# Manual of Digital Resistance

# v1.1

Created by Resistant Systems
https://resistant.systems

**Thank you to all of the individuals, organizations, projects, and movements that have contributed to this manual and the ideas within.**

# Hello.

Have you ever felt the need to do research on ideas that might go against the current status quo? Or that you didn't want to have that information connected to you? Does the private or incognito mode in your browser not feel that safe anymore?

The kit you will create from the instructions included here is in essence your disaster plan for identity.

Have you ever been scared to say something to someone by email, by text, or even over the phone? Perhaps you think that communicating in-person is the only secure way.

This manual will give you the digital tools to speak freely without worry that your messages could be intercepted. If you do it correctly, the information won't be tied to your identity.

Maybe you are in a country illegally and need to research your options or find someone to help you. Maybe you need to voice opinions or deliver

information to a journalist without anyone knowing you are the source.

Maybe you don't like knowing that everything you do on your phone and computer is being tracked, logged, and sifted through by governments and corporations.

If any of these scenarios ring true, this manual is right for you.

So here you are, ready to, as we say, go dark. You might be thinking to yourself, "What the fuck am I doing? Is this crazy?"

It's not, though it might be harder than you imagined it to be. At the end of the day there isn't a magic bullet. You need to be in charge of your safety and practice security and anonymity daily. One data mistake can make the whole system fall apart, so be vigilant.

Let's get started.

# Table of Contents


Hello. 1
Checklist 5
Buying Stuff 7
    Cash 7
    Plastic 9
    Coin 10
Anonymous Browsing 13
    Hijacking Desktops 15
    Tails: Amnesiac Mode 17
        Tor 18
    Tablets Not Phones 22
    Settings 24
    Passphrases 27
    Securing Your Connection 31
        Tor 32
        VPN 35
Pseudonymous Chats 39
    Communication Style 39
    Email Accounts 41
    Instant Messengers 43
        Wire 45
        Signal 46
Good Luck. 51
Social Contract 53
Revision History 57

# Checklist

This manual provides directions and best practices for how to buy devices and services anonymously, hijack desktops, configure tablets for anonymous browsing and communication, and set up an unregistered smartphone to anonymously use phone-based messaging applications. If you follow this manual to a T, you may end up with a Digital Resistance Kit containing the following.

1. Grab 'n' go stash
    a. This manual
    b. A USB stick with Tails, an anonymous operating system
    c. Credentials for an anonymous email account

2. Money in various currencies
    a. Cash
    b. Prepaid credit cards
    c. Phone plan refill cards
    d. Starbucks gift cards
    e. Bitcoin in a paper wallet

3. Main device
    a. 7-inch anonymous tablet

4. Alternate devices
    a. Anonymous smartphone
    b. Emergency flip phone
    c. SIM cards

# Buying Stuff

## Cash

There are a number of ways to pay for things anonymously. The most obvious and easiest technique is buying with cash. This leaves no transactional traces, unlike a credit card, which leaves a data trail with your bank and the store's point of sale system.

The only real problem with cash is being connected to the transaction in other ways. You could be recognized at the store, captured on video, tracked via your cellphone, or somehow have a bill's serial numbers traced.

When buying things in person, go to places you don't usually frequent. This will make it less likely that you will run into someone you know or someone will recognize you. It will also make it harder for you to be identified if someone comes looking for the person who bought X. Attempt to be as forgettable as possible and limit what digital or surveillance systems can record of you.

Limit your digital data trail when purchasing items anonymously. Never bring your own personal phone with you when buying things anonymously. Doing so can leave location data on your phone, on carrier servers, on retailer servers, and potentially on government servers, noting where you were and when.

Going by foot or bike to a store is usually your best option. Public transport can leave a trail of your face on cameras. License-plate readers are becoming quite common in parking lots, and some cities have license-plate reader vehicles that patrol and record, making cars a potential data point that can be traced. In the end, the transportation method that leaves the smallest data trail will be your best choice!

Always wear clothing that masks your identity. This could be clothing that is bulky and hides your face, like a hooded sweatshirt and baggy jeans. It might seem ridiculous, but a disguise is a reasonable option. A hat and sunglasses are a great way to make face detection and recognition harder.

Above all else, be sure to wear clothing that blends in with those around you. A cowboy outfit

in the middle of New York City might be more of an attraction than a disguise. You must fit into the crowd and be easily forgettable by those who see you.

## Plastic

A second common method for anonymous purchasing is to use prepaid Mastercard or Visa gift cards. These can come in handy at places that don't accept cash or when purchasing services online where cash wouldn't be an option.

When buying prepaid gift cards, be sure that you pay for them in cash and buy them in smaller values, like $25 or $50 maximum. Higher-value cards and variable-value cards often need to be registered online—which you do not want. Of course registration of cards can be done with a fake name and address, but should also be done using an anonymous internet connection (this is covered later on). Registering cards is dangerous unless done right. It creates another step one

must do and is a potential data point that could compromise your identity. Only buy prepaid gift cards with cash, and use the previously detailed techniques for the purchase.

