**March Hare Communication Security Guide**

November 2016

Please distribute freely

Since 1999, The March Hare Communications Collective helps social justice communities communicate securely.

**Table of Contents**

Purpose of This Guide..... 1
Enabling Security Updates on your System..... 2
Locking your Screen..... 3
Choosing a Secure Password or Passphrase..... 5
Setting a Secure Password or Passphrase..... 5
Managing your Passwords..... 6
Encrypting your Drive..... 7
Generating a PGP encryption key pair..... 8
Importing and Signing Someone's PGP encryption key..... 10
Using a Subpoena-Resistant Email Service..... 11
Encrypting your Email..... 12
Encrypting your Web Browsing..... 13
Encrypting your Text Messages and Phone Calls..... 14
Disabling your Device's Surveillance Features..... 14
Securely Erasing Data from your Drive..... 15
When all you Have is a USB Thumb Drive..... 15
Maintaining Active Security Culture..... 15

**Purpose of This Guide**

This guide is intended for a broad audience. Minimal technical understanding is required to follow the steps outlined here and secure your communications. This guide will walk you through the steps needed to meet the current best practices for activists and other people with a higher than average risk of equipment seizure, within the provisions outlined in each area.

This guide covers five of the most common operating systems. For desktops and laptops, the most recent versions of Mac OS,

Windows, and Ubuntu Linux are documented. For mobile, Android and iOS are covered. If you are running an older version of any of these, your system might not be securable. Throughout this guide, it is assumed that you have administrator access.

This guide is not intended to be an exhaustive review of all available encryption tools and technologies. Where an area is identified that needs to be secured, such as email, a single tool that works well is identified and demonstrated. For an intermediate review of tools, visit <https://ssd.eff.org/en>. For an advanced review, visit <https://prism-break.org/en/>.

**Enabling Security Updates on your System**

First, you need to make sure your system is installing the latest security updates.

On Mac OS X:

- Click the apple in the upper-left corner of your screen
- Select “System Preferences”
- Select “App Store”
- Ensure “Automatically check for updates” is checked
- Ensure “Download newly available updates” is checked
- Ensure “Install app updates” is checked
- Ensure “Install macOS updates” is checked
- Ensure “Install system data files and security updates” is checked

On Windows:

- Select the Windows icon in the lower-left corner of your screen
- Select “Settings”, then “Update & Security”
- Select “Windows Update” and scroll down to “Advanced Options”
- Under “Choose how updates are installed”, ensure “Automatic (recommended)” is selected
- Ensure “Give me updates for other Microsoft products when I update Windows” is selected

On Ubuntu Linux:

- Select the Ubuntu icon in the upper-left corner of your screen
- Type “terminal” and press return
- Type “sudo apt-get install unattended-upgrades” and press return

- Enter your password and press return
- Type “exit” and press return

On iOS:

- Find and open the “Settings” app
- Select “iTunes & App Store”
- Ensure “Updates” shows the slider to the right with a green background

On Android:

- Find and open the “Google Play” app
- Tap the menu button on your phone (or the three-dots icon if your phone doesn’t have a menu button)
- Select “Settings”
- Ensure “Auto-update apps at any time” is selected

**Locking your Screen**

If you don’t lock your screen when you’re not using it, regardless of any other steps you take, your system is not secure. Step one is setting up a screen lock.

In many jurisdictions, you can legally be compelled to provide a fingerprint to unlock a device you own. In most jurisdictions, you cannot legally be forced to surrender a password or PIN code. For this reason, do not use a fingerprint to unlock any device you own. Use a PIN code or a password.

