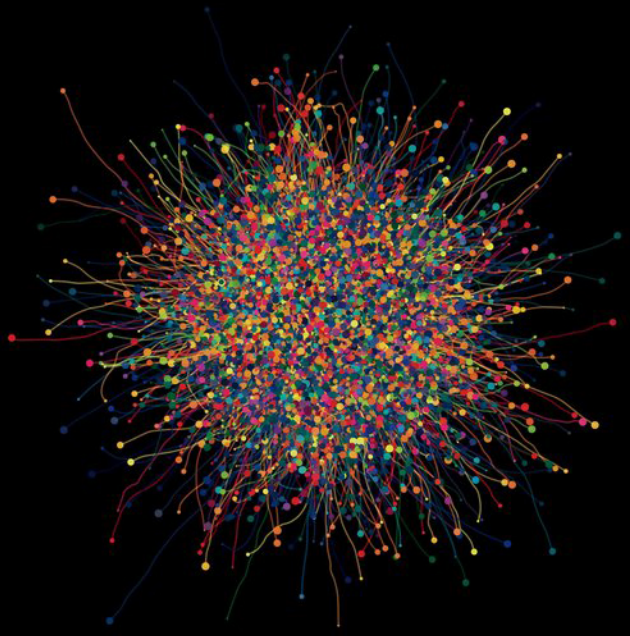
ANONYMITY IN THE SWARM

a practical guide to online security



ANONYMITY IN THE SWARM:

a practical guide to online security

version 1.3

The Truth of the Matter:

We are all under pervasive electronic surveillance. On the face of it this may seem 'alarmist,' but the evidence is undeniable:

- In 2006 an AT&T technician named Mark Klein made headlines when he revealed how the NSA, in full cooperation with AT&T, had set up a sophisticated system to sift through and analyze a large swath of internet communications travelling through AT&T's network[1].

- In May of 2006, USA Today reported that in addition to AT&T, both Verizon and Bellsouth were providing the NSA with access to their electronic and telecommunications networks[2].

- Due to Mark Klein's revelations a number of lawsuits regarding the legality of the telcom company's actions were made. In response, congress passed the FISA Amendments Act (FAA), which included a provision granting *retroactive* immunity to the telecommunications companies who passed along private information to the government despite the lack of any warrant[3]. Then-senator Obama opposed the amendment and declared he would filibuster any bill that provided retroactive immunity to telcom companies, but voted for it in the end.[4] The act passed with 69 in favor and 28 opposed[5].

[1] http://www.wired.com/science/discoveries/news/2006/04/70621
[2] http://yahoo.usatoday.com/news/washington/2006-05-10-nsa_x.htm
[3] http://epubs.utah.edu/index.php/ulr/article/viewArticle/268
[4] In October 2007, Obama spokesman Bill Burton issued an unequivocal statement to TPM (Talking Points Memo) which has since been removed from the TPM website, but can be found via Archive.Org's WayBackMachine (which has snapshots of the internet dating back to 1996):
http://web.archive.org/web/20080310152957/http://tpmelectioncentral.talkingpointsmemo.com/2007/10/obama_camp_says_it_hell_support_filibuster_of_any_bill_containing_telecom_immunity.php
Despite this statement, Obama voted for the bill :
http://www.politifact.com/truth-o-meter/article/2008/jul/14/obamas-wiretapping-flip-flop-yes/
[5] http://www.govtrack.us/congress/votes/110-2008/s168

The Truth of the Matter: (continued)

- Since the surveillance was uncovered numerous in depth stories have chronicled the rise of the American Surveillance State:

  Wired Magazine story on the NSA's Surveillance Efforts (3/15/2012):
  http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1

  PBS Analysis of NSA Surveillance:
  http://www.pbs.org/wgbh/pages/frontline/homefront/

  Washington Post investigation into NSA Surveillance:
  http://projects.washingtonpost.com/top-secret-america/

  NSA Whistleblower William Binney on State Surveillance (4/20/2012),
  http://www.democracynow.org/shows/2012/4/20

  PRISM Program Exposed: NSA access to Facebook, Apple, Microsot, etc. (6/7/2013)
  http://www.democracynow.org/2013/6/7/a_massive_surveillance_state_glenn_greenwald

What can be done:

The first step is to recognize that constant monitoring and analysis are under way. The next step is not to panic or feel overwhelmed! Understand that there are tools and techniques available which can assist in anonymizing our use of various telecommunications technologies.

Overview:

What is a "Living Document":
The tools of the trade are always changing and because of this, Anonymity in the Swarm will strive to be a "Living Document" - a document that will be updated as new information becomes available and the technological landscape evolves.

Although the technological landscape is constantly changing, the *trajectory* of change rarely shifts. Because of this, once one understands the basic rules of online security it will be easy to keep abreast of small changes in procedure (i.e. understanding and implementing the suggestions of this document will make digesting future revisions much easier).

Anonymity in the Swarm attempts to do several things:

Demystify Technology:
This document will attempt to explain key aspects of current technology in layman's terms, and provide resources for finding information on new technologies and those not included in this current version.

Provide a Framework for Action:
This document aims to provide an easy guide to performing actions such as browsing the internet, sending/receiving email, and sending/receiving files in a secure, more anonymous fashion.

ANONYMITY IN THE SWARM:

a practical guide to online security

version 1.3

Philosophy:

There is no such thing as *complete* anonymity. What I mean by this is if someone tries hard enough and spends enough resources and energy, your telecommunications activity can be compromised. Given this fact, some may question why they should even bother to secure their anonymity online.

I believe the answer is the same reason why we lock the front door of our house when we go out: Intellectually, we understand that with enough determination, time, or plain-old brute force anyone can break into our house. But, despite this we still lock our door. Essentially, by locking the door we are making it as difficult as possible for someone to break into our home, thereby doing our part to safeguard our belongings.

This work aims to *lock the front door*. We want to make it as difficult as possible for the Surveillance State, corporations and other unauthorized entities to track, infiltrate, and access our personal data and private communications.

-Jacques Laroche

ANONYMITY IN THE SWARM:

a practical guide to online security

version 1.3

Table of Contents:

ANONYMITY IN THE SWARM:

a practical guide to online security

version 1.3

Table of Contents:

Terminology:

Some Common Internet & Technology Terms and their Meaning:

ISP - Internet Service Provider

An ISP is the company that provides internet access to your home or office from their communications equipment. Internet communication is ultimately received by your computer, laptop or other device through a router, wireless router, cable modem, etc. configured to access data from the ISP.

IP Address

An IP address is a set of numbers (in the form **xxx.xxx.xxx.xxx** where x can be any number between 1 and 255) that uniquely identifies computers and other devices on a TCP/IP network.

Cipher Text

Text in an encrypted form which cannot be read without proper credentials.

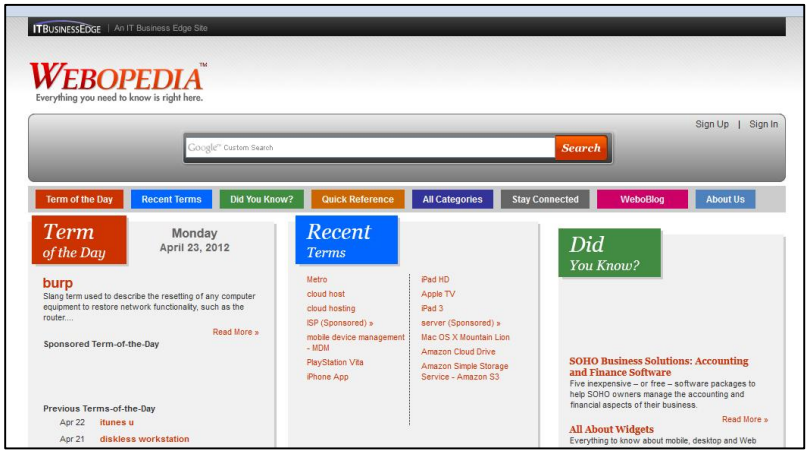
Plain Text

Text that is not encrypted or obfuscated and can be read without any credentials.

The Cloud

A large number of computers connected through a real-time communications network. These computers can over services like data backup/retrieval, content serving (music, videos, etc.), etc.

Defining other terms:



A good place to find definitions for technical terms is www.webopedia.com

ANONYMITY IN THE SWARM:

a practical guide to online security

version 1.3

Internet Browsing:

Since Google's domination of the internet many internet users have come to believe that Google.com is not only the best, but the only search engine available. Fortunately this is not the case: there are numerous search engine alternatives available and there are many troubling aspects about Google – specifically it's obsession with information gathering.

If you use any Google product (such as Gmail or Google Maps), Google has built a 'character profile' specifically for you. The way this works is after you log into Gmail (or any other Google product) information about you is entered into a database stored on Google servers. This information includes age, gender, location, what sites you visit and everything you search for when using Google.com.

Recently, Google allowed its users to clear out their "web history" however, according to Google: "as is common practice in the industry, and as outlined in the Google Privacy Policy, Google maintains a separate logs system for auditing purposes and to help us improve the quality of our services for users." Essentially, this means the information compiled about you is never deleted from all of Google's servers.

Another issue with Google is its differentiation of search results. As stated before, when signed into one of Google's services a character profile specifically for you is being built / updated with information based on your internet usage. But, Google doesn't stop there: your search results on Google.com are also being tailored to your profile. Effectively this means that different people receive different results for the same search queries on Google.com

The potential ramifications of this fact are troubling: If a user who tends to stay abreast of political information types in "Fred Hampton" in Google, they will have different search results compared to a user who does not tend to browse the internet for political information.

Tools and their Use: Secure Browsing

Duck Duck Go

https://duckduckgo.com/

DuckDuckGo is a search engine that uses information from crowd-sourced websites such as Wikipedia to obtain its results. The search engine's policy is to protect privacy, and does not record user information. Because users are not profiled, all users are shown the same search results for a given search term.

Internet Browsing (continued):

Tools and their Use: Secure Browsing

ixquick
https://ixquick.com

ixquick is a search engine that forms a secure connection between your computer and the ixquick servers which are generating the results to your search query. This allows your search query and results to flow between your computer and ixquick's computers with minimal possibility of interception, or eavesdropping.

Startpage (by ixquick)
https://startpage.com

Created by the ixquick team, Startpage uses Google.com to return search results from your query, but anonymizes the origin of the query (your computer), and returns the results via an https encrypted connection. For those who find ixquick's search results lacking, Start Page offers the best of both worlds: the familiarity and depth of Google's search algorithm, plus the security of an https connection.

HTTPS:

What is HTTPS?

HTTPS is a method of browsing the internet in a manner that is much more secure when compared to normal, HTTP web browsing. When you visit a website it's web address is usually "http://www.website.com", but a secure website's address would be "https://www.website.com ". Typically, banking websites and other sites where purchases and money transactions are be made use HTTPS, but any website can utilize it. In essence, what HTTPS does is add a layer of encryption (specifically SSL/TLS) to protect the traffic between you and the website you are visiting - effectively creating a secure channel over an insecure network. This secure channel ensures reasonable protection from eavesdropping and specific hacks such as a "man-in-the-middle attack."

Internet Browsing (continued):

Tools and their Use: Secure Browsing

Tor
https://www.torproject.org

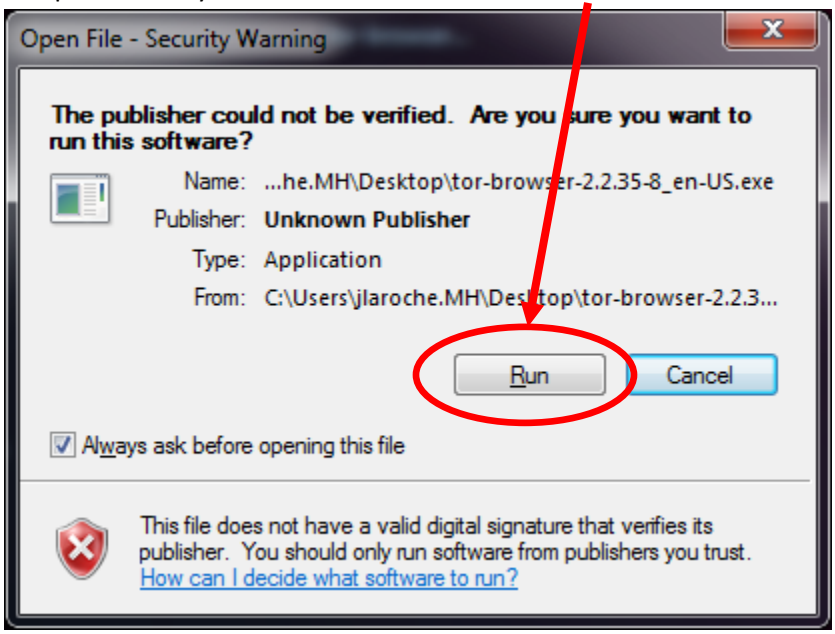
Tor is a program that helps anonymize not just your search engine queries (like ixquick and Startpage), but everything you do within your browser. Basically, this means that TOR aims to anonymize all communications between your computer and the webpages you visit.

This anonymization is achieved by sending your communications through a circuitous route towards your final destination via a distributed network. This prevents the websites you visit from discerning your actual physical location.

Installing Tor:

1. Visit https://www.torproject.org , click on the "Download Tor" button and then click on the "Download Tor Browser Bundle" button.

