Using Encrypted E-Mail and Encrypted Instant Messenger to Avoid "The Man"

by Michael W. Dean, Freedom Feen.
http://www.freedomfeens.com
Article intro by MWD. Tutorials done with help from some other freedom feens, credited in each tutorial.

WHY ENCRYPTION?
You have a safe for your guns, right? Computer encryption is a safe for your *thoughts*.

Other than owning the means to physically protect yourself against physical aggression, and knowing how to use those means, one of the most effective things you can do on a personal level to protect yourself from danger is using computer encryption.

I cannot stress this enough. I'll even put it in tough-love terms that might piss you off: If you are not yet using encryption and you spend your next hour listening to some talk radio show that's just bitching about the gub'mint (even if it's *my* talk radio show), instead of installing and testing one of the encryption methods shown below, YOU ARE A TALKER, NOT A DOER.

> NOTE: If you're using Hushmail and *think* you're actually using secure encryption, you're not. Keep reading....

Even if you say "But I have nothing to hide!", you should be using encryption. Because what's considered "illegal" expands every day. One reason for this is lawmakers. Lawmakers have to keep making more laws or they're out of a job.

A lot of us talk a lot about "LibPar", that is, "Libertarian Paradise." We speculate what life might be like if the government would just get out of our damn way. LibPar may come next year, or it may come in 500 years. But by using encryption, you and your friends can literally create government-free temporary autonomous zones *today* where you can hang out and not be hassled....Where you can say whatever you want without some sub-literate gov-goon hired off a pizza box reading your every thought. It's a freeing thing to do, it keeps you safer, and reduces the amount of fear in your life. And less fear is a good thing we could all use more of in these crazy times.

Many liberty people seem far more interested in spreading fear than doing anything about it. This statement isn't singling out any individual people, and there are exceptions. But many people are far more into yelling "THE SKY IS FALLING!" than putting on a virtual hard hat to protect their head from falling sky pieces.

This was very apparent to me the day I finally left Facebook for good. The straw that broke the antelope's back, for me, was the difference in responses to two things I posted on the same day…The first was a link to an article about new ways the government is

planning to read your e-mail. The second was a link to an article we wrote on setting up encrypted e-mail *so the government can't read your e-mail*.

The thing about government reading your e-mail got 170 likes and 76 shares. The piece about actually DOING SOMETHING ABOUT IT got 10 likes and 3 shares. To me, that says all you need to know about Facebook and why you shouldn't be on there. Most people on Facebook would rather live in a fear-spiral echo chamber than actually DO ANYTHING to protect themselves. I call it "Fear porn", and it's not a type of porn I'm interested in consuming.

This is true outside of Facebook too. A lot of "liberty media" is concerned with spreading the latest "tyranny today", showing the latest news of how the gub'mint is screwing everyone this week. But after a few years of this you realize "Yeah, governments screw people over. That's what they *do*. But what can I do, I'm just one person?"

One of the easiest answers, of course, is to USE ENCRYPTION! And get your friends to use it too.

If you haven't left in a huff to go check your Facebook and complain about the government, here are two tutorials, one on using encrypted e-mail, the other on encrypted instant messenger.

Licking The Envelope (An easy guide on how to use PGP ENCRYPTED E-MAIL)

by MWD

–A collaborative tutorial by freedom feens Link Porterfield, Adam Witthauer and Michael W. Dean. Tech checked and improved by Randall Perry and Randy Jasky. This is PART ONE in an ongoing series on the Freedom Feens Blog on easy computer security for honest people who just don't like gubmint idiots hired off an ad on a pizza box reading their love letters and chats about the weather.

Many people would rather spend hours a day complaining on the Internet about how the government is constantly deleting our rights (like PRIVACY) than spend an hour or two learning to actually PROTECT their privacy. Learn to keep your e-mail PRIVATE while doing so is still legal:

The so-called "Patriot Act" has shredded the US Bill of Rights. The US Government is building a giant data center in Utah to spy on every electronic communication every American makes all day, every day. (We call it, and the ideology behind it, "The Central Scrutinizer.") Cops are demanding e-mails and text messages be kept longer and longer, "just in case." Police in Michigan and California are even doing traffic stops and copying the contents of people's handheld internet devices and phones WITHOUT A WARRANT. If state and federal mucking around with your Internets isn't enough, The United Nations is trying to take over the Internet, right NOW, and doesn't want you to know they're doing it.

All of this has caused some who don't normally question the Central Scrutinizer's legitimacy to reflect on the privacy and security of their own emails. Most freedom feens like us are already likely to question why it takes little more than a subpoena, or sometimes just a friendly (or not so friendly) phone call to an email service provider, for law enforcement (at any level) to obtain *all* of your email. After all, it is potentially the digital equivalent of making off with all the letters and parcels you've received in your lifetime, and such action would at least require an all too readily issued warrant from a judge for any paper mail seized from your house to be admissible in court proceedings.

The good news is you can do something easy RIGHT NOW to make sure that the Central Scrutinizer winds up with nothing but gibberish when it snacks on your email.

You don't have to be a "criminal" (i.e. "actual violent bad guy") to need to hide your tracks. It's getting to the point where completely moral, normal things seem suspect to the Central Scrutinizer. LEARN TO USE PGP, AND USE IT! DO IT NOW!

Today we're going to teach you how to "lick the envelope" on your email. You may not think of it as such, but your email is like a postcard. OpenPGP encrypted email seals your message in an "envelope" to keep the contents shielded from prying eyes. OpenPGP is not some lightweight airmail envelope. It is one of those Tyvek envelopes that resists being opened even at knife point, if you cased a Tyvek envelope in diamond-hard steel.

While sending a "digital postcard" may initially seem just as innocuous as sending a regular postcard, there are some special considerations in the digital world. After all, your postman could likely care less about the mundane stuff you would be willing to put on a postcard. But in the digital world, you don't have to worry about just a few "probably too busy and don't care" postmen handling your postcard. Your "digital postcard" contains data that can be effortlessly collected and stored indefinitely, and easily mined by search algorithms for certain key words. This is not paranoia, this is something Gmail and Facebook already do with targeted marketing. They already mine data from your emails and profile to determine what ads you would be most interested in. Ever send an e-mail

by Gmail and talk to your friend about fishing, then get ads for fishing gear on the next site you view from a Google search? That's how they do it. Ever send a private message to a friend on Facebook about some band, then get ads on Facebook trying to sell you tickets to that band's next tour? That's how they do it. Facebook isn't even a mere postcard, it's more like standing in the town square with a bullhorn talking to a friend across a crowd of people.

"But isn't email encryption just for hackers and conspiracy freaks?" "What if I have nothing to hide?" There's a military term that has come into the mainstream since the beginning of the global war on terror: PATTERN OF LIFE ANALYSIS. The easiest way to describe pattern of life analysis would be to ask and answer the questions "What is normal day-to-day behavior for this person or group of people? Are they behaving normally today?" If email encryption is left just to hackers and conspiracy freaks, then email encryption practically becomes a crime in itself, if not probable cause for suspicion. If you wait until you "have something to hide" to begin using email encryption, you have just established that your pattern of life does not include email encryption, and therefore beginning the use of email encryption would establish a change in pattern of life…which warrants a closer look.

Occasionally someone will also make the claim that "It doesn't matter, the government has supercomputers that can crack any encryption." Most computer scientists, mathematicians, and cryptographers will claim that OpenPGP is, for all practical purposes, unfeasibly computationally difficult to crack; they will also generally tell you by how many orders of magnitude. But let's humor the worrier here: What if the government does have a cluster of supercomputers that could crack a OpenPGP message, with current levels of encryption, in say 1 hour? If there are only a handful of encrypted messages out there, their super-cluster could (and probably would for aforementioned purposes) catalog all OpenPGP messages they could find. But if a lot of people are using OpenPGP to talk about things like their cats and the weather, the problem becomes much more computationally unfeasible…a needle on a clean tiled floor has now become a needle in a warehouse of haystacks. That is why it's important to make OpenPGP a "normal thing." The good news is that once you have set up OpenPGP, using it for encryption is as simple as sending a message. While OpenPGP is a powerful tool that runs on a variety of computing platforms and email clients, we will be using Thunderbird with Enigmail on Windows for this lesson, though it will work equally well on Linux or Mac. (Note, on Linux, you can usually skip the step about adding GPG4Win, because most Linux installations come with PGP installed by default.)

Don't wait "until things get bad" to get up and running with this. That's like saying "I'll get a gun when the poop hits the fan." When the poop hits the fan, you won't be ABLE to get a gun, let alone learn to use it. And with electronic surveillance, things already ARE bad, and getting worse every day. Get used to using this stuff now, and use it even if you're just talking about fishing (which is actually becoming more and more regulated every day anyway, and once something is heavily regulated, the activity itself approaches being illegal, Mr. "I have nothing to hide.") The more people using encryption, for everything, the less attention individuals using it will attract. And learn to use it

combined with a good VPN (we recommend Boleh VPN), for added security and untraceability.

"But what about Hushmail?" Hushmail is web-based encrypted e-mail. It's easier to set up than PGP, but it has security flaws. Hushmail is kindergarten encryption. And moreover, the owners will comply with law enforcement requests to turn stuff over. Why have your encryption handled badly by someone else when you can do it yourself and have total control of it? It's my opinion that the same can be said of some "grandma-ware" encryption being sold as Apps for the iPhone. Partly because that encryption program isn't open source, which means that pro-freedom white-hat hackers can't look inside of it for backdoors. (PGP is open source and has been fully vetted and proven as backdoor-free for over two decades.) Also because an iPhone, by design, is NOT a secure computing environment. It's a closed system, no one can see how it works, you can't use non-Apple approved software on it, (without jailbreaking it, and once you do that, you've broken the law AND it's not really an iPhone anymore) and Apple is MORE than happy to hand over all sorts of stuff about you to any law enforcement person who asks. Richard Stallman, co-inventor of GNU/Linux, said "Steve Jobs made jail cool." He meant that Apple is a closed "jail" that tries to lock you into their services only. But that could also be re-envisioned by some as meaning "Apple doesn't care if using their products puts you in jail."

***VERY* IMPORTANT TIP!!!!!!**: Using BAD encryption is WORSE than using NO encryption, because it only gives you an *illusion* of security. The way the world is headed, that's like going into a war zone with a "magic" protection amulet instead of bullet-resistant body armor. Screw web-based encryption. Do it all on your end. No one should have your private keys and passwords but you.

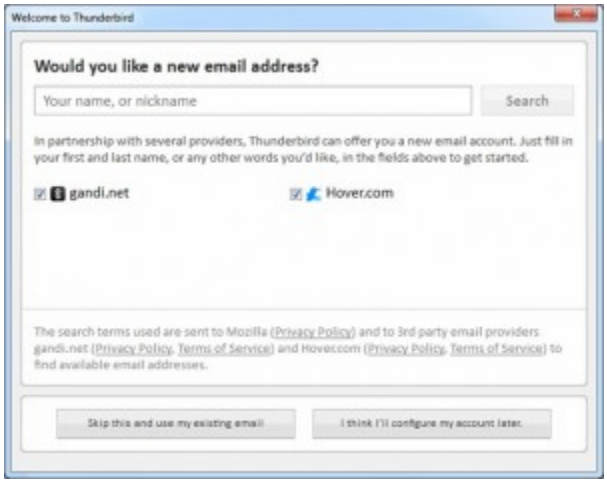
So let's do it, and do it RIGHT:

PART ONE – INSTALL THE REQUIRED SOFTWARE

You will need to download and install Mozilla Thunderbird to get started.