## Coin

Another way to pay for things anonymously is to use cryptocurrencies. They are the main currency used on the dark web, and with some cryptocoins it is possible to send money anonymously.

Some cryptocurrencies, like Monero and Zcash, are built to be privacy- and anonymity-focused from the very beginning. Look for services that accept one of these or another anonymity-focused cryptocurrency, rather than going through the process of acquiring other coins anonymously.

Unfortunately, most cryptocurrencies typically cannot be bought or transferred anonymously. To solve this, you need to use a laundering service or find a seller (typically on the dark web) who

will sell you cryptocurrencies anonymously. If this all sounds like a spy movie, it basically is. None of the ways of anonymously buying cryptocurrency are trivial, and most methods take time and practice to do it consistently and securely. This process also has a major downside: if done incorrectly, it can easily leave a connection between your true identity and an anonymous one. Be careful if you explore these pathways, and do more research.

A wealth of knowledge exists on cryptocurrency, especially on the dark web. Do your homework and use cash or a prepaid card to acquire it if you can, as that's generally safer.

Bitcoin can be stored offline as well. Storing your cryptocurrency offline will make it so that your coins are stored on a piece of paper in the form of a QR code and a long string of characters. This makes it easy to store anonymously, give to someone anonymously, and even load into an anonymous digital crypto wallet.

The main downside is that if the paper is ever lost, your coins are lost, just like cash—they can never be recovered. The other issue is that by

printing on paper, you can inadvertently leave a data trail, whether in printed microdots on the paper or with your DNA or fingerprints.

To generate your very own paper Bitcoin wallet, head to https://walletgenerator.net on a computer (this website isn't set up to work particularly well on a tablet or phone). Be careful: Some websites for creating paper wallets actually steal some of your money when you use them. Only use the site recommended here and be sure to do more research online. The standard for making paper wallets may change.

Follow the directions on the site. Pay close attention to its recommendation to open the generator page and then disconnect from the internet. This should greatly reduce the ability for anyone to gain access to your coins. Consider using Tails and Tor (covered later on in this manual) to connect to the site instead of your regular browser.

Note that transfers of Bitcoin cannot be reversed, so it's especially important to triple-check addresses and amounts before you confirm.

# Anonymous Browsing

Being able to do research anonymously is an essential skill. The ability to look up information without being tracked or allowing anyone to know what you are reading empowers you to get more information and answer questions that come up about the tools and techniques in this manual.

Browsing the web anonymously—looking at information without anyone knowing you're the one accessing it—is the most basic form of anonymity. It's easy to forget this, and we often do. Just searching Google from your phone or home computer creates a myriad of logs that governments and corporations use to track your every click.

By browsing anonymously, you can make it so that those data trails can't be connected to your true identity. Think of anonymous web-browsing as sneaking into a library in the middle of the night, reading whatever you want without anyone knowing you were ever there or what you read. The information and its transmission are secure.

There are three main ways to do research anonymously:

1. Go to a location such as a library and use a computer there anonymously.

2. Reboot a normal computer into the operating system Tails using a bootable USB stick, then use its prepackaged Tor browser to surf the web anonymously.

3. Create your own anonymous tablet and use it at a Wi-Fi location you don't use in your normal life.

# Hijacking Desktops

When you're going to the library or any location with computers to use anonymously, consider how you will get there and gain access while limiting the data points you leave behind.

Who sees you? With whom must you interact? What surveillance systems will record you? Will your license plate be tracked? Do you have cash to pay for things? Should you consider wearing a disguise? Is your clothing too unique? Are you going to need to register or otherwise provide identification to access a computer?

These are all reasonable questions to ask. The more you consider how you are surveilled offline and online, the more you will be able to blend into the crowd and go undetected. Remember to leave your regular phone behind whenever you are attempting to do things anonymously.

Seriously.

Your phone is a snitch. Leave it at home.

Or for some extra obfuscation, “accidentally” leave it in a friend’s car for the day.

The library you go to should not be close to your home, and hopefully no one will recognize you there. If possible, walk or bike—anything that leaves fewer traces of your movements is better.

Once you’re there and online, do not do anything you would normally do online.

Don’t log in to a non-anonymous account.

Don’t log in to your regular email account.

Don’t log in to Facebook.

Keep all your anonymous activities separate from your normal habits. Do not check your favorite blog or news site, and never ever log in to any site with your true identity. Leave no connections between what you do online anonymously and what you do normally on the internet.

Be smart and cautious. Think before you act.

# Tails: Amnesiac Mode

If using a computer in the library anonymously doesn't feel secure enough, consider another suggested means of connecting to the internet anonymously: by using a special USB thumb drive to reboot your normal computer or a library computer into the operating system Tails.

Tails is an acronym for The Amnesic Incognito Live System, and it's the choice of whistleblowers and those trying to remain anonymous in difficult scenarios. In fact, Edward Snowden used the Tails operating system to compartmentalize his communications with journalists.

The Tails operating system is based on Linux, which is a free and open-source operating system. Tails has a few key features that make it completely different than Windows, macOS, or other flavors of Linux.