2. Open the file you downloaded. Click on the "Run" button:

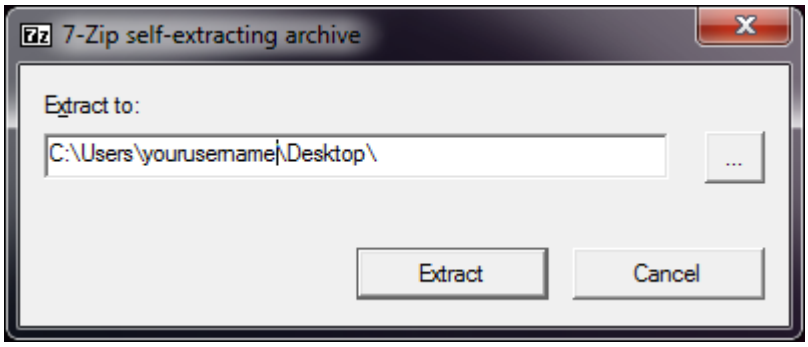


Internet Browsing (continued):

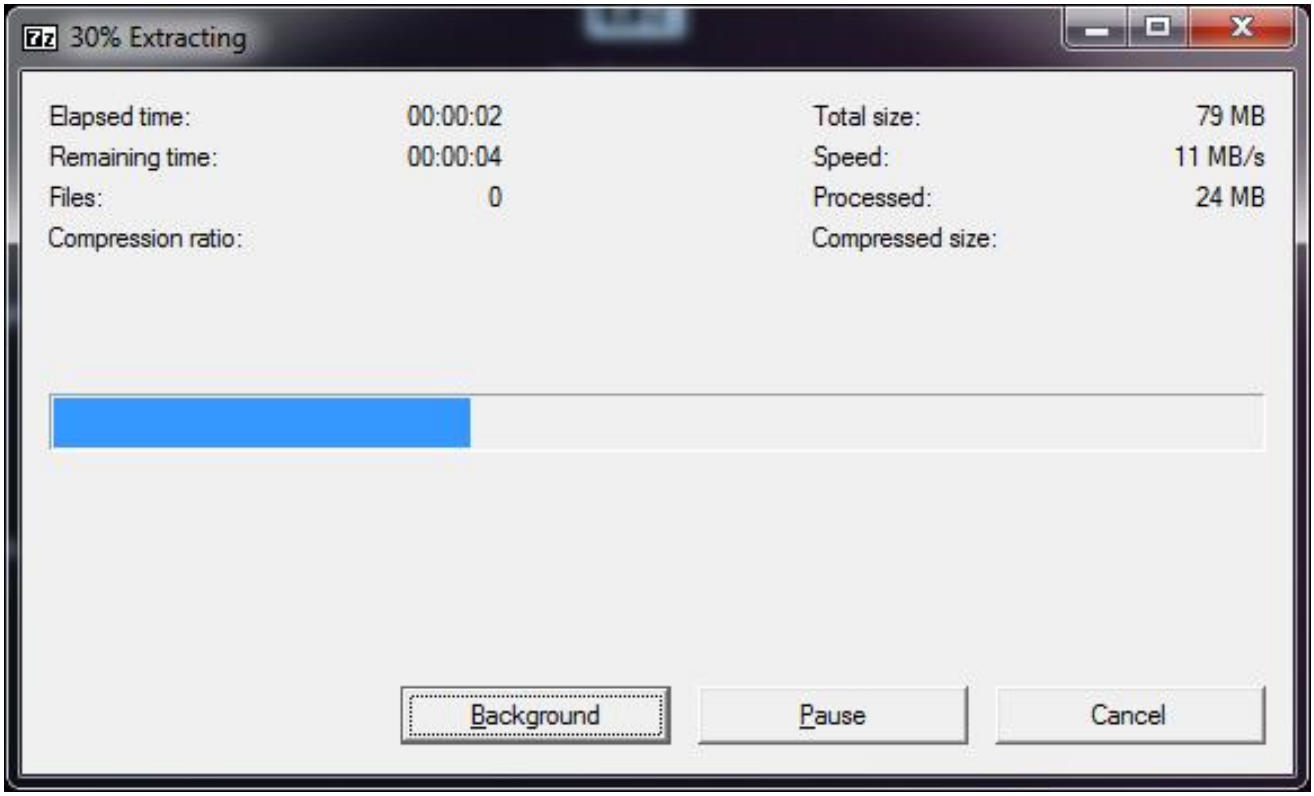
Tools and their Use: Secure Browsing

Installing Tor (continued**):**

3. Extract the contents of the file. In this case they are going to the Desktop:



4. You will see the following screen while the contents of the file are extracted:

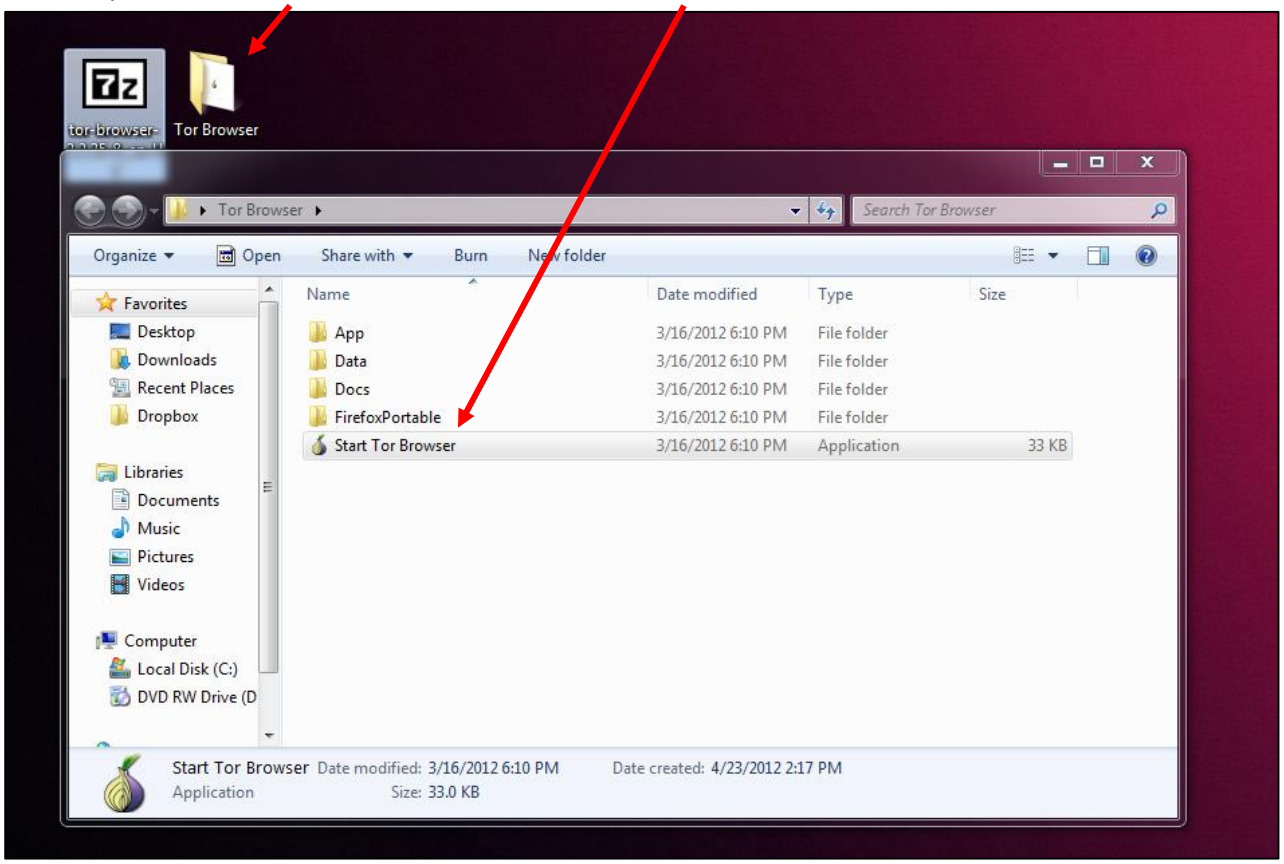


Internet Browsing (continued):

Tools and their Use: Secure Browsing

Installing Tor (continued**):**

5. Now open the 'Tor Browser' folder and launch "Start Tor Browser":

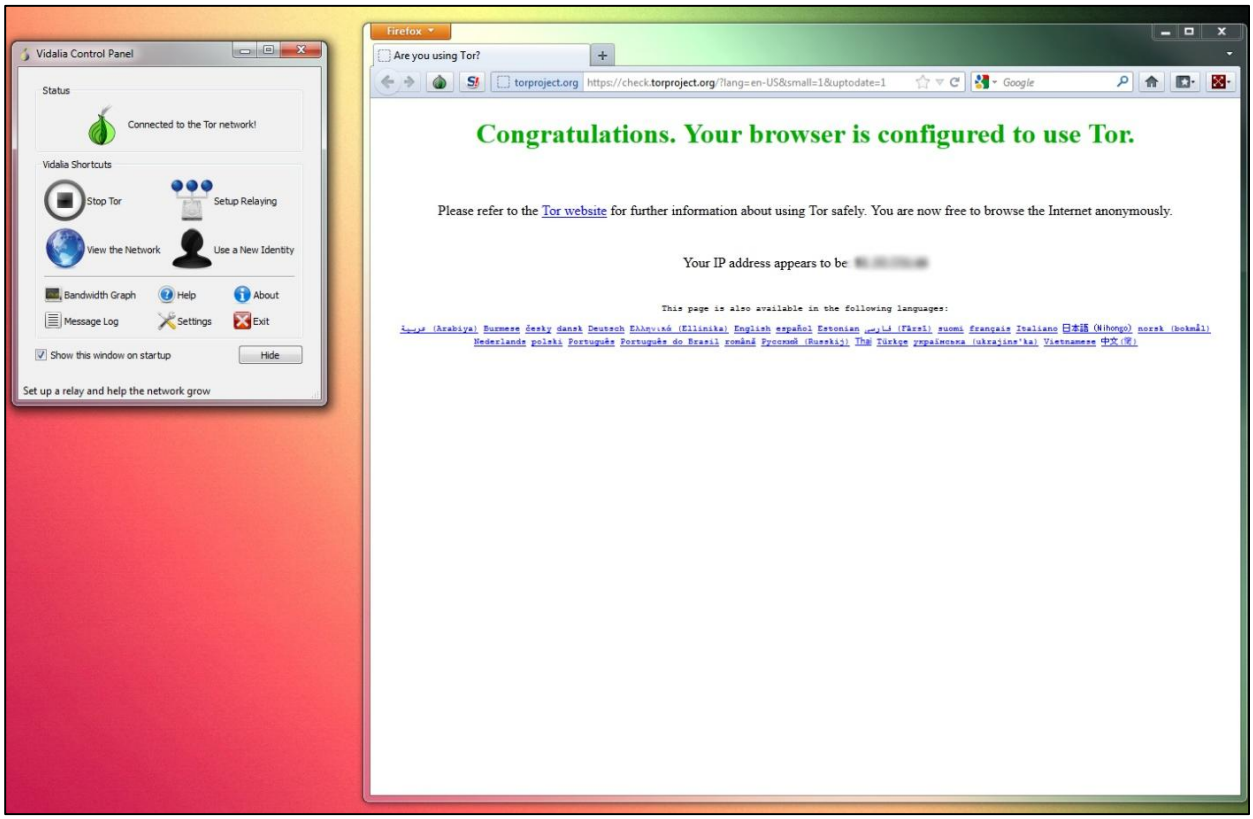


Internet Browsing (continued):

Tools and their Use: Secure Browsing

Installing Tor (continued**):**

6. You should now see a window titled "Vidalia Control Panel" that reads "Connected to the Tor Network!" and a Browser that says "Congratulations. Your browser is configure to use Tor.":



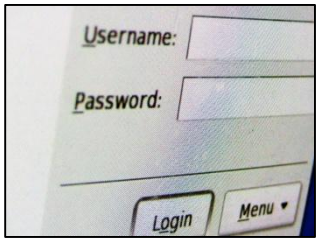
7. Now you can browse the internet via Tor's browser with anonymity.

Internet Browsing (continued):

Do You Really Need To Be Online?

As more and more people connect to the internet with their computers, laptops and other telecommunications devices, we increasingly transmit all manner of information via the web. But, if we take a step back and look at life 10, 5 and even 2 years back it becomes apparent that we can survive very comfortably without ubiquitous and persistent connection to the Internet. In terms of privacy, determining when and where we need to be online / utilize the services the internet offers is just as, if not more important to knowing how to navigate the internet anonymously.

For example, if you have a sensitive document that you need to give to someone, you may want to consider giving them the document in person (either printed, on a USB stick, burned onto a CD Rom, etc.) rather than sending the document via Gmail, Yahoo, Hotmail or any other email provider.



Passwords:

The role that passwords play in security is often overlooked: Passwords provide the first line of defense against unauthorized access. At the end of the day, if password etiquette is undervalued – such as using the same, weak password for all your accounts – the level of compromise can be profound.

Best Practices: Using Strong Passwords

Weak passwords can provide attackers with easy access to both your computers and online accounts. This is done with password-cracking software focusing on one of three approaches: intelligent guessing, dictionary attacks, or brute-force automated attacks that try every possible combination of characters. Though strong passwords are much more difficult to compromise, password-cracking tools continue to improve, and the computers that are used to run these tools are more powerful each year. Given enough time, the automated method can crack any password. Nevertheless, strong passwords are crucial because they require considerably much more processing power and time to crack when compared to weak passwords.

Elements of a Strong Password:

- Is at least seven characters long
- Does not contain your user name, real name, company name, birth date or any other obvious information
- Is not simply a complete dictionary word (for example: trust, turnip, valley, custard, etc.)
- Is significantly different from your previous passwords: Incremental Passwords (such as *Password1*, *Password2*, *Password3* ...) are not strong
- Contains Letters (both uppercase & lowercase), Numbers & Symbols (*, %, !, @, ~, etc.)

Things to Remember:

- If a password must be written down, store the paper in a secure place and destroy it when it is no longer needed
- Never share passwords with anyone
- Use different passwords for all of your online accounts and all your computers / devices
- Change a password immediately if you have the slightest inkling that it may have been compromised
- Be careful about where passwords are saved on computers. Some dialog boxes, such as those for remote access and other telephone connections, present an option to save or remember a password. Selecting this option poses a potential security threat

Encrypted Email:

What is Encryption?

Encryption is the translation of data into a secret code, and is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text* , while encrypted data is referred to as *cipher text*.

There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption. Asymmetric, public-key encryption uses one key to encrypt a message and another to decrypt the message. Asymmetric encryption is the type of encryption used in encrypted email communications. Conversely, Symmetric Encryption is a type of encryption where the same key is used to encrypt and decrypt information and is primarily used to encrypt data on one's computer.

Encrypted Email: An Overview

Encrypting your email is the most powerful way to reasonably keep your communications private and secure. There are two ways to encrypt your email communications: by setting up the ability to send encrypted email via your computer, or to send encrypted email via an online encrypted email service.

The benefit of setting up email encryption on your own computer is the knowledge that you are not placing all your trust in a third party to appropriately handle your sensitive communications. On the other hand, there are two important drawbacks to consider regarding setting up email encryption on your own computer. The first drawback is the relative complexity of configuring all the components that make encrypted communication possible. The second drawback is the fact that encrypted email can only be decrypted and read on computers that you have properly configured to do so. For example, reading your e-mail from a friend's computer, your smart-phone, a computer at the library, etc. isn't possible. In a sense, you will be anchored to the computer(s) where the encryption software and encryption keys are installed (more on that in a moment).

Additionally, let's say you set up encryption for your Gmail email: when you see an encrypted e-mail in the Web-based version of Gmail, it will appear as cipher text (unreadable encrypted text that resembles gibberish), and you will not be able to use Gmail's indexing and search feature to search through your mail to find the contents of your encrypted emails. Once again, you will only be able to read your encrypted email within the configured software on computers you have properly set up.

With all this said, I would still highly recommend setting up email encryption on your computer(s) because of the level of control you have over the sensitive material you want to email. When it comes down to it, online encrypted email providers cannot really be trusted to keep your communications private when legally pressured. For example, court documents show that a major provider of online encrypted email services called Hushmail (which is a Canadian company) was forced to provide 12 CDs

Encrypted Email (continued):

Encrypted Email: An Overview (continued)

worth of unencrypted email communications by its customers to the DEA in 2007.[6] Unfortunately, reading the Privacy Statements of other online web-based encrypted email providers shows that it is very unlikely that Hushmail's disclosure of data is an anomaly: SendInc's Privacy Statement states that "Sendinc employees do not examine the contents of customer email except when Sendinc in its discretion determines that it is required by law or government agency…"

Setting Up Encrypted Email

- Install software that performs the Encryption: GPG
- Install email software that will interface with GPG encryption software: Mozilla Thunderbird
- Install Thunderbird Plugin that connects Thunderbird with GPG: Enigmail
- Configure your email along with Enigmail
- Send and Receive Encrypted Email

Install software that performs the Encryption: GPG

The principle behind GPG Encryption is easy. Anyone who wants to send and receive encrypted email creates a public key and a private key. Your public key is the part of the encryption that you make public. Your private key is the part of the encryption that you never share with anyone, under any circumstance.

The two keys work together so that you need both to decrypt anything. To send an encrypted message to someone you lock the message with their public key and when they get it, they can unlock it with their private key. If they want to respond, then they encode the message with your public key and you can read it with your private key.