Run the Thunderbird installer file, run through and if you don't know the answer to the question, the default will be fine. The real "meat and potatoes" is when you open Thunderbird for the first time.

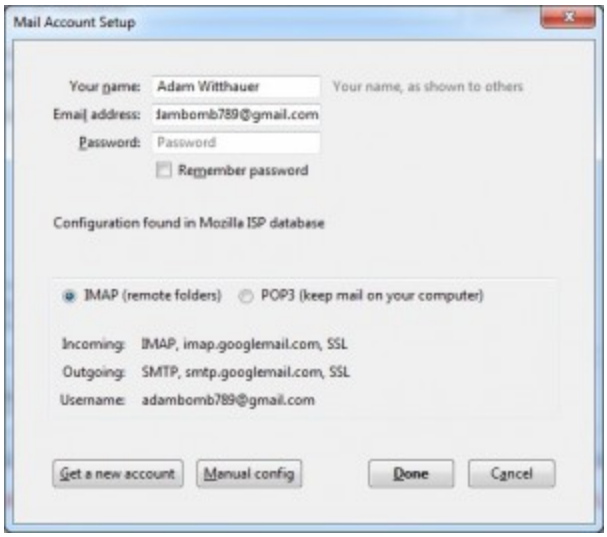
Default settings are OK here too. One nice feature Windows users will appreciate is now you will have a default email client; in other words no more harassment from MS Outlook when you accidentally click an email link!



Assuming you already have an email account that you want to use with Thunderbird, just click “Skip this…”

I’m going to include one with my actual Gmail address, since the wizard does some nice things when it identifies your email domain:

Enter the address for your existing email account, as well as its password. Thunderbird will use this to log into your email. You may want to un-check the “Remember password” block, unless you feel comfortable saving your password on your computer. Then just click Continue.

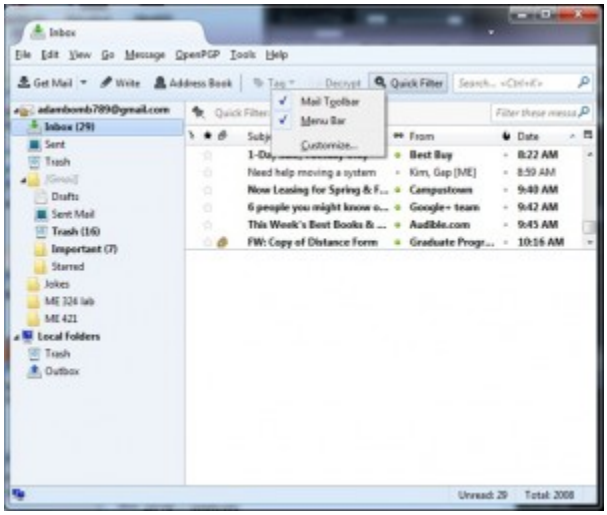


Thunderbird is fairly smart in knowing what mail settings you need for Gmail, Hotmail, and other common web mail providers. Unless you know what you're doing, or unless you're using an email provider that Thunderbird doesn't automatically provide settings for, you're best off just hitting "Done."

At this point your email account is all set up, and you can read or write emails from Thunderbird! Your email account is on the tree on the far left pane. After you first set it up it will take a while to sync up everything and download your email, so grab a beer or other suitable beverage.

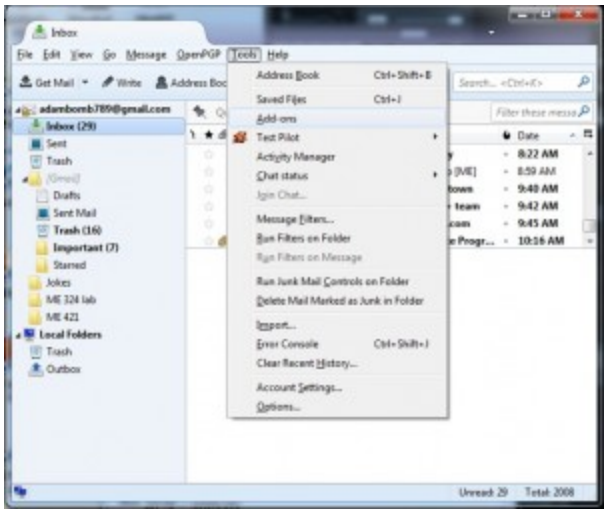
Note: If you want to have two different e-mail addresses, one for normal mail and one for encrypted only (like Michael Dean does), or if for some other reason you do NOT want Thunderbird to be your default e-mail program and can't change it from within Thunderbird (sometimes it grays out the option to uncheck that), the Windows tutorial on how to set the default e-mail program is HERE.

One last thing you'll want to do is set Thunderbird up so you can see the menu bar. With version 17.0 the menu is hidden by default, but it's much easier to get around in Enigmail with the menu bar. To turn on the menu bar, just right-click in the menu area and select "menu bar," or to get the menu bar to display one time only hit the "Alt" key next to the spacebar.



Next download and install GPG4Win. There are several downloads available. While any of the four should work, I suggest the current (not beta) light version. The light version contains everything we need. It does lack the instruction manual, but that is available for both online reading and as a standalone download on the Documentation section of the GPG4Win site. Don't panic when you reach the screen marked Define trustable root certificates. Just check the box and click next. (See following screenshot.)

Open the Add-ons Manger in Thunderbird (Tools/Add-ons) and search for Enigmail. Install it.

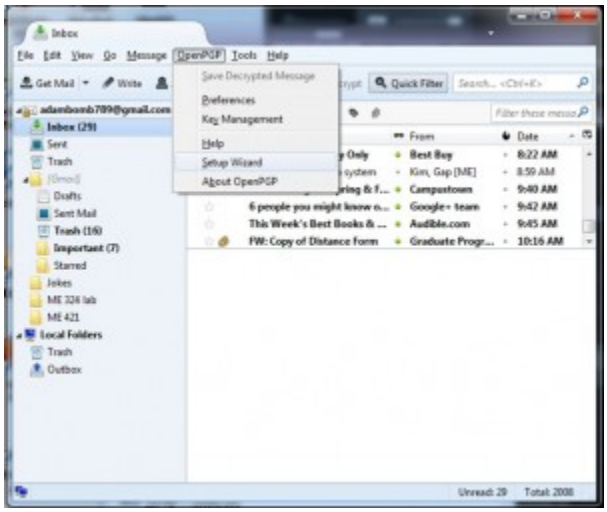


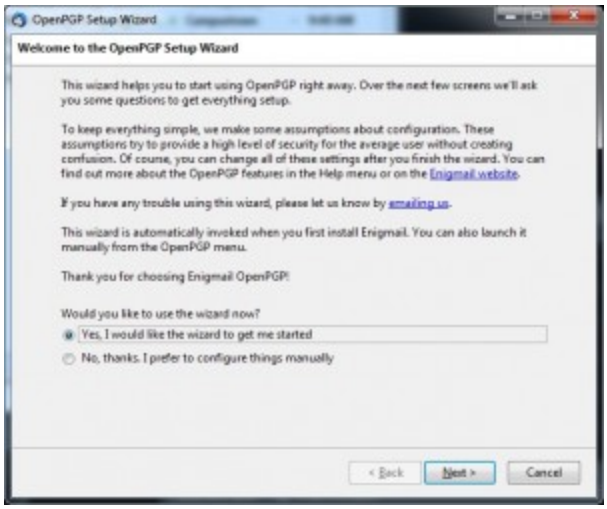
From here just type in “enigmail”. That’s what you want. It’s the first result that comes up. Now click “Install.”

Click the handy “Restart now” link to start Thunderbird with the Enigmail add-on.

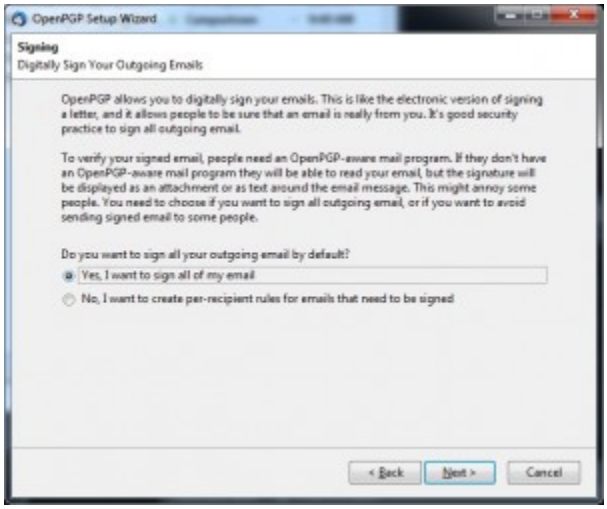
PART TWO – CONFIGURE THE SOFTWARE

Start by opening Thunderbird and opening OpenPGP/Setup Wizard leave the first choice set to Yes and click Next.

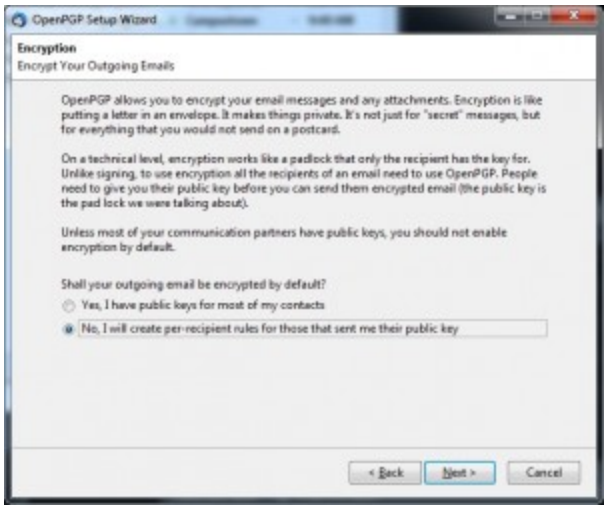




You can leave the next setting at Yes, since signing your emails won't pose problems for any recipients.



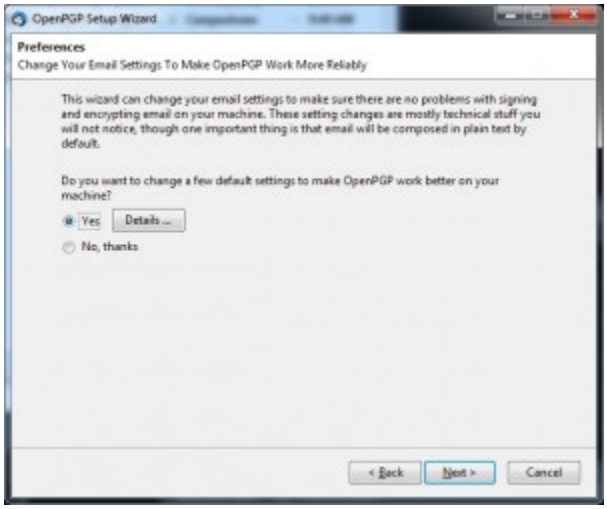
Up next you will set whether to encrypt all of your emails by default. Since you are likely just getting started with OpenPGP, most of your email recipients are unlikely to have public keys yet. Leave that selection at the default of No. (Be sure to send this blog post to as many people as possible. Not only is more people using PGP more useful to YOU, it's more useful to all good people of the WORLD.)



