# PGP FOR WINDOWS PC TOOL GUIDE

PGP for Windows PC Tool Guide  
Encrypted email for Windows ------------------------------

**Lesson to read:**  
**?** [**Email**](umbrella://lesson/email)  
**Download Location:**  
? GPG4Win  
? Mozilla Thunderbird  
? Enigmail  
**Computer requirements:** An internet connection, a computer running Mac OS X, an email account  
**Version used in this guide:**  
? Windows: Windows 7 Ultimate  
? Mozilla Thunderbird 24.6.0  
? Enigmail 1.7  
? GPG4Win 2.2.1  
**License:** Free Software; mix of Free Software licenses  
**Level:** Advanced  
**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.

**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 Windows users.

### 1.1 Overview

To use PGP to exchange secure emails you have to bring together three programs: GPG4Win (GNU Privacy Guard for Windows known as GnuPG), Mozilla Thunderbird and Enigmail.

? GnuPG is the program that actually encrypts and decrypts the content of your mail.  
? Mozilla Thunderbird is an email client that allows you to read and write emails without using a browser.  
? Enigmail is an add-on to Mozilla Thunderbird that ties it all together.

Note! What this guide teaches is how to use PGP with Mozilla Thunderbird, an email client program that performs a similar function to Outlook. You may have your own favorite email software program (or use a web mail service like Google Mail or Outlook.com). This guide won't tell you how to use PGP with these programs. You can choose either to install Thunderbird and experiment with PGP with a new email client, or you can investigate other solutions to use PGP with your customary software. We have still not found a satisfactory solution for these other programs.

**Using PGP doesn't completely encrypt your email: the sender and receiver information is still unencrypted and so is the subject line!**

Encrypting the sender and receiver information isn?t possible in the existing email system. What using Mozilla Thunderbird with the Enigmail add-on gives you is an easy way to encrypt the content of your email. Someone spying on your emails may still see the identities of the people you communicate with and when you email them.

You will first download all the software needed, install it, and then end with configuration and usage.

### 2 Downloading the software

### 2.1 Getting GPG4Win

You can get GnuPG (also known as GPG) on Windows by downloading the small installer from the GPG4Win download page.

Click on the most recent version of GPG4Win with GnuPG component only (Vanilla or Light) to download the GPG installer.

**Note: This version of GPG is available only on a web site that offers ?http? downloads, not secure ?https? downloads. If you are concerned that you may be targeted for surveillance by an organization that can tamper with your Internet connection, you may want to investigate more drastic solutions, such as downloading and running Tails, a secure operating system that replaces Windows.**

Many browsers will ask you to confirm whether you want to download this file. Internet Explorer 11 shows a bar at the bottom of the browser window with an orange border.

For any browser it is best to first save the file before proceeding, so *click the ?Save? button*. By default, most browsers save downloaded files in the Downloads folder.

### 2.2 Getting Mozilla Thunderbird

Go to the Mozilla Thunderbird website.

Click on the green button labelled ?Thunderbird Free Download.?

The Mozilla Thunderbird website will have detected your preferred language. If you want to use Thunderbird in another language click on the ?Other Systems & Languages? link and make your selection from there.

Many browsers will ask you to confirm if you want to download this file. Internet Explorer 11 shows a bar at the bottom of the browser window with an orange border.

For any browser, it is best to first save the file before proceeding, so click the ?Save? button. By default, most browsers save downloaded files in the Downloads folder.

### 2.3 Getting Enigmail

You can get Enigmail from the Enigmail website.

Many browsers will ask you to confirm if you want to download this file. Internet Explorer 11 shows a bar at the bottom of the browser window with an orange border.

For any browser it is best to first save the file before proceeding, so click the ?Save? button. By default, most browsers save downloaded files in the Downloads folder.

After downloading Enigmail, GPG4Win, and Mozilla Thunderbird you should have three new files in your Downloads folder:

### 3 Installing the software

### 3.1 Installing GPG4Win

Keep the Windows Explorer window open and double-click on gpg4win-xxx-x.x.x.exe. You'll be asked if you want to allow the installation of this program. Click the ?Yes? button.

