can reveal that you're using encryption, even if you don't use your own name. Also, as we'll see, others might upload your key and associate their own key with it, implying that you and they have a connection. That can be harmful if you are communicating and don't want people to know it. It can also be troublesome if you're not communicating, but your attacker wants people to think that you are associated.**

Here's a rough guideline: if you're thinking about using a pseudonym generally, use that pseudonym (and alternative email) when labeling your key. If you are in a more dangerous environment, when you don't want people to know you're using PGP at all, or know who you are communicating with, don't upload your key to the public keyservers ? and make sure the small group of people you're communicating with know not to upload your key either. There are other ways of verifying keys that don't rely on them being available on the public key server ? see EFF?s guide to [Key Verification](https://ssd.eff.org/en/module/key-verification#overlay=en/node/37/) for more information.

Click the "Upload public key after generation" box if you'd like to let others find your key quickly so that they can send you encrypted messages. It's like adding your phone number to a public phone directory: you don't need it, but it's convenient for others.

Before generating the key, expand "Advanced options." You can leave the comment blank, and leave the key type "RSA and RSA (default)." But make sure to change the Length field to 4096.

**Your key will expire at a certain time; when that happens, other people will stop using it entirely for new emails to you, though you might not get any warning or explanation about why. So, you may want to mark your calendar and pay attention to this issue a month or so before the expiration date.**

It's possible to extend the lifetime of an existing key by giving it a new, later expiration date, or it's possible to replace it with a new key by creating a fresh one from scratch. Both processes might require contacting people who email you and making sure that they get the updated key; current software isn't very good at automating this. So make a reminder for yourself; if you don't think you'll be able to manage it, you can consider setting the key so that it never expires, though in that case other people might try to use it when contacting you far in the future even if you no longer have the private key or no longer use PGP.

When you're ready, click the "Generate key" button.

You computer will start generating both your public and private key. It shouldn't take any more than a couple of minutes to finish (it takes a while because to create your keys, your computer needs to gather random numbers. Think of it as your computer throwing a pair of dice many, many, many times.)

When you're done generating your key, you'll see it key listed in GPG Keychain Access. You can double-click on your key to see information about it, including its "fingerprint ??a unique way to identify your PGP key.

Now is a good time to generate a revocation certificate. (A revocation certificate is a file that you can generate that announces that you no longer trust that key. You generate it when you still have the secret key, and keep it for any future disaster.) In the future, if you ever worry that your private key has been copied by someone, you accidentally delete or lose your private key, or you forget your passphrase, you can tell everyone it has been revoked, or cancelled, by using a revocation certificate.

It's better to create one now, because you need the private key and passphrase to create a revocation certificate. If you leave it until later, you might lose one or the other, and then it will be too late. So create a certificate by clicking on your key, choosing the ?Key? menu entry, and then ?Create Revocation Certificate.? You'll be prompted for somewhere to save the file. You might want to keep it with a backup copy of the key (see next step).

**Step 3: Back up your PGP key**

If you lose access to your private key, you won't be able to decrypt any incoming PGP mail, or your old mail. On the other hand, you want to keep your private key as securely as you can.

You might want to save a backup copy to a USB key, which you keep safely hidden. You will only need it if you lose your original key, but for safety you will want to keep it out of the hands of your potential attackers.

***Is everything lost if my attackers get hold of my PGP private key?***

What if you get your Mac stolen, or your backup key is taken from you? Does that mean your PGP messages are vulnerable? No: if you've chosen a good passphrase and nobody has been able to learn what it is, you should still be mostly protected. To be safe, you may want to revoke your old key, and create a new PGP key. This won?t stop your old key from being able to decrypt your old email, but it will discourage other people from using the old key for their new emails to you.

To backup your key, open GPG Keychain Access. Select your key, and click ?Export? in the toolbar. Put your USB drive into the machine, and choose it in the ?Where? part of the ?Save As...? dialog. Check the ?Allow secret key export? checkbox.

**OPTION A) Configuring Apple Mail**

When you first open Apple Mail, you'll see a first run wizard that helps you set up your email address. Fill out your name, email address, and your email password and click "Create."

**Mail account setup wizard**

If you use popular free email services like Gmail, Mail should be able to automatically detect your email settings when you click Continue. If it doesn't, you may need to manually configure your IMAP and SMTP settings. Talk to the company you use for email, or ask someone technical who is familiar with your email provider (so, an IT person at work, or a technical friend who uses the same ISP as you. They don't need to know about PGP, but you can ask them ?Can you set up Apple Mail for me??).