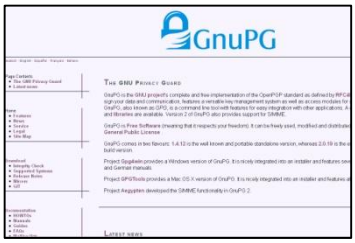
Additionally, you can use GPG to apply a digital signature to a message without encrypting it. This is normally used when you don't want to hide what you are saying, but rather want to allow others to confirm that the message actually came from you. Once a digital signature is created, it is impossible for anyone to modify either the message or the signature without the modification being detected by GPG.

[6] For detailed information on this please see Wired Magazine's piece on the incident:
http://www.wired.com/threatlevel/2007/11/encrypted-e-mai/
The Wired piece also has links to a PDF of the court document.

Encrypted Email (continued):

Setting Up Encrypted Email (continued)

Install software that performs the Encryption: GPG

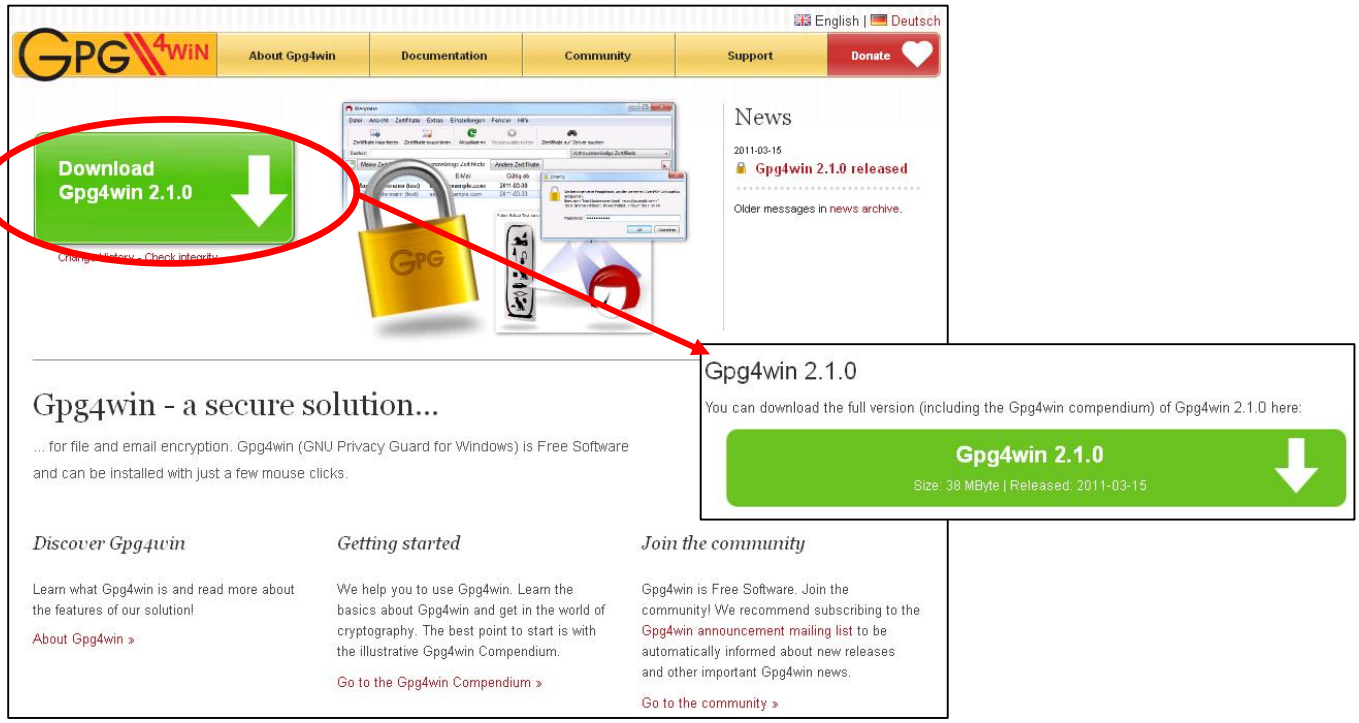


GnuPG
http://www.gnupg.org

GnuPG allows you to encrypt and sign your data and email communications.

Installing GnuPG:

1. Visit http://www.gnupg.org , click on the "Download" link on the left side of the page. Scroll down to the "Binaries" section of the page and click on the link associated with your Operating System. These instructions are tailored for a computer running Windows:

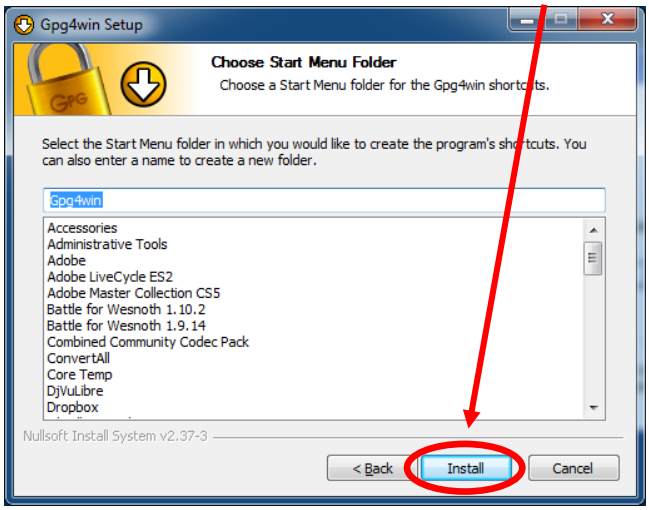


Encrypted Email (continued):

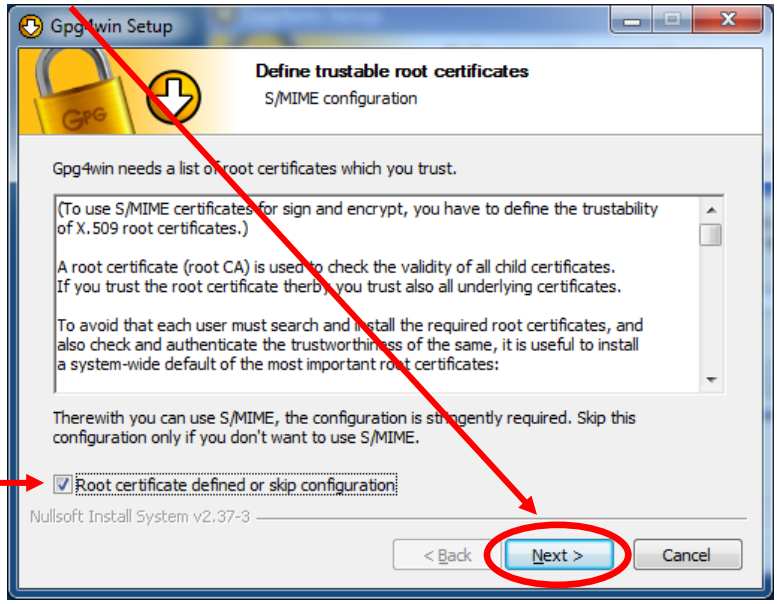
Setting Up Encrypted Email (continued)

Installing GnuPG (continued):

2. Open the file you downloaded. Leave all the default settings: Click on the "Next" button until you reach the screen below. Then click on the 'Install' button:



3. Click on "Next" button once the installation is complete. At this point you will see the screen below. Click on the checkbox next to "Root certificate defined or skip configuration" and then click on the "Next" button.



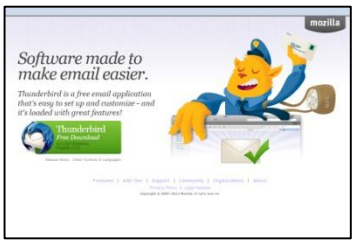
Encrypted Email (continued):

Setting Up Encrypted Email (continued)

Installing GnuPG (continued):

4. If you see the following screen go ahead and Reboot your computer.

Install email software that will interface with GPG encryption software: Mozilla Thunderbird



Mozilla Thunderbird
http://www.getthunderbird.com

Mozilla Thunderbird is an email client that has a plugin called Enigmail which interfaces with GnuPG and allows you to send and receive Encrypted email.

Installing Thunderbird:

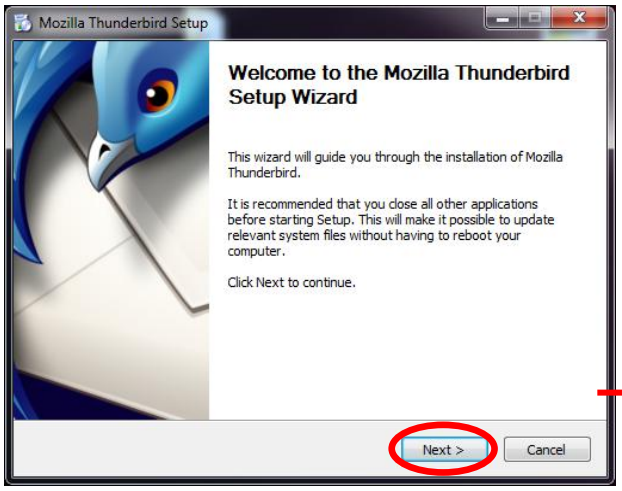
1. Visit http://www.getthunderbird.com , click on the "Thunderbird Free Download" button on the left side of the page. Save the file and open it once the download is complete. These instructions are tailored for a computer running Windows.

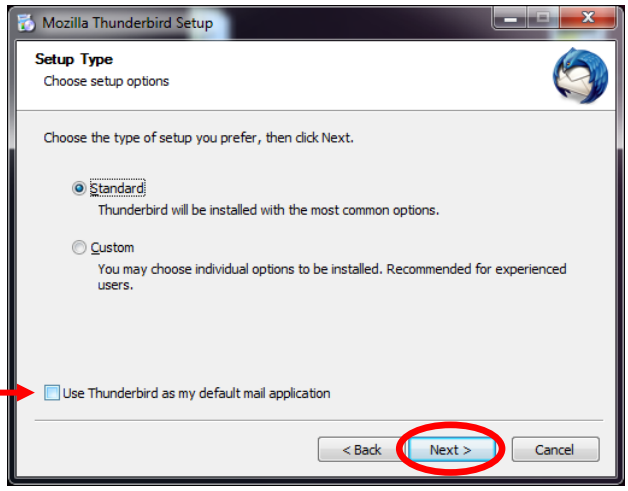
Encrypted Email (continued):

Setting Up Encrypted Email (continued)

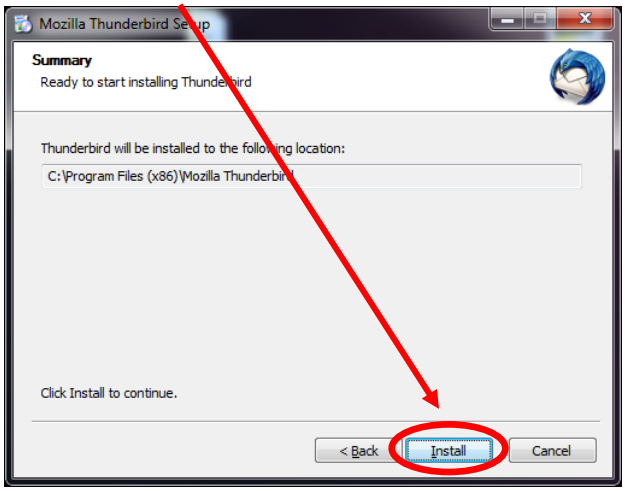
Installing Thunderbird (continued):

2. Click on "Next" button. Choose "Standard" installation and unclick the checkbox next to "Use Thunderbird as my default mail application" (helpful if you use something like Outlook as your usual email program). Click the "Next" button again. once the installation is complete. At this point you will see the screen below. Click on the checkbox next to "Root certificate defined or skip configuration" and then click on the "Next" button.





3. Click on "Install" button, then click the "Finish" button once the installation is complete.



Encrypted Email (continued):

Setting Up Encrypted Email (continued)

Installing Thunderbird (continued):

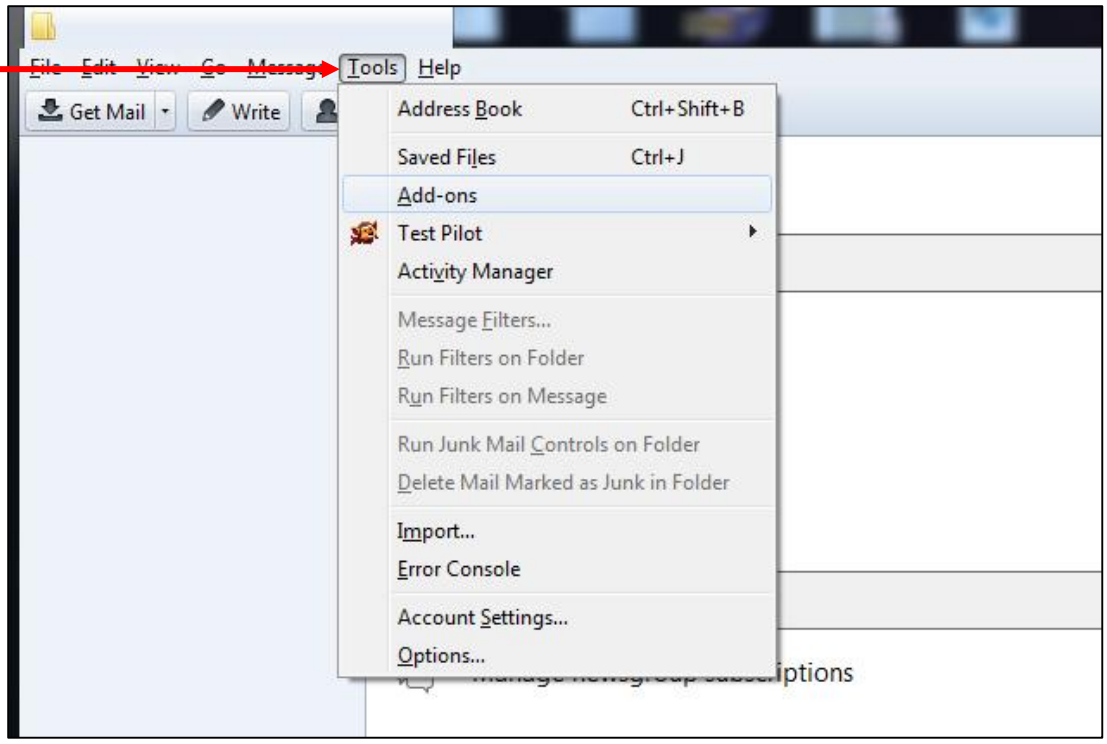
Install Thunderbird Plugin that connects Thunderbird with GPG: Enigmail

Enigmail Plugin for Mozilla Thunderbird
http://enigmail.mozdev.org/download/index.php.html

Enigmail is a plugin for Mozilla Thunderbird which connects Thunderbird with GnuPG and allows you to send and receive Encrypted email.