On Mac OS X:

- Click the apple in the upper-left corner of your screen
- Select “System Preferences”
- Select “Desktop & Screen Saver”
- Pick a screen saver you like
- Under “Start after”, select a time between 1 and 5 minutes
- Click “Hot Corners”
- Ensure all drop-down boxes say “Start Screen Saver”
- Click the back arrow in the upper-left corner of the window
- Select “Security & Privacy”
- Select the “General” tab
- Check the box next to “Require password after sleep or screen saver begins”
- Select “immediately” from the drop-down box

- Develop a habit of locking your screen whenever you're not using your computer by moving the mouse cursor to a corner of the screen

On Windows 10:

- Select the Windows icon in the lower-left corner of your screen
- Select "Settings", then "Personalization"
- Select "Lock Screen" in the left-hand menu
- Select "Screen Saver Settings"
- Pick a screen saver you like
- Next to "Wait", choose a time between 1 and 5 minutes
- Ensure "On resume, display logon screen" is selected
- Develop a habit of locking your screen whenever you're not using your computer by holding down the Windows key and pressing "L"

On Ubuntu Linux:

- Select the Ubuntu icon in the upper-left corner of your screen
- Type "system settings" and press return
- Select "Brightness & Lock"
- Next to "Turn screen off when inactive for", select a time between 1 and 5 minutes
- Ensure the "Lock" slider is enabled, with the word "ON" beside the slider
- Next to "Lock screen after", ensure "Screen turns off" is selected
- Ensure "Require my password when waking from suspend" is selected

On Android:

- Open your device's settings app
- Under "Personal", select "Security"
- Next to "Screen Lock", select "Settings", then "Screen Lock"
- Ensure "PIN" or "Password" is selected, and provide a PIN or password of at least five characters
- If your device supports erasing data after incorrect password attempts, enable that

On iOS:

- Find and open the "Settings" app
- Select "Touch ID & Passcode"

- Under “Use Touch ID for:”, ensure “iPhone Unlock” is disabled: that the slider is in the left-hand position with a white background behind it
- If you don’t have a passcode set, select “Turn Passcode On” and provide a PIN or password of at least five characters
- Scroll all the way down and ensure “Erase Data” is enabled, with the slider in the right-hand side and a green background behind it

**Choosing a Secure Password or Passphrase**

Shorter passwords are acceptable on mobile because most devices can be configured to erase all data after a small number of failed attempts. This feature isn’t present on most desktop operating systems, so you will need a longer password for them.

Do not reuse passwords or passphrases between devices or services.

Passwords fewer than ten characters that don’t use uppercase letters, lowercase letters, and symbols are insecure. These can conventionally be difficult to remember, so it’s recommended that you use a passphrase if you fear you’ll forget a secure password.

Passphrases consist of a series of random words, are are easier to remember, and are as secure as conventional passwords. To create a secure and easy to remember passphrase, a sure-fire method called Diceware is outlined at http://world.std.com/~reinhold/diceware.html:

- Download the diceware word list from http://world.std.com/~reinhold/diceware.wordlist.asc
- Roll a six-sided die five times and write down the numbers
- From the word list, find the word next to that sequence of numbers
- Repeat this process until you have six words written down

**Setting a Secure Password or Passphrase**

On Mac OS X:

- Click the apple in the upper-left corner of your screen
- Select “System Preferences”
- Select “Users & Groups”
- Next to your username, select “Change Password...”

On Windows:

- Select the Windows icon in the lower-left corner of your screen
- Select “Settings”, then “Accounts”
- Select “Sign-in options”
- Under the “Password” section, click “change”

On Ubuntu Linux:

- Select the Ubuntu icon in the upper-left corner of your screen
- Type “system settings” and press return
- Select “User Accounts”
- Under “Login Options”, click the series of dots beside the word “Password”
- Provide your current and new passwords and click “Change”

**Managing your Passwords**

To meet these best practices, it will help to use a password manager. These use a single password to maintain an encrypted database of other passwords, notes, and sensitive data. The program you’ll need to install to do this is called Keepass, which is open source and available on all major platforms

On Mac OS X:

- Download and install KeePassX from: https://www.keepassx.org/

On Windows:

