ENCRYPTION: THE PATH TO SECURE COMMUNICATION

Digital communications is the backbone for all of our organizing work. Whether it's phone, text, whatsapp or facebook messenger we are constantly in communication with each other, our families, and our movements.

The problem is that almost all of these forms of communications are easily surveilled. We must maintain habits that safeguard the data shared when collaborating or working with other communities, activists, and each other. Encrypted communication protects our right to privacy when the laws and corporate platforms do not.

That is where **End-to-End Encryption Messaging (E2EE)** comes in! E2EE is designed to keep eavesdroppers out of the conversation. Think of it as putting a seal on the users' messages, especially as they travel across the social web, and only the sender and recipient have the tool to break open this seal. Even companies that own the messaging platform would not have the means to decrypt the files.

While many apps say they offer E2EE, we give Signal our highest recommendation because they store the least amount of data and was developed by progressive developers to explicitly protect the right to privacy.

WhatsApp, Facebook, and Apple Imessage all offer some form of E2EE but these corporations still monitor and share the content of your data while not being transparent about what

they would share with a government agency if you are targeted.

Sometimes these platforms may be the only way to reach people. Implement Signal where possible but if you must use these other tools only do so when necessary. We highly recommend you practice resk reduction by enabling encryption and verifying contacts.

Finally, we want to emphasize that digital communications still comes second to face to face meetings. However, we do realize this may not be possible for many collaborations. So, ultimately, we emphasize that the best security is **discretion**. If you have things you want confidential then do not say them on communication platforms. Say only what you feel comfortable having a government official knowing because you do not know when your communications might be compromised.

SO PLEASE BE SAFE AND BE STRATEGIC IN WHAT YOU SAY, WHOM YOU SAY IT TO AND WHEN.

Now let's explore then how to send End-to-End Encryption Messages on each of these platforms.

SIGNAL

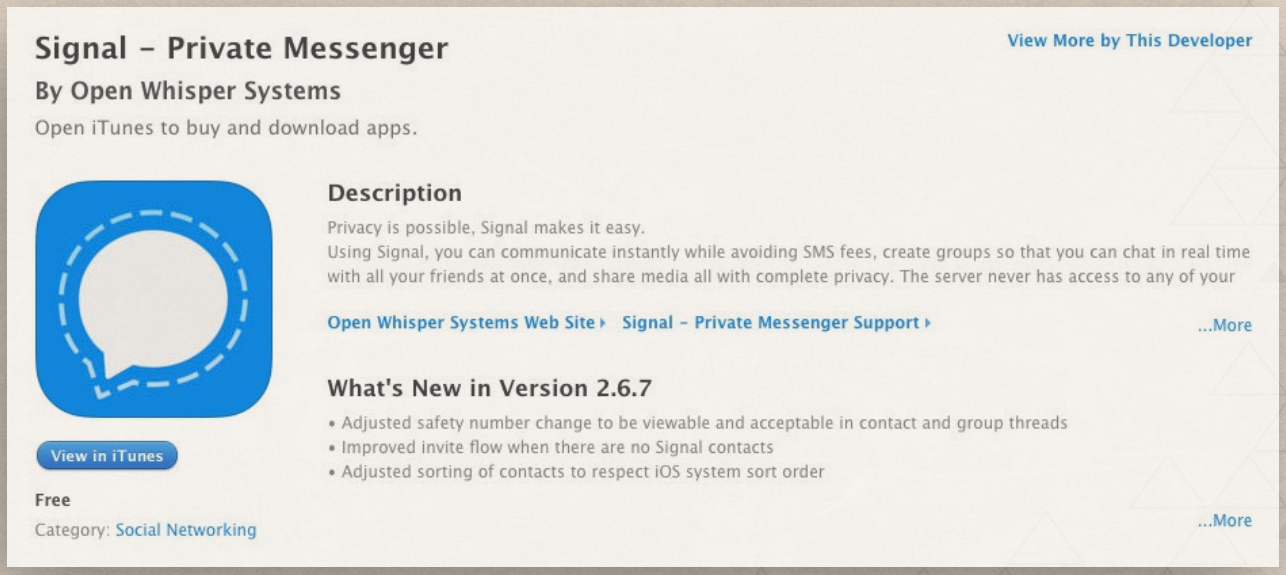
Signal[38] is a free and open source communication app for Android and iOS that employs end-to-end encryption, allowing users to have encrypted conversations with other Signal users and send end-to-end encrypted texts, group texts, photos, and video messages. Signal uses your data connection, so all parties in a Signal communication must have internet access on their mobile devices. **Signal users don't incur SMS and MMS fees**.

You can download Signal as an app on your phone or use it as a browser extension on your computer.

SIGNAL FOR ANDROIDS AND IPHONES

When you search for the app on your mobile device, make sure to select the version developed by Open Whisper Systems. Download the app, then click Install. You'll see a list of functions, such as TK, that Signal needs to access in order to work properly.

- ☑ Click **Accept**. After Signal has finished downloading, click **Open** to launch the app.

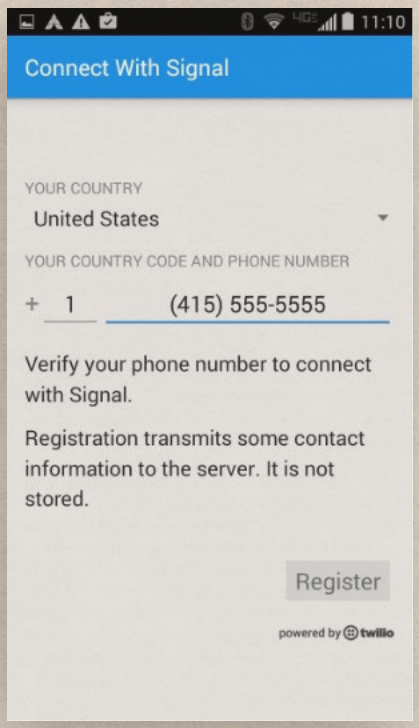


38 https://ssd.eff.org/en/module/how-use-signal-android

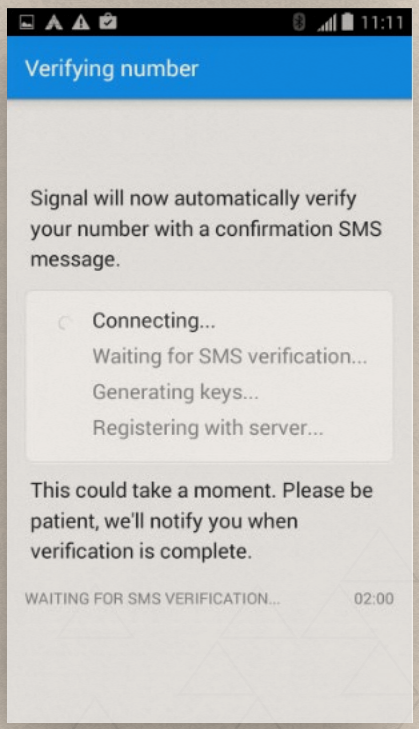
NOTE: The guiding screenshots here are from an Android phone but the procedure is similar for iPhones.

INSTALLING SIGNAL AND REGISTERING YOUR NUMBER

Register and verify your phone number. You will see a screen that looks like this:

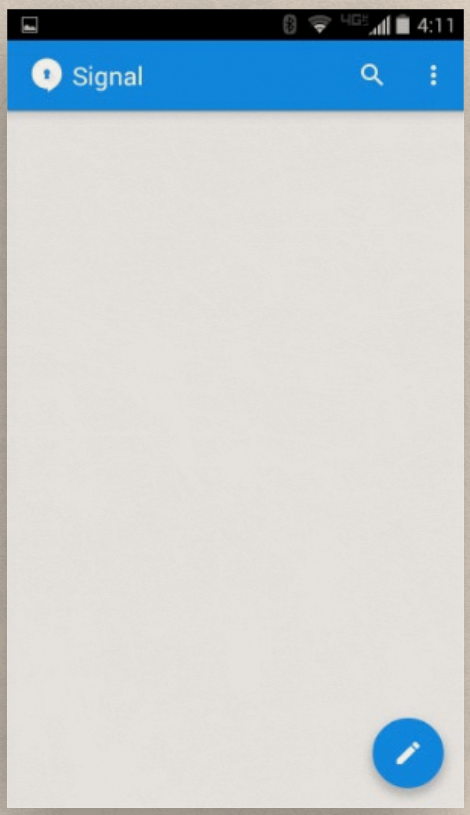


Enter your mobile phone number and click **Register**. In order to verify your number, you will be sent an SMS text with a six-digit code. Since Signal can access your SMS text messages, it will automatically recognize when you've received the code and complete your registration.

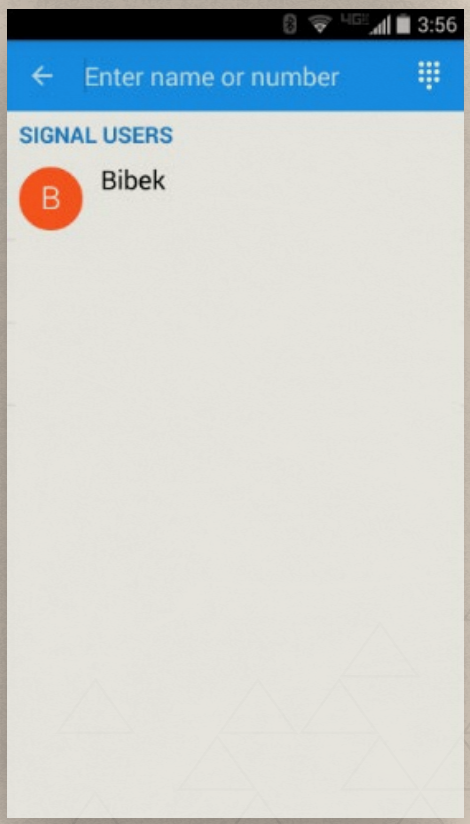


MAKING PHONE CALLS USING SIGNAL

In order to use Signal, the person you are contacting must also have Signal for Android or iOS installed. If you use Signal to send a message to someone who does not use the app, it will send a standard, non-encrypted text message. If you try to call the person, it will place a standard phone call. To get started, click the pencil icon in the lower-right corner of the screen.

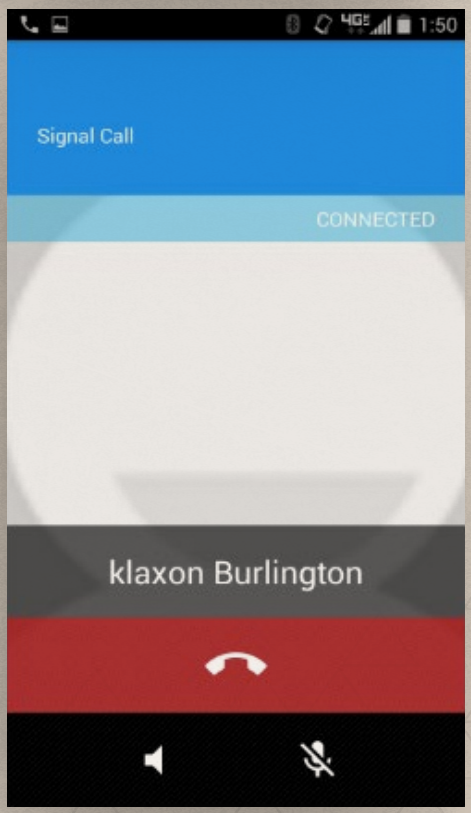


You will see a list of all the registered Signal users in your contacts. You can also enter the phone number of a Signal user who isn't in your contacts. When they are selected, you can choose to either call them or send them a message.



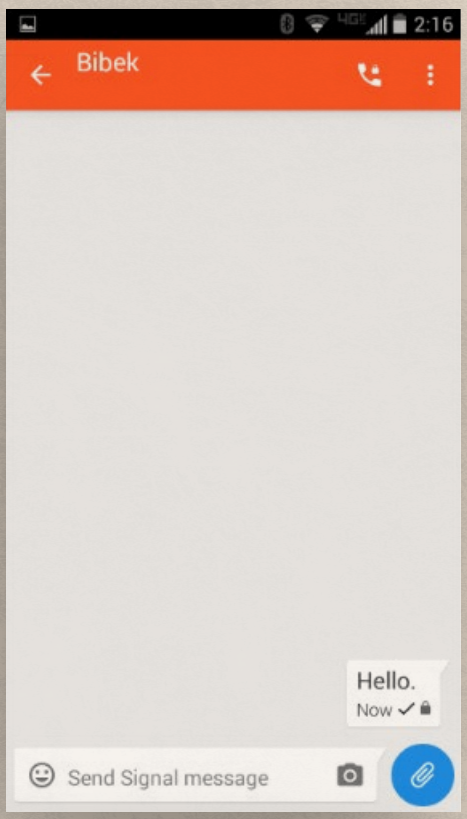
- To initiate an encrypted call to a contact, first check to see that the person can accept Signal calls. Select the contact from your list, then look for a small padlock icon next to the phone icon. Click the phone icon to initiate a call.

- The most trustworthy way to verify a caller's identity is to use out-of-band verification to verify the **word pair**. You can also read the words aloud if you recognize the caller's voice, although very sophisticated attackers might be able to defeat this. The word pair must be identical on both users' phones for you to be sure your message is not being intercepted.

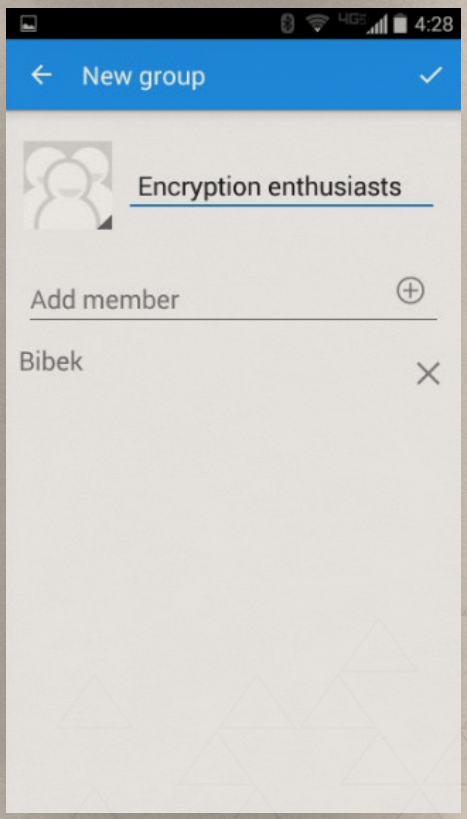


SENDING ENCRYPTED TEXTS

In order to send an end-to-end encrypted text, picture, or video message, navigate to your contact list, click on the contact's name, and send your message.