Installing Enigmail:

1. In Thunderbird click on 'Tools' and then click on 'Add-ons'.

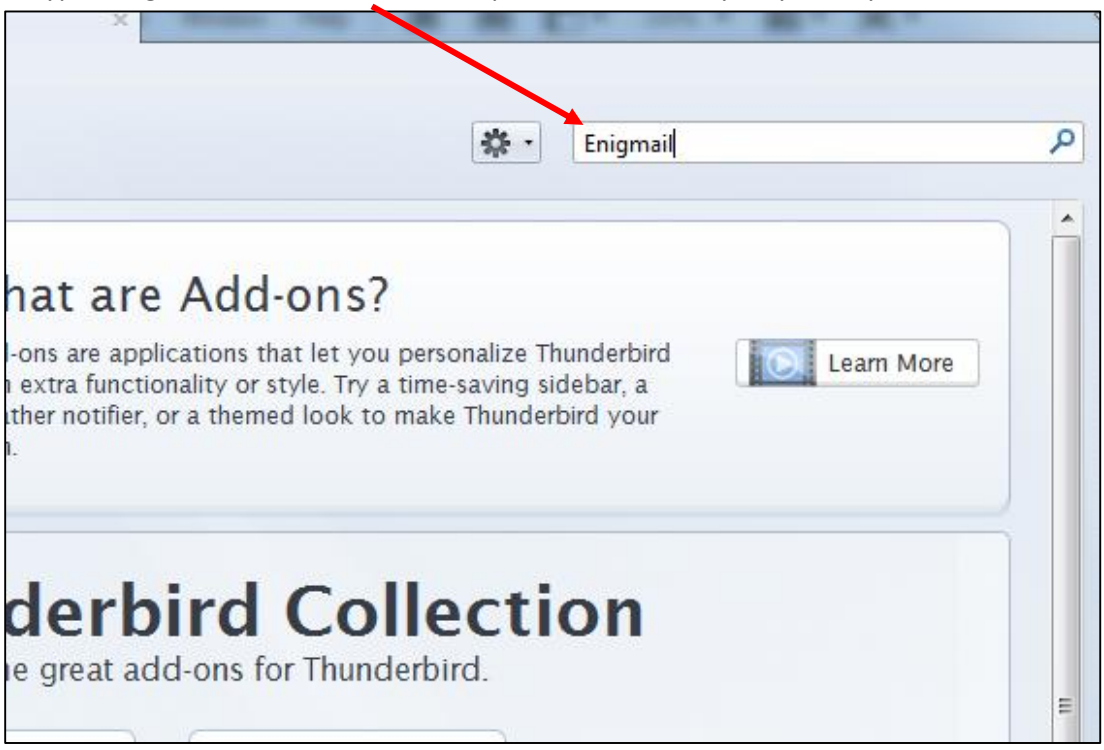


Encrypted Email (continued):

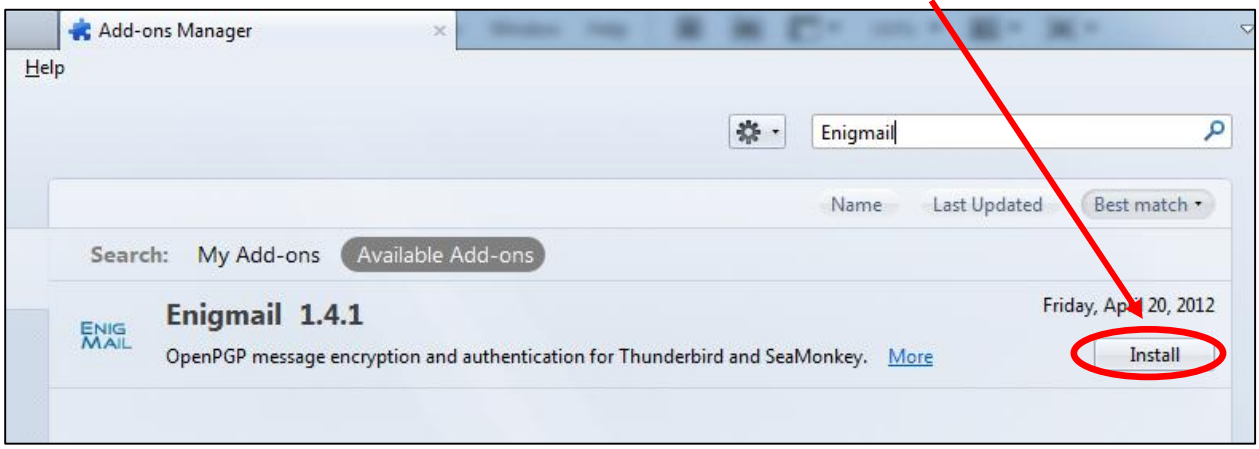
Setting Up Encrypted Email (continued)

Installing Enigmail (continued):

2. Type “Enigmail” in the Search box and press the 'Enter' key on your keyboard.



3. The newest version of Enigmail will show up in the search. Click on the ‘Install’ button.

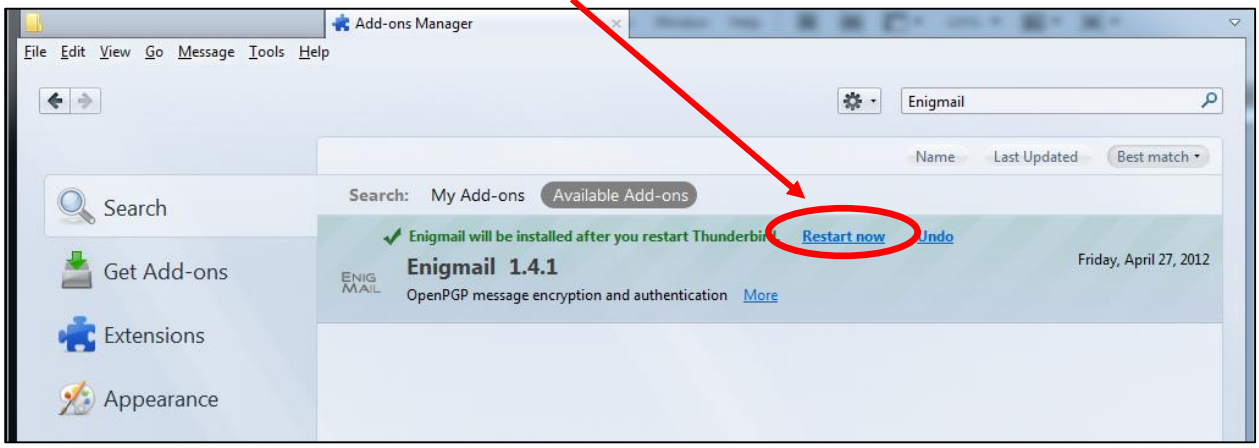


Encrypted Email (continued):

Setting Up Encrypted Email (continued)

Installing Enigmail (continued):

4. Once Enigmail is installed click on the "Restart now" link. Mozilla Thunderbird will now restart.



Encrypted Email (continued):

Setting Up Encrypted Email (continued)

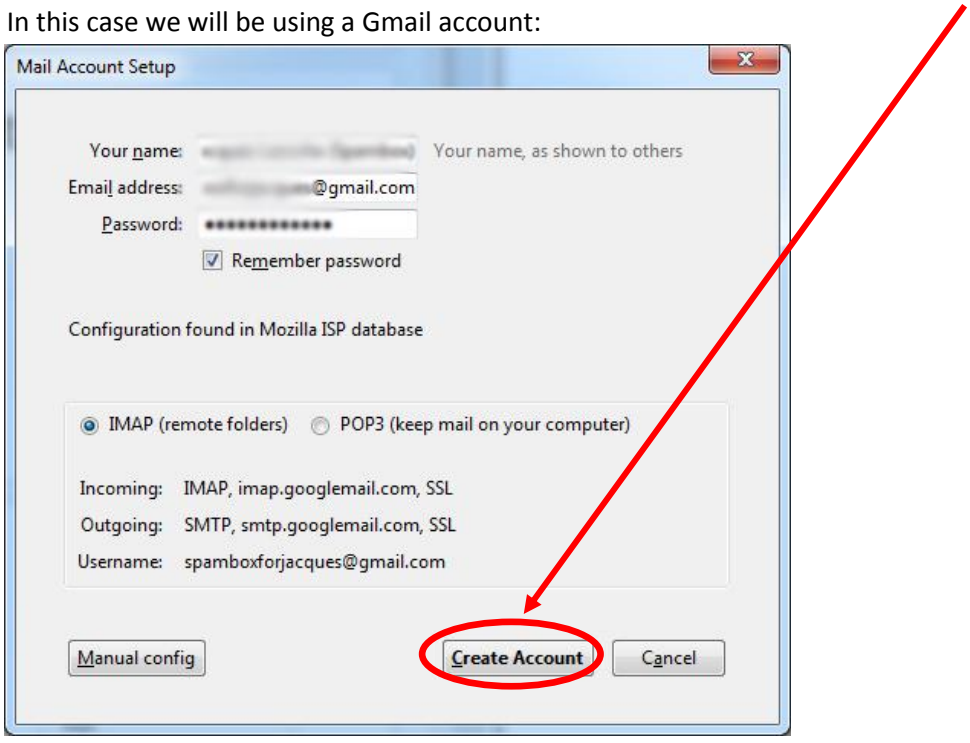
Configure your email along with Enigmail:

Configuring your email in Thunderbird and setting up the Enigmail Plugin
http://enigmail.mozdev.org/documentation/basic.php.html

Enigmail is a plugin for Mozilla Thunderbird which connects Thunderbird with GnuPG, allowing you to send and receive Encrypted email.

Configuring Thunderbird and Enimail:

1. Add the email account you want within Thunderbird, then click on the "Create Account" button. In this case we will be using a Gmail account:

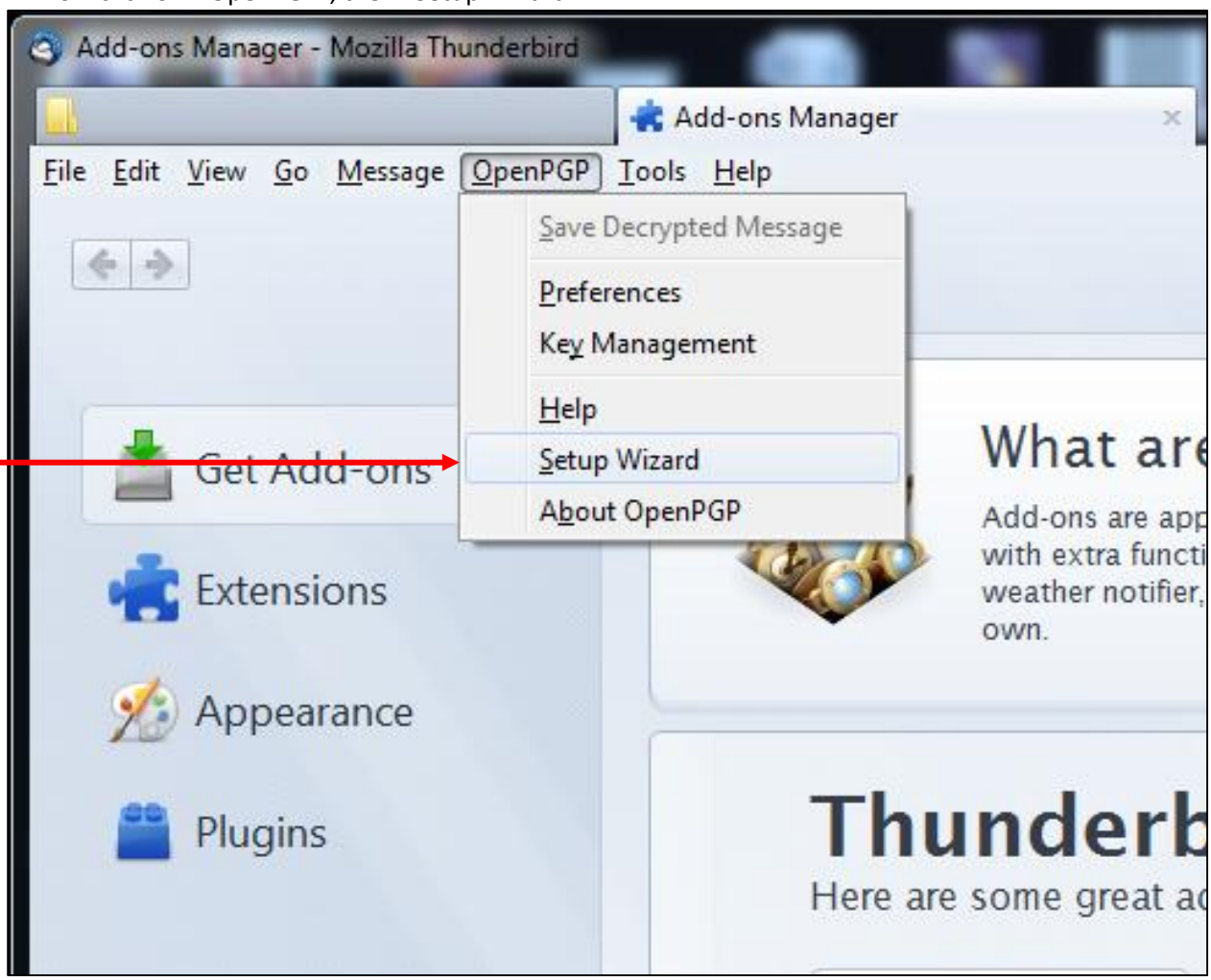


Encrypted Email (continued):

Setting Up Encrypted Email (continued)

Configure your email along with Enigmail (continued):

2. Now click on "OpenPGP", then "Setup Wizard".

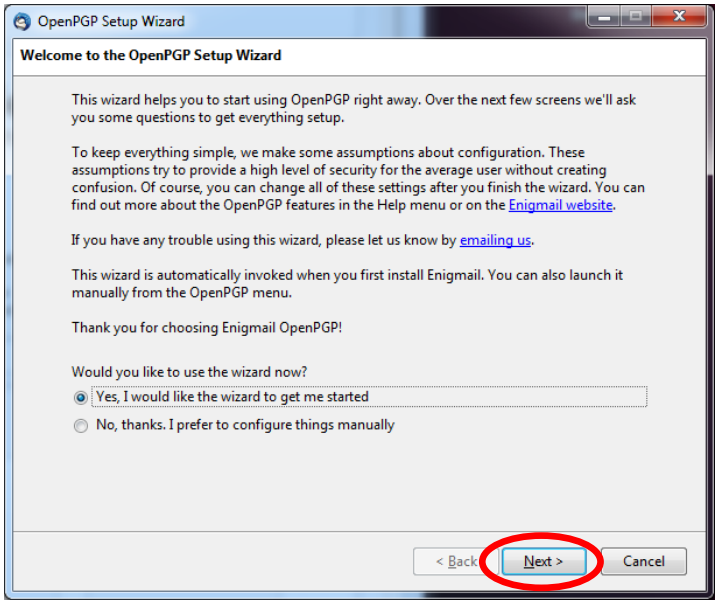


Encrypted Email (continued):

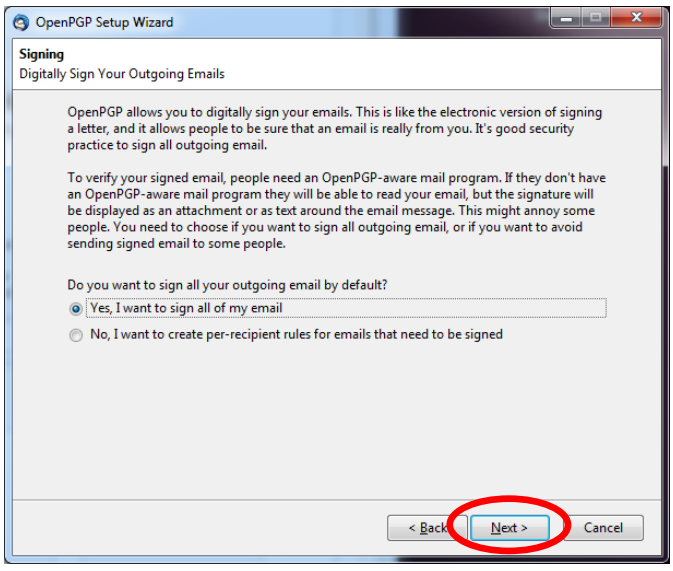
Setting Up Encrypted Email (continued)

Configure your email along with Enigmail (continued):

3. Click on the "Next" button to start the wizard.



4. This tutorial assumes you will be using Thunderbird for encrypted mail exclusively, so select "Yes, I want to sign all of my email" and click on the "Next" button to continue.