"Yes" here will make things easier if you let the Setup Wizard change some of Thunderbird's default settings. If you want to know what settings are being changed, click Details.

Once you have everyone you regularly email using PGP, you can adjust your Message Composition Defaults to Encrypt messages by default: Edit/Account Settings/OpenPGP Security

then click "Encrypt messages by default, and hit "OK." (No screenshot needed.)



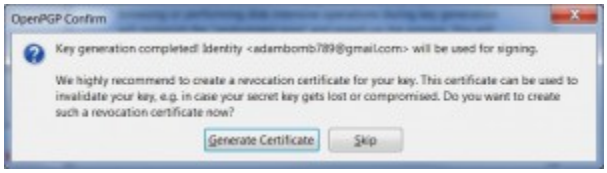
There is an unlikely chance that the Next button may now trigger a message that the Wizard cannot find the GnuPG executable. Skip to the next step if you did not encounter the warning pictured in the screenshot below. Otherwise browse for the GPG program on your computer at C:\Program Files\GNU\GnuPG\pub\gpg.exe

Now generate a key pair.

Pick a good password during this step. It shouldn't be easy for someone to guess, or a machine to crack, but it is important that you don't forget it either. There is a wealth of information online covering passphrase selection and we haven't time to cover it all here, so I recommend this quick read on picking good passphrases.

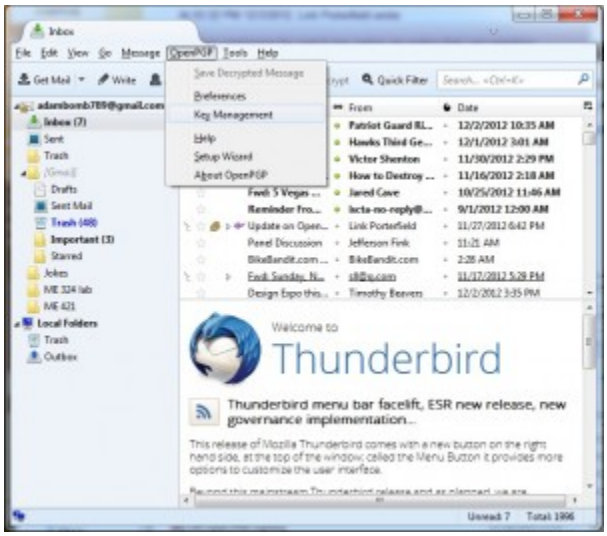
Unlike with most other memory-intensive computing operations, while your key "cooks", it will go FASTER not SLOWER if you do something else, like surf the web. Computers are an interesting mix of science and voodoo…..

It's a good idea to generate and save a revocation certificate now, too. You will use that let the world know your key should not be used in the event it is lost, stolen, has had the password compromised, etc.

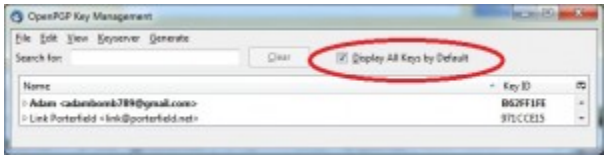


With the Setup Wizard finished you now need to add at least one public key to your key ring. There are a few different ways to do this. All will start in the OpenPGP/Key Management window where you just made your new key pair. I suggest one of the first three methods to keep things simple for now.

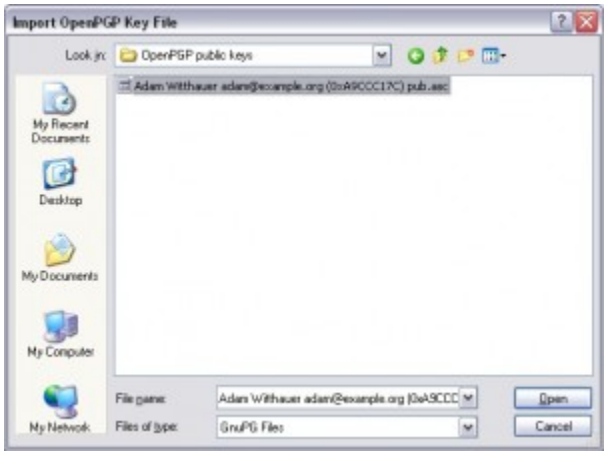
There are several ways to manage your keys from various screens, but all key management functions are available from the key manager. This is found under the OpenPGP menu.



With the key management menu open, make sure to click "Display all keys by default" so all of your keys show up automatically.



If you already have a saved public key file choose File/Import Keys From File.

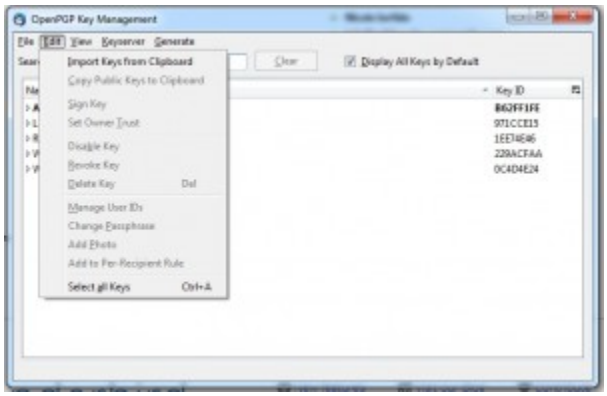


You can copy a public key in plain text format then use Edit/Import Keys From Clipboard. (Include the

—–BEGIN PGP PUBLIC KEY BLOCK—–

and the version info at the beginning, then the key block (random numbers), all the way through the

—–END PGP PUBLIC KEY BLOCK—–
at the end.)



If you were sent an email with an attached public key, right click the message and pick OpenPGP/Sender's Key/Import Public Key

You can also search for keys online with Keyserver/Search For Keys (use a Key ID in hexadecimal, for example: 0xABCDEF12)

Assign trust to the key you just imported. You will want to do this because deliberate (or inadvertent) impersonation is trivial to accomplish, and Enigmail won't let you encrypt to an untrusted key. This can be done quickly by enabling

OpenPGP/Preferences/Sending/Always Trust People's Keys, but it will leave you able to readily encrypt email to a forged key. (You will need to Display Expert Settings to see that option.) A more deliberate use of key trust mechanisms will better protect you from impostors. I recommend confirming the key fingerprint with the key's owner via another channel like the telephone, or an alternate email account, a text message, or encrypted Instant Message. Then you can sign the key which will make it trusted. (OpenPGP/Key Management: right-click the key & select Sign Key) When you sign the key you are essentially vouching for its authenticity. You will be presented with the choice of creating a local or an exportable signature. This setting just defines whether anyone else may rely on your signature to assign key trust on their keyring. (Suppose Michael Dean and I have already exchanged and verified keys, and I want to send Neema some OpenPGP email. When I import Neema's key, I can view signatures and see that it has been signed by Michael's key, and know that the key is authentic. Personally viewing Michael's signature on Neema's key isn't required for the key to be trusted. OpenPGP will already be aware of it.)

PART THREE – START SENDING OPENPGP ENCRYPTED EMAILS!

You can manually encrypt individual messages by selecting OpenPGP/Encrypt Message (or clicking the picture of a key in the bottom corner of the message). The OpenPGP/Sign Message option (or the picture of the pen in the bottom corner of the message) will sign your message, so the recipient knows it is authentic. You can attach your public key public key so the recipient can easily encrypt his reply or verify your signature. (OpenPGP/Attach My Public Key) Alternatively you can generate per-recipient rules (OpenPGP/Edit Per-Recipient Rules) to always sign, encrypt, or both. You will need to Display Expert Settings in the OpenPGP Preferences to get the Edit Per-Recipient Rules to appear on the OpenPGP menu.

NOTE: PGP encrypts the body of the e-mail, and any attachments, but it does NOT encrypt the subject line. So we recommend you use vague subject lines. We like "Yo", "What up?" and "Hey man." lol.

MAKING YOUR KEY PUBLIC SO ANYONE CAN SEND YOU ENCRYPTED E-MAILS

If you copy and paste your key into an HTML or text document, then upload to the web, it may malform, and scroll, looking like this:

That will probably not work. What you want it to do is look like a block, like this:

```
Key for Michael W. Dean, ONLY for THIS e-mail:
mwd-ahhhh@libertariampunk.com


-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.19 (MingW32)

mQENBFDA9QIBCADEIBaY5hsdJi03CgYaMzDkv9bPdl7k/IamcVc0yOYkTm32MntM
QxAxhSJC5Prnr/+U7046AThT2y47pwsRkF5J73PGNN/baOzN4ymPADq6ZKf7wzc5
F0KlNwoMqPR/vpa3m847O9yHDtBuTQ6SLMxDq6xI0rbeObyk9eNlnJtl2dxHwK8l
qIV6OoKKtMRwZSOTCNDgHnApQnEaNWaqyQwJolYKh7zfpqCwPS7pGjmTsTMZI4+f
yaHrtsljUENvTwogVocp1lq7clgA9VDaooQkwvYwkL8/NtmOKJbE0dobToKU3tk
s6CqZj7/SDLJVGyHoS5wKtpM9imxKcogZqahABEBAAG0OElpYJhhZWwgVy4gRGYh
biAtIHNlY3VyZ2ASTVdKlXNoaGhoQ0xpYmVyd0FyaWFucHVuay5jb20+iQE+BBMB
AgAoBQJQwPUCAhsjBQkJZgGABgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRDL
Q0pXN+wgFWPmB/9pwdk+aGcNxYkRIMpDDdNA6AaFtS82J70CpRDMQQpXg9aVNV4g
ALY+Q/t3YGk17fCVW6UzqJGz9izCvVq0Je3EFjeL9dityl2qXIKr/TM2MgPis/A
hFq7kgo3vg7qt5IyHzdgycKDPgLVwN3luR3naqolKJNpm3JqbLcbYNwLeqfMLIyO
qnV+G94SDCserVVWbgaIIStmBVg6SXgmjX5holrk72Ca9Ca0VUJmFOu2OKZ1hJvj
7kdVPcOI4mVVxI6nwlcpa/TwaTmbwu6iC184pPgXmXFqSBf4yrIFTG6zywxm2vqp
yM3gU200TFQKLecTVgf4EmAff/NMbF6W0AUuQENBFDA5QIBCADfDXCn/k0tLqgn
zpS8SK+mhitp9P5KlZYDfuNMoixlET3CERBlHZPG0b5zbmgMZcHLwBFVv4d2I4hu
vCW0NDe3R/ngHUdF9aMlEA3l8QGla8/WjovmWMmQCmbemna8FGAvFJvWK2AbXm7D
hTYshvAFtVqE5MrrvkpOBw6yoC7KN/wOCFvwnuascBahkExY2EBBF7QY9MnnVXtN
xF39gmZ7q7Z+0TjLVHQLeJOmKOh+5EO6gWFLLOsCgp2BJ+tvgFlT7RE436C8DuA6
OJ6Iq/DkfDTMdsirJKgM/+ShzQ/0sgEvr9SUIVg1GMd+PtaSpyBvFkdBGlm4auxO
xmoafkuvABEBAAGJAsURGARCAA8FAlDA9QICGwwFCQlmAYAACgkQy0GqV1vsIRXt
vAgAmqefdjnVEQ6ze32p05DCMBMYy9JhqQ03lprcK5H+akifOu880LoU1VzAS+zT
MLRtdUptf5Tixth++ukqnSPAidIKArAbG4GCDva9t2IsJoksy7GbuBMv3d5R+nkG
88ltc64aMjbON5kzLsoGnbomW6C7MoKsMqx1rbpU5O+2LdfOJb5PsefF+2whKQk9V
IgXGuS52lJYEIH/K93YicxWTmlEZar47nMRRSTC5ASGXZTL14BQBpQrmJGX91SWf
kEf4rhu7+P0BayzgJmI8H879JmU3dbU6gqBdUplAsO/EMKtle0rP9RRMJ7daWQYI
dctgePc7DAuKaThRpNQDt2In4A==
=gsp/
-----END PGP PUBLIC KEY BLOCK-----
```

You can do that in any HTML editor by adding the HTML tag <pre> before the block and </pre> after the block. Those tags should not show up in the browser. You can even do that without a HTML editor, in Notepad. When you save, just use the drop-down menu in Notepad to change the file type from “Text” to “All files”, and change the extension from “.txt” to “.htm” (without the quote marks.) Then upload to your web server and give people the link.