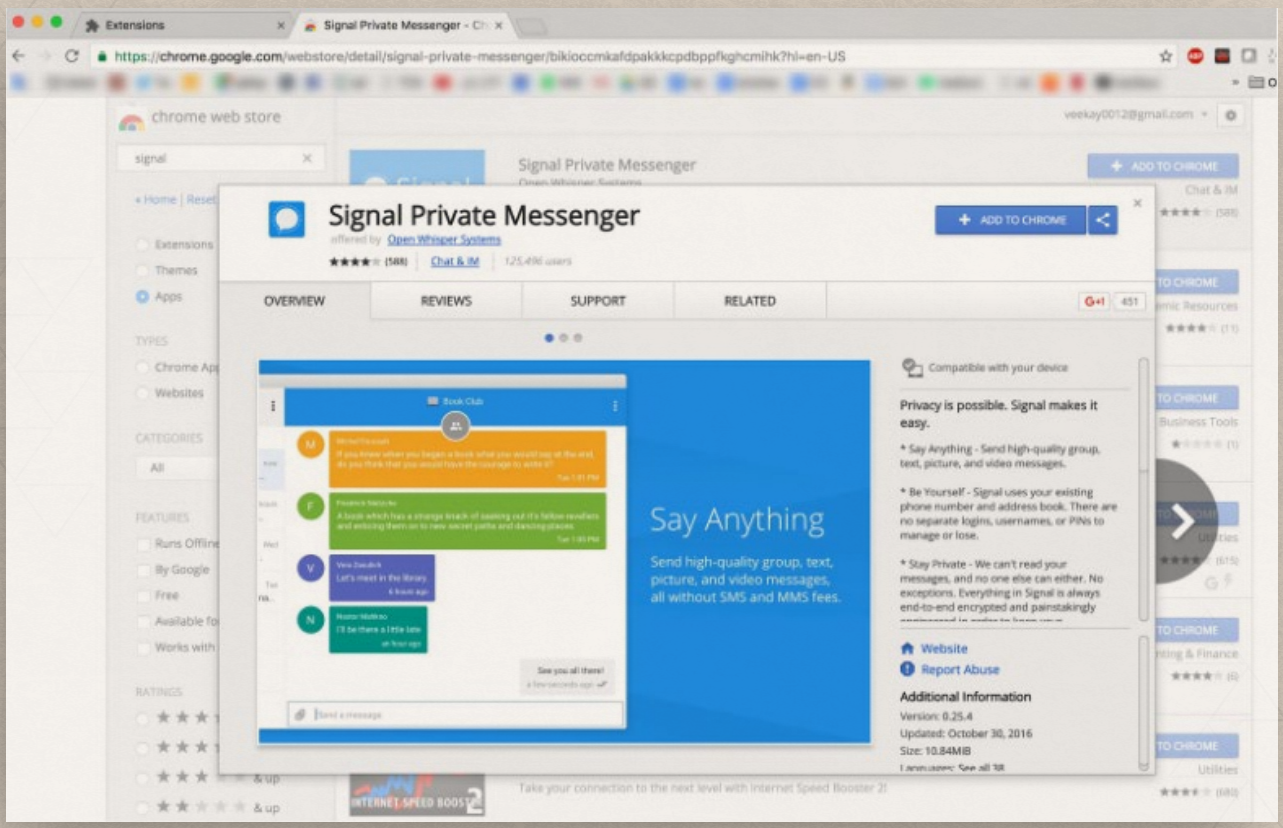


You can send an **encrypted group message** by clicking the overflow icon (the three dots in the upper-right corner of the screen) and selecting "**New group**".

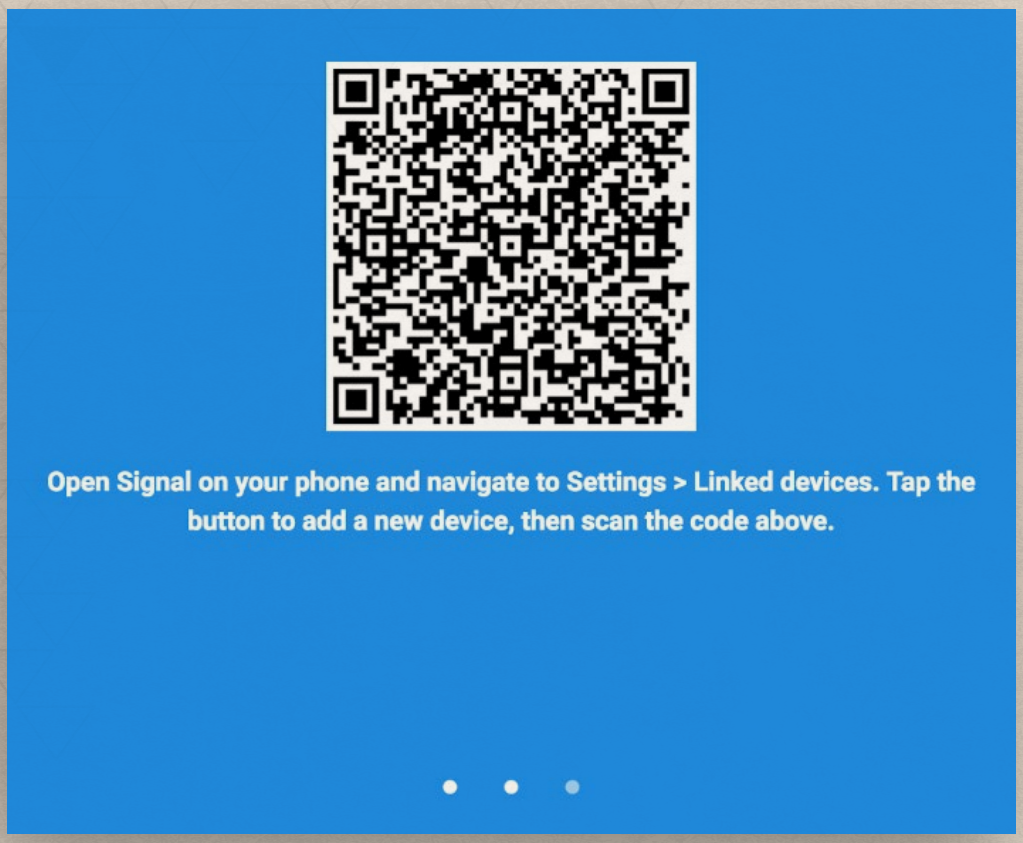


SIGNAL FOR COMPUTER—CHROME EXTENSION

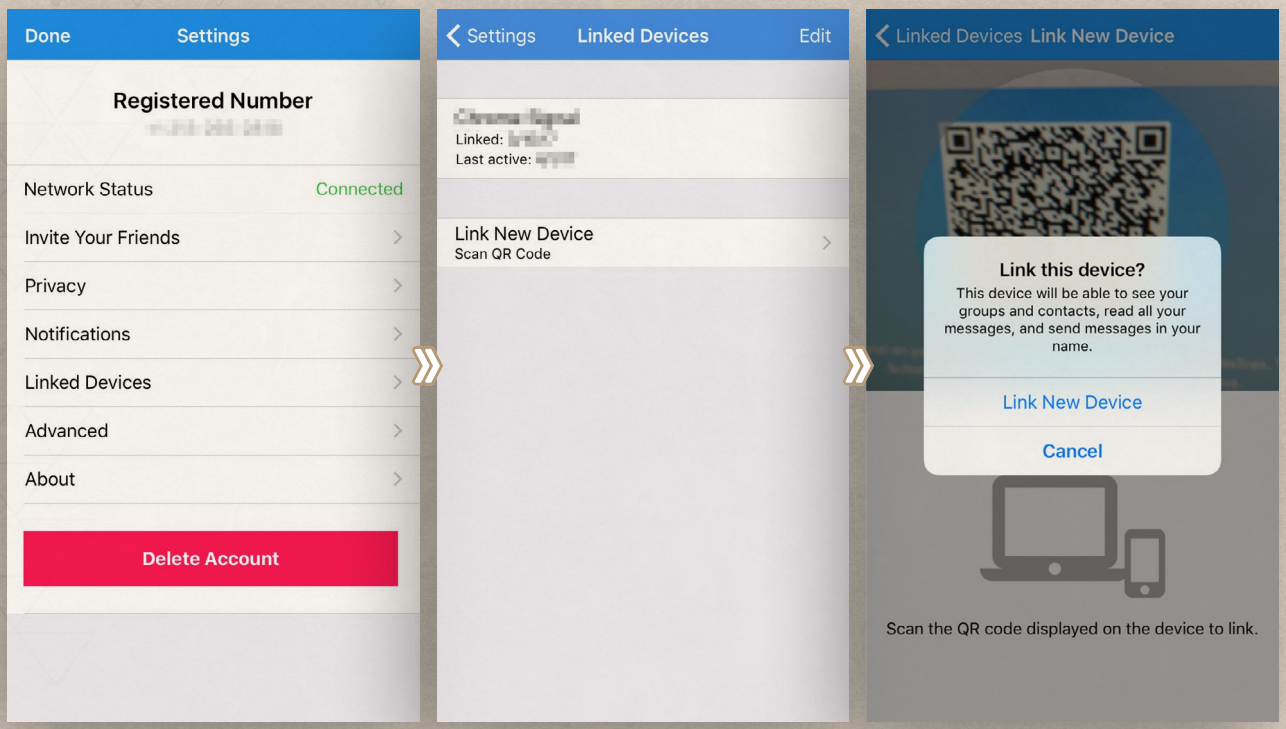
Signal's Google Chrome extension allows you to seamlessly continue text conversations on both your mobile device and computer. All your communications will remain encrypted throughout the process. Signal Private Messenger is a Chrome app that links to your phone, so all incoming and outgoing messages are displayed consistently on all your devices. You can comfortably chat using your full desktop or laptop keyboard.



- [x] Click on Add to Chrome. You will see a scan code, as below.



- Open the Signal app on your phone. Go to **Settings → Linked Devices → Link New Device**. This selection will activate your camera and allow you to scan the code on your computer screen. When prompted, click on **Link New Device**.



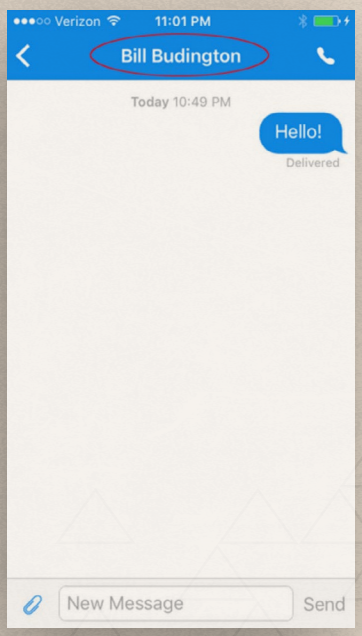
Signal automatically syncs your contacts and messages, so you are good to go.

SAFETY NUMBERS ON—SIGNAL

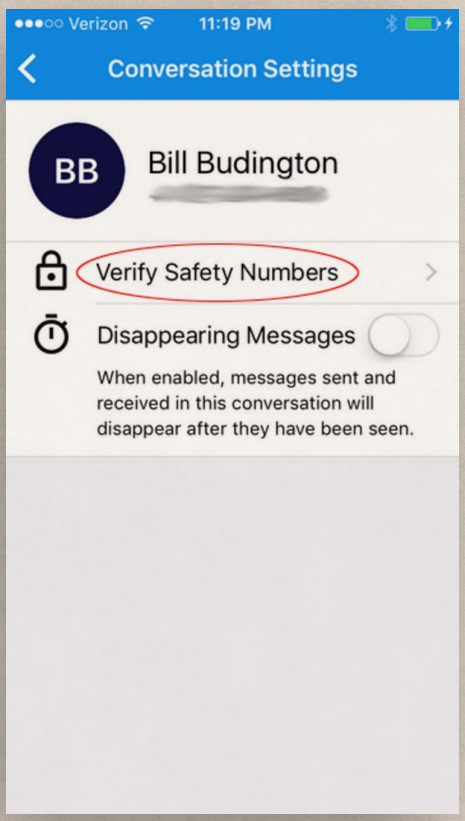
Safety numbers allow Signal users to verify the privacy of their communication with a contact, either by comparing a number or by scanning a single QR code.

- To set this up, open the screen where you are able to message your contact, as described above. From this screen, tap the name of your contact at the top of the screen.

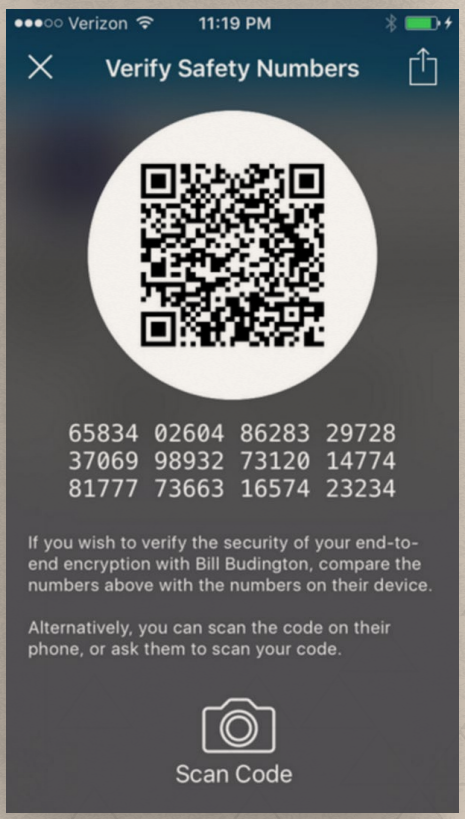
  On the following screen, tap **Verify Safety Numbers**.



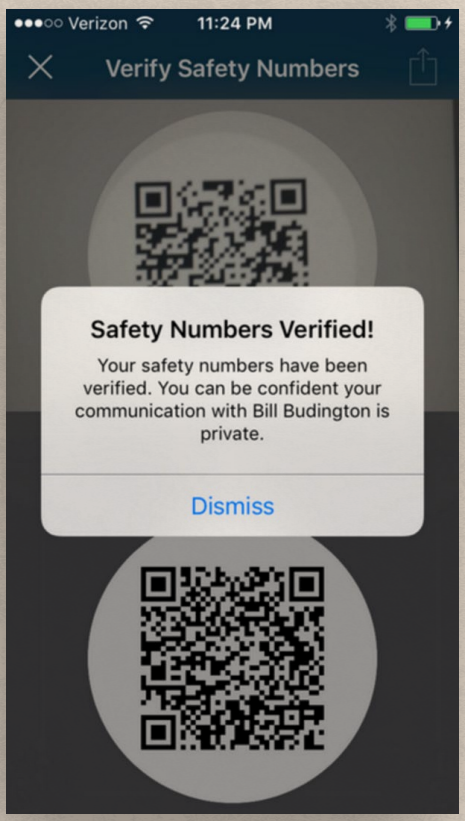
- This will take you to a screen with a QR code and a list of "safety numbers." This code will be unique for every contact. Have your contact navigate to the corresponding screen for their conversation with you, so they have a QR code displayed on their screen as well.