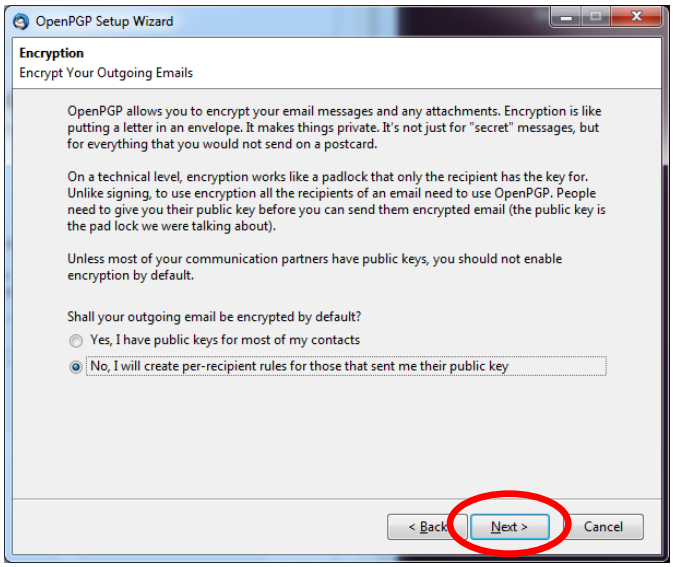


Encrypted Email (continued):

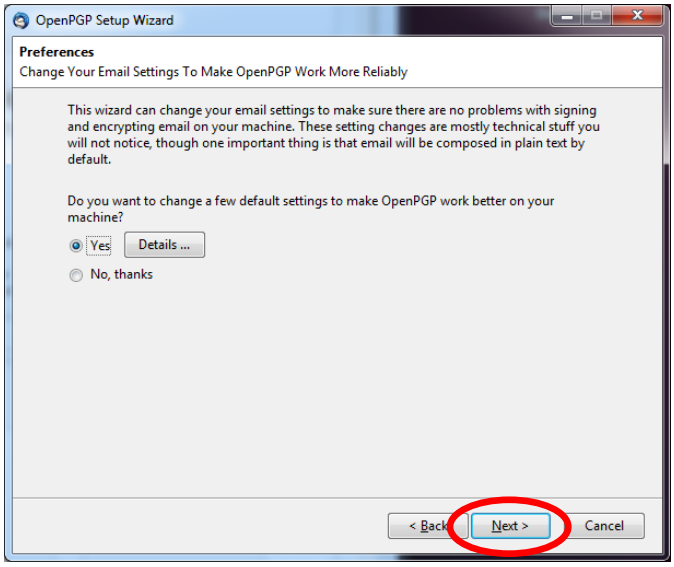
Setting Up Encrypted Email (continued)

Configure your email along with Enigmail (continued):

5. Select "No, I will create per-recipient rules for those that sent me their public key" and click the "Next" button.



6. Select "Yes" on the following screen and then click on the "Next" button.

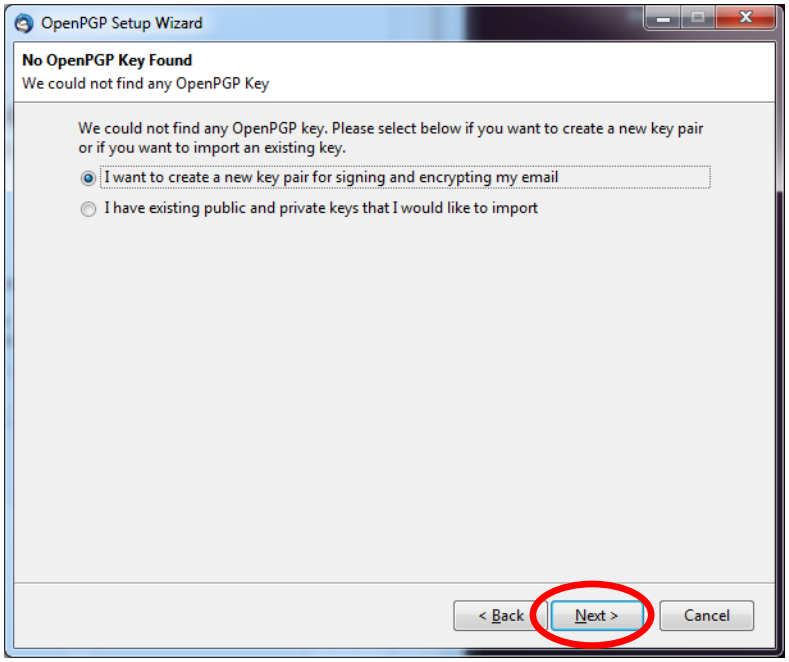


Encrypted Email (continued):

Setting Up Encrypted Email (continued)

Configure your email along with Enigmail (continued**):**

7. Since you do not have a public and private encryption key for your email address Enigmail will create them for you. Select "I want to create a new key pair for signing and encrypting my email" and click on the "Next" button to continue.

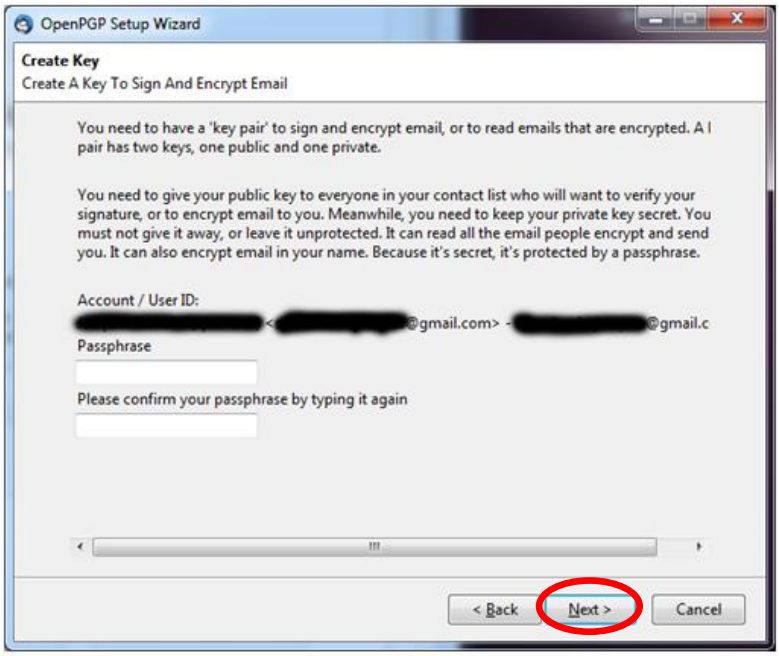


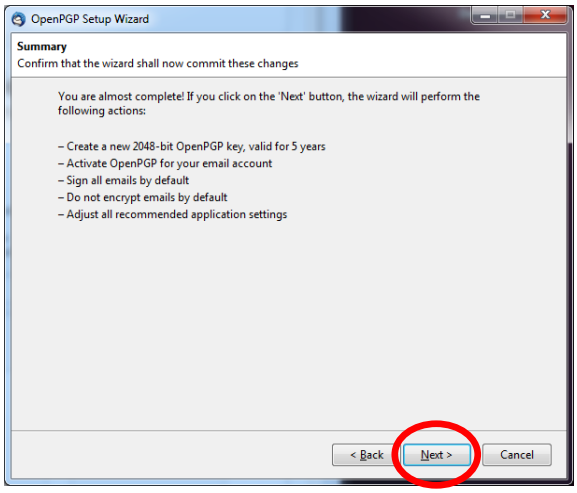
Encrypted Email (continued):

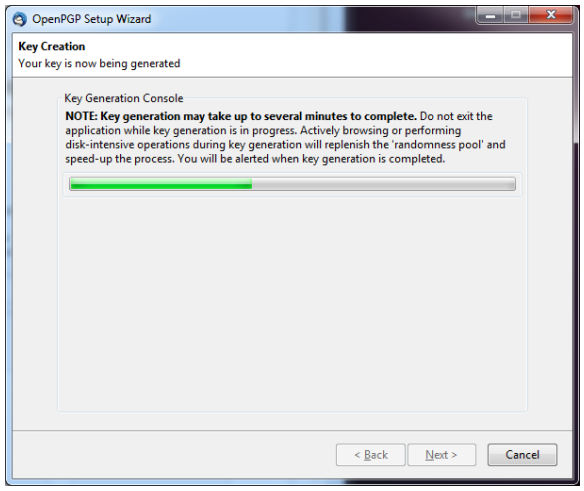
Setting Up Encrypted Email (continued)

Configure your email along with Enigmail (continued):

8. Enigmail will show you the email address you are creating the encryption keys for and ask you to enter a password for the encryption key. Make sure your password follows the guidelines suggested in the Password section of this document.





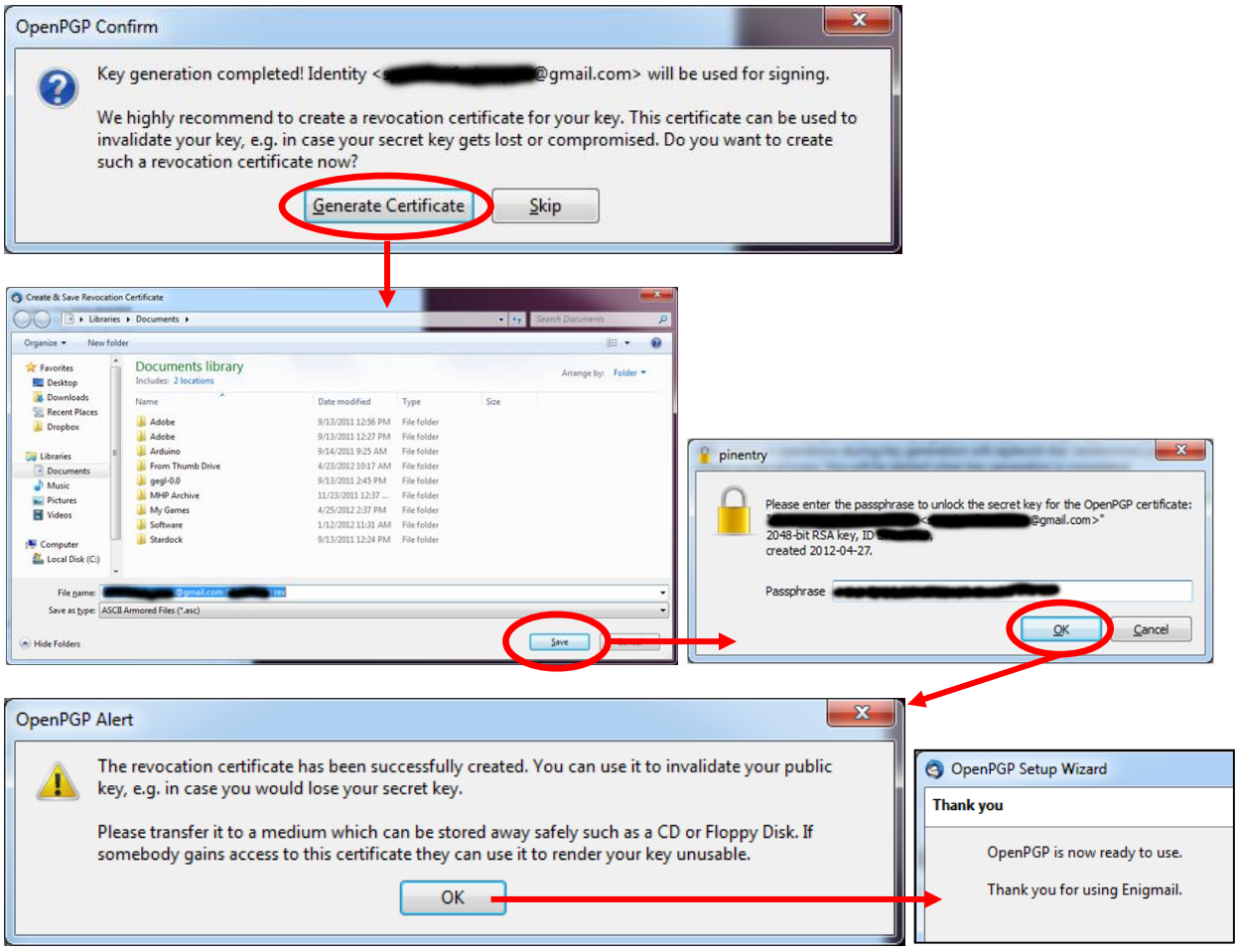


Encrypted Email (continued):

Setting Up Encrypted Email (continued)

Configure your email along with Enigmail (continued**):**

9. After the encryption keys are created you will be given to option to create a Revocation Certificate. This certificate will allow you to discontinue the encryption key associated with your email. This can be helpful if you feel the password for your encryption key has been compromised, or someone has gained access to your private encryption key. Keep this file in a safe place (stored offline, preferably on a CD or USB key only you have access to). Click on the "Generate Certificate" button, then save the file in a safe place and enter the password you created for your encryption key.



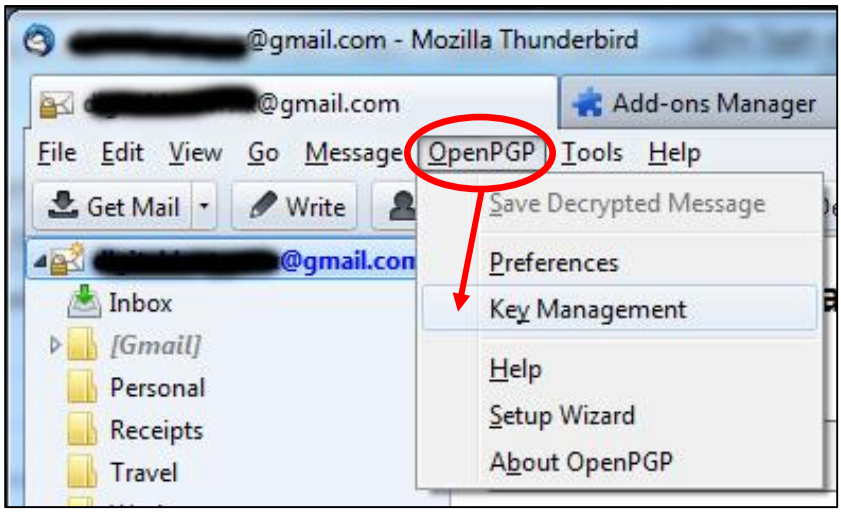
Encrypted Email (continued):

Setting Up Encrypted Email (continued)

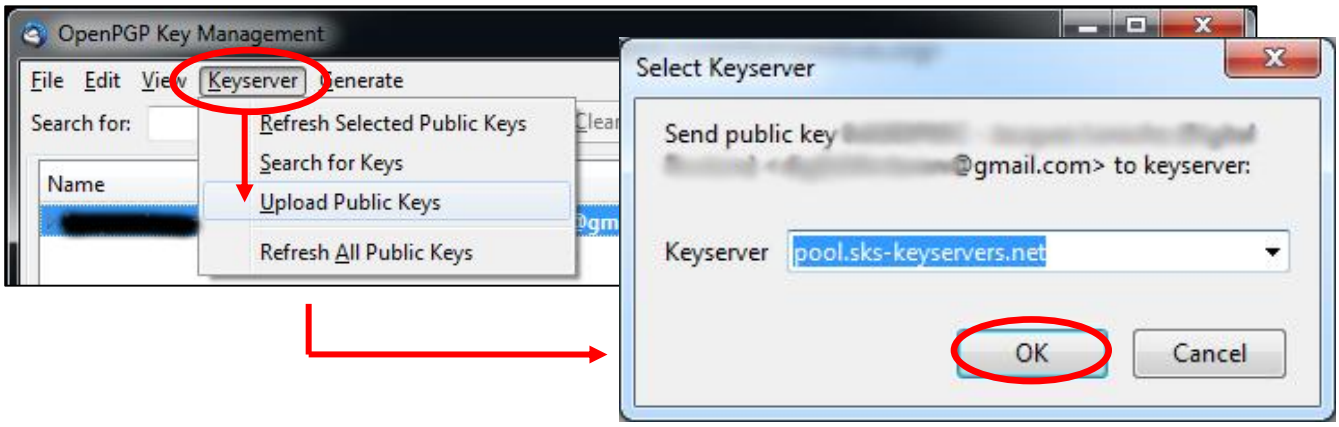
Send and Receive Encrypted Email:

1. Before sending out encrypted mail to your intended recipient you will need to share your public key with them. You can either give it to them directly (either personally on a thumbdrive, CD, etc.), or via email. You can also put your public key on a server which hosts public keys and then tell your recipient to download your key from that server.