A window will open, giving you an overview of what will be installed. Click the ?Next? button.

A window with the license agreement will open up. Click the ?Next? button.

The GPG4Win Vanilla package doesn't have components to select, so click the ?Next ?button again. For the GPG4Win-Light package, unselect all optional components to install GnuPG only.

Next, you'll have the ability to choose where GPG is installed. Don't change the default setting. Click the ?Next? button.

The next two windows will have some installation options. Click the ?Next? button and then click the "Install" button:

You will see a window with a progress bar?when it's done it will say ?Installation Complete.? Click the ?Next? button again.

Finally, you are at the last installation step. Remove the check mark next to ?Show the README file? and click the ?Finish? button.

That's it. Now let's move on to installing Mozilla Thunderbird.

### 3.2 Installing Mozilla Thunderbird

Similar to GPG4Win, you install Mozilla Thunderbird by double-clicking the Thunderbird Setup 24.6.0.exe file. As usual, you will be asked if you want to run this file. Click the ?Run? button.

You will be asked if you want to allow Mozilla Thunderbird to make a change to your computer by installing software. Click the ?Yes? button.

You will see the Mozilla Thunderbird Setup window. Click the ?Next? button.

Next, you will get a choice between a Standard setup and a Custom setup. Keep the Standard setup selection and click the ?Next? button.

You will be given a summary of where Mozilla Thunderbird's files will be installed. Click the ?Install? button.

When the installation process is complete, you will see a final window that enables you to launch Mozilla Thunderbird. Click the ?Finish? button.

### 3.3. Enigmail installation

**Step 1. Preparation**

When Mozilla Thunderbird launches for the first time, you will see this small confirmation window asking about some default settings. We recommend clicking the ?Set as Default? button.

Next, you will be asked whether you would like a new email address. Click the ?Skip this and use my existing email? button. Now you will configure Mozilla Thunderbird to send and receive email. If you are used to only reading and sending email through gmail.com, outlook.com, or yahoo.com, Mozilla Thunderbird will be a new experience, but it isn't that different overall.

**Step 2. Adding a mail account to Mozilla Thunderbird**

A new window will open.

Enter your name, email address, and the password to your email account. Mozilla doesn't have access to your password or your email account. Click the ?Continue? button.

In many cases Mozilla Thunderbird will automatically detect the necessary settings. In some cases Mozilla Thunderbird doesn't have complete information and you'll need to enter it yourself. Here is an example of the instructions Google provides for Gmail:

Incoming Mail (IMAP) Server - Requires SSL  
? imap.gmail.com  
? Port: 993  
? Requires SSL:Yes

Outgoing Mail (SMTP) Server - Requires TLS  
? smtp.gmail.com  
? Port: 465 or 587  
? Requires SSL: Yes  
? Requires authentication: Yes  
? Use same settings as incoming mail server

**Full Name or Display Name:** [your name or pseudonym]

**Account Name or User Name:** your full Gmail address (username@gmail.com). Google Apps users, please enter username@your\_domain.com

**Email address:** your full Gmail address (username@gmail.com) Google Apps users, please enter username@your\_domain.com

**Password:** your Gmail password

**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.**

When all the information is entered correctly, click the ?Done? button.

Mozilla Thunderbird will start downloading copies of your email to your computer. Try sending a test email to your friends.

**Step 3. Installing Enigmail**

Enigmail is installed in a different way from Mozilla Thunderbird and GPG4Win. As mentioned before, Enigmail is an Add-on for Mozilla Thunderbird. Click the ?Menu button,? also called the Hamburger button, and select ?Add Ons.?

You'll be taken to the Add-ons Manager tab.

Click the cog to bring up a small menu and select ?Install add-on from file? which will bring up a file-selection window.

The file selection window will very likely open to the Downloads folder. If it doesn't, go to the Downloads folder (where Enigmail was saved to) click on enigmail-1.7-tb+sm.xpi then click the ?Open? button.

Now you will see a small window asking you to confirm whether you want to install Enigmail. Click the ?Install Now? button.