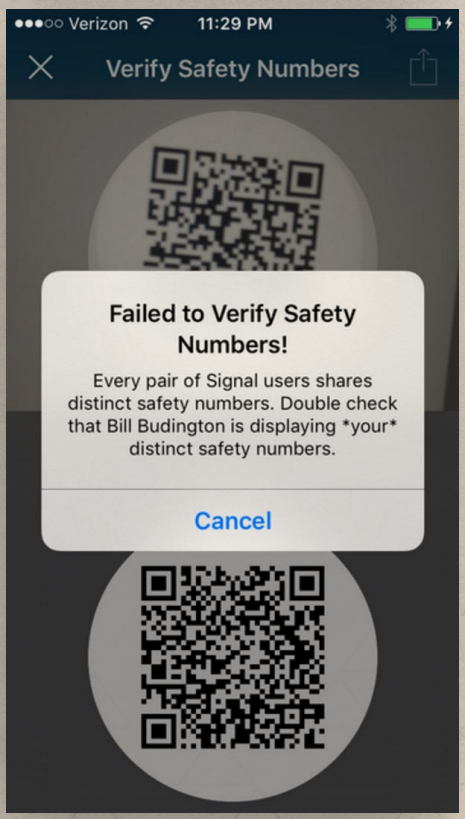
- Tap **Scan Code**. At this point, Signal may ask for permission to access the camera. Tap OK.



- If verification didn't work, you'll see a notification that says "Failed to Verify Safety Numbers!"



- You may want to avoid **discussing sensitive topics with anyone until you have verified keys with them**.

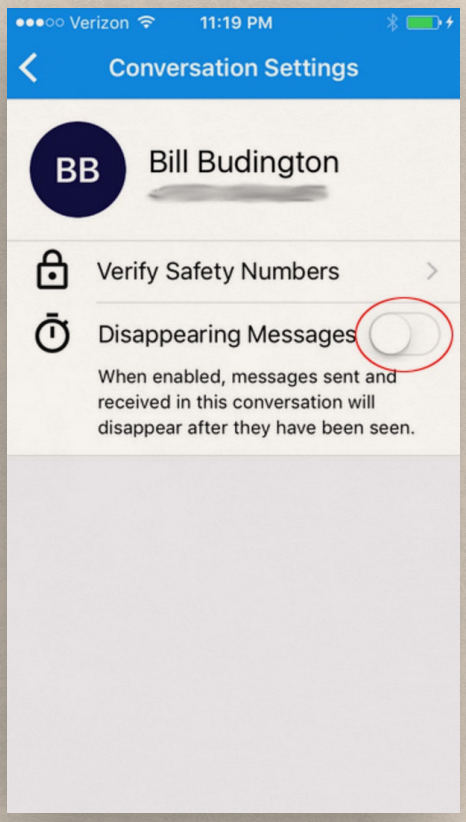


NOTE: Power users the screen displaying your QR code also has an icon to share your safety numbers in the top-right corner. It's best to verify contacts in person when possible, but you may have already authenticated your contact using another secure application, such as PGP. Since you've already verified your contact, you can verify safety numbers within Signal without having to be with your contact in person. In this case, you can share your safety numbers with that application by tapping the "share" icon, and send your contact your safety numbers.

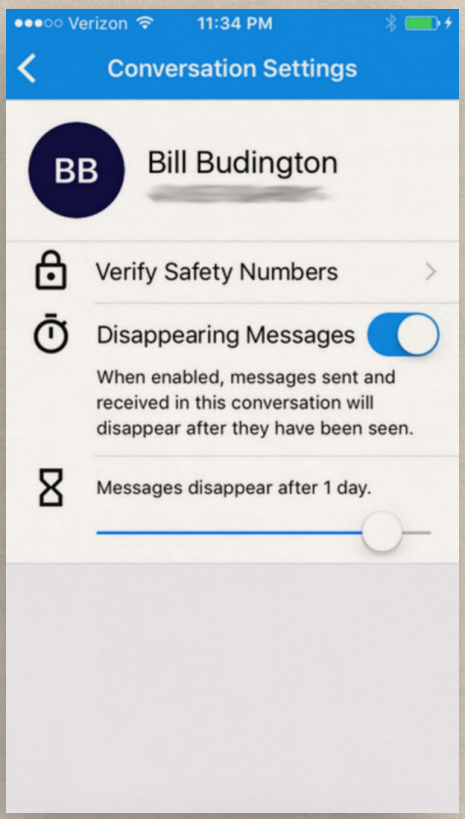
DISAPPEARING MESSAGES ON—SIGNAL

Signal has a feature called “disappearing messages” that automatically removes messages from you and your contact's devices after a chosen period of time after they’ve been seen. To enable disappearing messages for a conversation, open the screen where you message your contact. From here, tap the name of the contact at the top of the screen, then tap the slider next to **Disappearing Messages**.

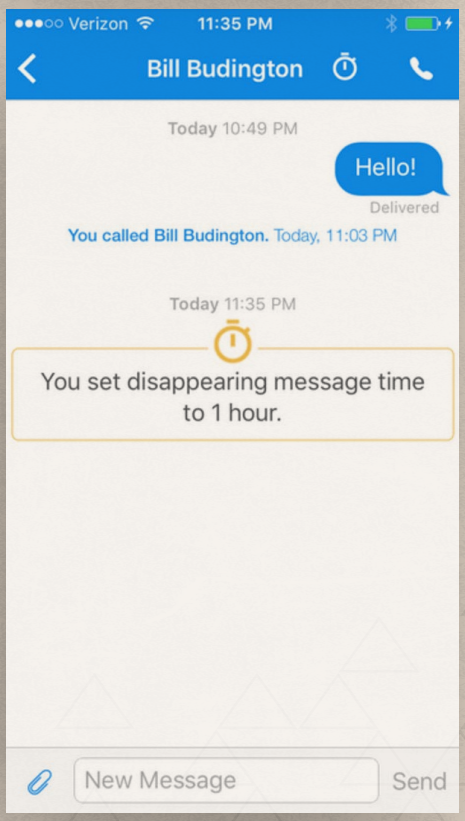
- You'll then see a slider that allows you to choose how quickly messages will disappear.



- After you select an option, tap the < icon at the top-left corner of the screen. You should see a notification indicating that disappearing messages has been enabled.



- You can now send messages with the assurance that they will be erased after the chosen amount of time.

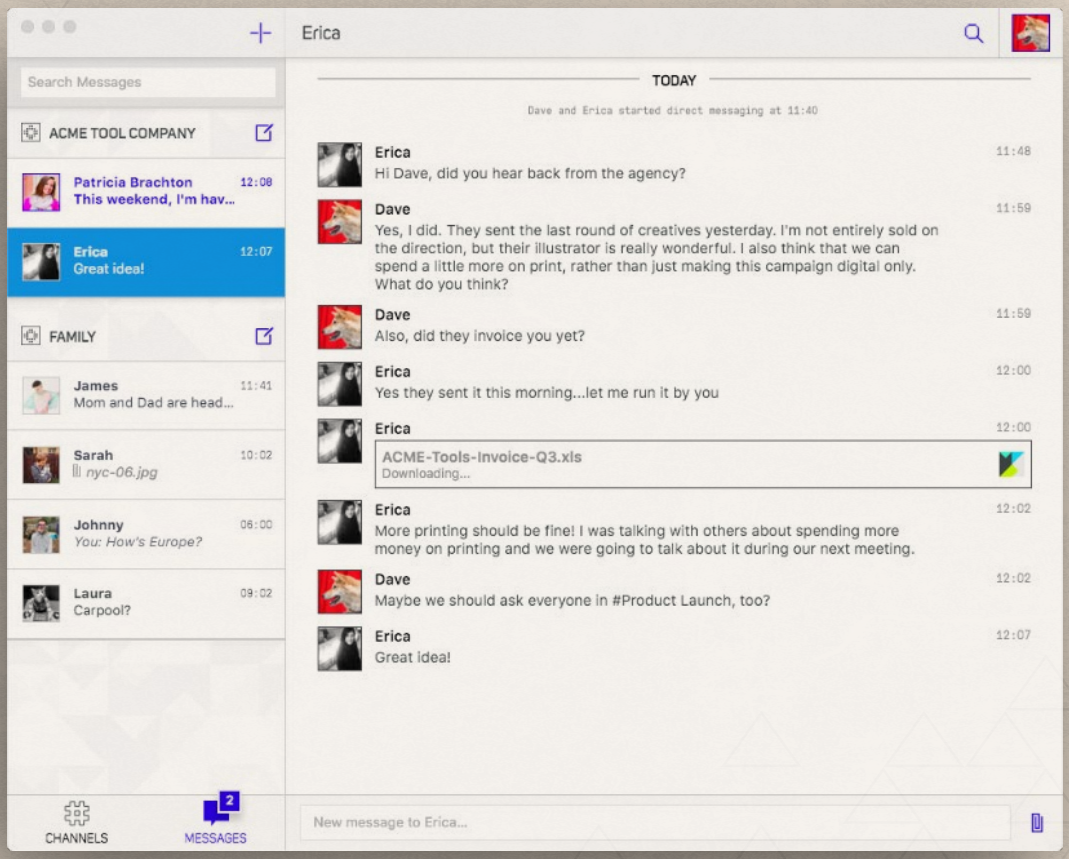


SEMAPHOR

SpiderOak has been a trusted company in the backup space for almost a decade, known for their Zero Knowledge privacy practices. They have been endorsed by Edward Snowden in general and specifically as an alternative to Dropbox in October of 2014.

Semaphor[39] is a real-time team collaboration application created by SpiderOak intended to provide an experience comparable to products like HipChat, Slack, or IRC. Because they are Zero Knowledge, it means that they know nothing about the encrypted data you store on their servers. Their unique design means nothing leaves your computer until after it is encrypted and is never decrypted until it is unlocked with your password on your computer.

Each conversation is cryptographically compartmentalized meaning only the participants in any given conversation have access to that data or the encryption keys; however members who join the conversation later can see content created before their entry into the conversation.



[39] https://spideroak.com/solutions/semaphor

Here is how Semaphor lines up with other similar services in terms of security provisions.

Semaphor is user-friendly and easy to navigate. You can get it both on your phone and your computer. Overall, it gives you the ability to communicate safely and robustly with your colleagues and co-organizers. The downside is that it is a paid service but we do recommend the investment.

	Semaphor	Slack	Hipchat	Microsoft Teams	Skype for Business
Reviewable source code	✓	✗	✗	✗	✗
Zero knowledge end-to-end encryption	✓	✗	✗	✗	✗
Visitor data not shared with third parties	✓	✗	✗	✗	✗
Protects content from blind subpoena risks	✓	✗	✗	✗	✗
Man-in-the-middle SSL attack protection	✓	✗	✗	✗	✗
Vendor admin can't see user data	✓	✗	✗	✗	✗
End-to-end encrypted message content	✓	✗	✗	✗	✗
End-to-end encrypted channel metadata	✓	✗	✗	✗	✗
End-to-end encrypted file sharing	✓	✗	✗	✗	✗
Invulnerable to password-based attacks	✓	✗	✗	✗	✗
Secure key exchange	✓	✗	✗	✗	✗
Contact verification	✓	✗	✗	✗	✗
Message and content verification	✓	✗	✗	✗	✗

WHATSAPP

WhatsApp messenger (**now a subsidiary of Facebook**) is used all around the world, it was one of the first corporate messaging apps to provide end-to-end encryption by default for all users.

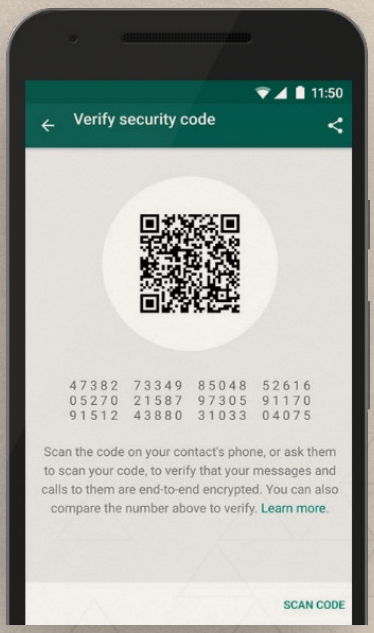
This makes WhatsApp far safer than other platforms. But keep in mind WhatsApp still retains the metadata of your chat logs, which reveal who you were talking with and when. **Additionally, content in WhatsApp helps to inform your Facebook algorithm and contributes to your Facebook profile**.

So use WhatsApp carefully. First and foremost, make sure all of your contacts are using the most recent version of WhatsApp, to make sure encryption is enabled.

Then, it is good practice to authenticate the person you're talking to in order to make sure it's really them. Each of your chats has its own security code used to verify that your calls and messages are end-to-end encrypted.

NOTE: The verification process is optional and is used only to confirm that the messages you send are end-to-end encrypted.

This code can be found in the contact info screen, both as a QR code and a 60-digit number. These codes are unique to each chat and can be compared between chat participants to verify that the messages you send are end-to-end encrypted. Security codes are visible versions of the special key shared between you. Don't worry, the codes don't represent the actual key itself; the key is always kept secret.



To verify that a chat is end-to-end encrypted

- ✓ Open the chat, tap on your contact's name to open their info screen.
- ✓ Tap **Encryption** to view the QR code and the 60-digit number.