Mail account setup auto-detect

When you're composing a new message, there are two icons just beneath the Subject field. There's a padlock (encrypt email) and a star (digitally sign email). If the padlock is closed it means this email will be encrypted, and if the star has a check in it, it means this email will be digitally signed.

**Sending PGP Signed or Encrypted Email**

You can always sign your email, even if the recipient doesn?t use PGP. Because digitally signing emails requires your secret key, Mail will pop up a window asking for your passphrase when you first sign an email.

You can only encrypt emails if the person you?re emailing uses PGP and you have that person?s public key. If the encryption padlock icon is unlocked and greyed out so you can't click on it, this means you first need to import the recipient's public key. Either ask them to send it to you, or use the GPG Keychain Access app to find the key to from a public keyserver.

To be absolutely safe, you'll need to verify the keys you get from the keyserver or your colleague. See EFF?s guide to [Key Verification](https://ssd.eff.org/en/module/key-verification#overlay=en/node/37/) for more information.

**OPTION B) Using PGP with Mozilla Thunderbird**

This walkthrough shows how to use GPG with the free, open source, Thunderbird mail client from Mozilla, together with the Enigmail plugin for email encryption.

First, download Thunderbird from <https://www.mozilla.org/thunderbird>, mount the disk image as you did with GPG Tools, and drag the Thunderbird into Applications. When you open it for the first time it will ask if you want to set it as your default email client. Go ahead and click "Set as Default.?

Then you will see the first run wizard. To set up your existing email address, click "Skip this and use my existing email." Then enter your name, email address, and the password to your email account.

If you use popular free email services like Gmail, Thunderbird should be able to automatically detect your email settings when you click Continue. If it doesn't, you may need to manually configure your IMAP and SMTP settings?ask your ISP, or a technical friend who knows about setting up email, to help. Sometimes, Thunderbird can just guess the correct settings.

**If you use two-factor authentication with Google (and depending on your threat model you probably should!) you cannot use your standard Gmail password with Thunderbird. Instead, you will need to create a new application-specific password for Thunderbird to access your Gmail account. See** [**Google's own guide**](https://support.google.com/mail/answer/1173270?hl=en)**for doing this.**

After you're done configuring Thunderbird to check your email, click "Done." Then click on "Inbox" in the top left to load your emails.

Now that you've installed and configured Thunderbird to work with your email, you need to install [Enigmail](https://www.enigmail.net/home/index.php), the GPG add-on for Thunderbird. In Thunderbird, click the menu icon in the top-right, and choose Add-ons.

Search for "enigmail" in the search box in the top right.

Click the Install button next to the Enigmail extension to download and install Enigmail. When it's done, click "Restart Now" to restart Thunderbird.

The first time you run Thunderbird with Enigmail enabled it opens the OpenPGP Setup Wizard. Click "Cancel." We will manually configure Enigmail instead.

Click the menu button, hover over Preferences, and choose Account Settings.

Go to the OpenPGP Security tab. Make sure "Enable OpenPGP support (Enigmail) for this identity" is checked. "Use specific OpenPGP key ID" should be selected, and if your key isn't already selected you can click "Select Key" to select it.

You should also check "Sign non-encrypted message by default," "Sign encrypted messages by default," and "Use PGP/MIME by default," but not (for most people) "Encrypt messages by default."

If most of the people that you email use PGP (or you would like to encourage them to do so), you may wish to encrypt by default. It would be ideal to encrypt all the emails you send, but that is not always possible. Remember that you can only send encrypted email to other people who use PGP, and you need to have their public keys in your keychain. For most people, manually choosing to encrypt each email you send will probably work best.

Then click "OK" to save all of the settings.

Congratulations, you now have Thunderbird and Enigmail set up! Here are a couple of quick pointers:

? You can click the menu button, hover over OpenPGP, and open Key Management to see the PGP key manager that's build-in to Enigmail. It's very similar to GPG Keychain Access, and it's your choice which you use.  
? When you're composing a new message, there are two icons in the bottom right corner of the window: a pen (digitally sign email) and a key (encrypt email). If the icons are gold it means they are selected, and if they're silver it means they're not selected. Click on them to toggle signing and encrypting the email you're writing.