You can also just post it into a WordPress page, as I did at the very end of this post to show what they look like in WordPress. That should format fine, unless you use a template with wide margins, then the key block may scroll. As long it doesn’t add extra line breaks, it will be a useable key.

NOTE: Do not keep your passphrase unencrypted on any computer. Memorize it.

Further reading:

GPG4Win instruction manual

GNU Privacy Guard How To at Ubuntu

PGP article at Wikipedia

Gnu Privacy Guard article at Wikipedia

Pro-Liberty Information About PGP & Encryption

PGP FAQ

PGP Attack FAQ

Diceware random strong passphrase generation technique

GRC's Interactive Brute Force Password "Search Space" Calculator

ADVANCED INTO ON CHANGING THE PASSPHRASE REQUIREMENTS: By default, Thunderbird will ask you to type in your passphrase for EVERY encrypted e-mail you read. You can change this. In Thunderbird, go to Tools/Add-ons/Enigmail/Options/ and change the option. 600 minutes didn't work. But 120 minutes did seem to work for me (On Linux. It may not work on Windows, see below if it doesn't). You still have to type your passphrase once in a while in less than 120 minutes, but you won't have to type it EVERY time for every e-mail. Keep in mind though that the longer you have to go without typing it, the less secure your e-mail will be. But that is mostly only an issue if you walk away from your computer and other people have access to it and could just sit down and read what's on the screen. Also keep in mind that if someone manages to put a keylogger on your computer, they can get your passphrase.

If you want to TOTALLY eliminate having to type your passphrase more than once per session (remembering that it makes you less secure if anyone has physical access to your computer), you can adjust the timeouts in GPG agent. You should be able to re-run the GPG4Win installer and select only the GPA component to add it to your system. You can then adjust your GPG Agent settings by running GPA from your Start menu. This mailing list message has some brief, but useful information on that setting.

-=-=-=-=

Link Porterfield is a networking and systems consultant with QPG. His current PGP key can be found at that same link.

Adam Witthauer is a graduate student at Iowa State University. His current PGP key can be found at

http://www.public.iastate.edu/~adambomb/PublicKey.txt

Randall Perry started writing code in 1986 and started his first tech company in 1995. He's held adjunct Professor positions at several colleges and universities.