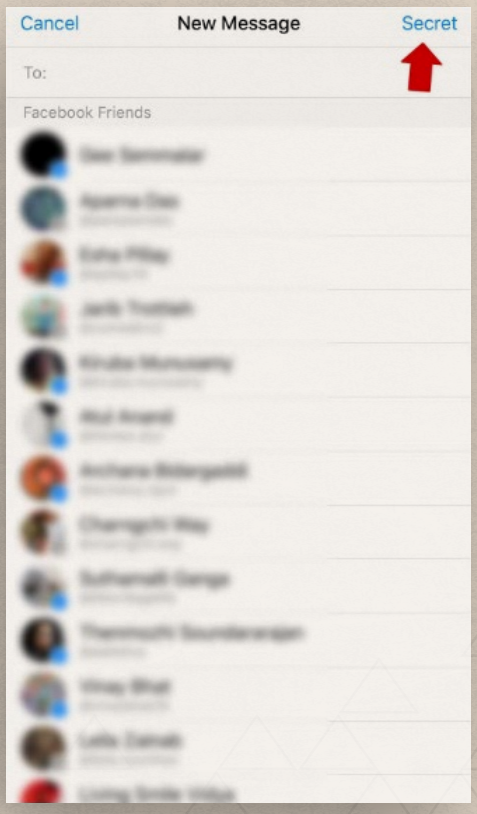
If you and your contact are physically next to each other, one of you can scan the other's QR code or visually compare the 60-digit number. If you scan the QR code and it is indeed the same, a green checkmark will appear. Since they match, you can be sure no one is intercepting your messages or calls.

FACEBOOK MESSENGER

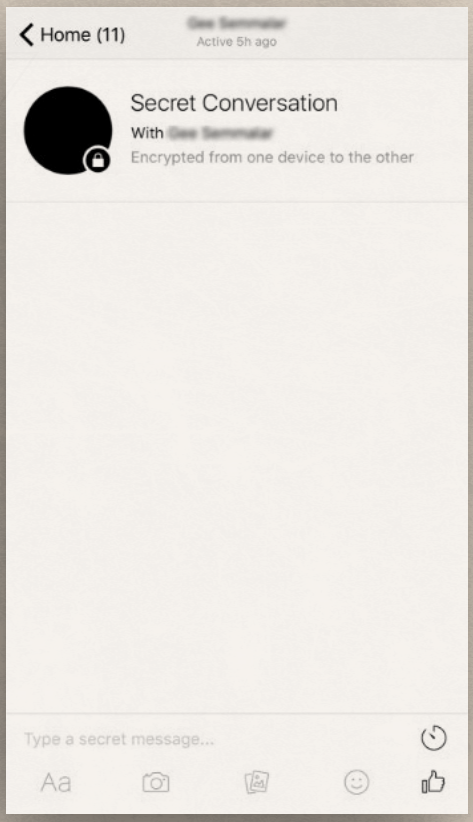
Facebook Messenger has recently introduced the option to send encrypted private messages. Since many of us use Messenger to organize protests and meetings, it is important that we know how to securely use this line of communication.

WARNING: Again, please keep in mind that by turning on Facebook's encrypted messaging you are practicing harm reduction—**not guaranteeing your complete privacy**. Facebook's privacy policies leaves much to be desired by activists since they are willing to hand over personal information to authorities. Be safe and practice risk assessment to gauge your level of safety on this platform.

To start a new encrypted conversation:
Tap the new conversation icon at the top right, then tap **Secret** in the top-right corner.



Choose your recipient and begin messaging.



Tap **Secret Conversation** to switch it over.

SENDING SECURE EMAIL USING ENCRYPTION

WHAT IS ENCRYPTION?

Encryption[40] as we've explained, is when data is scrambled in such a way that only someone with the secret password or key can read it. The scrambling relies on mathematical techniques. These techniques are powerful enough that even major governments cannot unscramble the data you choose to encrypt.

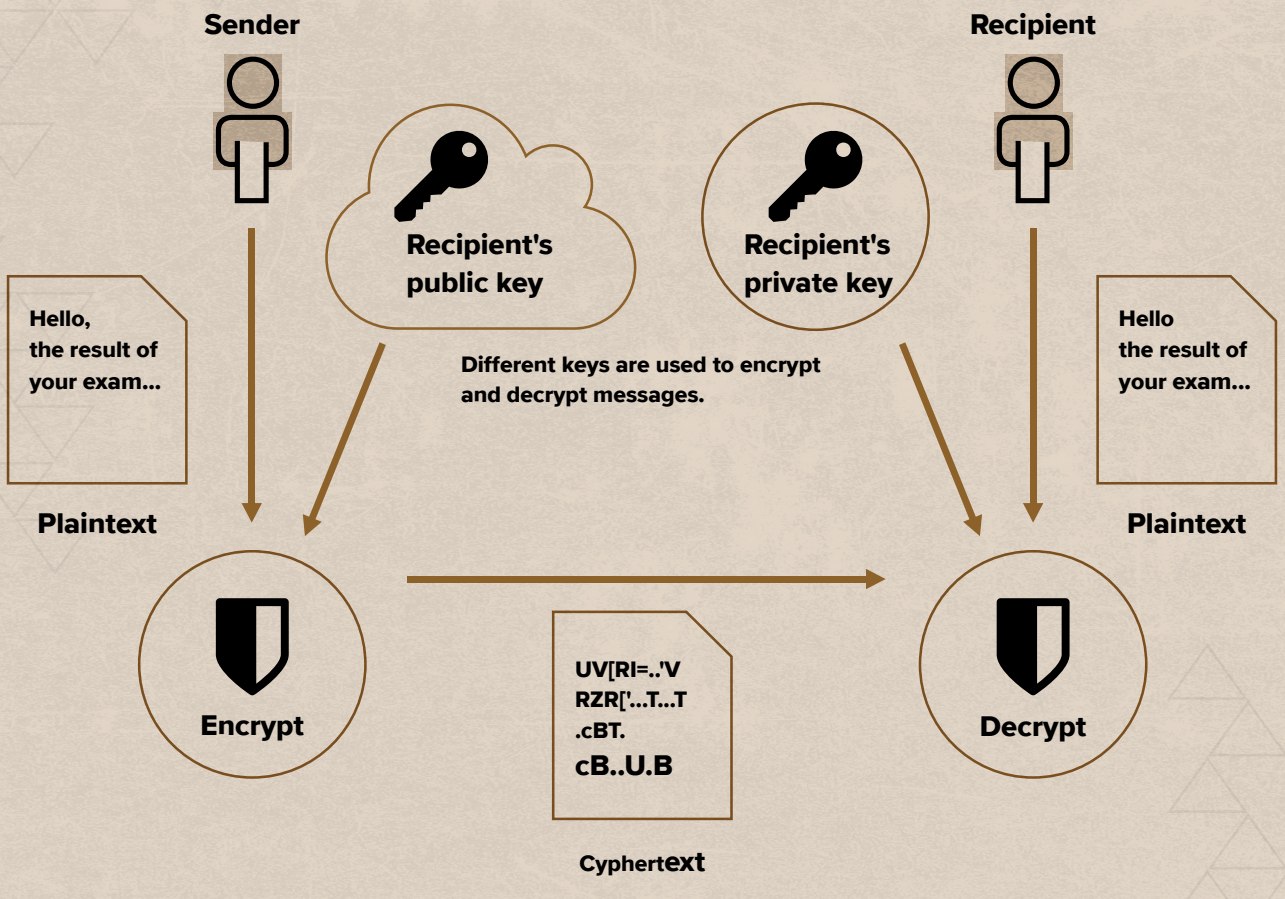
ENCRYPTION FOR PERSONAL USE

When you encrypt data on your computer, it will require a password—also known as a **private key**—that only you know. This process is called private key encryption, and it's good for protecting your data on physical objects that you carry with you such as a USB drive, phone, or laptop hard drive.

[40] https://www.virtru.com/blog/encryption-basics-quick-guide/

ENCRYPTION TO COMMUNICATE BETWEEN PEOPLE

There is a dilemma if you want to have secure and private email or communication between you and your collaborators, and you're the only one using private key encryption. You can encrypt your data and send it to your friend, but then you'd need to tell your friend the password so they can unscramble it. This can be a problem if the government, an ISP, or a hacker has access to your communications and can overhear or capture this password/private key.



To address this problem, we use public key encryption. To understand how this process works, consider the following example:

- You want to communicate securely to your friend. Instead of sending them a private key, you ask your friend to send you a lock that only they have the key to. The lock your friend sends is called a public key.
- You receive your friend's lock, then put your message in a box and lock it with that lock.
- You send the locked box to your friend.
- Your friend uses their private (secret) key, is paired to the lock to unlock it and securely read the message.[41]

You may be thinking, "What if a government or hacker hires a locksmith to pick the lock?" In this scenario, a **weak encryption technique** (low-bit encryption algorithm) would represent an easy-

[41] https://help.gnome.org/users/seahorse/stable/about-diff-private-public.html.en

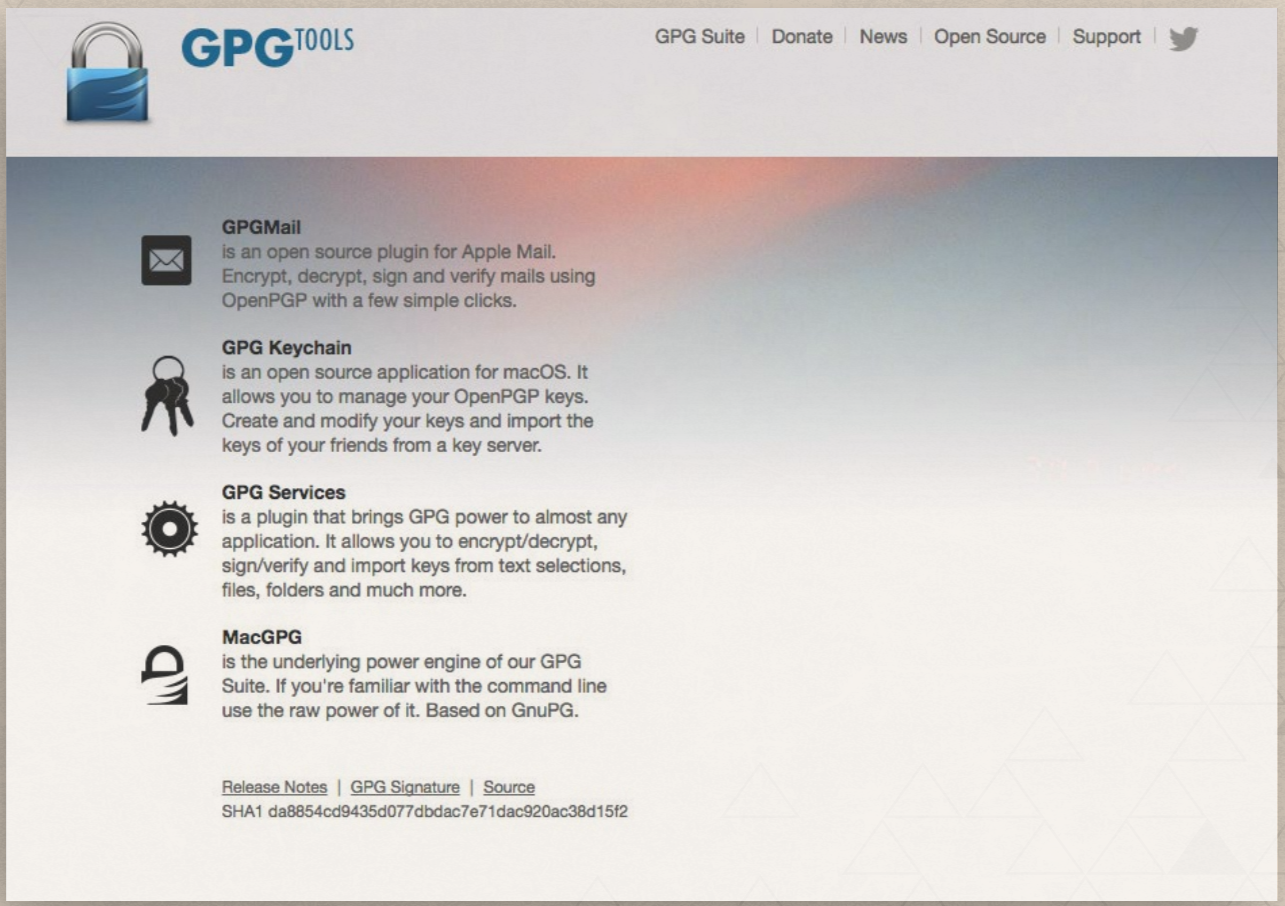
to-pick lock that would only take a few minutes to break. A **strong encryption algorithm** (known as an RSA, which is used in the GPG software package you'll read about on the next page), would take a locksmith hundreds of years to pick.

Using a technique like this, you can communicate over an insecure network and still have security. The set of mathematical techniques that allow this to happen electronically is called **public key encryption**. This encryption techniques is the basis for all secure communication on the internet, whether it's HTTPS, GPG, Signal, Tor, or VPNs.[42]

NOTE: To begin using encryption, we recommend **GPGTools for Mac** and **GNU Privacy Assistant for PC**. You will learn about both in the following pages.

USING GPGTOOLS FOR MAC

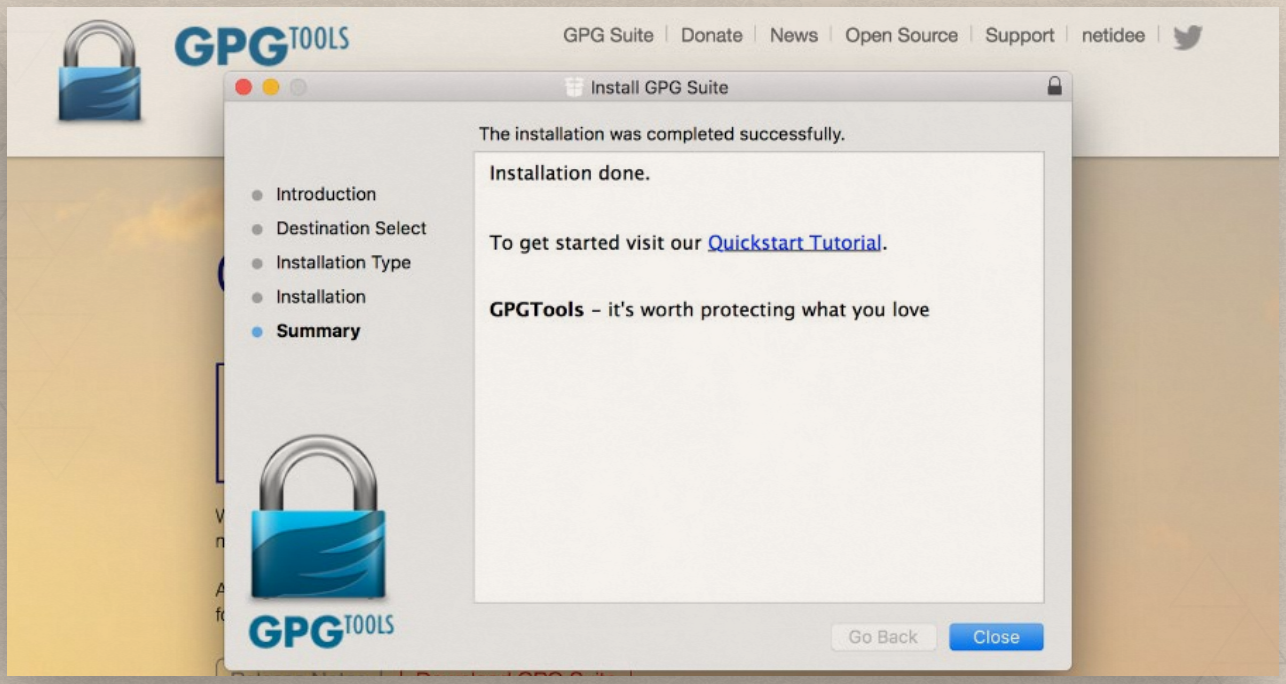
GPGTools is a free open-source software package that allows you to use public key encryption in your communications, primarily over email. You and your collaborator will both need to have a copy of GPG installed on your device.