- Download and install KeePass from: http://keepass.info/download.html

On Ubuntu Linux:

- Select the Ubuntu icon in the upper-left corner of your screen
- Type “terminal” and press return
- Type “sudo apt-get install keepassx” and press return
- Enter your password and press return
- Type “exit” and press return

On iOS:

- Install iKeePass: http://ikeepass.de/

On Android:

- Install KeePassDroid: https://play.google.com/store/apps/details?id=com.android.keepass

**Encrypting your Drive**

In case your device is lost or otherwise removed from your control, you will want to have Full Disk Encryption enabled. This will prevent anyone else from being able to access the files saved on your drive. This also means that if you forget your password, your data is irrecoverable. Many platforms offer the ability to save a recovery key. If you have a safe place to store one, such as a fireproof safe, you may do so.

On Mac OS X:

- Click the apple in the upper-left corner of your screen
- Select “System Preferences”
- Select “Security & Privacy”
- Select the “FileVault” tab
- At the bottom of the window, select “Click the lock to make changes”
- Enter your password
- When prompted for a recovery method, Select “Create a recovery key and do not use my iCloud account”. Write this key down and store it in a safe place.
- Once you click “Continue”, your drive will begin the encryption process.

On Windows 10

- Download and install Diskcryptor from https://diskcryptor.net/wiki/Downloads
- From the start menu, select Diskcryptor
- In the “Disk Drives” list, select the “C:” drive and press the “Encrypt” button
- Click “Next”, and then “Next”
- Enter a secure password or passphrase and click “OK”
- Your computer will now begin the encryption process. Once it has completed, restart your computer.

On Ubuntu Linux

If your drive is not already encrypted, you have three options:

- Reinstall the operating system and encrypt your drive during install

- Manually configure dm-crypt and LUKS, which is an error prone and lengthy process beyond the scope of this guide
- Create another user account and encrypt that home directory with encfs during account creation

On Android

- If your device is rooted, un-root it before continuing
- Open the Settings app on your device
- Make sure your battery is at least 80% charged and plugged into a power source
- Select “Security”, then “Encrypt phone”, then “Encrypt phone”, then “Encrypt phone”

On iOS

- If you’re using the latest version of iOS, your disk is already encrypted and you need to take no further action

**Generating a PGP encryption key pair**

In order to encrypt your email, you will need to generate a PGP key pair if you don’t have one already. This is done using an open source program called GPG, or GNU Privacy Guard. This guide does not cover PGP on mobile devices. On mobile, use Signal to communicate via voice and text message.

Do not generate PGP encryption keys on a virtual machine.

This process will generate a pair of keys: a public key and a private key. The public key is what you distribute to other people with whom you want to email securely. The private key is never to leave the encrypted drive on your system.

Do not save PGP private keys to an unencrypted drive.

This process will generate a new key pair and display your public key so you can copy it and send it to people with whom you want to communicate securely over email.

On Mac OS X:

- Download and install MacGPG from https://macgpg.sourceforge.net/
- On your drive, go to “Applications” and open “GPG Keychain”
- Click on “New”
- Give the Full name that you would like to have appear with this key in public as well as the Email address you will associate with this key

- Under “Advanced Options”, make sure “RSA and RSA” is selected, and create a key of 4096 bits in length
- Set your key to expire two years from now
- Enter a passphrase twice, and click “Generate key”
- In the key list, right-click on your key and click “Export”
- Give a location to save the exported key file, and ensure “Include secret key in exported file” is NOT checked.
- Click save. Your PGP public key is in that file, ready to be distributed.

