# PIDGIN TOOL GUIDE

Pidgin Tool Guide  
Encrypted instant messaging for Windows ---------------------------------------

**Lesson to read:**  
**?** [**Sending a message**](umbrella://lesson/sending-a-message)  
**Download Location:**  
? <https://pidgin.im/download/>   
? <https://otr.cypherpunks.ca/>  
**Computer requirements:** An internet connection, a computer running Windows XP or higher, and an XMPP (Jabber) account.  
*(Pidgin is able to work with many chat systems, such as AIM, Facebook, Google Talk, MSN, MXit and Yahoo, but here we'll focus on XMPP, formerly known as Jabber)*  
**Version used in this guide:**  
? Windows 7 Ultimate  
? Pidgin 2.10.9, pidgin-otr 4.0.0-1  
**License:** Free Software; mix of Free Software licenses  
**Level:** Beginner  
**Other reading:** <https://pidgin.im/cgi-bin/mailman/listinfo/support>  
**Time required:** 20 minutes

**Using OTR with Pidgin will give you:**  
? The ability to organise and manage some of the most popular instant messaging services through a single program.  
? The ability to have encrypted chats on instant messenger, without the server logging those chats.  
? The ability to make sure that the person you are chatting with really is that person.

### 1.0 Before you start

Pidgin is an easy-to-use, instant messaging client for Windows that uses a protocol called OTR (Off-the-record), which allows users to have confidential conversations.

? Note: OTR should not be confused with Google's ?Off the record,? which just disables chat logging, and does not have encryption or verification capabilities.  
? Pidgin supports the following IM services: AIM, Bonjour, Gadu-Gadu, Google Talk, Groupwise, ICQ, IRC, MSN, MXit,MySpaceIM, SILC, SIMPLE, Sametime, Yahoo!, Zephyr and any IM clients running the XMPP messaging protocol.  
? Pidgin does not permit communication between different IM services. For instance, if you are using Pidgin to access your Google Talk account, you will not be able to chat with a friend using an ICQ account.  
? However, Pidgin can be configured to manage multiple accounts based on any of the supported messaging protocols. That is, you may simultaneously use both Gmail and ICQ accounts, and chat with correspondents using either of those specific services (which are supported by Pidgin).  
? Pidgin, automatically logs conversations by default, however you do have the ability to disable this feature. That said, you do not have control over the person with whom you are chatting?she could be logging or taking screenshots of your conversation, even if you yourself have disabled logging.

**Why should I use Pidgin + OTR?**

When you have a chat conversation using Google Hangouts or Facebook chat on the Google or Facebook websites, that chat is encrypted using HTTPS, which means the content of your chat is protected from hackers and other third parties while it?s in transit. It is not, however, protected from Google or Facebook, which have the keys to your conversations and can hand them over to authorities.

After you have installed Pidgin, you can sign in to it using multiple accounts at the same time. For example, you could use Google Hangouts, Facebook, and XMPP simultaneously. Pidgin also allows you to chat using these tools without OTR. Since OTR only works if both people are using it, this means that even if the other person does not have it installed, you can still chat with them using Pidgin.

Pidgin also allows you to do out-of-band verification to make sure that you?re talking to the person you think you?re talking to. For every conversation, there is an option that will show you the key fingerprints it has for you and the person with whom you are chatting. A "key fingerprint " is a string of characters like "342e 2309 bd20 0912 ff10 6c63 2192 1928,? that?s used to verify a longer public key. Exchange your fingerprints through another communications channel, such as Twitter DM or email, to make sure that no one is interfering with your conversation.

**Limitations: When should I not use Pidgin + OTR?**

Pidgin is a complex program, which has not been written with security as a top priority. It almost certainly has bugs, some of which might be used by governments or even big companies to break into computers that are using it. Using Pidgin to encrypt your conversations is a great defence against the kind of untargeted surveillance that is used to spy on everyone's Internet conversations, but if you think you will be personally targeted by a well-resourced attacker (like a nation-state), you should consider stronger precautions, such as PGP -encrypted email.

### 2 Downloading and installing

### 2.1 Getting Pidgin

You can get Pidgin on Windows by downloading the installer from the Pidgin download page.