[42] https://wordtothewise.com/2014/09/cryptography-alice-bob/

How to send encrypted email

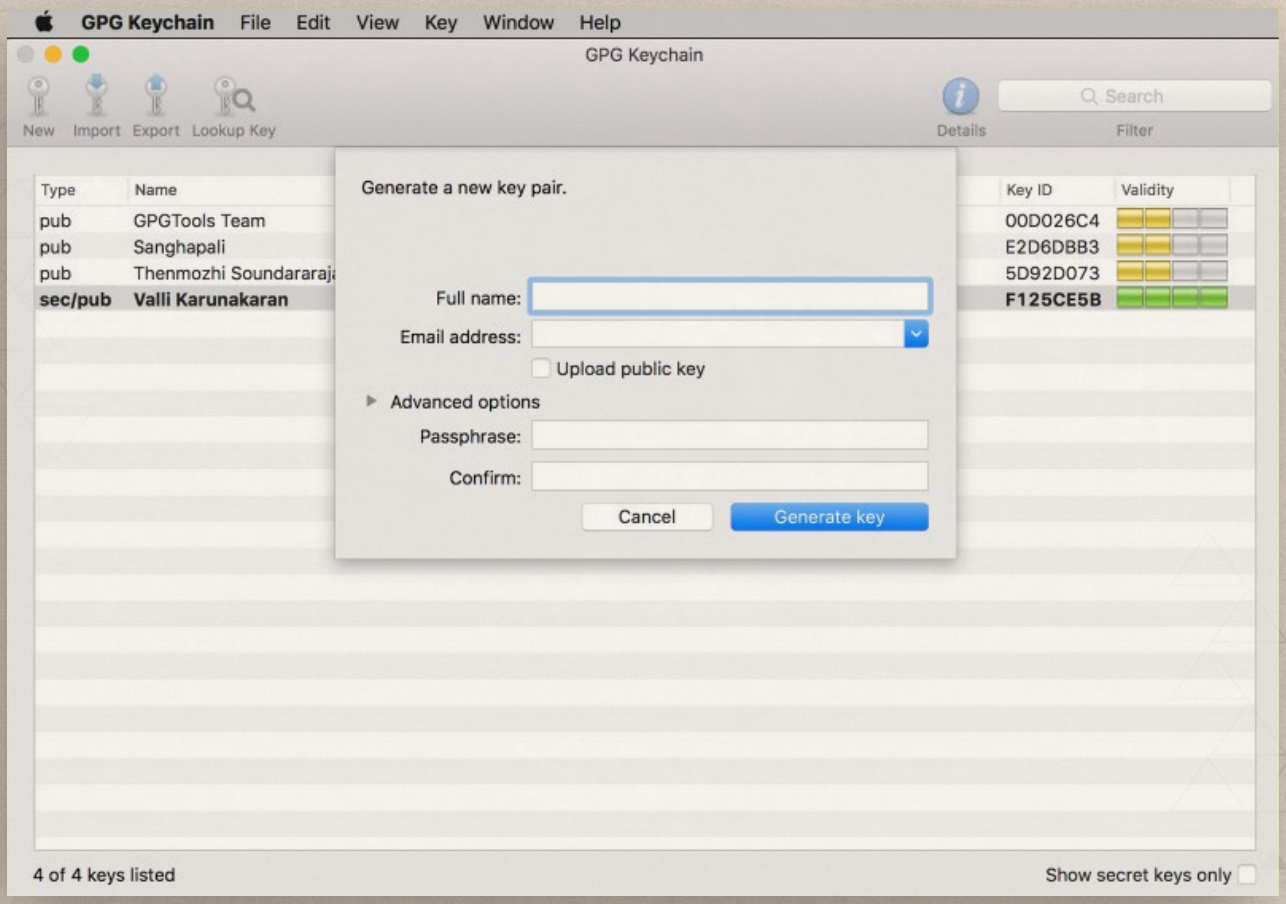
- [x] Download and install the GPG suite from here
- [x] Create a private and public key pair for your use (in other words, generate both your lock and your key). You only need to do this once.
- [x] On the GPG Keychain program window, click **File → New Key → Enter your name**, your email address and your passphrase.



PASSPHRASE RULES

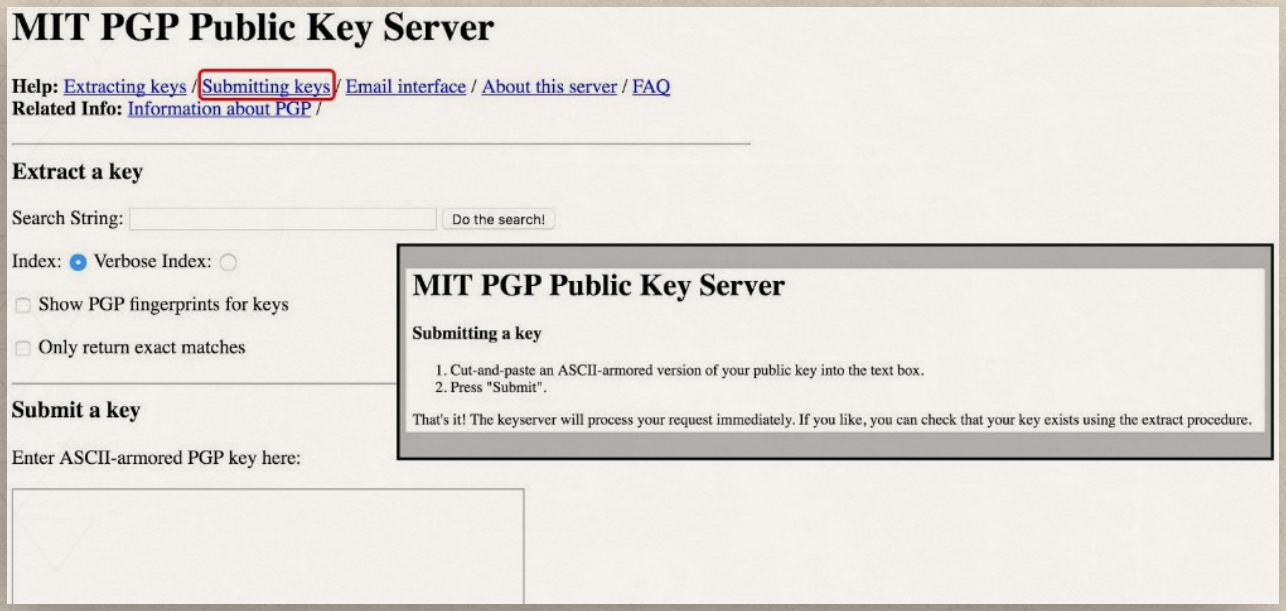
Make sure your passphrase is one you haven't used elsewhere, contains at least one capital letter, one number, and one special character. **MOST IMPORTANTLY: MAKE SURE YOU REMEMBER THE PASSPHRASE.**

WARNING: For initial convenience, jot down your passphrase on a piece of paper. We strongly recommend that you memorize your passphrase, then destroy the paper.



Next, if you are frequently communicating with new contacts add your key to the MIT PGP Public Key Server. This is like making sure you're listed in the yellow pages of the PGP community. Depending on the extent to which this key is tied to your personal identity, you may instead choose to share it directly with people you wish to correspond with, as opposed to sharing it publicly.

- To add your key to the server, first you must export it by clicking on **Export** in the GPG keychain. Open that file on your desktop and copy it. Then, go to pgp.mit.edu and enter your key into the text box under "**Submit a key**" and click "**Submit this key to the keyserver**! Here you can also look for other users by searching for names, emails, or specific key IDs in the "**Search String**" field. Finally, you can also use the file of your exported key to send your public key to a collaborator via email.

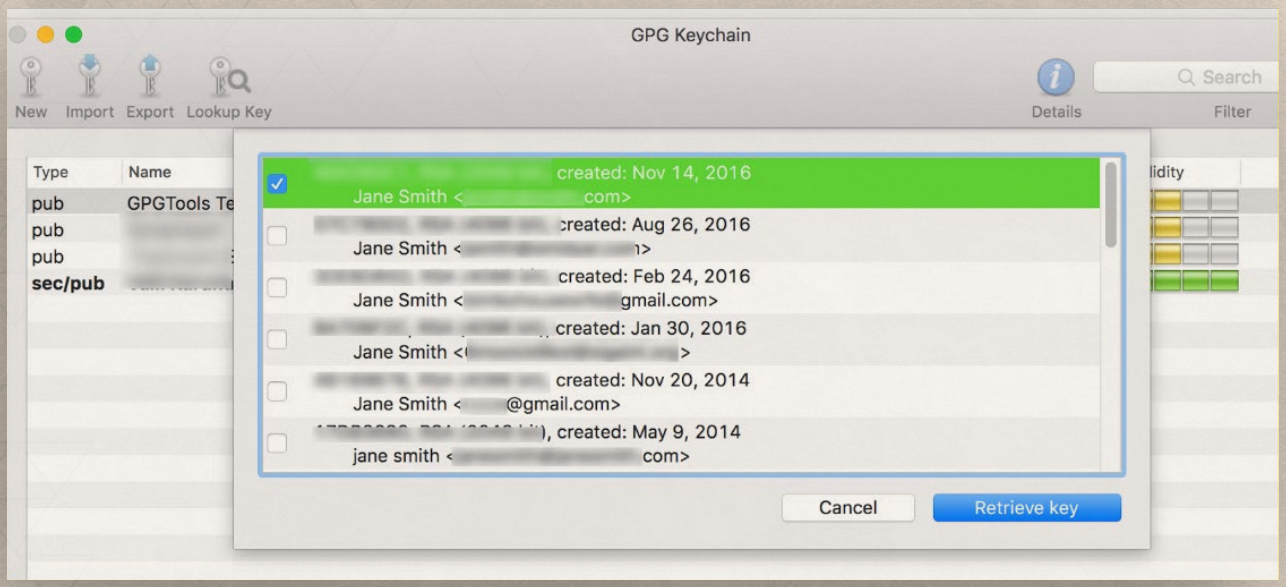


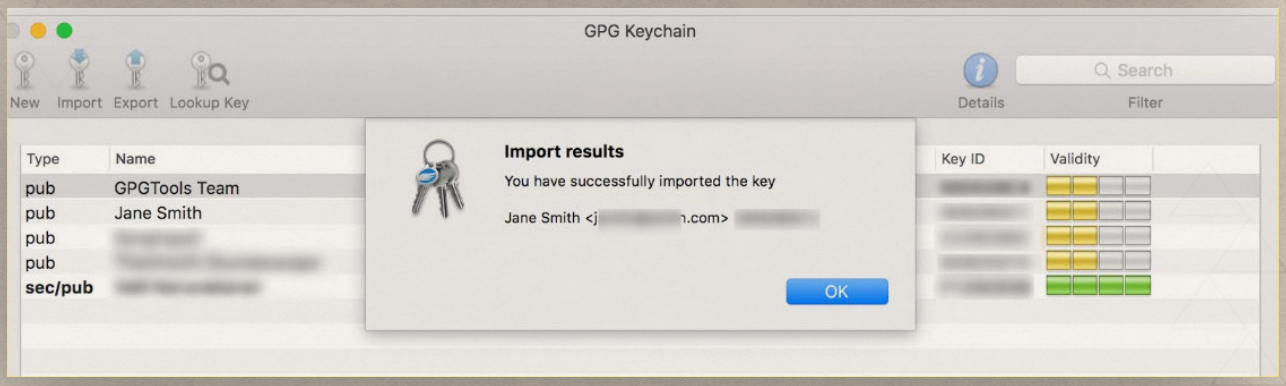
SENDING AN ENCRYPTED EMAIL

First, find your recipient's key on the PGP key server.

- You can do so by going to **Key → Look up key on server**. In the search box, enter the email address of the person you are looking for.

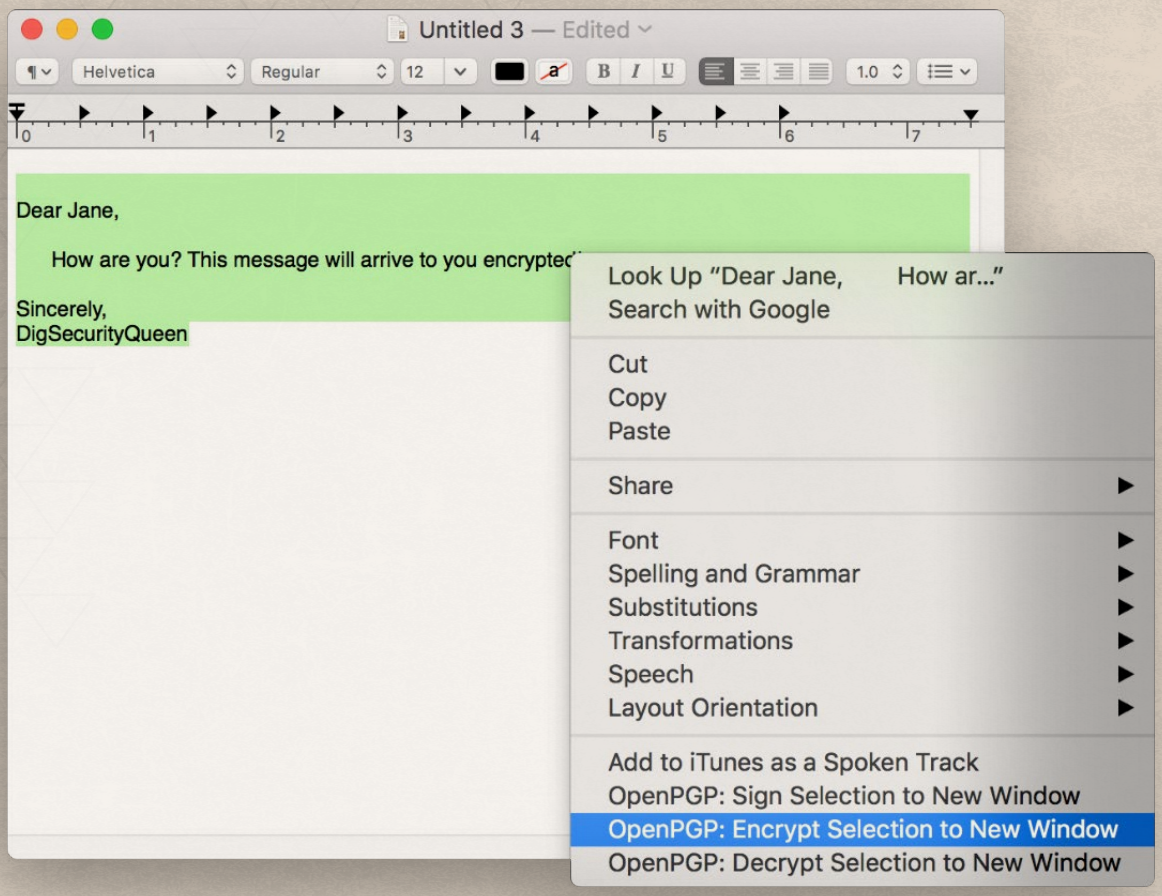
- Find the person you wish to communicate with in the search results. Click on their name, then click **Retrieve Key**.