Michael W. Dean is a tech writer and filmmaker and does the Freedom Feens Podcast with Neema Vedadi. If you don't know Michael, his public key is none of yo' damn business! (While the nature of public key cryptography is such that a public key can safely be made available to anyone, Michael just likes to be left alone.) Just kidding, his public key is HERE, (note the e-mail address, it's not Michael's usual one). It's also pasted below:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.19 (MingW32)
```

mQENBFDA9QIBCADEZBaYShxdJiO3CgYaRzDxv9bPd17x/IamcVc0yOYkTn32NntM
QxAxhSJC8Prnr/+U7046AThT2y47pwsBkF5JT3PGNW/baOzN4ymPADq6ZKf7wzc8
F0KiWwoMqPR/vpa3m847O9yHDrBuTQ6SLRxDq6xI0rbeObyx9eNinJtl2dxHwK8l
qZV6OoKKtMRwZSOTCWDgHnApQnEeWWaqyQwJolYKh7zfpqCwPS7pGjmTsTMZI4+f
yaHritsljUENvTwcgVocpi1q7clgA9VDucoQkwvYwkL8/NtmOX3bE0dobTcKUGtk
s6CgLjT/8DLJVGyHoS5eKtpM9isxXcogZgahABEBAAG0OE1pY2hhZWwgVy4gRGVh
biAtIHNlY3VyZSA8TVdELXNoaGhoQGxpYmVydGFyaWFucHVuay5jb20+iQE+BBMB
AgAoBQJQwPUCAhsjBQkJZgGABgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRDL
QGpXW+wgFWPmB/9pwdk+nGcNxYkRDMpDDSNA6AsFtB82JU8CpRDMQQpXg8aVNV4S
ALY+Q/t3YGx17fCVW6UzqJGZ9irCvVq0Je3EFjeL9dityl2qZXIKr/TR2KgPis/A
hFq7kgo3vg7qt5IyKrdgycEDPgLVwNSluR3naqolKJKpm3JqbLcbYMwLsgfML2yO
qnV+G94KDtserVVWbgaIIZtmBVg6SXgmjX5ho1rk72Ca9Cx0VUJmFOu2OKZ1hZvj
7kdVPcOI6mVVxZ6nw1cpa/TwaTmbwu6iC184pPgXmXFqdBf4yrIFTG6zyuxm2vqp
yMZgU200TFQXLecTVgf4EmAff/NNbhF6W0AUuQENBFDA9QIBCADfDXCn/k0tLqgn
spS8SK+nhitp9P5X1ZYDfuNMoizlET3CEkBlHZPG0b5zbngMZcHLwBPVv4d2Z4hu
vCWGNDe3R/ngKUdF8aMlEAZlSGQ1a8/WjovmWMxQCnbsmnaSF0AvFJvWKZAbXm7D
hTYshvAFtVqE5MrrvkpOBe6yoC7XN/e0CFvwnuascBahkBxY2EBRF7QY9MnnVXtN
rF39gm27q7Z+GTjLVHQLs30mXOh+5EO6qWFLL0sCqpZBJ+tvgFlT7HE436C8DuA6
OJ6Iq/OkfDTHdsirJXgM/+ShzQ/0sgEvr9SUIVg1QBd+PtxSpyBvFkdBGlm4auxO
xmoafkuvABEBAAGJASUEGAECAA8FAlDA9QICGwwFCQlmAYAACgkQy0BqV1vsIBXt
vAgAmqefdjnUEQ6ze32p05DCHBMYy9Jhq003lprcK9H+akif0u880LoU1VzAS+zT
MLRtdUptf5Tixth++ukqnSPAidIXArAbG4GCDvs9t2ZsJokoy7GbuHMv3d5R+nkG
R8itc64aKjbON5kzLscGnbcmW6C7HoEsMqx1rbpUSO+2LdfOJb5Psef+2whKQk9V
IgXGuS5ZlJ7EZH/K93YioxNTm1E2az47nMRRSTC5ASGXZTL14BQSpQrmJGX91SWf
kEf4rhu7+P0BayzgJmIBHS79JmGZdbU6qgBdUp1AsO/ENKtle0rP9RRMJ7daxQYI
dctgePc7DAuKaThHpWQ0t2In4A==
=gsp/
-----END PGP PUBLIC KEY BLOCK-----

=-=-=-=-=-=-=-

How to Do Encrypted, Off-The-Record Instant Messenger With Pidgin

by MWD

Written by Michael W. Dean, Freedom Feen. Most screenshots by Aida_Aida. Tech testing and proofreading by Link Porterfield/QPG, amifreetogo, feendaveoh, Adam Witthauer and Skippy.

The Freedom Feens recently wrote and published an extensive and kick-ass tutorial on setting up encrypted e-mail, here. However, e-mail isn't always the best tool, especially if you're going back and forth in a conversational manner. But there is a way to set up encrypted instant messenger, OTR (off-the-record) Pidgin. OTR Pidgin is more instant than e-mail, better for back-and-forth conversations, keeps no record and leaves no trace. It provides actual Plausible deniability (to borrow a phrase from the CIA). I don't use OTR Pidgin for everyone, only like eight people I trust and know really well, but it's even better than PGP mail because there is no record, the only record of the conversation is *in the heads of both people involved*.

A lot of serious hard-core white-hat hacker computer security experts don't even use e-mail, EVER. They use OTR Pidgin for all Internet communications.

With e-mail and a public key, if someone can get your passphrase, they can read any saved e-mails. But with the OTR Pidgin, NOTHING IS SAVED. Again: **The only record is IN THE BRAINS of the two people talking**. And it's even better if you're using it over a VPN or Tor.

The OTR plugin was created by Cypherpunks. More on them and OTR is here. I showed this tutorial to Cypherpunk Ian Goldberg**,** who *invented* the OTR Pidgin plugin. He made a few suggestions for changes, and I made those changes. He added: "If you use OTR and also something like Tor, you can break the link between the username and your physical identity, but *only* if you _always_ use Tor with that IM account, even when creating it….If you need to break the link between the username and your identity, you need to use an anonymous communications network such as Tor in addition to OTR (they're designed to work well together!)."

Setting up OTR Pidgin is a lot of steps, but each step is simple. The problem with getting more people to use encryption is there's no way to do it that's as easy as picking up a phone or using Skype (both of which are uber NOT secure). And so far, the really easy ways of doing encryption (like Hushmail) are not secure. The problem is human stupidity and State evil. Most people say "I have nothing to hide", and governments don't want people using encryption. In a real LibPar (without governments, and with all "power" removed from idiots and returned to each honest, smart person), encryption would be in all Internet programs *by default*.

Instead we get shit like Facebook, where if you're one of their users, they add a chat bar EVEN IF YOU DON'T WANT one. And if you set it to go away, it randomly comes back from time to time like a stalker ex. They WANT you chatting on their un-secure chat program, and they're a company that will give any information to any law enforcement entity without a warrant. I recently left Facebook, and if you're interested in security, you should too. You should also use Internet security programs like PGP e-mail

and OTR Pidgin, EVEN IF YOU HAVE NOTHING TO HIDE. Because these days, not matter how "legal" or "ethical" your conversations, intentions and actions are, governments around the world (as well as some individuals, and almost all corporations) will try to use what you say against you. The repercussions of this can run the gamut from being spammed to being *imprisoned*….even if you think you're not breaking any laws. We're in a post-Patriot Act world, where doing things that one branch of the government tells you to do (like having a stockpile of food) can get you targeted as a suspect by another part of the government.

VERY IMPORTANT NOTE: There is a lot of "fake security" these days. For instance, the "Off The Record" option in the Google Talk client is *not* OTR. (They explain that here.) And as I said in our PGP tutorial, using BAD encryption or no encryption when you THINK you're using encryption is far WORSE than using NO encryption and knowing it, because it only gives you an *illusion* of security. The way the world is headed, that's like going into a war zone with a "magic" protection amulet instead of bullet-resistant body armor. Screw web-based encryption. Do it all on your end. No one should have your private keys and passwords but you. OTR Pidgin is secure. It is not fake security.

So, let's set up OTR Pidgin….

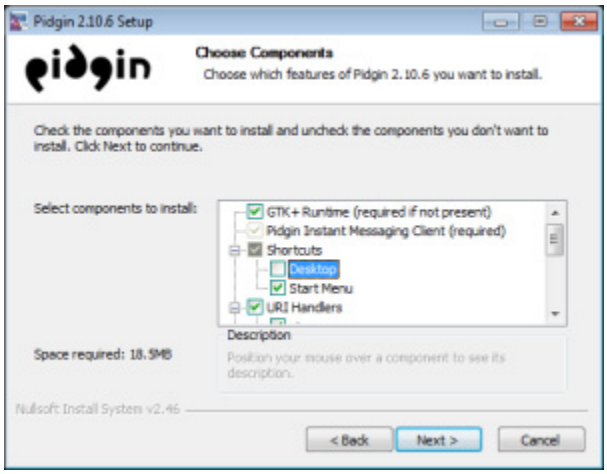
