Privacy Café

How to use PGP on a Windows PC

Emails can be intercepted by third parties as they are being sent from one email server to another. There are two ways to prevent this from happening: You can secure the communication between the email servers, or encrypt the contents of the emails. Securing the communication between email servers is good but does not protect emails from evesdropping while being stored on the servers. The second and much safer option is to encrypt the message itself end-to-end. A popular and freely available encryption method for email is **PGP (Pretty Good Privacy)**, also known as **OpenPGP** and **GnuPG**.

PGP is a computer program that protects your email communications from being read by anyone except their intended recipients. It can protect against companies, governments, or criminals spying on your Internet connection or your computer. It can also be used 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.

To use PGP, you will need to install some extra software that will work with your current email address. You will also need to create a **"private key"**, which you will keep private. The private key is what you need 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 send you encrypted mail, and that they can use to verify emails you send.

OVERVIEW

To use PGP to exchange secure emails you have to bring together three programs: Gpg4win, Thunderbird and Enigmail. Gpg4win is the program that actually encrypts and decrypts the content of your mail, Thunderbird is an email client that allows you to read and write emails without using a browser, and Enigmail is an addition (or "add-on") to Thunderbird that ties it all together.

Note! Using PGP only encrypts the content and attachments of your email: the sender and receiver information (so-called metadata) is still unencrypted and so is the subject line. Encrypting email metadata is unfortunately technically impossible.

GETTING GPG4WIN AND THUNDERBIRD

You can get Gpg4winfromhttps://www.gpg4win.org. Click on the green download button for Gpg4win-Vanilla. Then go to the Thunderbird website at https://www.mozilla.org/thunderbird and click on the green button labelled "Thunderbird Free Download" to download the Thunderbird email client. Go to the folder in which you have downloaded the two program files (usally your download folder or desktop) and install Gpg4win first. Run through the installation procedure without changing the standard settings. Next, install Thunderbird the same way.

After successful installation of both Gpg4win and Thunderbird, launch Thunderbird for the first time. In the confirmation window 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 Thunderbird to send and receive email. If you are used to only reading and sending email through gmail.com, outlook.com, or yahoo.com, Thunderbird will be a new experience, but it is still very similar to Outlook.

A new window will open. Enter your name, email address, and the password to your email account and click the "Continue" button. In many cases, Thunderbird will automatically detect the necessary settings. In some cases Thunderbird doesn't have complete information on mail servers and you'll need to enter it yourself. You should find the information needed via the help pages of your email provider. When all the information is entered correctly, click the "Done" button. Thunderbird will start synchronizing with your email account. From now on, all you see in Thunderbird is a 1:1 copy of your email account. Try sending a test email to your friends.

GETTING AND SETTING UP ENIGMAIL

Enigmail is installed differently from Thunderbird and Gpg4win. As mentioned before, Enigmail is an Add-on for Thunderbird. Click the "Menu button" at the very right end of the button bar and select "Add Ons." You'll be taken to the Add-ons Manager tab.

Use the Add-ons search bar to find and install Enigmail. After installation, you will need to restart Thunderbird. After that, 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. We believe this option to be a good choice for most users.

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 (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 twice without making any further changes.

You finally need to manually enable PGP/MIME which makes sending encrypted and signed attachments easier. You can find this setting by clicking on Thunderbird's Menu Button, hovering over "Options", then clicking "Account Settings". In the Account Settings window, click the OpenPGP Security tab then select "Use PGP/MIME by default". Next click the OK button.

CREATING A PUBLIC KEY AND PRIVATE KEY

For an explanation of the private and public keys, please see our one-pager on "what is encyrption".

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

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 password for your private key. A strong password is a random selection of at least 10 upper and lower case letters, numbers and special characters. It must not contain any words you could find in a dictionary. Make absolutely sure that you've memorised your password (for example write it down on paper, and only throw it away once you've memorised the password). 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.

You can set an automatic expiration date for your key, after which your key pair will need to be replaced with a new one. The easiest way is to not set an expiration date at all and instead revoke your key manually should you ever stop using it in the future.

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 (in case you want to stop using it). 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.

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

Privacy Café

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. You can easily email your public key to another person by sending them a copy as an attachment. But you reach a wider audience by uploading your public key to a so-called key server. Key servers are like public phone books: they make it easier to search for and download public keys from people all over the world. Most key servers synchronize among each other, meaning that a public key uploaded to one server will eventually reach all servers. Although uploading your public key to a key server might be a convenient way of letting people know that you have a PGP public key, it is good to take a moment to consider whether you want the whole world to know that you use PGP without the ability to remove this information at a later time.

If you choose to upload your public key to key servers, you will go back to the Enigmail Key Management window. Click the Key server menu item and select the Upload Public Keys option.

FINDING OTHER PEOPLE WHO ARE USING PGP

You might get a public key sent to you as an email attachment. In this case, right-click on the attachment and select "Import OpenPGP Key." It's also possible that you get a public key by downloading it from a website or someone might have sent it through chat software. 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.

Finally, key servers can be a very useful way of getting public keys. Open up the key manager then click the "Key server" menu and select "Search for Keys." You can search by a complete email address, a partial email address, or a name. In the search results window you'll notice some public keys are italicized and grayed out. These are keys that have either been revoked or expired on their own. In some cases a person may have more than one public key, all appearing valid. Note that it's possible for anyone to upload a public key 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 key's fingerprint is extremely important.

SENDING AND RECEIVING PGP ENCRYPTED MAIL

Now you will send your first encrypted email to a recipient. In the main 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 private 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.

Let's go through what happens when you receive encrypted email. Notice that that Thunderbird is letting you know you have new mail. Click on the message. A small window opens asking you for the password to the private key. Now the message will show up decrypted.

REVOKING THE PGP KEY

You might have a good reason to disable your key before it expires (if it expires at all). Perhaps you want to generate a new, stronger PGP key or your key or password has been compromised. Note that you only have to do this if you do not want to continue using your PGP key!

From the previous section you remember that you generated a revocation certificate which you can now use 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. 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 keyservers, you will want to re-upload the now-revoked key to the key servers, so that others see not to use it anymore.