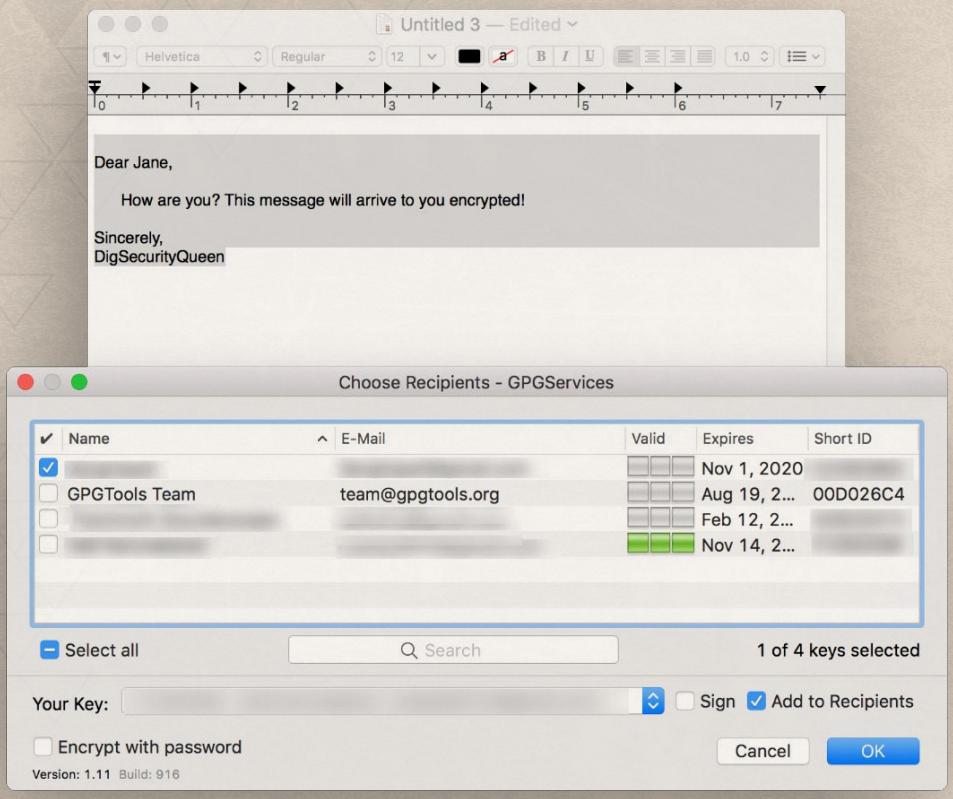


Once you have their key, you are ready to send an encrypted message.

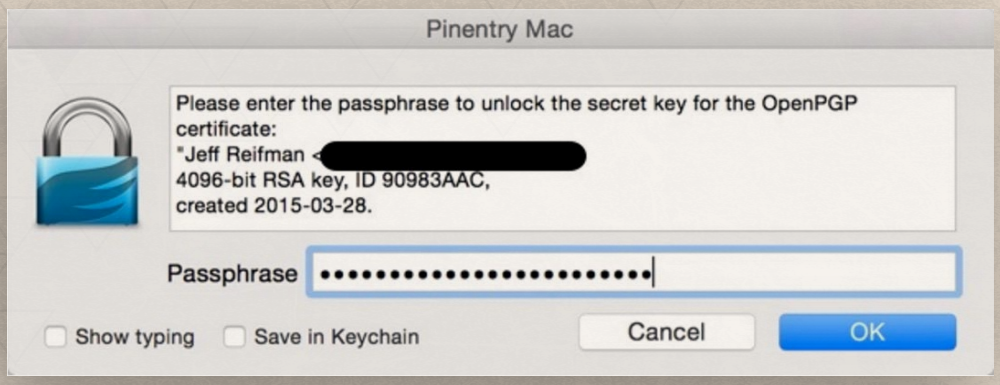
- Open TextEdit on your computer. Type your email message, highlight all of the text, and **right-click (or Control + click)**. Click on the option "**Open PGP: Encrypt Selection to a New Window**."

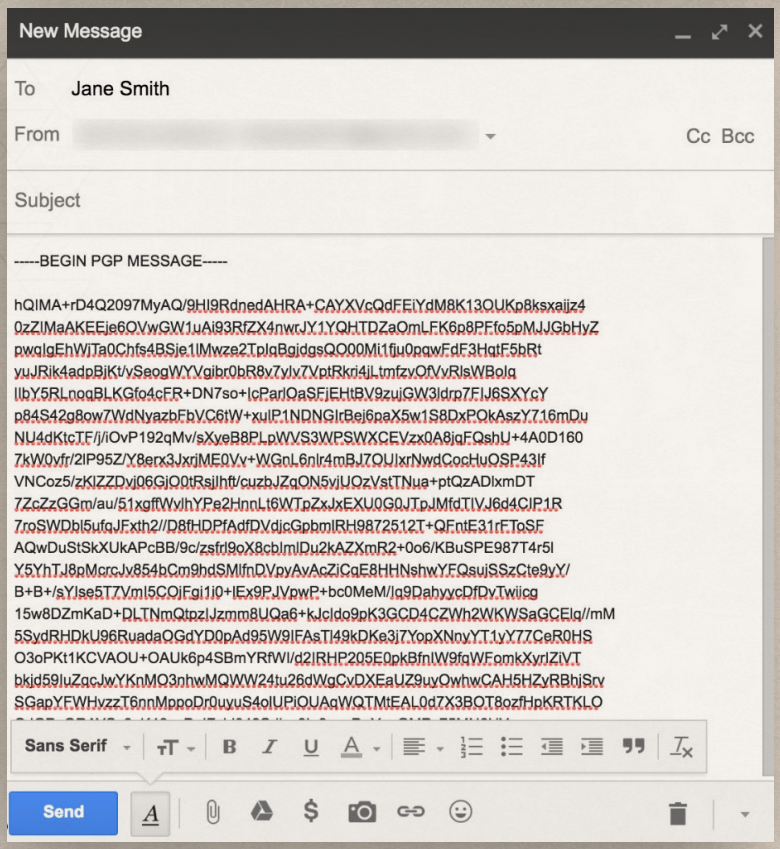


- A window will pop up asking you to select the recipients with keys on your list. Select one or more recipients to whom you would like to send the message.

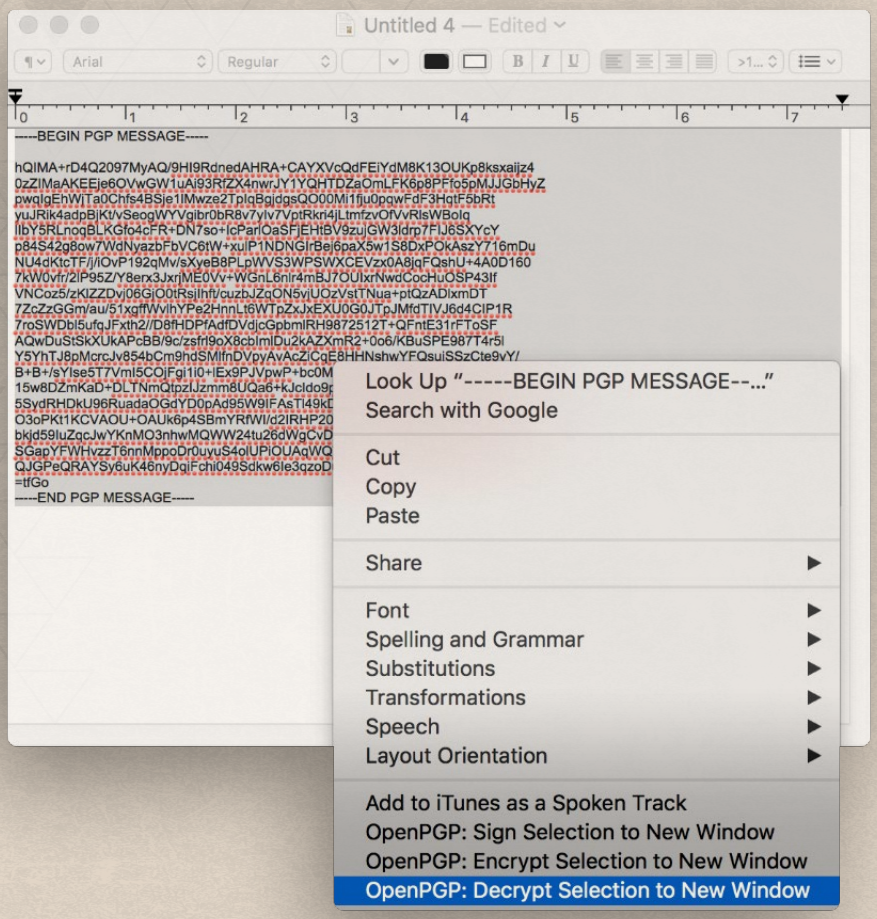


- [x] Copy the body of this message and email it to your collaborator.





- Once they receive the email, they will select use their passphrase to decrypt the message and read it in plain text.



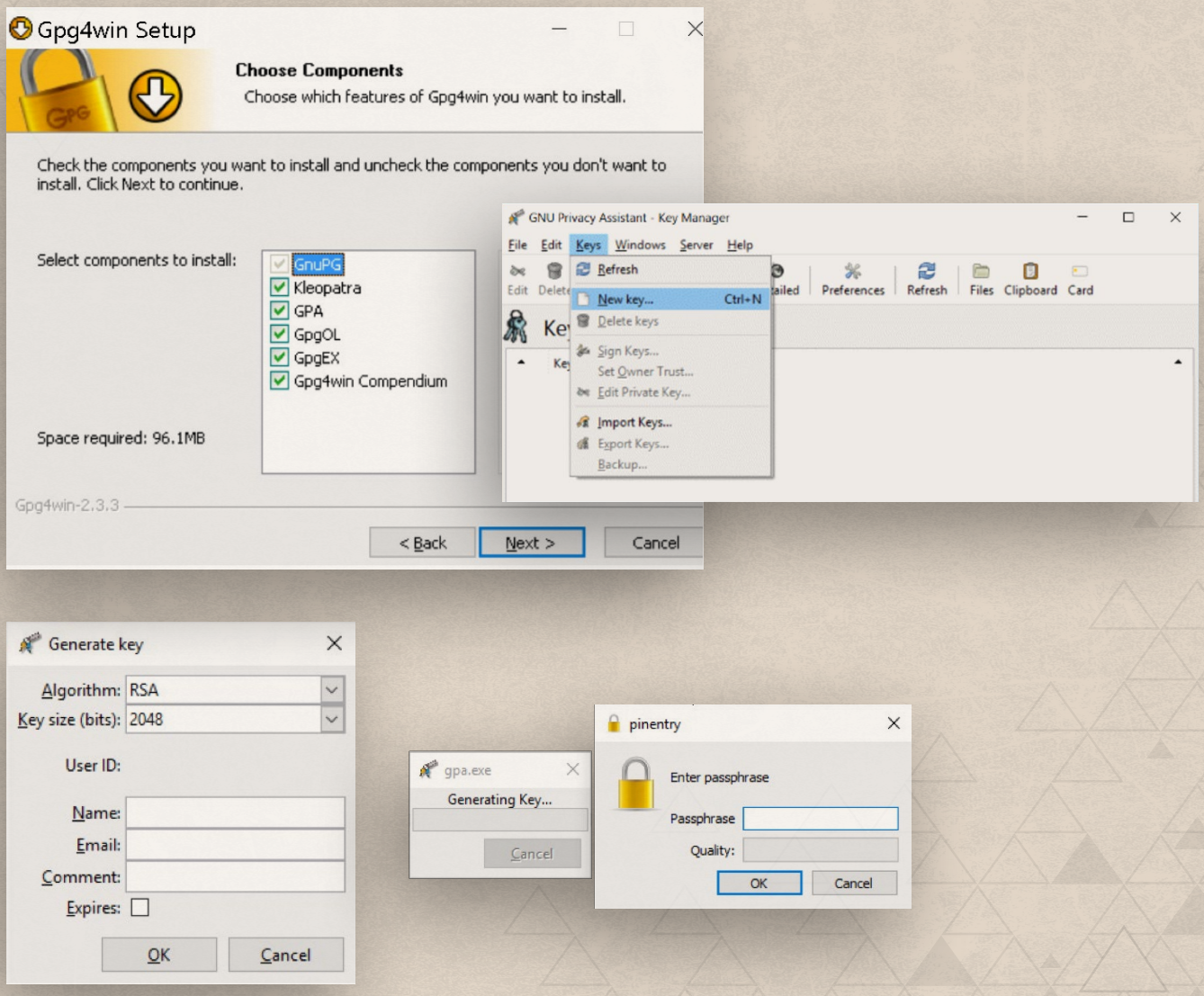
GPG FOR WINDOWS USING GNU PRIVACY ASSISTANT

GNU Privacy Assistant is a useful application that's comes bundled with Gpg4win. You can download Gpg4win at https://www.gpg4win.org/download.html