To upload your key to the public key server click on the 'OpenPGP' tab, then click on 'Key Management'



2. Select the public key you want to send to the Keyserver. Click the 'Keyserver' tab, then click on 'Upload Public Keys'. A dialog box will appear showing you which public key will be uploaded to the Keyserver. Click the 'Ok' button.

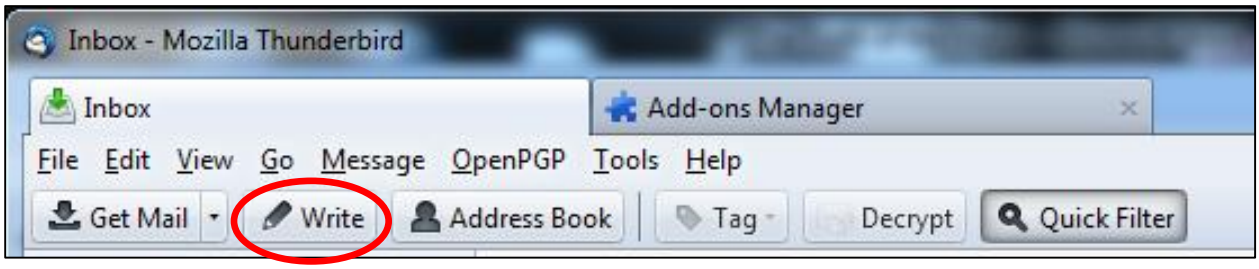


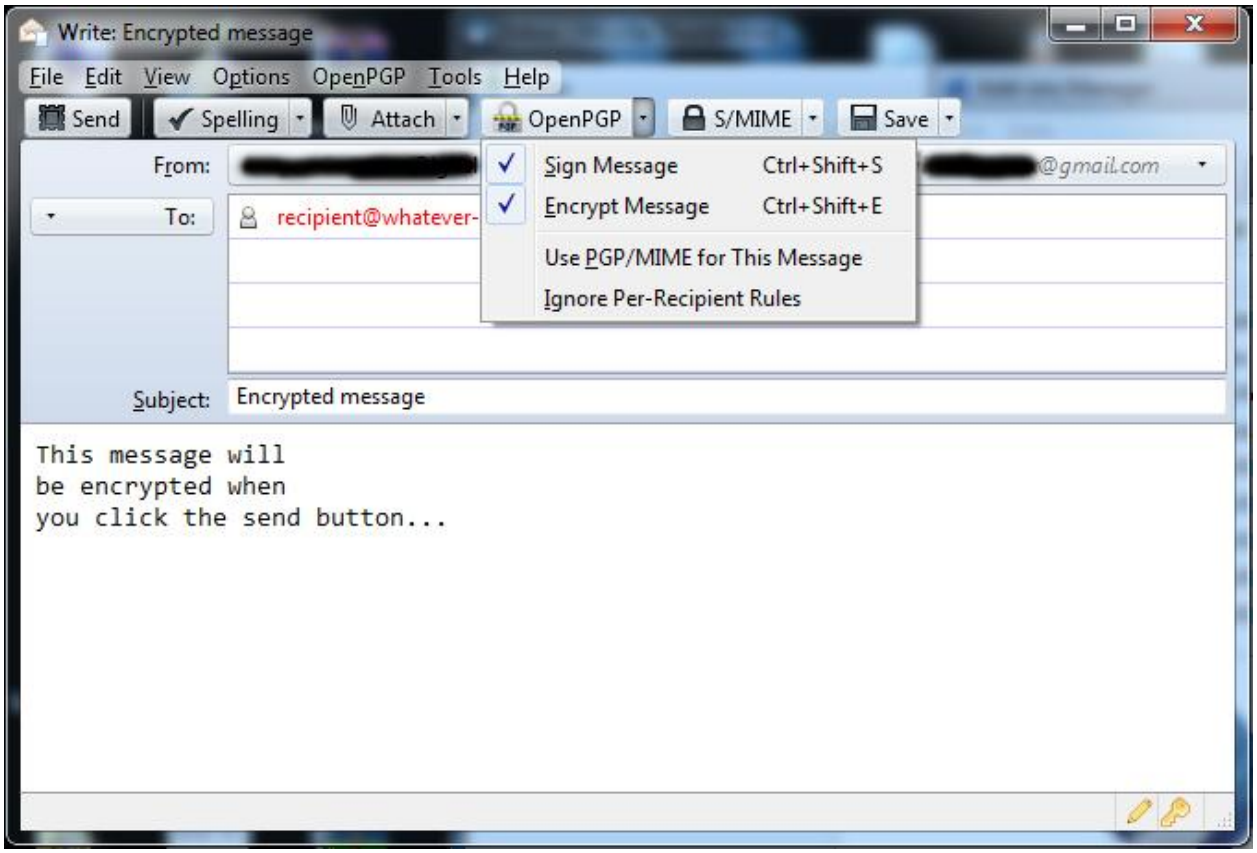
Encrypted Email (continued):

Setting Up Encrypted Email (continued)

Send and Receive Encrypted Email (continued):

3. Now that your recipient has your public key you can send them encrypted mail. Click on the 'Write' button in Thunderbird. Compose your email and before sending it click on the "OpenPGP" button. Make sure "Sign Message" and "Encrypt Message" are both checked.



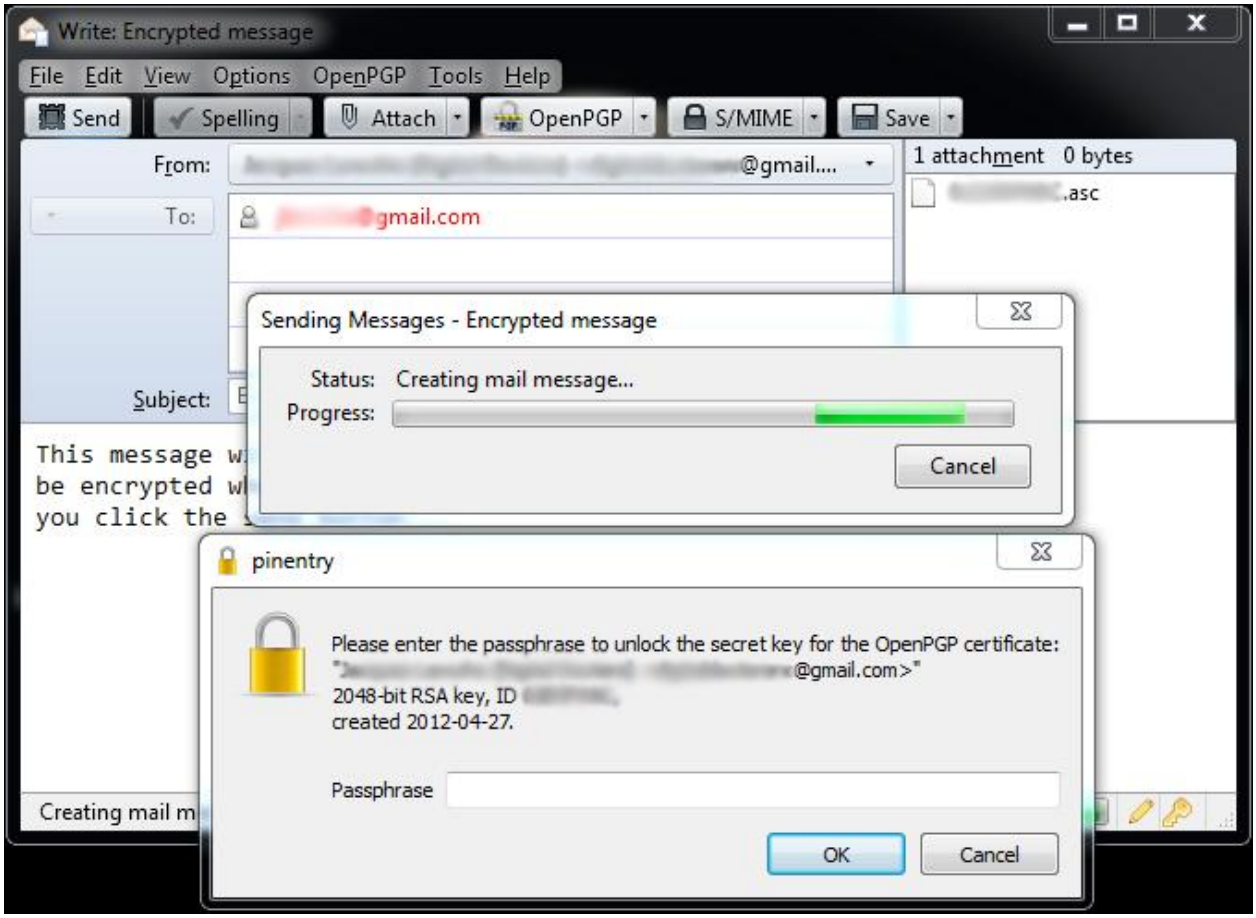


Encrypted Email (continued):

Setting Up Encrypted Email (continued)

Send and Receive Encrypted Email (continued**):**

4. After clicking the "Send" button you will be prompted to enter the passphrase associated with the encryption key you generated earlier. Enter your passphrase and click on the "OK" button to send your encrypted email.

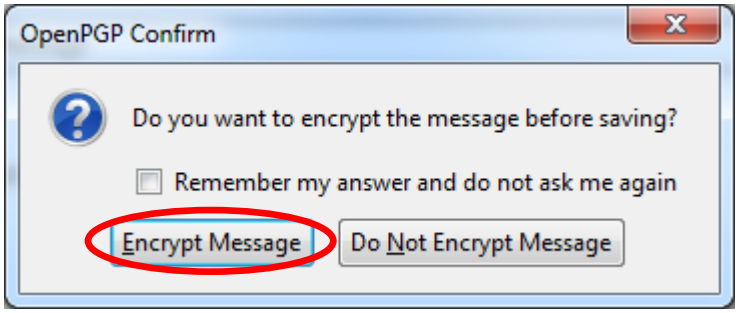


Encrypted Email (continued):

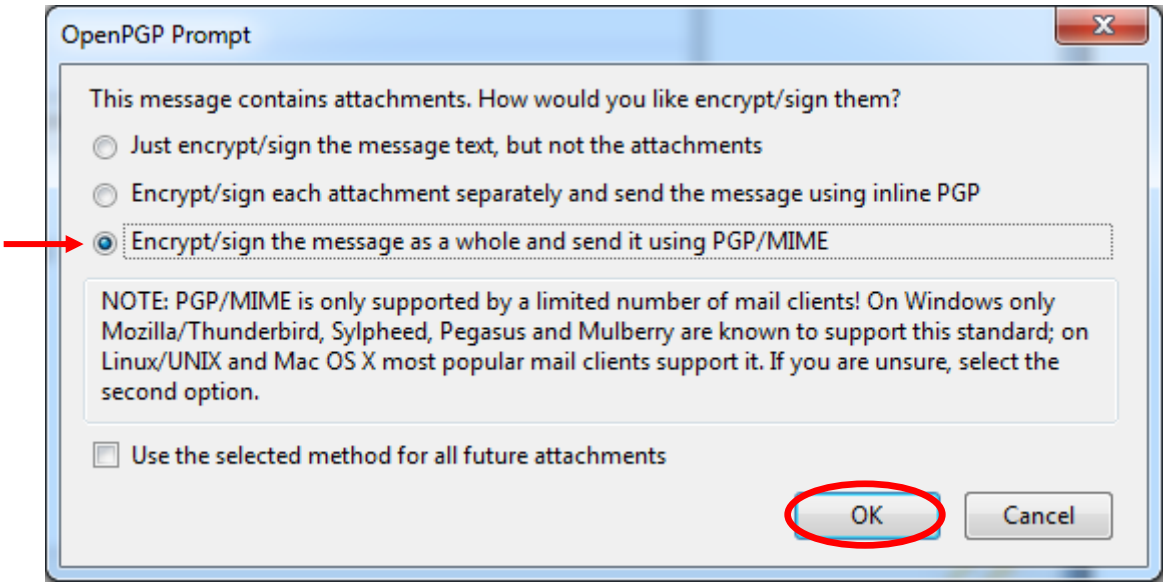
Setting Up Encrypted Email (continued)

Send and Receive Encrypted Email (continued):

Note: Many email services periodically save your email messages as a draft *before* they are even sent out to your recipient. This is a legitimate feature that can save you a lot of time and heartache if you are in the middle of drafting an email and your computer freezes, the power on your laptop runs out, etc. Unfortunately, if you are sending sensitive information to someone you probably don't want to have the content of your emails sent over to your email providers servers in legible 'plain text'. Fortunately, when your message is going to be saved as a draft Enigmail will ask you whether you would like to encrypt the saved the draft of your email.



Also, if you are sending an email with an attachment you will be prompted with the following message. For maximum security you want to make sure you Encrypt the attachment(s) along with your email.



Encrypted Email (continued):

Using Encrypted Email: Best Practices

As stated in the Encrypted Email Overview, the way typical email encryption works is that you have a public key and a private key (also known as Public Key Infrastructure, or PKI). You, and only you, will be using and have access to your private key. Your public key is to be handed out to anyone you choose, or can even made publicly available on keyservers (highlighted in the **Send and Receive Encrypted Email** section above).

When you send an email to someone you can use your private key to digitally "sign" the message so that the recipient can be sure it is from you. Digitally signing is a great way to ensure authenticity: if your friends and family are conditioned to know that messages from you will contain your digital signature, they will realize that any unsigned message they receive from your email address (which could be spoofed) is not really from you.

It is also important to encrypt *all* of your messages, not just the confidential or sensitive ones. If you only encrypt a single email message because it contains sensitive information an attacker intercepting your email traffic they will see that 99% of your email is unencrypted plain-text, while one message is encrypted. This instantly makes the lone encrypted email a target to focus time and resources into. If you encrypt all of your messages it would be a much more daunting task for an attacker to sift through. For example, after investing the time and effort into decrypting countless messages that simply say "Lets meet for dinner" or "how was your weekend?" the attacker will most likely not waste any more time on your email (or at least will be significantly slowed down).