The first step (on Windows, though you can also do this on Linux from the same link) is to download Pidgin (here) and the OTR plugin (latest Windows version, 4.0.0-1, is here. If you want to check for a newer version, check here, where it says "OTR plugin for Pidgin."

Many flavors of GNU/Linux actually ship with Pidgin AND the OTR plugin installed. But if you're using Linux, you probably already *write* encryption software to relax, and wouldn't need this tutorial. And if you're on Mac, oh well. But as Richard Stallman said "Steve Jobs made jail cool."

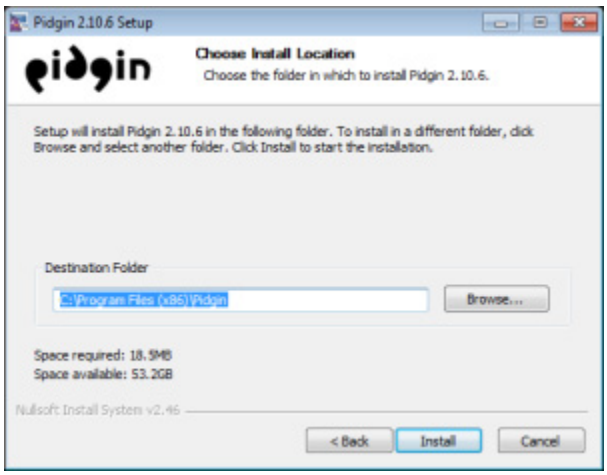
But if you're on Windows (the PC jail – see Footnote 1):

Install Pidgin:

Accept the license. Then accept all the default installs:

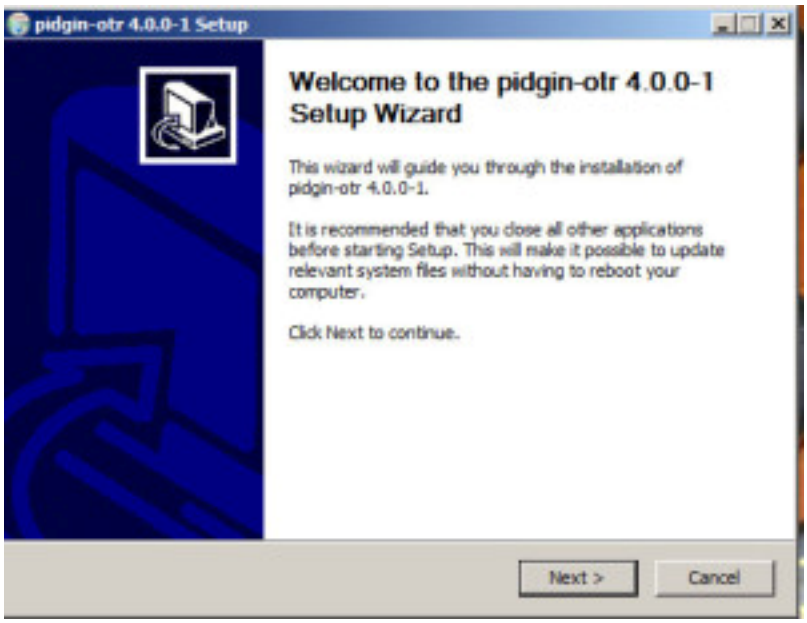


Pick your destination folder. The default should be fine:

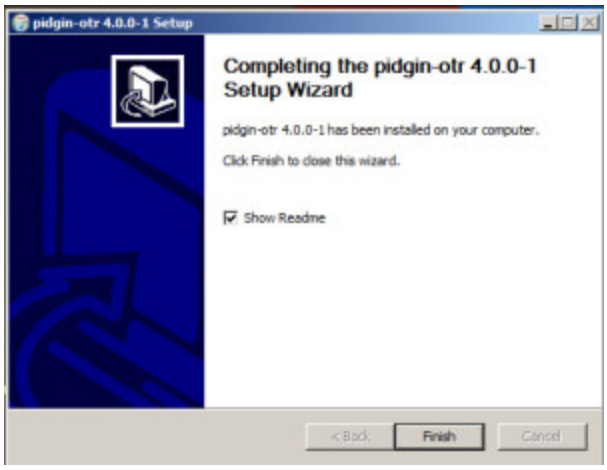


You will get this screen when it's done installing:

Install the Pidgin OTR plugin:



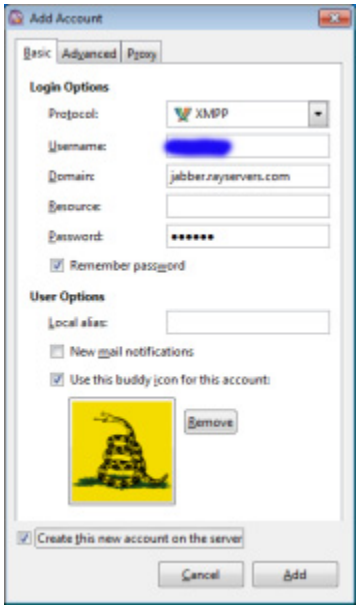
Accept the license, let it install, and when you're done you'll see this screen:



Now you need to configure your Pidgin Account. You may notice that Pidgin looks almost exactly like the old AOL instant messenger. Well, it was branched off of that project by the guys who wrote it for AOL, but they didn't like working at AOL, so they went off on their own and made it into Pidgin.

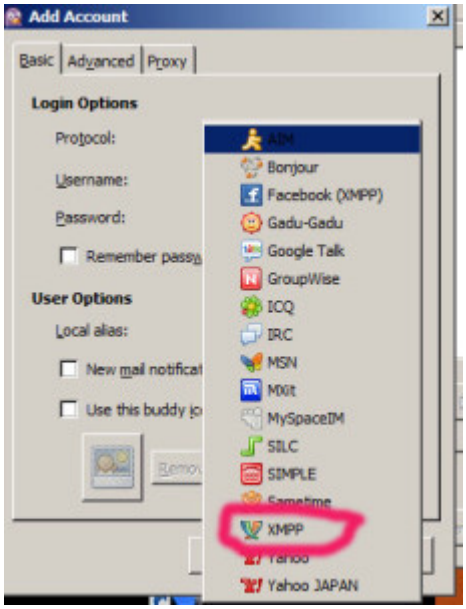
Also notice that while Pidgin comes up as a program in your program list and/or task bar, the OTR plugin does not. That's normal. the OTR plugin is not a stand-alone program, it's a behind-the-scene add-on for Pidgin. We'll configure it later, from within Pidgin. But first you need a Pidgin account. Click Add Account:

There are three tabs. The first we'll configure is the Basic Tab:



^ (I've blurred out all contact info and keyprints in these screenshots, for security reasons.)

Under protocol, pick XMPP. **This is very important**. None of the other protocols will work in a truly secure manner, and many of them (like Google and Facebook) will send your info through servers of companies that gladly bend over for "The Man" without so much as a warrant. So use XMPP. Do NOT use "Facebook XMPP", it's not secure. Use the one near the bottom that just says XMPP:



You can use a gMail *address*, if you must, breaking the user name and domain up into the two boxes (username, and @gmail.com), but I prefer to use Rayservers. Rayservers is a VPN run by a cool security-minded guy named Ray (more on his VPN is here), and Ray

allows cool people to set up free jabber accounts for OTR messaging. You can set up an account right through the Pidgin interface.

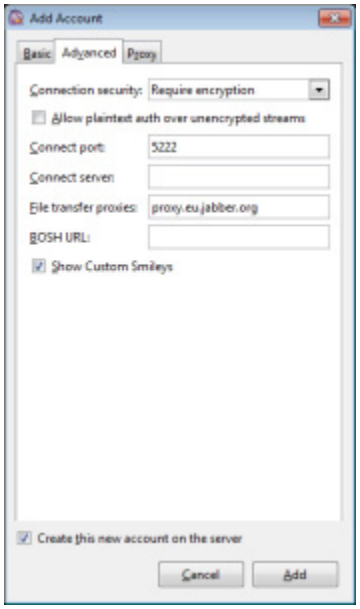
Pick a user name that is unique, and somewhat anonymous. Don't use your real full name, or a nickname that can be absolutely tied to you. Pick something your friends would recognize, but not something that can be proven to be you. Enter it in the username field. For domain, enter

jabber.rayservers.com

Leave "Resource" blank. Enter a password. (Info on picking a good password is here.) Make sure "Remember Password" is checked. (Might be best to NOT check this if for use on a laptop that you travel with frequently, where physical access to your computer could easily be denied to you, and someone could log on and pretend to be you. But if you do not have it set up to remember password, you'll have to manually enter it each time you start your computer. Remember, computer security is always a tradeoff between privacy and ease of use.)

Leave Local Alias blank, keep New Mail Notifications unchecked, and you can either accept the default buddy icon, or add your own. For this example, we've added our own.

Make sure "Create this new account on the server" is checked. Do NOT yet click "Add", we've got a few more things to set up. Go to the Advanced tab:



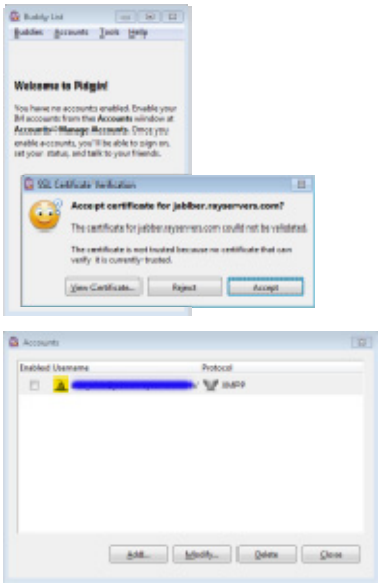
Setting for Connection Security should be "Require Encryption." "Allow Plaintext auth over unencrypted streams" should NOT be checked. Connect Port should be 5222. Leave Connect Server blank. File Transfer Proxy should be left as

proxy.eu.jabber.org

BOSH URL should be blank. Show Custom Smileys should be checked. Now go to the Proxy tab:

Proxy Type should be "Use Global Proxy Settings."

Make sure "Create this new account on the server" is checked, then click the "Add" button in the bottom right. You will get this window:



Go ahead and accept the jabber certificate, even if you get a message saying it's out of date or cannot be trusted. Trust me on this. SSL certificate issuance is controlled by government monopolies, and if you issue your own without paying The Man, the SSL

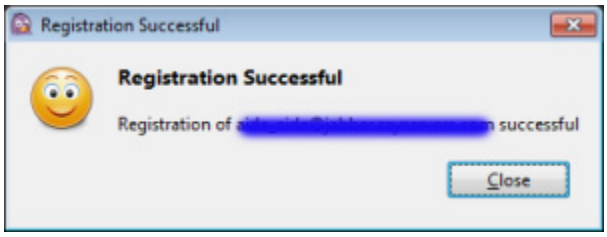
cert is still valid, but SSL cert notifications try to scare you. Ray's Cert is self-issued, but solid. After you click "Accept", you will get a window with these certificate details :

SHA1
Fingerprint=20:A8:54:9E:BA:60:93:5C:2A:0F:CE:6E:43:B5:FB:13:E7:D6:20:1B

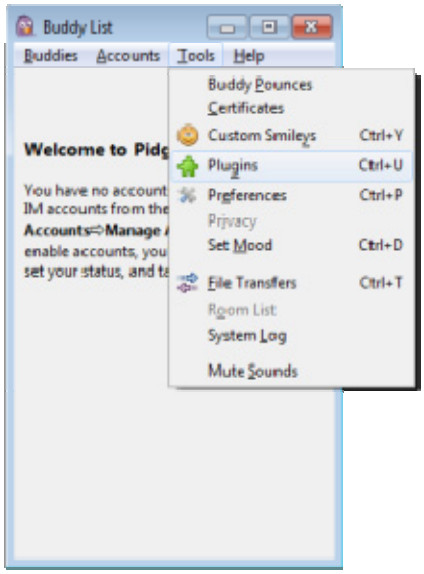
(That certificate is good to year 2020. After that, if this stuff isn't either freely included everywhere automatically already, or punishable by death, there should be a new cert on Ray's site when this one stops working, and you should get a notification from Pidgin when it is no longer any good.)

Hit "Close" and you will get this window:

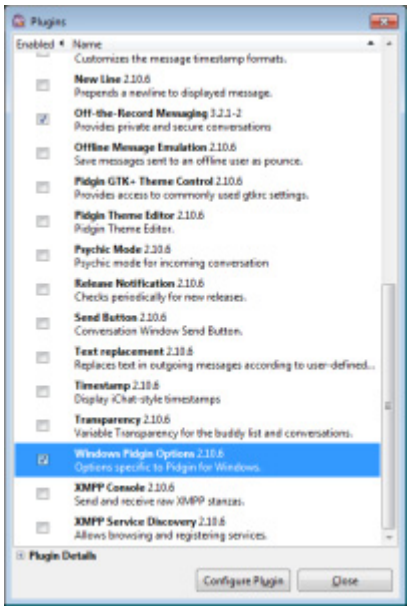
go ahead and click Register, and you will get this:



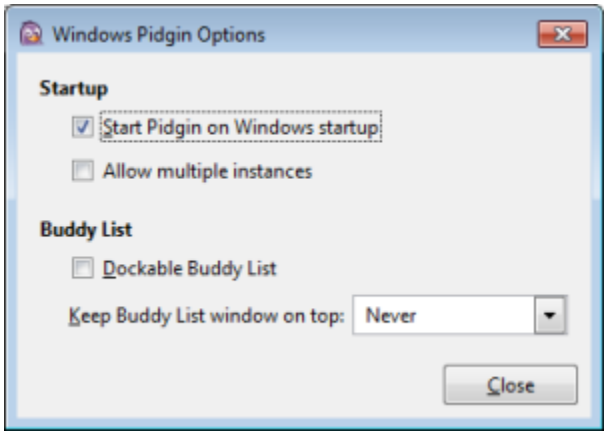
You now have an account. But we're not done yet. Go to your Buddy List window and click on Tools/Plugins:



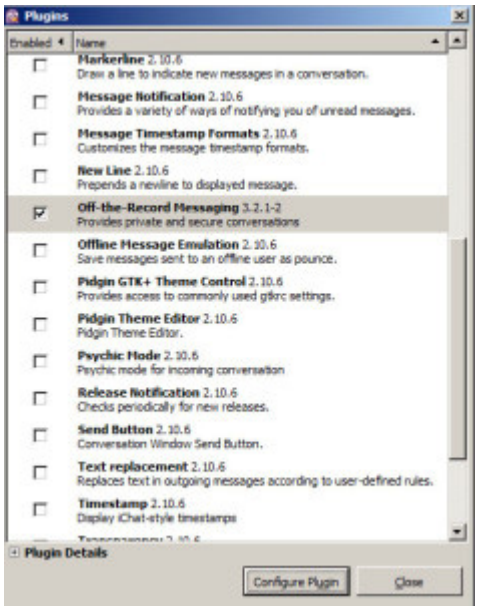
Scroll down to “Windows Pidgin Options”, Single click on it, then click “Configure Plugin” at the bottom:



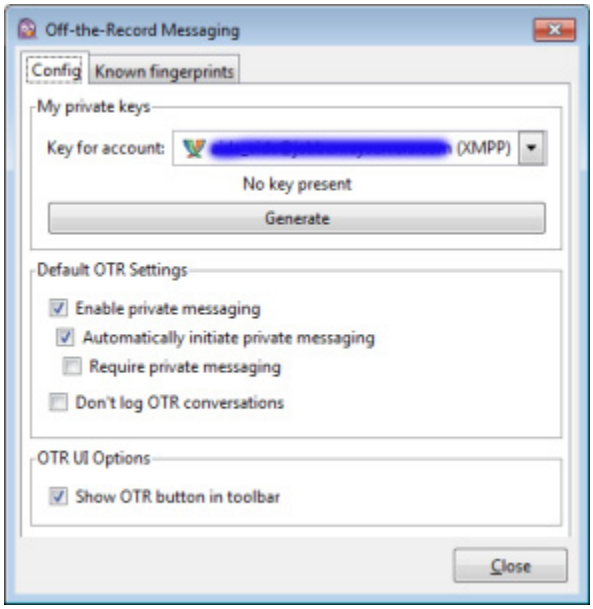
Make sure “Start Pidgin on Windows Startup” is checked. (It’s fine to leave Pidgin running all the time. It takes very little memory and will not affect your computing performance. It’s about as memory intensive as having Notepad running.)



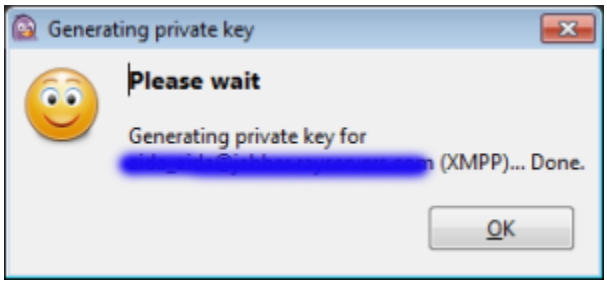
Do not check anything else, then click “Close.” Now go back to your Buddy List window and click on Tools/Plugins. This time, single click “Off-The-Record Messaging” and click “Configure Plugin” at the bottom:



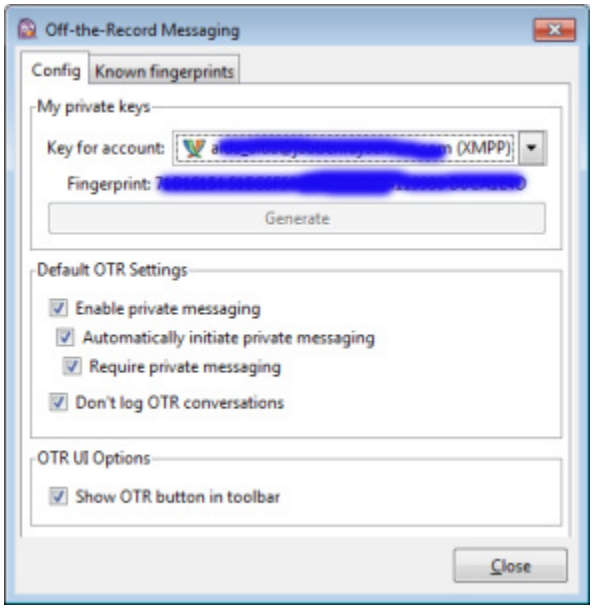
You’ll get this window:



It should automatically generate a key. If it doesn't, it will say "No Key Present." In that case, under where is says "No Key Present", click the "Generate" button. When it's done generating a key, you will get this message:

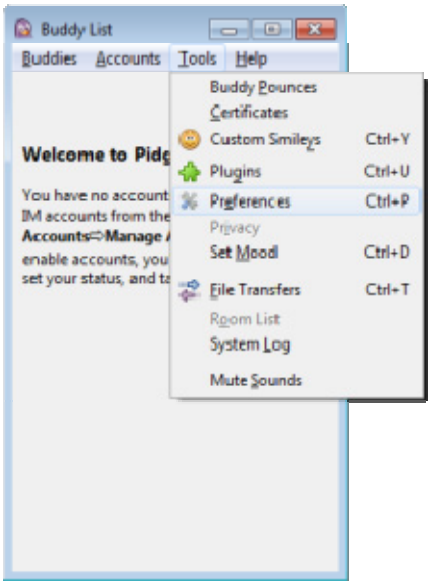