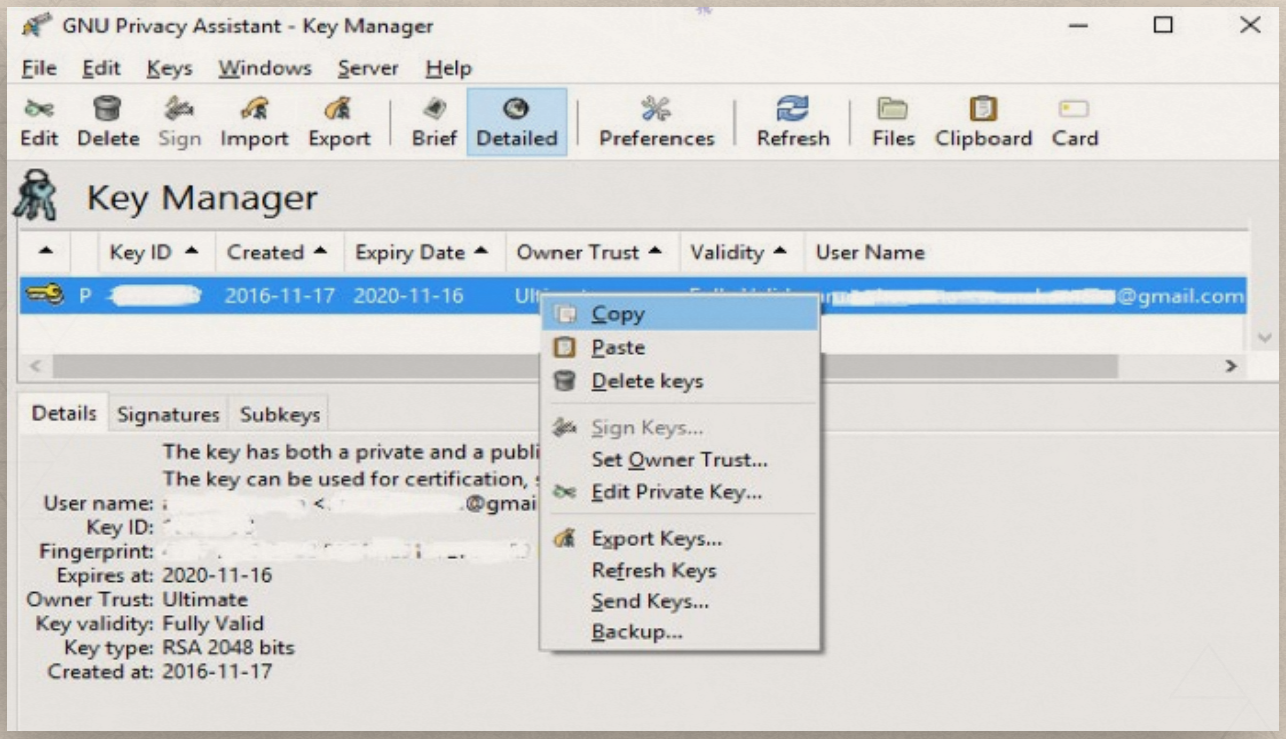
NOTE: When installing Gpg4win, check the “GPA” box to activate it, as it is not turned on by default.

CREATE AND PUBLISH A KEY

Create a public/private key pair for yourself by going to **Keys → New key**. You will be asked to give a name and email address for this key. The private key will be for your use only and kept secret at all times. Others will use your public key to encrypt messages to you. You can also use your public key to “digitally sign” your communications.



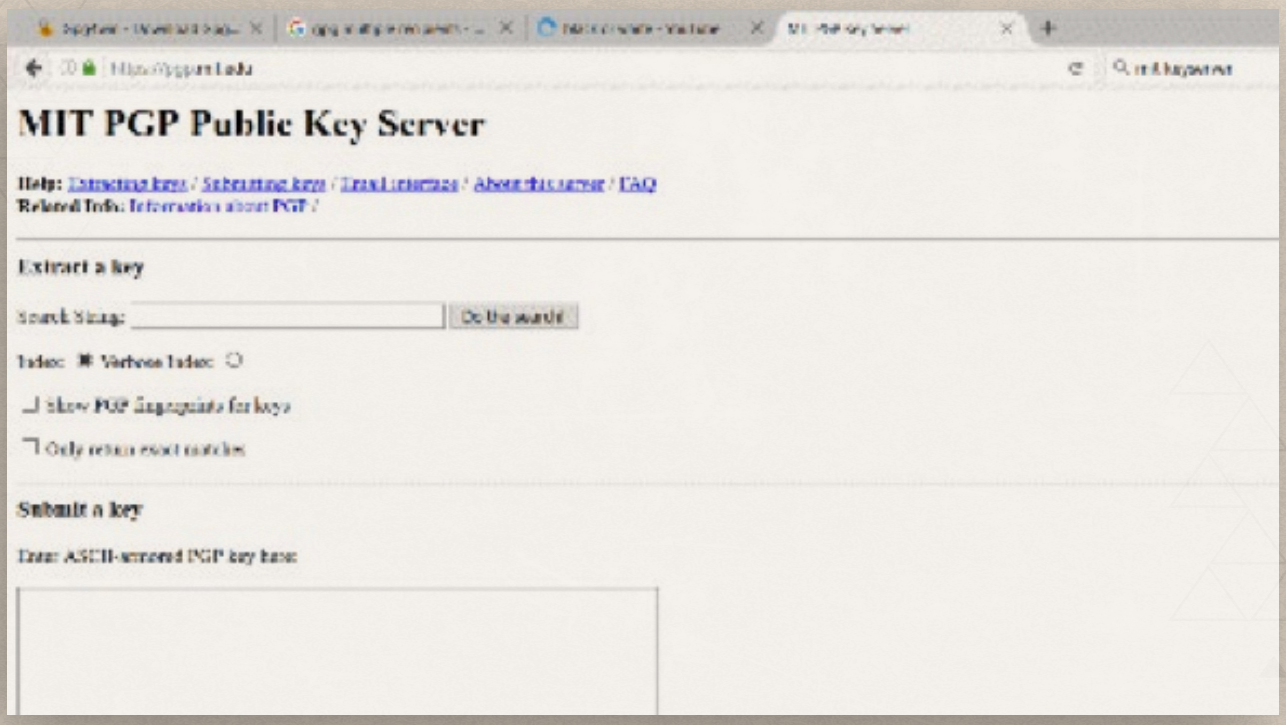
- Once the private/public key pair is created, you will want to publish your public key on the internet to a keyserver, so that people who wish to communicate with you can search for you and find your keys. You can publish your public key at https://pgp.mit.edu/. This is like making sure you are listed in the yellow pages of the PGP community. Depending on how tied this key is to your personal identity, you may choose instead to share it directly with people you wish to correspond with, as opposed to sharing it publicly.



- To do so, you'll first export your key by right-clicking on the new key that appears in the **Key Manager**. Then, select Key. You will see a notification that says, "**The keys have been copied to the clipboard**."

TIP: There is so much to learn with GPG encryption. If you would like to read more, check out this handy kit from the folks at Riseup https://riseup.net/en/security/message-security/openpgp/best-practices

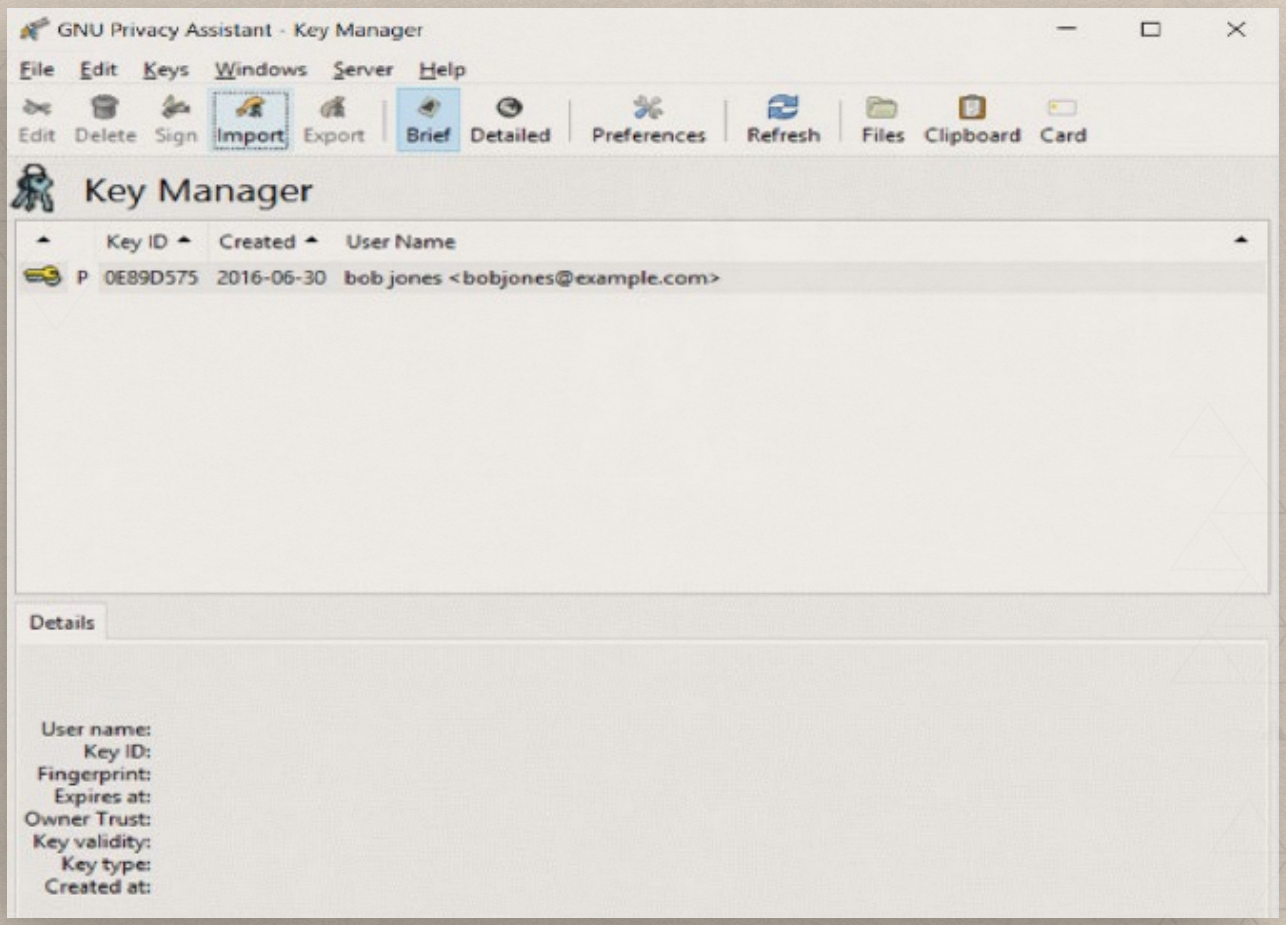
- Go to pgp.mit.edu. There, you can upload your key by copy-pasting from the clipboard. You can also look for other users by searching for names, emails, or specific key IDs (as can anyone!). Finally, you can also use the file of your exported key to send your public key to collaborator (over email).



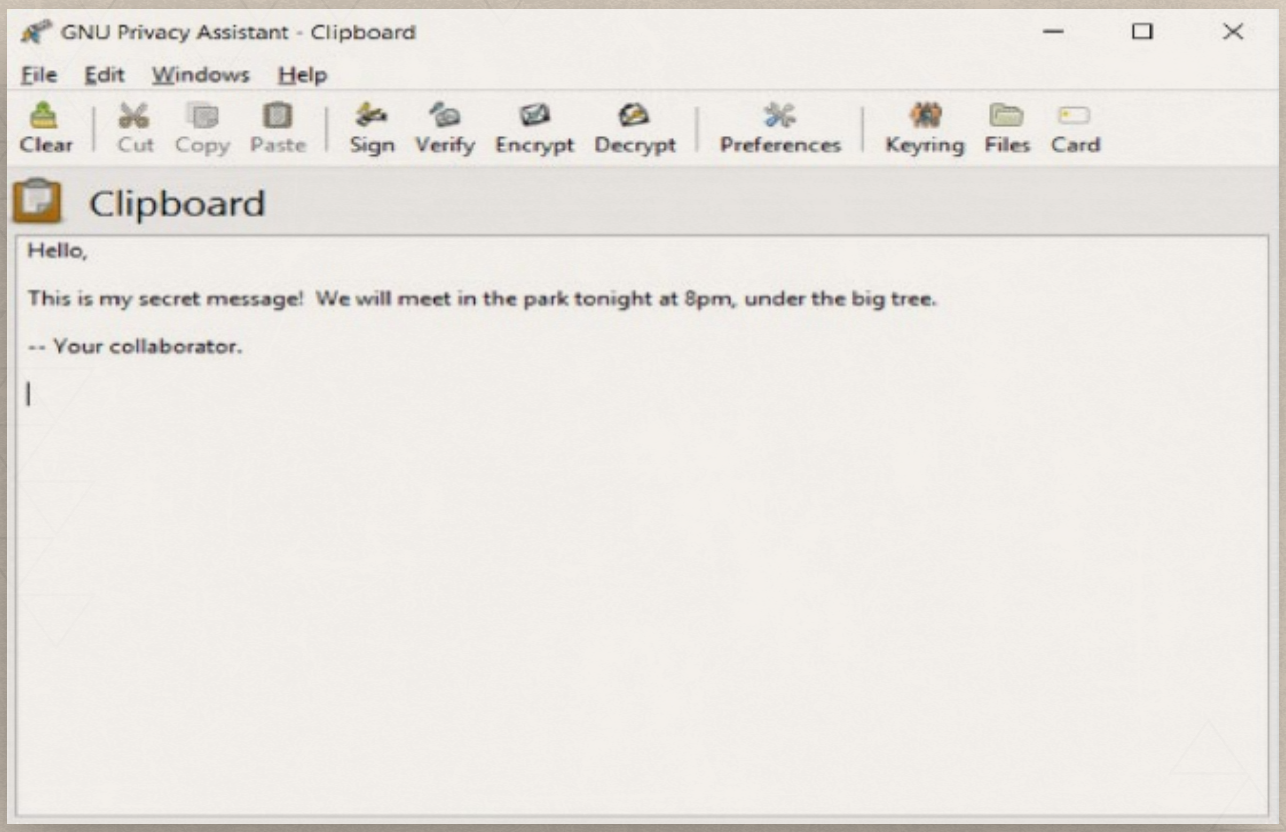
ENCRYPT A MESSAGE

- In order to encrypt a message, you will need to obtain your collaborator's public key. You will use their public key to encrypt your message, which they will later decrypt using their private key. You can use the MIT PGP Public Key Server to look up your collaborator's public key, if it's published there.