ANONYMITY IN THE SWARM:

a practical guide to online security

version 1.3

Chatting:

An Overview

Since the release of ICQ in 1996 and AOL Instant Messenger in 1997 Instant Messaging (or, IM) has increased in prominence as a means of communication. Unfortunately, a majority of the transmissions sent via IM are done so with no privacy or security protections. Logs containing information about who is chatting (Username), where the parties are located (IP addresses), when they were chatting (Time and Date Stamps) and what they were chatting about can be retrieved by the companies providing the chat software, 3rd parties requesting that information, eavesdroppers, and other unauthorized entities. Fortunately, it is very easy to use IM technology with encryption to keep your communications private.

A Little Background Into IM Technology

Today, there are numerous companies offering IM services. Some of these include Google Talk, MSN Messenger, Yahoo!, MySpaceIM, and Jabber. Infrastructurally, these services are set up in one of three ways: in a centralized setup, in a peer-to-peer setup, or with a mixture of the two.

In a centralized setup, users are connected to each other through a series of servers. These servers link together to form a large network. When you send a message, the servers locate your recipient's computer and route your message through the network until it ultimately reaches its destination. MSN Messenger uses this method to send messages.

In the peer-to-peer setup a central server keeps track of who is online and what their unique IP addresses are. After you log into your IM client, the central server sends you the IP addresses of everyone on your contact list that is currently logged on. When you send a message to one of your contacts it is sent directly to the person's computer without being routed through any of the IM sclient's servers. ICQ uses this method to send messages.

In a mixed setup both setup methods are employed. For example, AOL's AIM combines the centralized and peer-to-peer setup methods. When you send a message, it travels along AOL's servers. However, when you transfer files, pictures, or voice messages, a peer-to-peer connection is established between the sender and receiver with no AOL servers involved.

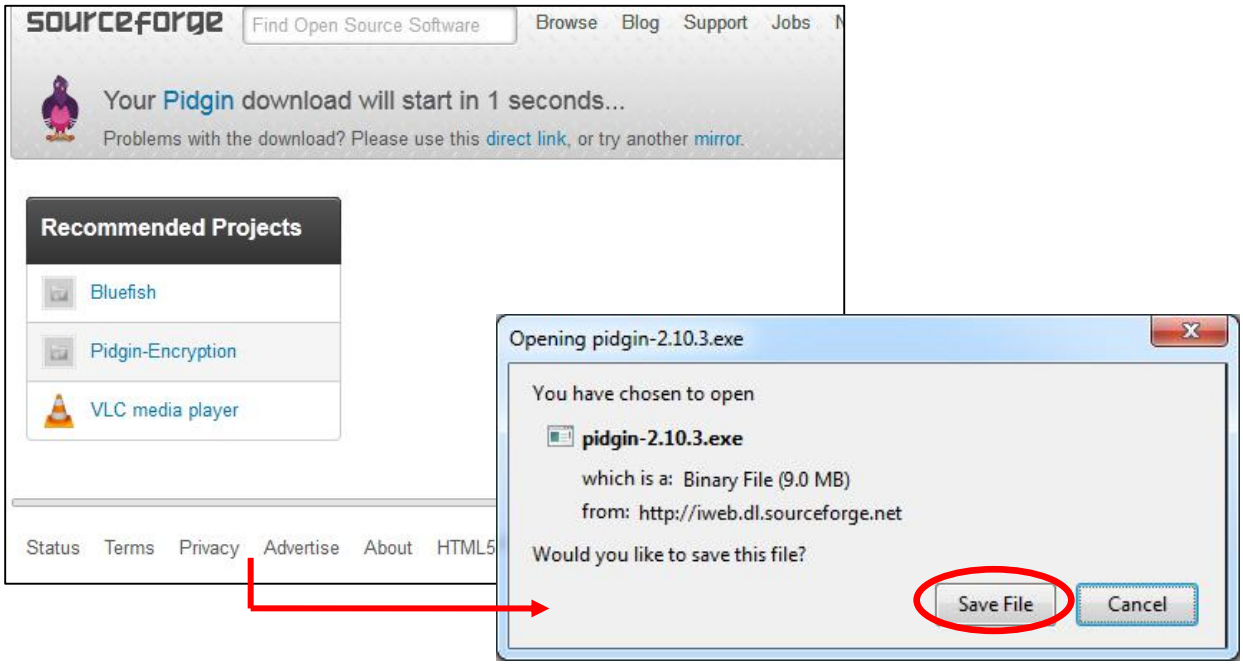
Chatting (continued):

Using IM More Securely: Pidgin, and the Pidgin Encryption Plugin

Although encryption isn't typically offered in the IM software clients released by AOL, Yahoo!, or MSN it is still possible to encrypt your messages so they are secure and private - regardless of the IM client you use. This can be done through a program called Pidgin which allows you to use any of the popular IM clients all from within one simple interface. The following instructions are tailored for a computer running Windows.

Installing Pidgin
http://pidgin.im/

1. Go to http://pidgin.im and click on the "Download Pidgin" button on the left-hand side of the page. Your download will start automatically and a dialog box will appear allowing you to save the file on your computer.



Chatting (continued):

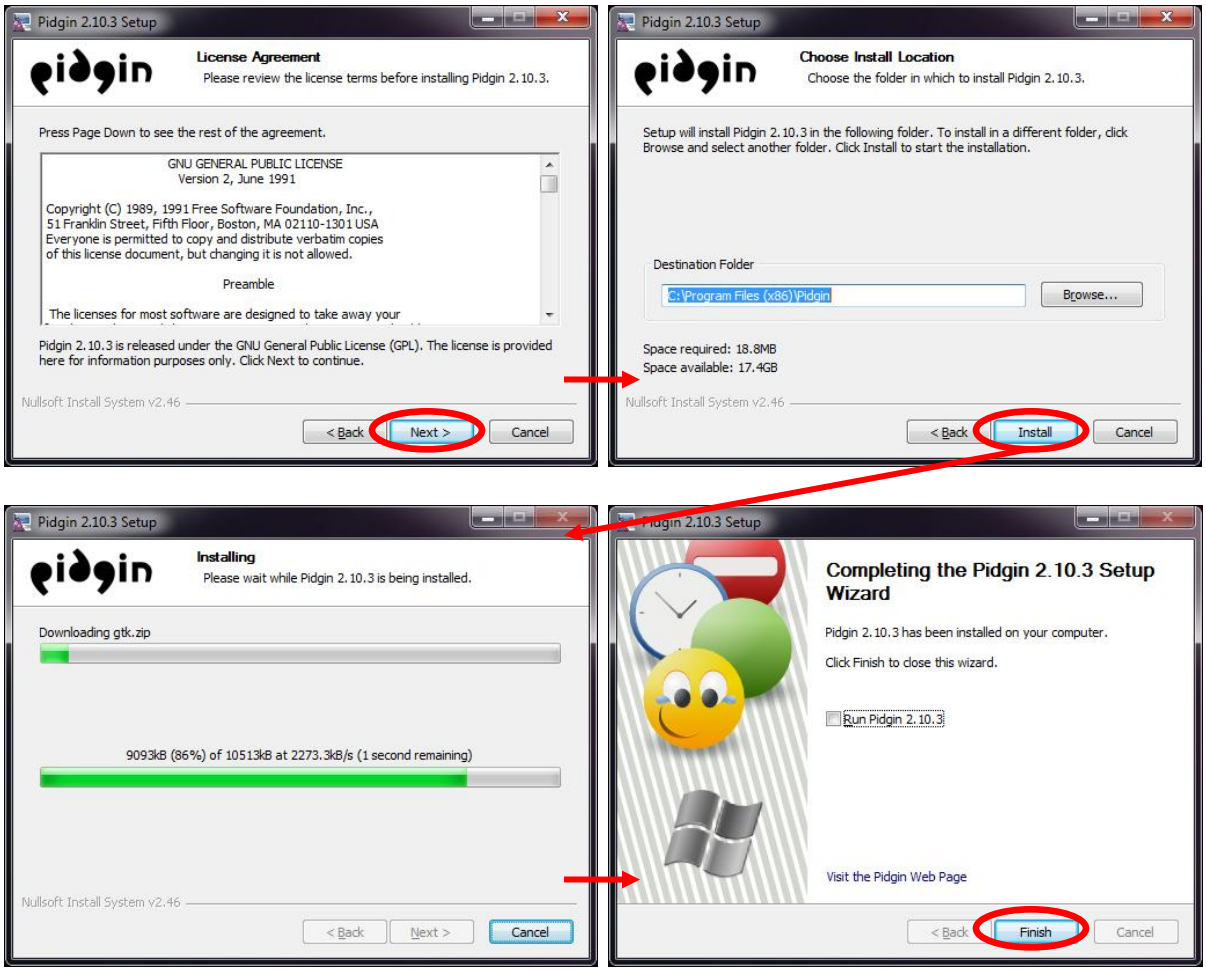
Installing Pidgin (continued)

2. Open the downloaded file. Click on the "OK" button, then click "Next" in the Setup Wizard.

Chatting (continued):

Installing Pidgin (continued)

3. Click the "Next" button on the License Agreement page, then click the "Install" button and the "Finish" button once the installation is complete.

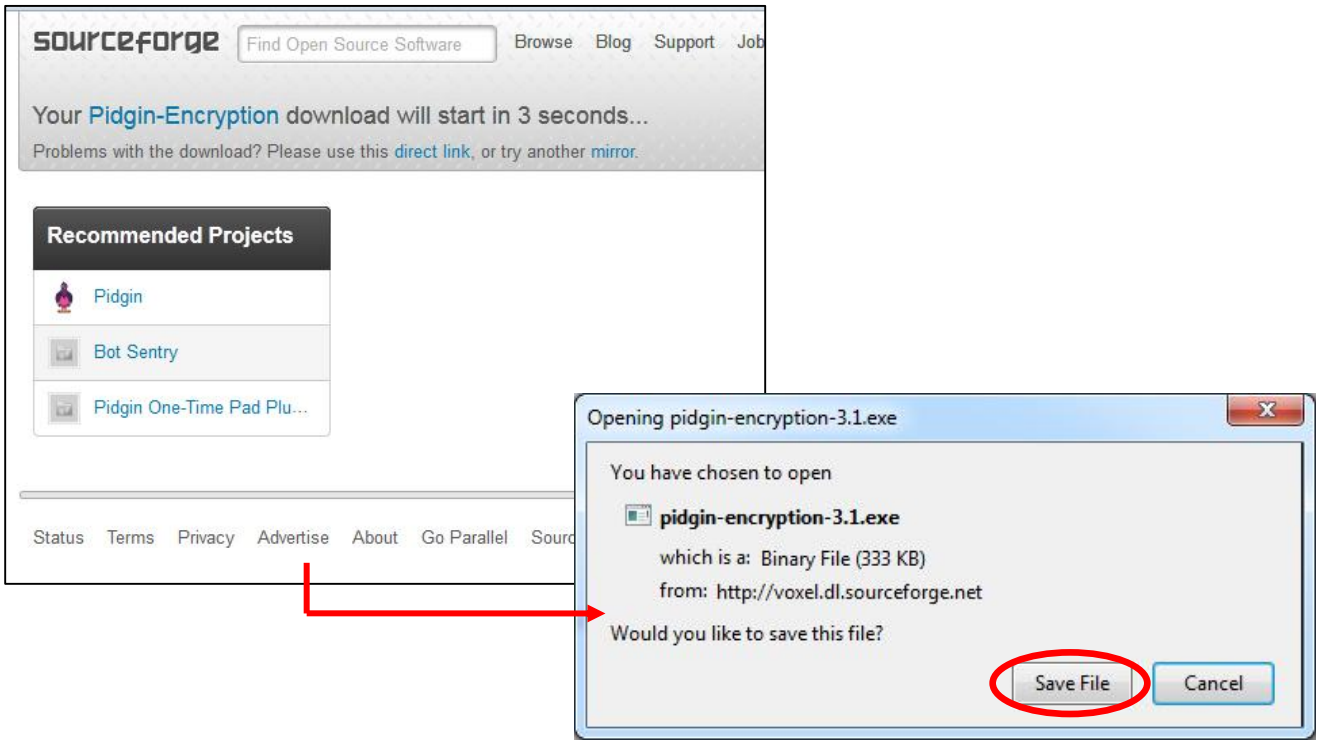


Chatting (continued):

Using IM More Securely: Pidgin, and the Pidgin Encryption Plugin

Installing Pidgin Encryption
http://pidgin-encrypt.sourceforge.net/

1. Now that you have installed Pidgin you need to install the Pidgin Encryption Plugin. Go to http://pidgin-encrypt.sourceforge.net/ and click on the "Win32 self-extracting binary" link. Your download will start automatically. Click on the "Save File" button to start the download.



Chatting (continued):

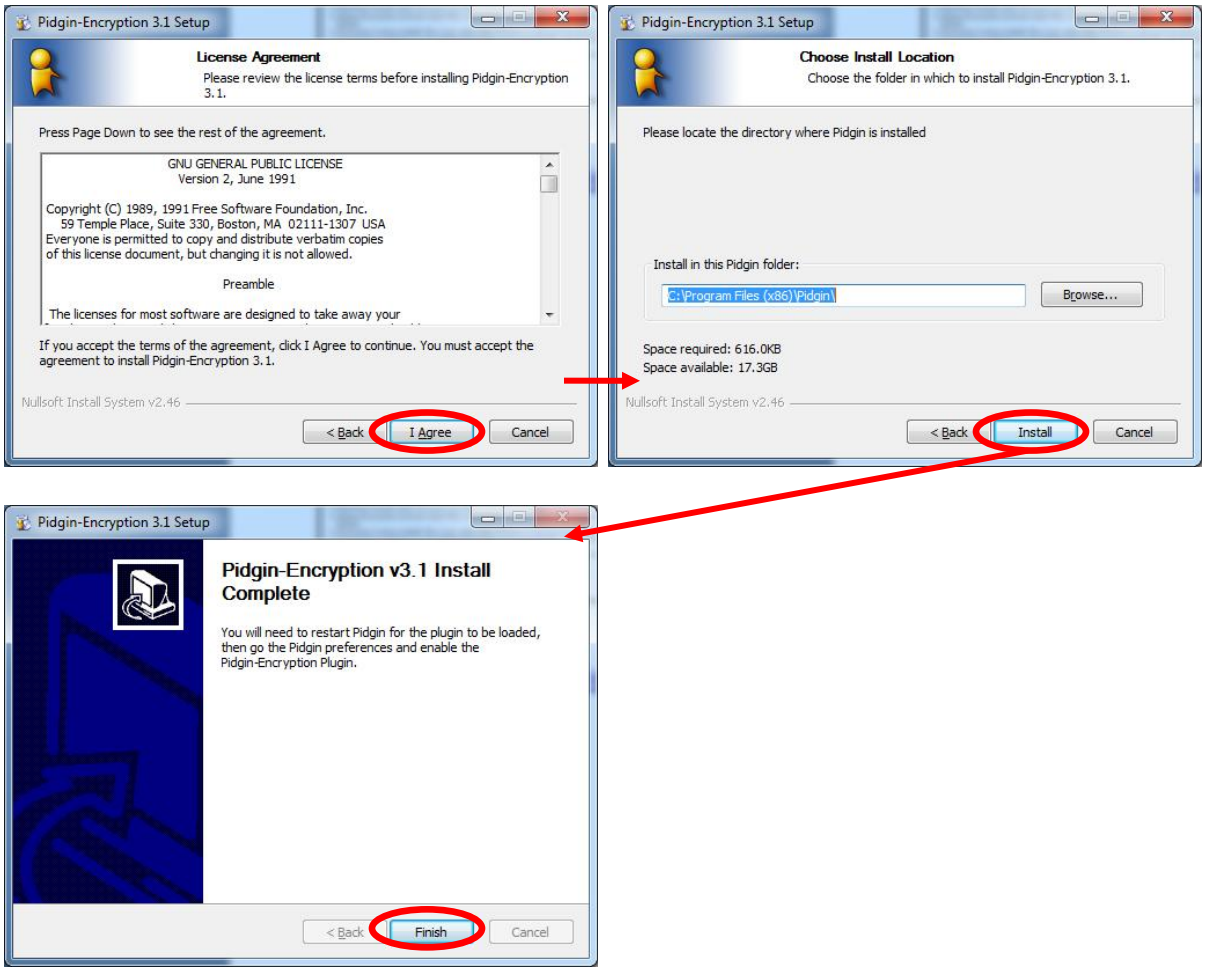
Installing Pidgin Encryption (continued)