After the Enigmail add-on is installed, Mozilla Thunderbird will ask to restart the browser to activate Enigmail. Click the ?Restart Now? button and Mozilla Thunderbird will restart.

When Mozilla Thunderbird restarts, an additional window will open up that will start the process of setting up the Enigmail add-on. Keep the ?Yes, I would like the wizard to get me started? button selected and click the ?Next? button.

Enigmail provides you with three options for handling mail. The default option is to encrypt emails if you have the ?public key? of another person, Enigmail will encrypt the email you send but leave emails unencrypted if you don't have the public key of the recipient yet. You also have the option to encrypt emails all the time to everyone with PGP keys, which means that you will have to find the public keys for people for whom you don't have them already, or turn off automatic encryption completely and only use PGP when directed.

We don't know what the appropriate option is for you, but believe the ?Convenient auto encryption? option to be a good choice. If you are in doubt, choose ?Don't encrypt my messages by default.? Click the ?Next? button.

Now you have an option to digitally sign all outgoing emails. Signing your email with PGP allows the recipient to check that you sent the message, and that the contents of the message were not tampered with. Click the ?Sign my messages by default? button to turn this feature on. The downside of doing this, however, is that it can also flag to anyone you send mail to that you use PGP. [In some parts of the world](www.cryptolaw.org/) (including China, Iran, Belarus, and some Middle-East states) using unlicensed encryption, even for personal use, is illegal, so you might have very good reasons to not let others know you use PGP.

Click the ?Next? Button.

Now you'll see an option to have Enigmail make some changes to the configuration of Mozilla Thunderbird.

If you click the Details button you can review what those changes are.

The following options can be unchecked (reenabled), for a more seamless transition, if you use PGP/Mime by default (we'll set that later):

? Disable flowed text  
? View message body as plain text  
? Do not compose HTML messages

The final option prevents potential problems in the encryption and decryption of your email. Be aware that selecting this box will remove the ability to send text that is bolded, underlined or colored. After reviewing the changes, click the ?OK button.?

The small window will close. Click the ?Next? button.

Now you will start creating your private key and public key.

### 4 Creating a public key and private key

Installation and setup of the Enigmail add-on is complete. Now you'll have the option of creating your public and private key pair. This assumes you have not created a private key before.

Click the ?Next? button.

Unless you have already configured more than one email account, Enigmail will choose the email account you've already configured. The first thing you'll need to do is come up with a strong passphrase for your private key. See the [**Passwords lesson**](umbrella://lesson/passwords) for more information on how to do this.

Make sure that you've written down this passphrase on paper until you have memorized it. Keep it somewhere where you can tell if it has been taken or viewed (like your wallet or purse). Just make sure you don't leave this paper lying around.

Click the ?Next? button.

Enigmail will display some information about your private key as well as the configuration settings. We recommend creating 4096-bit length keys. Click the ?Next? button.

**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.

Enigmail will generate the key and when it is complete, a small window will open asking you to generate a revocation certificate. This revocation certificate is important to have as it allows you to make the private key and public key invalid. It is important to note that merely deleting the private key does not invalidate the public key and may lead to people sending you encrypted mail that you can't decrypt.

Click the ?Generate Certificate? button.

A window will open to provide you a place to save the revocation certificate. While you can save the file to your computer, we recommend saving the file on a USB drive that you are using for nothing else and storing the drive in a safe spot. We also recommend removing the revocation certificate from the computer with the keys, just to avoid unintentional revocation.

Even better, save this file on a separate encrypted disk. Choose the location where you are saving this file and click the ?Save? button.

Now Enigmail will give you further information about saving the revocation certificate file again. Click the ?OK? button.

Finally, you are done with generating the private key and public key. Click the ?Finish? button.

### 5 Optional steps

### 5.1 Display long key-IDs

The next steps are completely optional but they can be helpful when using OpenPGP and Enigmail. Briefly, the Key ID is a small part of the fingerprint. When it comes to verifying that a public key belongs to a particular person the fingerprint is the best way. Changing the default display makes it easier to read the fingerprints of the certificates you know about. Click the configuration button, then the Enigmail option, then Key Management.