Under "Default OTR Settings", make sure these are checked: "Enable Private Messaging", "Automatically Initiate Private Messaging", "Require Private Messaging" and "Don't log OTR conversations." In other words, check EVERYTHING. Also check at the bottom under OTR UI Options where it says "Show OTR button in toolbar."

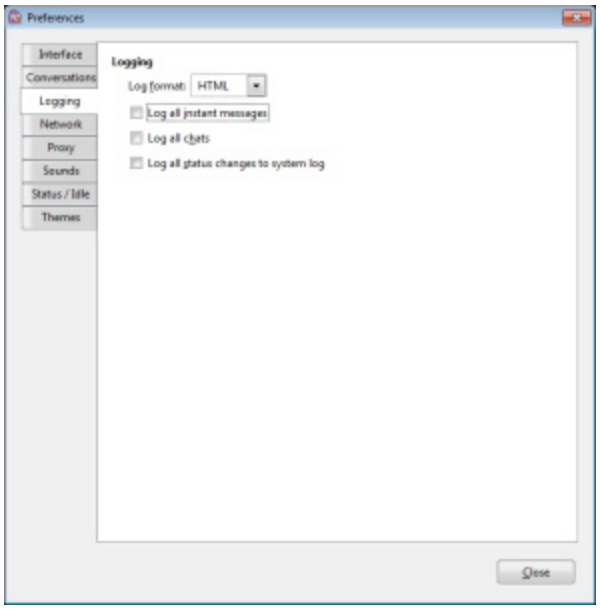


(Do not check “Require Private Messaging” if you plan to be chatting with any people who are not using the OTR plugin, but in my opinion, you should not be chatting with those people. lol.)

Hit Close. Then in the Plugins window hit Close. Then on your Buddy List window, go to Tools/Preferences:



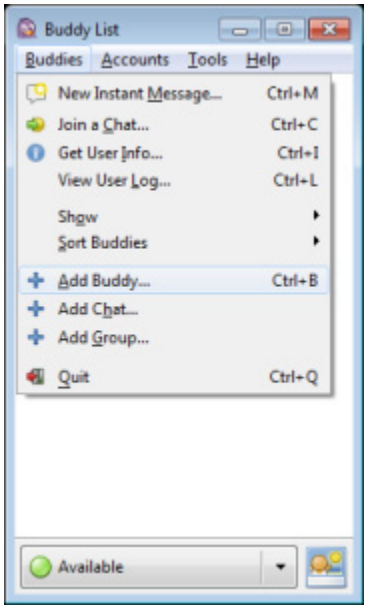
UN-CHECK “Log All Instant Messages”, “Log All Chats” and “Log all status changes to system log.” THIS IS VERY IMPORTANT, even though you’ve already set this in “Default OTR Settings” . For some reason, you have to do it both places.



Then hit Close. You are now set up for OTR encrypted instant messaging.

ADDING A BUDDY AND TESTING:

On your Buddy List window, go to Buddies/Add Buddy:



Add the Buddy's user name under "Buddy's Username." This will be info you get from the person you're trying to contact. It will be in the form of TheirUserName@domain.com (or .net or whatever.) If they're on Rayservers, it will be TheirUserName@jabber.rayservers.com

We've actually got a few volunteers who have set up TEMPORARY THROW-AWAY TEST ADDRESS FOR YOU TO TEST THIS WITH US. For a limited time, when we're online, we'll accept requests, type a little with you to confirm that it's working, and then delete you as a contact. We do this for free, because we're the Feens, and we care about Freedom.

You can try any of these test address, one of us should be online:

carrierpidgin@jabber.rayservers.com

gumbo@jabber.rayservers.com

amifreetogo2@jabber.rayservers.com

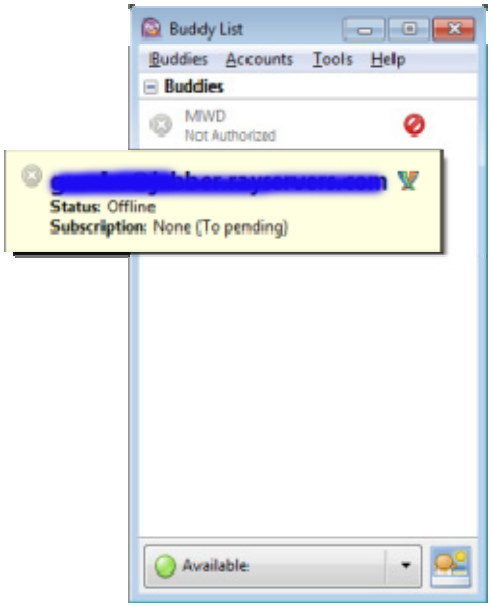
otr-test@jabber.org

feendaveoh@jabber.rayservers.com

And you're welcome. Please note, we will not accept file transfer tests, just text chat tests.

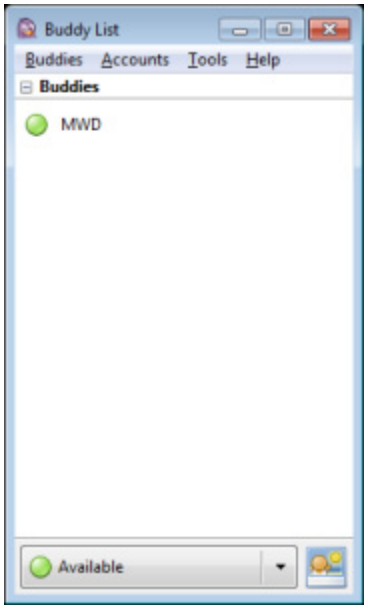
So, add your buddy's username (with domain) or our test address. You can add an alias if you'd like, but it's optional (like a person's nickname if their username is a bunch of random letters and numbers). Then click "Add."

If they're offline, they will appear grayed out:

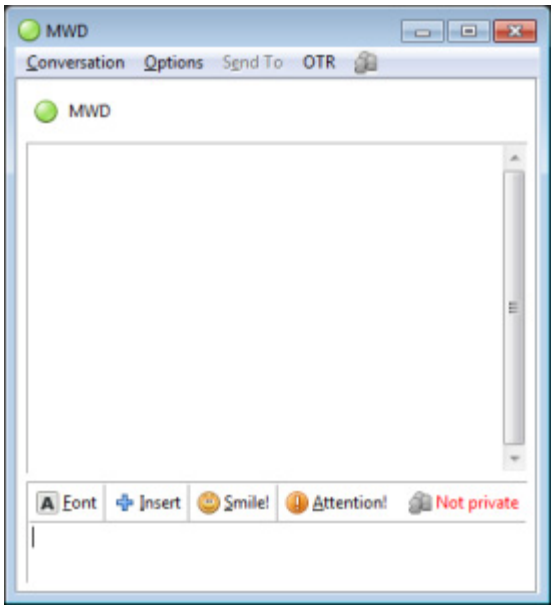


It will also be grayed out if they are online, but if they are online, within about 30-60 seconds, the gray dot will turn green to show that they are available.

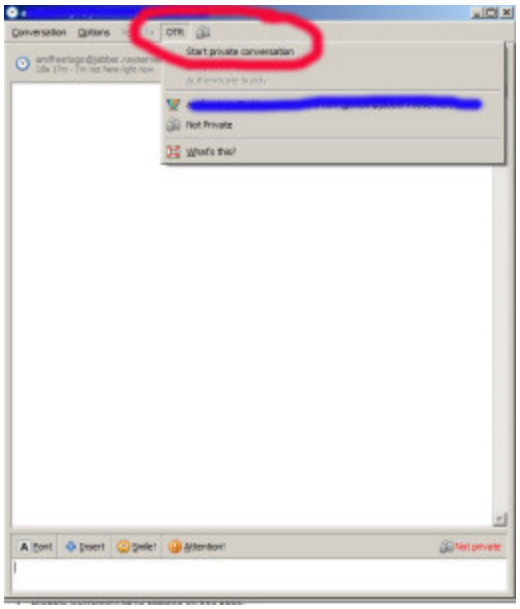
You can ONLY communicate using OTR when both parties are online. If the other party is online, and have their status set to “Available” (which is the default), they will appear as a green dot:



To initiate chatting with them, double click on their green dot in your Buddy List. This will open up a chat window:

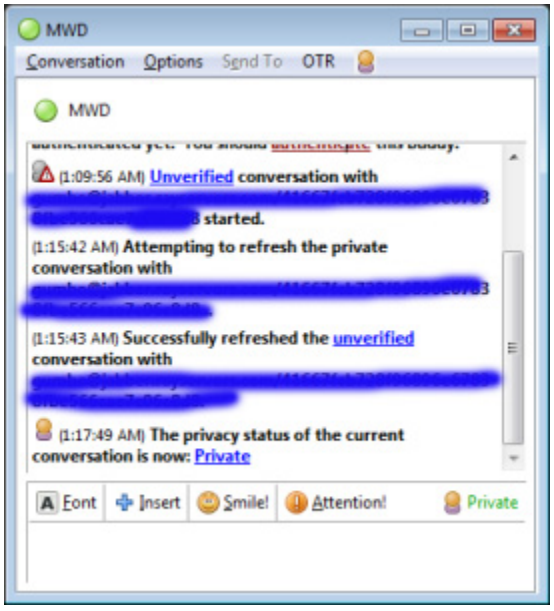


You’re still not chatting securely. Note that it says “Not Private” in the bottom right, above the chat area. You need to click on the OTR icon near the top right, and click “Start Private Conversation”:



It will say “attempting to start conversation”, and then within several seconds, you’ll be secure, and it will say “Private” in the bottom right.

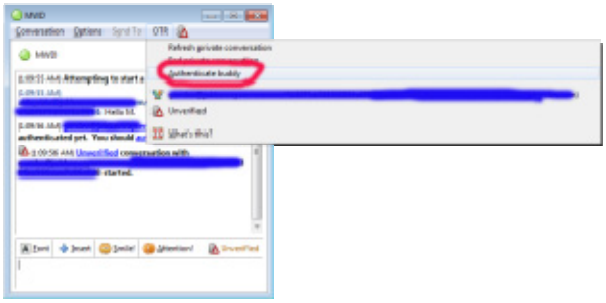
(If it already says Private, then click on the OTR icon near the top right, and click “Refresh Private Conversation”)



Note that you are now OTR and encrypted, but not yet Authenticated (verified). Authenticating is proving that you are talking to who you think you’re talking to. You only have to verify a user once. You both authenticate each other. This is done by typing a text request with a question/answer response that only the other person would know. This is best done while in the same room in person, or on the phone, so you know by the voice that you’re talking to who you think you’re talking to. Even better is doing it with a

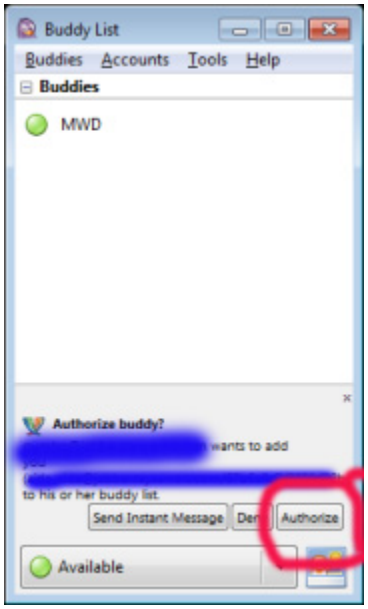
person you know in real life, where you both share a secret that only you each would be able to answer.

To Authenticate, click on OTR/Authenticate Buddy:

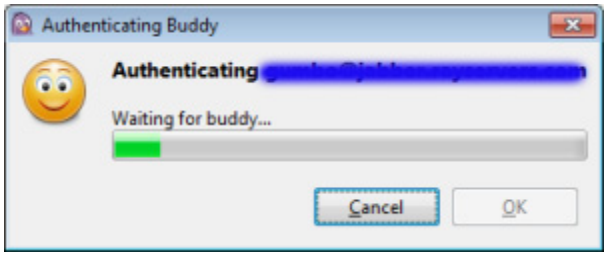


You'll get this window where you are to type a question and an answer. The answers are case sensitive:

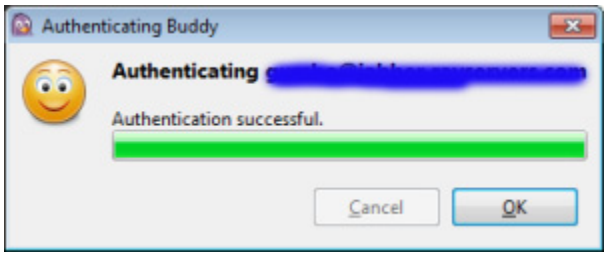
Your buddy will get this message, and should choose "Authorize":



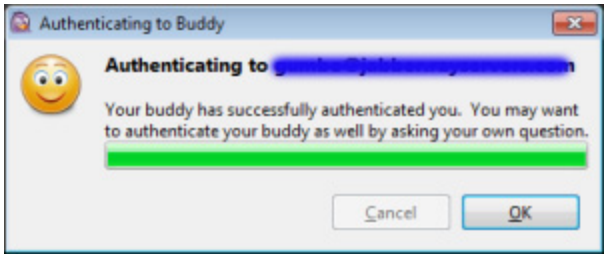
You'll get this message while you're waiting for your buddy to answer your secret question:



And this message once they've successfully answered:



Hit "OK", and you'll be prompted to do the same process in the other direction:

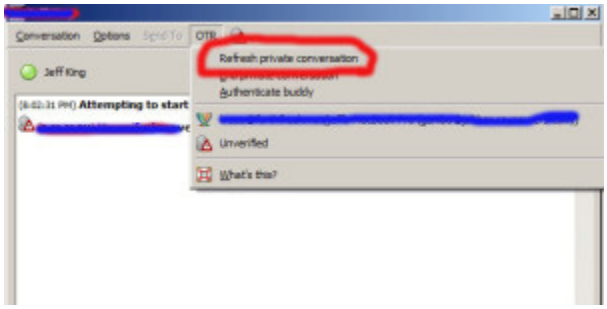


You should. Authentication is a two-way street.

KEEPING THINGS PRIVATE

If set up properly, as in this tutorial, Pidgin OTR is secure if you do a few things:

1. Refresh your conversation every half-hour or so. Do this by clicking on OTR in the top right of a chat window, and click on "Refresh Private Conversation."



In addition to the OTR menu in the chat window, you can click the "Not Private" button to initiate private chat, refresh private conversation, authenticate buddy, etc.

2. Keep your computer free of spyware and key-logging bullshit. This is obvious, but even though the conversation over the Internet is encrypted, if someone is logging your keystrokes on your computer (or over your network, if you're in a corporate environment), they're going to see what you're typing. Same is true if they are taking screenshots of what you're seeing on the screen. The best way to avoid this is to use Linux and never click on anything you don't need or understand. Second best is using Windows with anti-spyware, anti-virus software, keeping up to date and running scans, and never click on anything you don't need or understand.

It can be useful to have hidden motion-sensing cameras in your computer area, uploading encrypted to a non-public web folder. This is not only useful if you're robbed, it's also useful if someone does a "sneak and peak" where they break in while you're gone, and without leaving a trace, physically add keylogging software to your computer. Most virus programs have deals with governments to NOT detect government keylogging software and backdoors, so cameras could be the only way you'd know that this had happened. The Feens will be doing a tutorial on security cameras in the future.

True Freedom Feens never click on anything we don't need or understand. Many people will, but that's not how or why we use computers. We use computers for communication, real communication, two-way with people we know, and one-way to the world. But this is not the way most people use computers. The way most people use computers is more like running naked through the town square yelling "LOOK AT ME! INTERACT WITH ME! TOUCH ME! LOOK AT THIS CUTE CAT PHOTO! LOOK HOW THE GOVERNMENT IS HARMING YOU, BUT DON'T TAKE ANY PRECAUTIONS TO PROTECT YOURSELF! AND LOOK AT THIS OTHER CUTE CAT PHOTO!"