On Windows:

- Download and install GPG4win from https://gpg4win.org/download.html
- From the Start menu, under “Gpg4win”, run “Kleopatra”
- From the “File” menu, select “New Certificate”
- Click “Create a Personal OpenPGP pair”
- Give the Full name that you would like to have appear with this key in public, as well as the Email address that you will associate with this key
- Under “Advanced Settings”, make sure “RSA and RSA” is selected, and create a key of 4096 bits in length, expiring two years from now
- Click “Next”, then “Create Key”
- Enter the passphrase you would like to use with this key
- On the “Key Pair Successfully Created” screen, select “Finish”
- In the certificate list, select your certificate, then from the “File” menu, select “Export Certificate”
- Give a location to save the exported key file and click Save
- Your PGP public key is in that file, ready to be distributed

On Ubuntu Linux:

- Select the Ubuntu icon in the upper-left corner of your screen
- Type “terminal” and press return
- Type “sudo apt-get install gnupg” and press return
- Type “gpg --gen-key” and press return
- Press “1” for RSA and RSA and press return
- Enter “4096” for key length and press return
- Enter “2y” for a key that expires in two years and press return, then press “y” and press return
- Enter the Real name you would like to have appear on this key in public and press return

- Enter the Email address you will associate with this key and press return
- Don't enter a comment, and press return
- Press "O" for "Okay"
- Enter a passphrase twice, pressing return after each time
- Enter "gpg --export –a " and the email address you entered previously, then press return
- Your PGP public key is displayed. Copy it, save it to a text file with the ".asc" extension, and distribute it

**Importing and Signing Someone's PGP encryption key**

In order to verify the identity of people you communicate with, you will need to sign each other's public keys. As you might have noticed when creating key pairs, you are able to enter any name and email address for your key. The same is the case when sending email.

Email and key creation do not verify anyone's identity. Signing each other's keys verifies identity.

Once you sign a person's key, do not push that signature to a key server or share it with anyone else without that person's consent. Instead, email the signed public key back to the person who sent it to you.

To sign a person's key, you will need to have a trusted communication channel open with them. This generally requires sitting in the same room and speaking with each other.

What you're going to do is take turns reading the other person's fingerprint while they verify, character for character, that the fingerprint you read is the one they created. If the fingerprints match exactly, you are free to sign that key and email that signed key back to them.

To import another person's public key:

- Save the file they emailed you to your computer
- On OS X, open "GPG Keychain", click on "Import", and select the file that you saved
- On Windows, open Kleopatra, click on "File", then "Import Certificate", and select the file that you saved.
- On Ubuntu Linux, open Terminal, and type "gpg --import " followed by the path to the file you saved, then press return

To show the fingerprint of a key:

- On Mac OS X, open “GPG Keychain”, hold down the control button and click on the key you’d like to show the fingerprint of, then click “Details”
- On Windows, open Kleopatra, and double-click on the key you’d like to show the fingerprint of
- On Ubuntu Linux, open Terminal, and type “gpg --list-key “ followed by the email address of the key you’d like to show the fingerprint of, then press return

To sign a key:

- On Mac OS X, open “GPG Keychain”, hold down the control button and click on the key you’d like to sign, click “Sign...”, answer how carefully you have verified the key, and click “Generate signature”
- On Windows, open Kleopatra, and select the key you’d like to sign, then from the Certificates menu select “Authenticate certificate...”, select the key you want to sign and make sure “I have verified the fingerprint” is checked, click “Next”, then select which key of yours to sign with and whether you want the signature to be exportable to other people, and click “Certify”
- On Ubuntu Linux, open Terminal, and type “gpg --sign-key “ followed by the email address of the key you’d like to sign, press return, and press “y” to sign their users IDs

To email a signed key:

- On Mac OS X, open “GPG Keychain”, hold down the control button and click on the key you’d like to export, click “Mail Public Key
- On Windows, open Kleopatra, select the certificate you just signed, then from the “File” menu, select “Export Certificate”. Save that to a file and email it to them.
- On Ubuntu Linux, open the Terminal, then enter “gpg --export –a “ and the email address of the person who’s key you just signed, then press return. Copy the key that is displayed and email it to them.