A window will open showing two columns: Name and Key ID.

On the far right there is a small button. Click that button to configure the columns. Unclick the Key ID option and click the Fingerprint option.

Now the columns will look like this:

Now you are set up to send and receive regular and encrypted email. Next you will go through the steps of actually finding the people to exchange encrypted mail with.

### 5.2 Using PGP/MIME

There is a final optional configuration step is to enable PGP/MIME which makes sending encrypted and signed attachments easier.

You can find this setting by clicking on the Menu Button, hovering over Options, then clicking Account Settings. The Account Settings window will open.

When the Account Settings window opens click the OpenPGP Security tab then click the checkbox next to Use PGP/MIME by default. Next click the OK button. Now Enigmail will use PGP/MIME by default.

**Using PGP doesn't completely encrypt your email so that the sender and received information is encrypted. Encrypting the sender and receiver information would break email. Using Thunderbird with the Enigmail add-on gives you an easy way to encrypt and decrypt the content of your email.**

### 6.1 Letting others know you are using PGP

Now that you have PGP, you want to let others know that you are using it so they can also send you encrypted messages using PGP.

Let's look at three different ways you can let people know you are using PGP.

**a) Let people know you are using PGP with an email**

You can easily email your public key to another person by sending them a copy as an attachment.

Click the ?Write? button in Mozilla Thunderbird.

Fill in an address and a subject, perhaps something like ?my public key,? click the Enigmail menu and select the ?Attach My Public Key? option.

You can send the email and the recipient will be able to download and use the public key you sent.

If this method is used, it's a good idea to have the recipient verify your public key's fingerprint over some other form of communication, in case email is already being intercepted and tampered with.

**b) Let people know you are using PGP on your website**

In addition to letting people know via email, you can post your public key on your website. The easiest way is to upload the file and link to it. This guide won't go into how to do those things, but you should know how to export the certificate as a file to use in the future.

Click the configuration button, then the Enigmail option, then Key Management.

Highlight the certificate in bold, then right-click to bring up the menu and select Export keys to file.

A small window will pop up with three buttons. Click the ?Export Public Keys Only? button.

Make sure you don't click the ?Export Secret Keys? button because exporting the secret key could allow others to impersonate you if they are able to guess your password.

Now a window will open so you can save the file. In order to make it easier to find in the future please save the file to the Documents folder.

Now you can use this file as you wish.

**c) Uploading to a keyserver**

Keyservers make it easier to search for and download public keys. Most modern keyservers are synchronizing, meaning that a public key uploaded to one server will eventually reach all servers.

Although uploading your public key to a keyserver might be a convenient way of letting people know that you have a public PGP certificate, you should know that due to the nature of how keyservers work, there is no way to delete public keys once they are uploaded, you can only mark them as revoked.

**Before uploading your public key to a keyserver, it is good to take a moment to consider whether you want the whole world to know that you have a public key without the ability to remove this information at a later time.**

If you choose to upload your public key to keyservers, you will go back to the Enigmail Key Management window.

Click the Keyserver menu item and select the Upload Public Keys option.

### 6.2 Finding other people who are using PGP

**a) Getting a public key by email**

You might get a public key sent to you as en email attachment.

Double-click on the new message, and it'll open a new tab. Notice the attachment at the bottom of the window. Right-click on the attachment and select ?Import OpenPGP Key.? A small window will open giving you the results of the import. Click the OK button.

If you open up the Enigmail key management window again, you can check the result. Your PGP key is in bold because you have both the private key and the public key. The public key you just imported is not bold because it doesn't contain the private key.

**b) Getting a public key as a file**

It's possible that you get a public key by downloading it from a website or someone might have sent it through chat software. In a case like this, you will assume you downloaded the file to the Downloads folder.

Open the Enigmail Key Manager and click on the ?File? menu. Select ?Import Keys from File.?

The public key might have very different file name endings such as .asc, .pgp, or .gpg. Select the file and click the ?Open? button.

A small window will open, giving you the results of the import. Click the ?OK? button.