Click on the *purple* DOWNLOAD tab. ***Don't*** *click the green Download Now button because you?ll want to choose a different installer file.*

You'll be taken to the download page.

*Again,* ***don't*** *click the green Download Now button because we want to choose a different installer file.*

The default installer for Pidgin is small because it doesn't contain all the information and downloads the files for you. This sometimes fails so you will have a better experience with the ?offline installer? which contains all the necessary installation material.

Click the ?**offline installer**? link. You will be taken to a new page titled ?Sourceforge? and after a few seconds, a small popup will ask whether you want to save a file.

? Note: While Pidgin's download page uses "HTTPS" and is therefore relatively safe from tampering, the website it directs you to to download the Windows version of Pidgin is currently Sourceforge, which uses unencrypted "HTTP," and therefore offers no protection. That means that the software you download could be tampered with before you download it. This risk would mostly come from either someone with access to the local Internet infrastructure attempting to conduct targeted surveillance against you personally (for instance a malicious hot-spot provider), or a state or government planning to distribute compromised software to many users. The [HTTPS Everywhere](https://www.eff.org/https-everywhere) extension can rewrite Sourceforge download URLs to HTTPS, so it's recommended you install HTTPS Everywhere before downloading any other software. Additionally, in our experience, Sourceforge often has confusing full-page ads on its download pages that can trick people into installing something they may not want to.  You can install an ad blocker before any other software to avoid these confusing ads.

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 OTR

You can get pidgin-otr, the OTR plugin for Pidgin, by downloading the installer from the [OTR download page](https://otr.cypherpunks.ca/).

Click the ?Downloads? tab to be taken to the ?Downloads? section of the page. Click the ?Win32 installer for pidgin? link.

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.

After downloading Pidgin and pidgin-otr you should have two new files in your

Downloads folder:

### 2.3 Installing Pidgin

Keep the Windows Explorer window open and double-click on pidgin-2.10.9-offline.exe. You'll be asked if you want to allow the installation of this program. Click the ?Yes? button.

A small window opens asking you to select a language. Click the ?OK? button.

A window opens up giving you a quick overview of the installation process. Click the ?Next? button.

Now you get a license overview. Click the ?Next? button.

Now you can see what different components are installed. Don't change the settings. Click the ?Next? button.

Now you can see where Pidgin will be installed. Don't change this information. Click the ?Next? button.

Now you'll see a window with scrolling text until it says ?Installation Complete.? Click the ?Next? button.

Finally, you?ll see the last window of the Pidgin installer. Click the ?Finish? button.

### 2.4 Installing pidgin-otr

Go back to the Windows Explorer window and open and double-click on pidgin-otr-4.0.0-1.exe. You'll be asked if you want to allow the installation of this program. Click the ?Yes? button.

A window opens up giving you a quick overview of the installation process. Click the ?Next? button.

Now you get a license overview. Click the ?I Agree? button.

You will see where pidgin-otr will be installed. Don't change this information. Click the ?Install? button.

Finally, you?ll see the last window of the pidgin-otr installer. Click the ?Finish? button.

### 3 Configuration

### 3.1 Configuring Pidgin

Go to the Start menu, click the Windows icon, and select Pidgin from the menu.

### 3.2 Adding an account

When Pidgin launches for the first time, you will see this welcome window giving you an option to add an account. Since you don't have an account configured yet, click the ?Add? button.

Now you'll see the ?Add Account? window.

***Pidgin is able to work with many chat systems, such as AIM, Facebook, GoogleTalk, MSN, MXit and Yahoo, but here we'll focus on XMPP, formerly known as Jabber.***

At the Protocol entry, select the ?XMPP? option.

At the Username entry, enter your XMPP username.

At the Domain entry, enter the domain of your XMPP account.

At the Password entry, enter your XMPP password.

Checking the box by the ?Remember password? entry will make accessing your account easier. Be aware that by clicking ?Remember password,? your password will be saved on the computer, making it accessible to anyone who may happen to access your computer. If this is a concern, do not check this box. You will then be required to enter your XMPP account password every time you start Pidgin.