**Using a Subpoena-Resistant Email Service**

If you would like an email service that’s subpoena-resistant and highly unlikely to hand over any data about your email communications, go to http://riseup.net/ and request an email account be created for you. If you have two invites from other Riseup users, you may create an account instantly. If you don’t

have two invites, you will need to fill out a short questionnaire about the reasons you're requesting an account.

**Encrypting your Email**

To encrypt your email, you will need to use Thunderbird and Enigmail. This will encrypt the contents of your email, but not the metadata. Metadata includes the contents of the To:, From:, CC:, BCC:, subject, date, time, and many other attributes of the message. These things will not be encrypted. The only thing that will be encrypted is the body of the email itself and any attachments, so be sure to use generic or meaningless subject lines that don't give away the contents of the email.

When encrypting an email, everyone you communicate with will need to have these tools installed as well. Otherwise, they will not be able to view your messages or respond to them. Further, you will need to have copies of their PGP public keys saved to your computer using the processes outlined previously.

PGP public keys are text files that can safely be emailed without encryption, or exchanged over USB keys.

Configuring these tools on Mac OS X, Windows, or Ubuntu Linux:

- Download and install Thunderbird from https://mozilla.org/thunderbird
- Open Thunderbird
- Configure Thunderbird with the username and password of the email address you'd like to use to communicate with encryption
- Under the "Tools" menu, select "Add-ons"
- Search for "Enigmail" and install it
- Restart Thunderbird
- When Thunderbird restarts, Enigmail will ask which GPG key to use with your account. Select the appropriate key.

Sending encrypted email on Mac OS X, Windows, or Ubuntu Linux:

- Open Thunderbird
- Click "Write"
- Under the "To" line, provide the email address of someone for whom you have a PGP public key saved. You can send encrypted emails to multiple people at once if you have everyone's PGP public keys saved.
- In the Enigmail bar on the email window, make sure the Lock and Pencil icons are both selected, and that the words "This message will be signed and encrypted" appear

- Provide a generic or meaningless subject line
- In the body of the email, provide your message
- Click “Send”
- Enter the password for the PGP key associated with the account you’re sending the email from and press Return.

**Encrypting your Web Browsing**

For your day-to-day web browsing, including the use of services that you authenticate to using a username and password such as Facebook, you can take a few precautions to make your browsing safer from surveillance:

- Go to DuckDuckGo and set it as your default search engine, since they don’t employ trackers: https://duckduckgo.com/
- Install and use the EFF’s browser plugin HTTPS Everywhere to force web services to use secure connections if they are able to: https://www.eff.org/https-everywhere
- Install and use the EFF’s browser plugin Privacy Badger, which blocks a wide variety of trackers: https://www.eff.org/privacybadger

For end-to-end encryption of web traffic that for any reason needs to be as immune as possible to surveillance or censorship, you will need to install and use the Tor Browser Bundle. To do this, go to http://torproject.org/ and download and install it.

Tor works by routing your browsing traffic through other computers on the internet in such a way that it can’t be tracked back to you--but your traffic is still going through other people’s computers on the internet, and you can’t know who owns them or how they treat your data. Tor does not route other people’s traffic through your computer unless you explicitly configure it to do so by making it a “bridge” or “exit node”.

When using Tor, you will need to take some additional precautions:

- Turn off JavaScript. This will break a wide variety of sites, but will make you safer from a variety of attacks on your anonymity. Make sure this is off by checking for a red “no” sign over the NoScript icon in the upper-left corner of the Tor Browser window.
- Do not log in to any services such as Facebook through Tor. Doing so might compromise your credentials to those services.

**Encrypting your Text Messages and Phone Calls**

To encrypt text messages and phone calls from your mobile devices, use an application called Signal from Open Whisper Systems: https://whispersystems.org/

This will encrypt the body of your text messages and the content of your phone calls, but not the metadata. Metadata includes the date, time, sender, and recipient of the message or phone call. Those things are still susceptible to surveillance. The body of your messages and content of a phone conversation sent through Signal are secure.