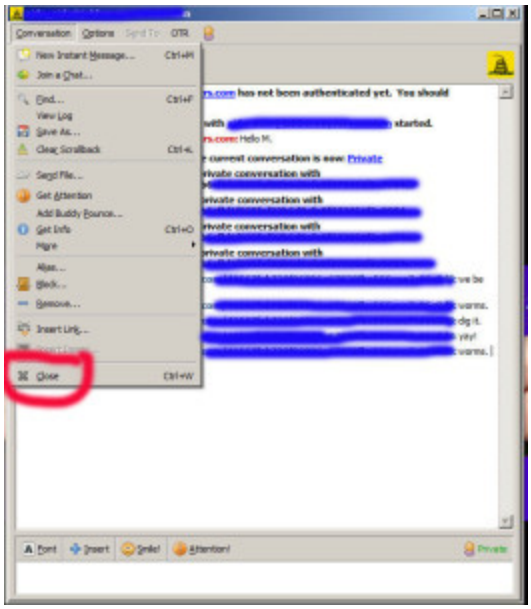
Doing this is not wise, but most people do it. If you do, please re-think it, you're putting yourself in constant danger of everything from spam to blackmail to arrest.

3. Have an anti-rubber hose decryption "I'm in trouble" secret phrase with people you know, and establish this phrase when you know you're secure, that is, you know there's no one holding a (literal or figurative) gun to either of your heads. What this means: With Pidgin OTR, you can be absolutely sure you're talking to the COMPUTER of the person you think you're talking to. But if that computer is seized by authorities, they could log in and chat as your friend and try to trick you into giving up information. Or, authorities or some other criminal gang could kidnap your good childhood friend, and threaten him/her with incarceration or torture and make them chat with you via Pidgin OTR and trick you into giving up some detail you would only give that friend.

You should have a pre-planned innocuous-sounding crypto-safeword to use if you're typing under duress. Like calling the person "bro" if you never do, or saying "what up?" or using the world "indubitably"….basically anything you would never normally say. Don't use those examples, find your own. Protecting your friends against being tricked by someone typing on your computer would be harder, but perhaps you could also have some pre-planned innocuous-sounding phrase you ALWAYS use.

For total safety, you should have a different phrase with each person you do OTR with. This could get complicated to remember, which is one more reason to not have a lot of people you do OTR with, keep OTR for real friends, and use PGP e-mail for everyone else.

4. CLOSE YOUR CONVERSATION WHEN YOU'RE DONE. And if you're talking about particularly sensitive information, do that anyway every half-hour or so and start a new conversation. OTR Pidgin does not log chats internally when set up as above. But as long as you have a chat window open, if someone kicked in your door and your computer was still on with a Pidgin conversation open, they could scroll up and see both sides of the conversation. Close a conversation by going to Conversation/Close in the chat window. Once that is gone, the only record of what you've said is in your head and in the head of the other person.

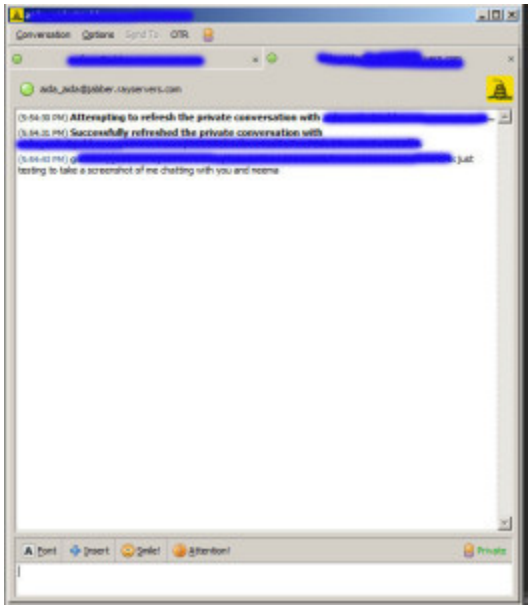


Note: BOTH sides have to close the conversation to have it fully gone. Closing it on your end still leaves a record of it on the other person's side until they close it too!

PIDGIN TIPS AND TRICKS

You can have two or more secure conversations with two or more different people at the same time, but there is no way to have a three-way or more-way secure conversation in Pidgin.

When you add a second conversation, it will open up in a second tab, like this:



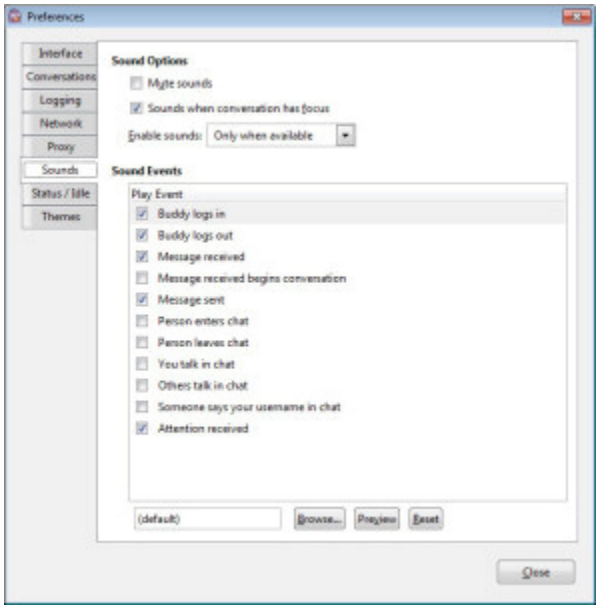
You will have to close each one separately to leave no record.

Sending Files

While in a conversation, you can send a file to another authorized Pidgin buddy, but this is NOT secure, per the readme, so we do not recommend it. Lines 237 & 238 of the README file in the current source code says:
"This plugin only attempts to protect instant messages, not multi-party chats, file transfers, etc."

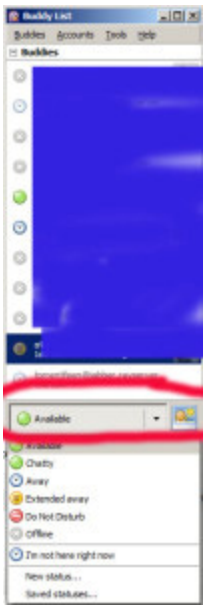
PIDGIN NOISES

Pidgin, by default, makes a lot of notification sounds. It lets you know things like when a buddy goes online, when someone changes their availability status, when they try to start a conversation with you, and when they send you a new message. The noises are useful, and they're rather pretty sounds. I got used to it really fast. But if you'd rather not hear them, you can turn them off. In your Buddy List, go to Tools/Preferences/Sounds, and turn off what you don't want to hear:



CHANGING AVAILABILITY

Sometimes having people constantly pinging you with Pidgin can interpret your work flow, or your life flow. lol. But you can set yourself as "not available" by clicking on the green "Available" button at the bottom of your Buddy List window and changing the status:



CONCLUSION:

As white-hat hacker god Smuggler said in his interview on Anarchy Gumbo, "Security is a process, not an event." It's something you need to constantly work toward improving and perfecting. But using Pidgin OTR is a great start, and it's kind of neat to be able to install something in under an hour that the biggest governments in the world cannot crack. Using Pidgin OTR gives you security that was only available to the CIA, MI6 and KGB not that long ago, and it's free.

There's really no reason NOT to use OTR. And get your friends to use it. Encryption used to be considered "munitions", and it really is like guns in a few ways. One way is that the more people using encryption, the harder it is to stop, and the less "odd" casual use seems.

–MWD

Footnote 1: regarding my use of the phrase "the PC jail" for Windows, Richard Stallman, the inventor of the GNU part of GNU/Linux, said when Steve Jobs died "I'm not glad he's dead, but I'm glad he's gone. Steve Jobs made jail cool."

My feeling is this: I know PCs are a jail too, but I get really irked with people who are religious about Macs but hate PCs. One is not "freer" than the other. They're both jails because they have too many rules, try to keep you in their "pen", and actually cooperate with governments in a way that can LITERALLY get you put in real jail for doing things that do not aggress against anyone. I look at it that Apple is like tyrannical Democrats, Microsoft is like tyrannical Republicans, and GNU/Linux is freedom-loving libertarians/anarchists. That is, anyone who is arguing the value of the Apple jail over the PC jail is a total sheepish statist. And the only real argument is for GNU/Linux. Though I

tend to write tutorials for PC, because of the large installed user base. And Linux users are smart enough that they don't need my help. lol.

CONCLUSION:

As white-hat hacker god Smuggler said in his interview on Anarchy Gumbo, "Security is a process, not an event." It's something you need to constantly work toward improving and perfecting. But using Pidgin OTR is a great start, and it's kind of neat to be able to install something in under an hour that the biggest governments in the world cannot crack. Using Pidgin OTR gives you security that was only available to the CIA, MI6 and KGB not that long ago, and it's free.

There's really no reason NOT to use it. And get your friends to use it. Encryption used to be considered "munitions", and it really is like guns in a few ways. One way is that the more people using encryption, the harder it is to stop, and the less "odd" casual use seems.

–MWD