### 3.3 Adding a Buddy

Now you will want to add someone to chat with. Click the ?Buddies? menu and select ?Add Buddy.? An ?Add Buddy? window will open.

At the ?Add Window,? you can enter the username of the person you want to chat with. This other user does not have to be from the same server, but does have to use the same protocol, such as XMPP.

At the ?Buddy's username? entry, enter your buddy?s username with the domain name. This will look like an email address.

At the ?(Optional) Alias? entry, you can enter a name of your choice for your buddy. This is entirely optional, but can help if the XMPP account of the person you are chatting with is hard to remember.

Click the ?Add? button.

Once you have clicked the ?Add? button, Boris will get a message asking if he gives authorization for you to add him. Once Boris does, he adds your account and you will get the same request.

Click the ?Authorize? button.

### 3.4 Configuring the OTR plugin

Now you will configure the OTR plugin so you can chat securely. Click the ?Tools? menu and select the ?Plugins? option.

Scroll down to the ?Off-the-Record Messaging? option, and check the box.

Click on the ?Off-the-Record Messaging? entry and click the ?Configure Plugin? button.

Now you will see the ?Off-the-Record Messaging? configuration window. Notice that is says ?No key present.?

Click the ?Generate? button.

Now a small window will open and generate a key. When it is done, click the ?OK? button.

You'll see new information: a 40 character string of text, broken up into 5 groups of eight characters. This is your OTR fingerprint. Click the ?Close? button.

Now click the ?Close? button on the Plugins window.

### 4.0 Chatting securely

You are now able to chat with Boris. The two of you can send messages back and forth. However, we're still not chatting securely. Even if you are connecting to the XMPP server, it is possible that the connection between you and Boris is not secure from snooping.

If you look at the chat window, notice that it says ?Not private? in red on the bottom right. Click the ?Not private? button.

A menu will open up, select ?Authenticate buddy.?

A window will open up. You are asked: ?How would you like to authenticate your buddy??

The drop-down has three options:

**Option 1: Shared secret**

A shared secret is a line of text you and the person you want to chat have agreed to use ahead of time. You should have shared this in person and never have exchanged it over insecure channels such as email or Skype.

You and your buddy need to enter this text together. Click the ?Authenticate? button.

The shared secret verification is useful if you and your buddy have already made arrangements to chat in the future but haven't yet created OTR fingerprints on the computer you are using.

**Option 2: Manual fingerprint verification**

Manual fingerprint verification is useful if you were already given your buddy's fingerprint and are now connecting with Pidgin. This will not be useful if your buddy changed computers or had to create new fingerprints.

If the fingerprint you were given and the fingerprint on the screen match, select ?I have? and click the ?Authenticate? button.

**Option 3: Question and answer**

Question and answer verification is useful if you know your buddy but have not established a shared secret nor had a chance to share fingerprints. This method is useful to establish verification based on something both of you know, like a shared event or memory.

Enter the question you want to ask. Don't make it so simple that someone can guess it easily, but don't make it impossible. An example of a good question would be ?Where did we go for dinner in Minneapolis?? And example of a bad question would be ?Can you buy apples in Tokyo??

**The answers must match exactly; so keep that in mind when choosing an answer to your question. Capitalization matters, so you might consider including a note like (for example: use capitals, lower case).**

Enter the question and answer then click the ?Authenticate? button.

Your buddy will have a window open with the question displayed asking for the answer. They will have to answer and click the ?Authenticate? button. Then they will receive a message letting them know if the authentication was successful.

Once your buddy had completed the authentication procedure, you will get a window letting you know the authentication succeeded.

Your buddy should also verify your account so that both of you can be sure that the communication is secure. Here is what it would like for Akiko and Boris. Notice the green ?Private? icons in the lower right of the chat window.

### 5 Working with other software

The mechanisms to verify the authenticity should work between different chat software such as Jitsi, Pidgin, Adium, and Kopete. You are not required to use the same chat software to use chat over XMPP and OTR, but sometimes there are errors in the software. Adium, a chat software for OS X, has an error receiving the Question and Answer verification. If you find that verifying others is failing for you when you are using Question and Answer verification, check whether they are using Adium and see if you can use another verification method.