**Disabling your Device's Surveillance Features**

Modern devices have more firmware and software running on them than you can review, approve, or control. At a baseline, if you're concerned about surveillance, you will want to put black tape over any cameras in your devices.

Further, mobile devices are nearly impossible to secure. Every cellphone has at least three separate computers in it:

- The main computer, which is running Android by Google or iOS by Apple
- The "baseband layer", which is generally made by Qualcomm and coordinates how your device talks to cell towers
- The SIM card, which is running software by your phone carrier

Because of this complexity, if you need to know unequivocally that your phone is not transmitting any data to anyone, you will need to turn it off, implement signal blocking through a faraday cage, and leave it in a location away from you. Never trust that "airplane mode" isn't communicating with towers.

Faraday cage bags can be bought online, or they can be made. A basic faraday cage consists of a layer of insulator such as a paper towel wrapped around the device, then a layer of conductor such as aluminum foil. If you don't use an insulator, there is a chance that the foil can simply act as an antenna.

Test the faraday cage by calling the device before relying on it for signal blocking.

**Securely Erasing Data from your Drive**

If you need to securely erase a drive, you need to first know what kind of drive it is. If it is a solid-state drive, due to wear-leveling algorithms, you will need to physically destroy the drive with force and fire to ensure all data is removed from it. This includes USB keychains and many newer laptop drives.

For magnetic media such as conventional hard drives, you can use a program called Darik's Boot and Nuke from https://sourceforge.net/projects/dban/

You will want to use the fourth option presented under "wipe methods", which is a standard seven-pass erasure procedure. It will take a very long time.

**When all you Have is a USB Thumb Drive**

If you don't have access to a computer but do own a USB Thumb Drive, go to https://tails.boum.org/ and download and install Tails to it. It is a complete installation of Linux that you can boot any available computer with that can securely run all of the tools outlined in this guide.

**Maintaining Active Security Culture**

1) Know when to call something secure enough

Security isn't a question of absolutes: nothing is ever completely insecure or completely secure. To gauge the security of a system, one reasonable approach is to compare the value of what it's protecting versus the cost of the easiest attack that can circumvent the security measures. This implies you can ascribe a value to what's being protected--including assets, freedoms, information, and other intangible things. It also implies that you know the threats that face your system.

A full treatment of threat modeling is beyond the scope of this guide. For a more thorough treatment of threat modeling, see https://en.wikipedia.org/wiki/Threat_model

2) Security through Obscurity doesn't work

Security through Obscurity relies on secrecy or obfuscation to hide information rather than relying on encryption. These methods are less mathematically rigorous than encryption and

aren’t reliable long-term. Don’t simply hide things and assume they’ll stay hidden. Encrypt them and prove it.

3) If you don’t know how it works, don’t trust it.

You should know the basics of how each tool you’re using works, including at very least how to sign keys, how Tor works, and why and how to encrypt a disk.

Every tool recommended in this guide is open source. You can download and read through every single instruction each of these programs are asking your computer to run. This allows for peer review, which is a cornerstone of modern cryptography. Anyone can develop a cryptosystem that they themselves can’t break. A good cryptosystem is one that most or all others can’t as well.

4) Whitelisting offers better protection than blacklisting

It’s far safer to include those you specifically want to include rather than excluding those you specifically know to be unsafe.

5) Keep your mouth shut.

Need to know governs who knows about what you do.

6) On an insecure connection, don't speak in code.

Without encryption, don’t be explicit in any way. If you’re talking about anything you don’t want on the cover of a newspaper, secure your connection first or do not use that connection.

7) Put things away when you're done with them.

Log out of things when you're done. Remove or unload keys when you're done using them. Get into the habit of locking your screen. Set an auto-lock screensaver timer.