**c) Getting a public key from a key server**

Keyservers can be a very useful way of getting public keys. Try looking for a public key. Open up the key manager then click the ?Keyserver? menu and select ?Search for Keys.?

A small window will pop up with a search field. You can search by a complete email address, a partial email address, or a name. In this case, you will search for certificates containing ?eff.org.?

A larger window will pop up with many options. If you scroll down you'll notice some certificates are italicized and grayed out. These are certificates that have either been revoked or expired on their own.

Let's take the public keys of Danny O'Brien for example, he has one expired or revoked certificate and one valid certificate. Select the valid certificate by clicking the box on the left then press the OK button.

In some cases a person may have more than one certificate, all appearing valid. Note that it's possible for anyone to upload a public certificate for anyone else, and that one of these keys may not belong to the person that owns the email address associated with it. In this case, verifying the fingerprint is extremely important.

A small notification window will pop up letting you know if you succeeded:

The Enigmail Key Manager will now show you the added certificates:

### 7.1 Sending PGP encrypted mail

Now you will send your first encrypted email to a recipient. In the main Mozilla Thunderbird window click the ?Write? button. A new window will open.

Write your message, and enter a recipient. For this test, select a recipient whose public key you already have. Enigmail will detect this and automatically encrypt the email.

*Note that the subject line won't be encrypted, so choose something innocuous, like ?hello.?*

When you click the ?Send? button, you'll be given a window to enter the password to your PGP Key. Remember this is different from your email password!

Enter your password then click the ?OK? button and your email will be encrypted and sent.

The body of the email was encrypted and transformed. For example this text:

Will be transformed into:

### 7.2 Receiving PGP encrypted mail

Let's go through what happens when you receive encrypted email. Notice that that Mozilla Thunderbird is letting you know you have new mail. Click on the message.

A small window opens asking you for the password to the PGP key. Remember: Don't enter your email password. Click the ?OK? button.

Now the message will show up decrypted

### 8 Revoking the PGP Key

**a) Revoking your PGP Key through the Enigmail interface**

The PGP keys generated by Enigmail automatically expire after five years. So if you lose all your files, you can hope that people will know to ask you for another key once the key has expired.

You might have a good reason to disable the PGP key before it expires. Perhaps you want to generate a new, stronger PGP key. The easiest way to revoke your own PGP key in Enigmail is through the Enigmail Key Manager.

Right-click on your PGP key (it's in bold), and select the ?Revoke Key? option.

A window will pop up letting you know what happens and asking for your confirmation. Click the ?Revoke Key? button.

The password window opens, enter your password for the PGP key and click the ?OK? button.

Now a new window will open up letting you know you succeeded. Click the ?OK? button.

When you go back to the Enigmail Key Management window you'll notice a change to your PGP key. It is now grayed out and italicized.

**b) Revoking a PGP Key with a revocation certificate**

As mentioned before, the PGP keys generated by Enigmail automatically expire after five years. So if you lose all your files you can be sure that people will know to ask you for another key once the key has expired.

Like we mentioned before, you might have a good reason to disable the PGP key before it expires.

Similarly, others might have good reasons to revoke an existing key.

You might get sent revocation certificates from friends as a notice that they want to revoke their key.

In the previous section you might have noticed that Enigmail generates and imports a revocation certificate internally when you use the Enigmail Key Manager to revoke a key. Since you already have a revocation certificate, you will use the one you generated earlier to revoke your own key.

Start with the Enigmail Key Manager and click the ?File? menu and select ?Import Keys from File.?

A window will open up so you can select the revocation certificate. Click on the file, and click the ?Open? button.

You'll get a notification that the certificate was imported successfully and that a key was revoked. Click the ?OK? button.

Once you click the ?OK? button, you'll be taken back to the Enigmail Key Manager and you see the certificate you revoked greyed out and italicized.

If the key you revoked is your own, and you previously uploaded your public key to the key servers, you will want to re-upload the now-revoked key to the key servers, so that others see not to use it anymore.

Now that you have all the proper tools, try sending your own PGP-encrypted email.