  The keyserver will associate an ID with the key that looks something like "0x5db78.7" You can make note of this ID and ensure that it is the correct (authentic) with your collaborator via phone or email. This step will add an additional layer of security, similar to the two-factor authentication used in WhatsApp or Gmail. Once you confirm the key, go ahead and copy it into your clipboard, starting with the line that begins with "-----**BEGIN PGP PUBLIC KEY BLOCK**-----."

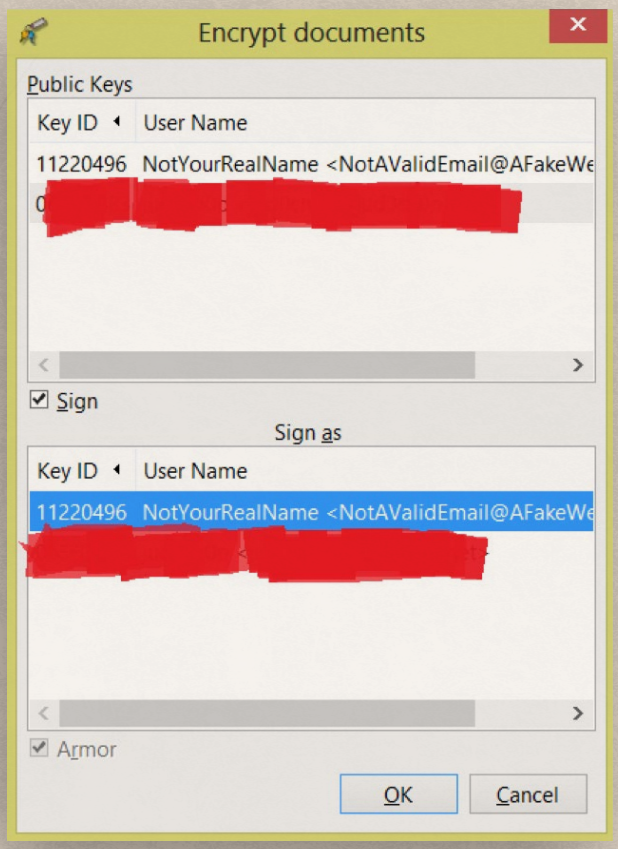


- Once you've copied the key, you can import your collaborator's public key by clicking “**Import**.”
- After you’ve imported the public key, you are ready to encrypt a message. To do so, click on “**Clipboard**" and enter your message.



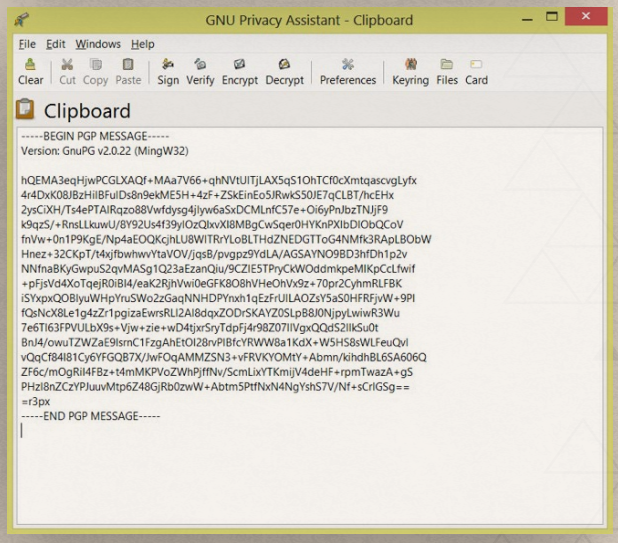
- In the clipboard window click on “**encrypt**” and use your collaborators public key to encrypt. If you check the “**sign**” box, your message will be “**signed**” using your key. This way, your collaborator can verify that the message that is sent is really coming from you. Your text in the clipboard should transform into an encrypted block.

- You are now ready to send your encrypted email. Copy and paste the encrypted block into an email or SMS, and send it to your collaborator.



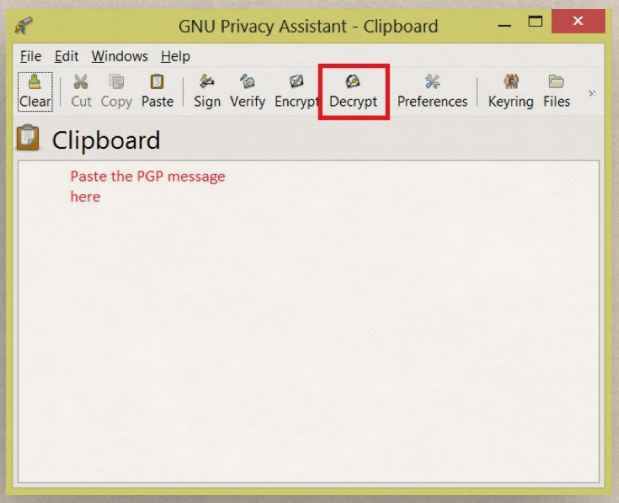
DECRYPT A MESSAGE

- When you receive an encrypted message that was sent using your public key, you can copy that message into the clipboard, hit the **Decrypt** button, and enter private key and password.



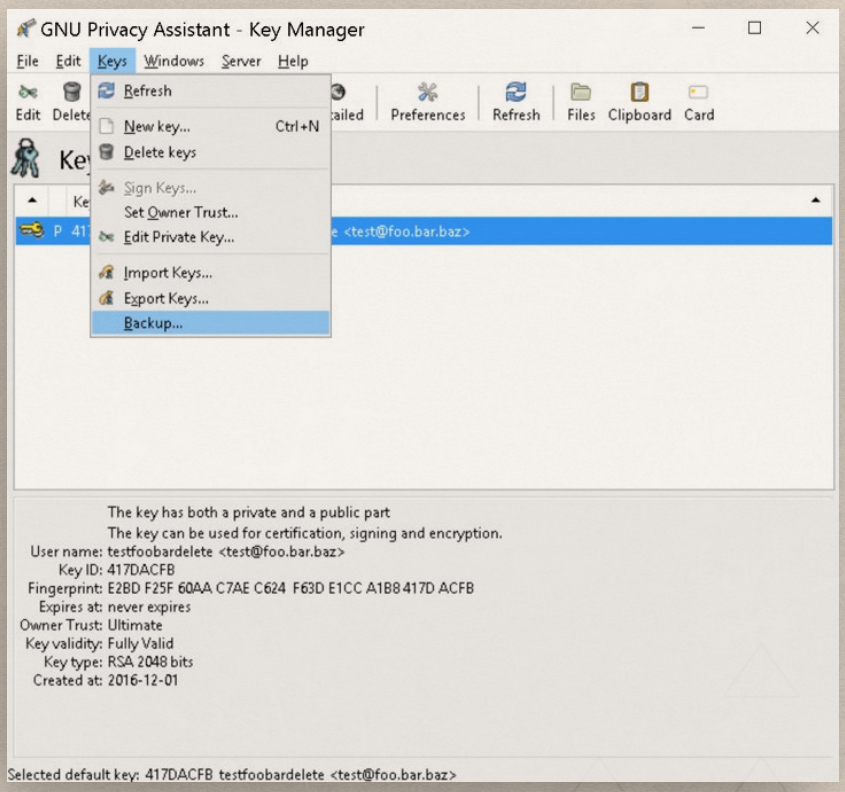
BACKING UP YOUR KEY

You may want to store a copy of your encryption key on a USB stick for carrying around. Or, you can back up your private key by going to **Keys → Backup**. Your key will be saved to the appropriate location.



USING GPG IN YOUR BROWSER

With some caveats based on browser security, there are plugins for Chrome and Firefox to enable OpenPGP encryption for webmail. Mailvelope (https://www.mailvelope.com/) provides a relatively simple option for users who are new to encryption and unable to easily switch to a different desktop email application. Mailvelope is open source, audited in 2014, and compatible with most webmail providers, such as TK or TK. Mailvelope works by adding a button in the "**compose**" window to open a pop-up window in which you can write an email. You can then encrypt the message and send only the encrypted text to the webmail system you primarily use.



TIP: Mailvelope is working to improve its support for email attachments, so stay tuned!

SAFER ONLINE ACTIVISM 101: SETTING UP SOCIAL MEDIA ACCOUNTS THAT CAN'T BE TRACKED

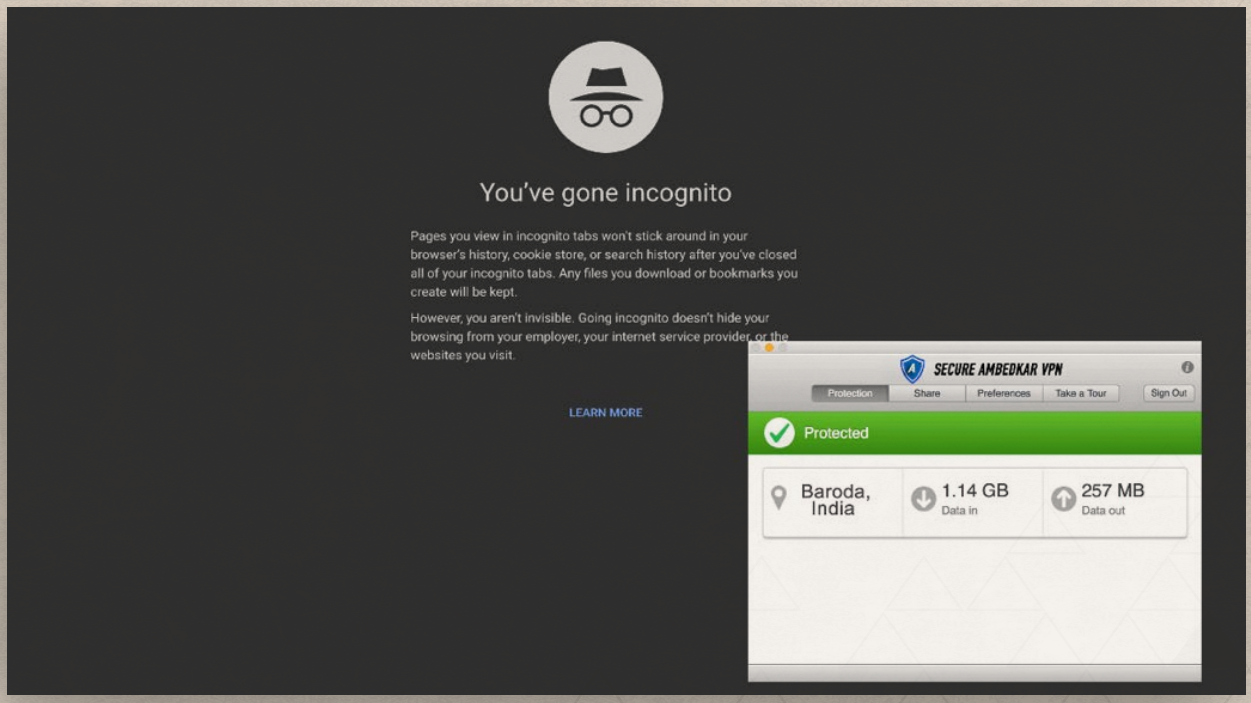
Online activism can leave you vulnerable to trolls and other more malicious actors who can threaten your online and physical safety because they disagree with your politics or activism. In the past year, many activists have shut down online. This means that, sometimes, you have to position yourself as an anonymous entity in order to TK.

This section will cover how to make accounts that can easily be traced back to your physical self. In order to create anonymous social media accounts, you will need services that can generate temporary and anonymous email addresses, or temporary phone numbers and a secure VPN network.

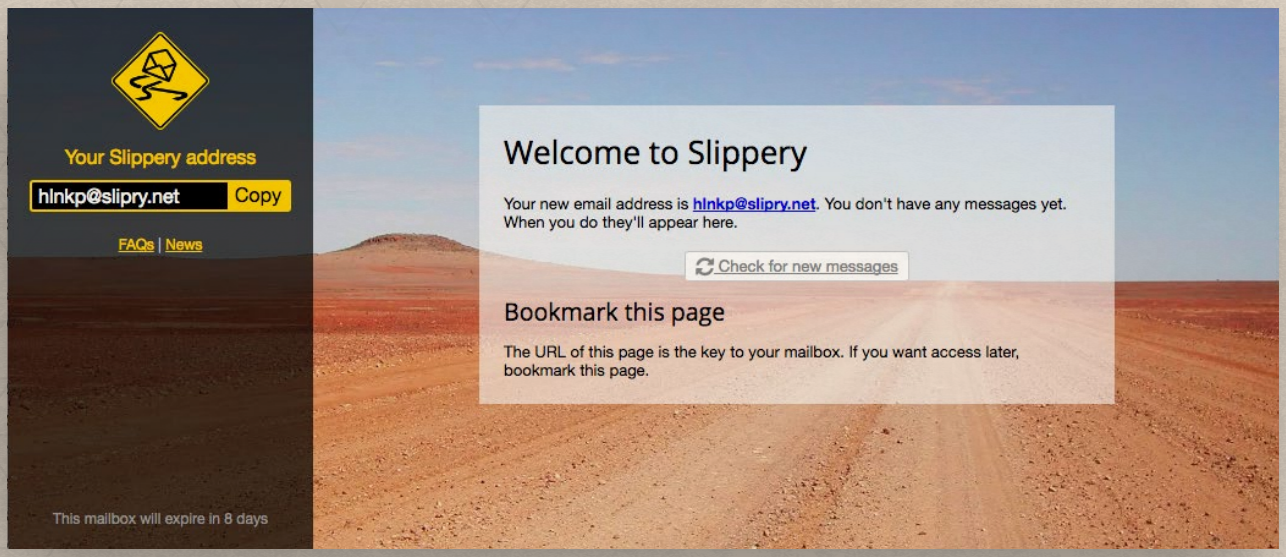
First, sign out of all your accounts, close your browser, and restart your computer. Make sure you are logged in to Tor and/or a secure VPN network and are using private browsing.

You can then use the following services to generate temporary emails

- Riseup: https://user.riseup.net/forms/new_user/first
- Slippery: https://slippery.email
- Guerrilla Mail: https://www.guerrillamail.com



NOTE: It is crucial that you use Tor use only HTTPS sites and are signed out of all other accounts every time you access an anonymous account you have created.



These emails self-destruct within a period of days or weeks, which reduces the chance that accounts created with these emails can be traced back to you.

Using your new temporary email address, register your anonymous social media account.

NOTE: It is crucial that you use Tor use only HTTPS sites and are signed out of all other accounts every time you access an anonymous account you have created.