2. Open the downloaded file. Click on the "OK" button, then click "Next" in the Setup Wizard.

Chatting (continued):

Installing Pidgin Encryption (continued)

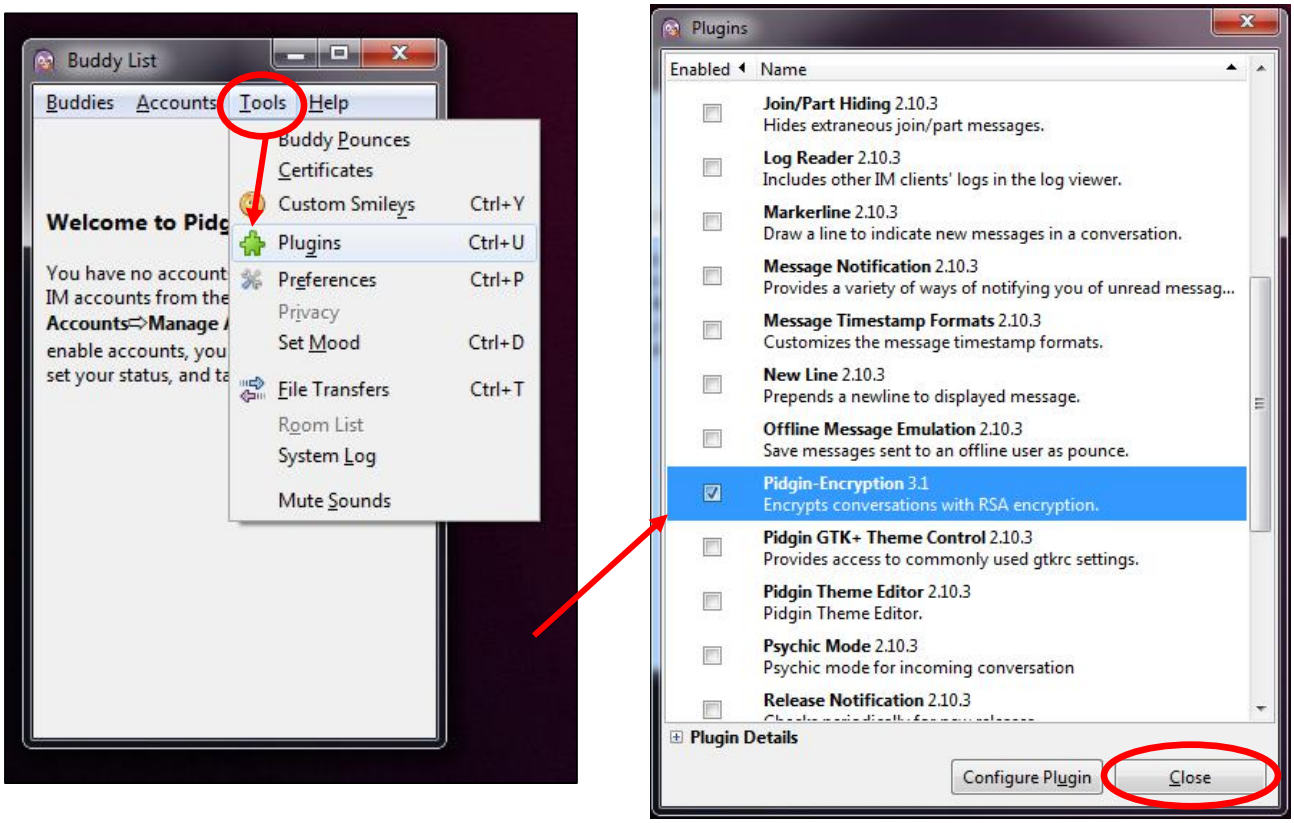
3. Click the "I Agree" button on the License Agreement page, then click the "Install" button and the "Finish" button once the installation is complete.



Chatting (continued):

Installing Pidgin Encryption (continued)

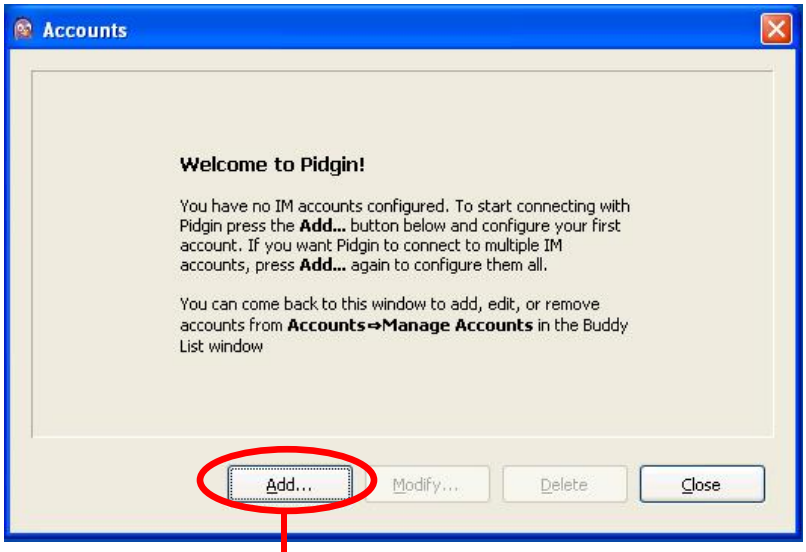
4. Open Pidgin (close any dialog about adding an account - we will do that later). Click on the "Tools" tab, then click on "Plugins". Scroll down until you see the "Pidgin-Encryption 3.1" plugin and click on the checkbox next to it. When you are done click the "Close" button.

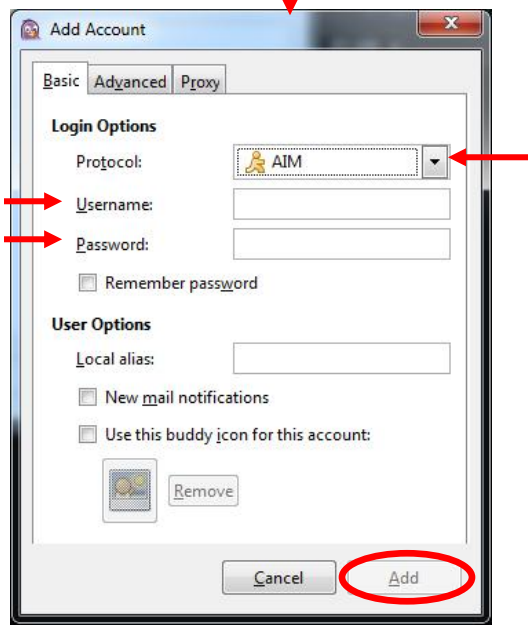


Chatting (continued):

Setting Up Pidgin, Chatting with Encryption

1. When you open Pidgin you should see a dialog welcoming you to Pidgin and telling you no accounts are configured. Click on the "Add..." button. Choose the Protocol you will be using (AIM, Facebook, MSN Messenger, Google Talk, etc.), then enter your username and password for that account. Click on the "Add" button when finished.

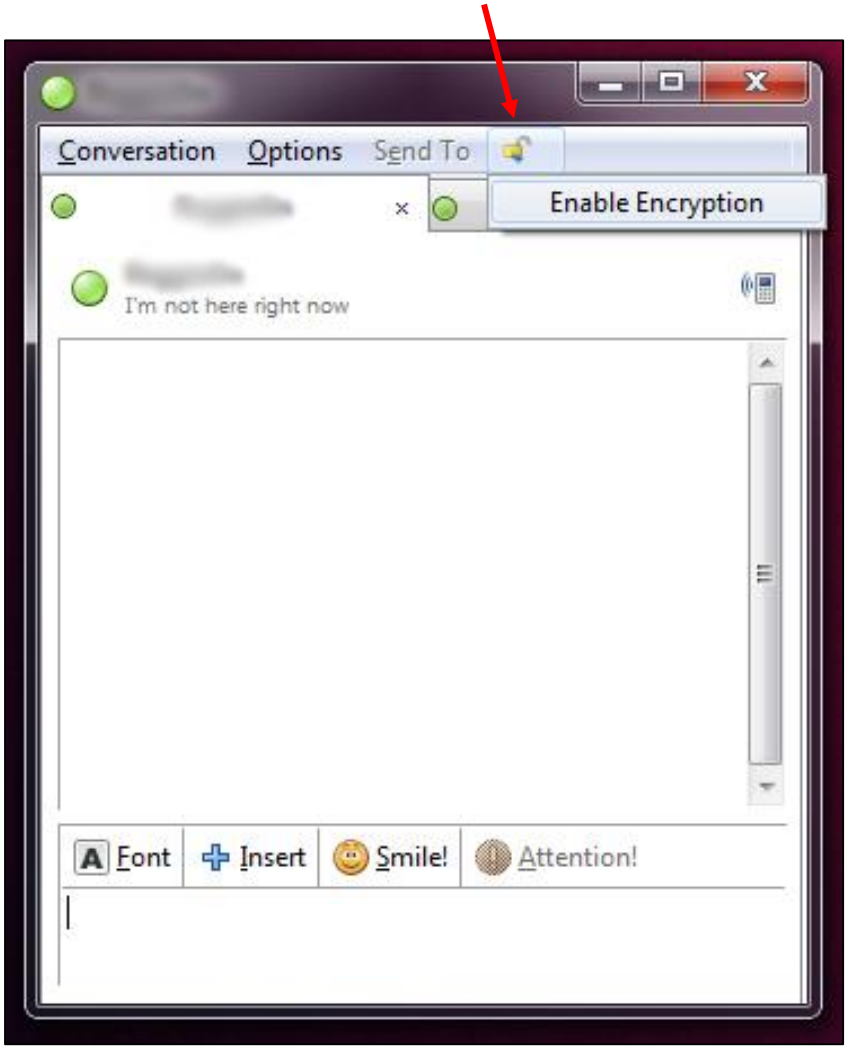




Chatting (continued):

Setting Up Pidgin, Chatting with Encryption (continued)

2. Now you can have an encrypted conversation with someone. Remember that both you and the person you are chatting with must have Pidgin Encryption set up. When you open a chat window with someone in your friend list you will see a small lock at the top of the screen. Click on the lock and then click on "Enable Encryption" to begin encrypted communications.



Note: For added anonymity I would suggest all parties who plan to communicate set up an IM account via AIM (or another client) without any personally identifiable information via TOR. Trade your login names in person and then use Pidgin with Pidgin Encryption to chat.

VoIP:

What is Voice Over IP?

Voice Over IP, or VoIP is a communication method where traditional phone data is transmitted via Internet Protocol (or, IP). Basically this means services like phone calls are transported over the internet rather than traditional phone lines. In addition to voice, VoIP systems can also transmit video information.

VoIP can be software-based or hardware based. Software-based VoIP can be installed on a computer, or a smart phone allowing the user to make telephone calls – usually for free. Skype is a good example of software-based VoIP. An example of hardware-based VoIP is a phone that connects directly to the internet (e.g. via a cat-5 network cable). These phones are usually sold to businesses as a cost-saving method when compared to older telephone service.

Secure VoIP: The Trouble with Skype

A few years ago Skype was a good choice for secure audio & video communication and was receiving attention from governments due to its effectiveness. Wikileaks documents showed that in late 2007 the German government apparently had trouble tapping into Skype communications, and in 2009 the NSA seems to have been troubled by Skype's encryption methods as well.[7]

Unfortunately, things have changed. In early 2011 Skype was purchased by Microsoft and there are concerns that a backdoor has been installed in Skype which will allow the government to intercept Skype communications.[8] These concerns seem valid as Microsoft filed a patent in December 2009 called "Legal Intercept" which details a system that can inconspicuously record VoIP communications and mentions Skype specifically (despite the fact they had not even purchased Skype yet).[9] Additionally, even without Legal Intercept, a number of academic studies show that sophisticated analysis of Skype's encrypted communications can reveal key

[7] See http://www.techdirt.com/articles/20080127/10382079.shtml for the German government's trouble with Skype encryption. See http://www.theregister.co.uk/2009/02/12/nsa_offers_billions_for_skype_pwnage/ for the NSA's trouble with Skype's encryption.
[8] See http://memeburn.com/2011/07/microsoft-and-skype-set-to-allow-backdoor-eavesdropping/ and also http://www.thetelecomblog.com/2011/06/29/microsoft-patents-legal-intercept-technology-will-skype-have-a-backdoor/
[9] The patent can be seen here: http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&f=G&l=50&d=PG01&p=1&S1=20110153809&OS=20110153809&RS=20110153809

VoIP:

Secure VoIP: The Trouble with Skype (continued)

aspects of the of the unencrypted data: the length of the conversation, the language being spoken, and portions of the actual conversation.[10]

Back In 2005 Phil Zimmerman (the creator of encrypted email) began work on an encrypted VoIP software solution called Zfone.[11] Regrettably, the software is still in Beta development and as of January 29th, 2011 the download section of the Zfone website is not functional. After locating the Zfone software from other sources I ran a number of tests, but could not get it to running properly.

In the end, doing anything that you consider sensitive via VoIP and Skype in general is strongly discouraged. If you must have real-time communication it is advisable to meet in person[12].

[10] Language Identification: http://www.cs.jhu.edu/~cwright/voip-vbr.pdf
The pitfall of variable-bit-rate encoding: http://www.technologyreview.com/Infotech/20913/?a=f
Linguistic analysis attack: http://www.securityweek.com/defeating-skype-encryption-without-key
On data leakage despite encryption: http://www.csee.usf.edu/~labrador/Share/Globecom/DATA/01-038-02.PDF

[11] See http://zfoneproject.com/getstarted.html

[12] If meeting in person is not possible due to geography, please stay tuned for the next installment of Anonymity in the Swarm which aims for include a section on Mobile Phone security.

Upcoming Editions:

Mobile Phones

Smartphones have all but replaced phones that aren't overstuffed with technological capabilities. As a result, many of us are walking around with and using phones that are virtually mini-computers. But, with all that computing power and all those features come a lot of risks for security: SMS (text messages), email and phone calls are all generally unsecure and unencrypted.

The next edition of Anonymity in the Swarm will cover Mobile Phone security and usage.

File Transmission

Transferring files and documents online is an essential task many of us perform daily, but delivering those files securely is not done with the same frequency.

The next edition of Anonymity in the Swarm will cover methods for transferring files securely online.