Tails is built specifically for safeguarding anonymity and privacy, and it accomplishes this in a few interesting ways. It is an amnesiac system, meaning by default, the operating

system saves nothing as you use it, and each time you boot up you start from a blank slate. During shutdown or whenever the USB drive is removed from the computer, Tails attempts to clean up after itself so that even a sophisticated adversary can't recover any data pertaining to what the user was doing.

Security-wise, Tails is configured to send all network traffic through the Tor network.

## Tor

Tor is a network and web browser. It works by sending your web traffic around the world through randomized routes of computers within the Tor network. Through a special networking protocol, Tor enables your web-browsing to be close to anonymous. This means you can use it to anonymously visit a website like Reddit and start searching for more information on how to be anonymous online. In this example, Reddit's servers won't know who you are, and anyone observing the network traffic, such as the library's internet provider or the National

Security Agency, will be kept from knowing both who you are and what website you are visiting. For example, the library's internet service provider might know that you are using Tor, but it wouldn't know that you are visiting Reddit. And an NSA server might be able to see that someone is visiting Reddit, but it wouldn't know that it is you.

Of course, this only works if you are simply viewing websites and not logging into them. For example, if you log in to your personal email through Tor, your browsing may no longer be anonymous. So only view sites anonymously or use anonymous online accounts through this connection.

Generally speaking, if you use the Tor Browser and don't modify it at all, don't enable Javascript, and don't log in to any websites, you can assume that your browsing is anonymous. There are always caveats, so please do more research.

Tails is quite different than just using the Tor Browser on a Mac or Windows computer. In those cases, the Tor Browser is focused on just anonymizing your web-browsing. While you're using the Tails system, though, any connection

to the internet, whether it's from an email application or a chat program, flows through the Tor network. This enables an even greater level of anonymity, obscuring even your connection to fetch your mail.

Tails also has a number of useful built-in tools: the Metadata Anonymisation Toolkit, KeePassX password manager, and open-source software for image and video editing.

One of the biggest obstacles to using Tails is just creating the initial USB stick. This can seem daunting. Those who aren't as tech-savvy might be inclined to avoid such things, but it isn't actually too hard to do. Acquaintances of the authors have reported that while this step seemed hard, it wasn't particularly difficult after all. To make a Tails USB, follow the instructions at https://tails.boum.org/install.

Have a computer ready and two 32 GB USB sticks on hand (8 GB is the minimum required, but extra space never hurts). Go step-by-step, and if need be, print out the instructions or keep them on a tablet or phone, so you can read them while you work.

If you find the instructions overwhelming, seek out a local trustworthy techie for advice.

Once you have a working Tails USB, plug it into a computer and restart it, holding down the key or key combination that makes the computer boot from USB. (This will differ on various computers, so look up how to do this on the particular machine you're using.)

Once you have a copy of Tails up and running, it is trivial to make a new USB stick to give to someone else. While you're using Tails, just connect another USB stick to the computer and use the Tails Installer tool to clone the USB stick. This is by far the best method for creation and distribution. You can follow the cloning instructions here: https://tails.boum.org/install/linux/clone-overview.

A last note on Tails: It's important to keep the Tails operating system up-to-date. This can be done by creating a new USB installation from scratch or downloading the newest ISO copy of Tails, then installing it onto a blank USB stick via the same Tails Installer program. Tails will notify you if a new version is available when it starts up.

# Tablets Not Phones

The other way of doing anonymous research is to set up an anonymous Android tablet—one that's bought with cash and that has never been online at your home, your office, or anywhere you normally go.

When buying a tablet, get a small one. Tablets with 7-inch screens look an awful lot like large phones, which can be useful in two ways:

1. This makes it look like you are just using a phone outside a building when you are actually using its Wi-Fi anonymously.

2. If you ever need to take photos anonymously, it's better to be using a device that looks like a phone rather than a tablet—you can conceal it more easily and go unnoticed.

As the title suggests, unlike smartphones, most tablets typically do not have embedded GPS or baseband microchips. A tablet without such chips can't automatically leak location information to a provider or to applications

that would have access to GPS or cell signal. Tablets aren't perfect (Wi-Fi can still be used to determine your location), but they are more secure than smartphones.

Take your tablet to a location that has free Wi-Fi. Make sure that this is somewhere away from your usual routines. This can be a coffee shop, a public library, or even a McDonalds.

When using free Wi-Fi, remember that if it doesn't require a password, it isn't secure. Without a password to join a network, the connection between the tablet and the Wi-Fi router will flow unencrypted. This makes it possible for someone at the coffee shop on the same unsecured Wi-Fi network to eavesdrop on all of your unencrypted network traffic.

This is a reasonable time to remind you that if you are visiting websites that don't require HTTPS, that data between you and the website is unencrypted, allowing anyone along the communication flow to eavesdrop on you.

Fortunately, eavesdropping doesn't need to be a huge concern. With this tablet, we will be focused

on using software that by default encrypts everything, making eavesdropping nearly impossible.

When you're first setting up any anonymous device, do it from an anonymous internet connection. See the previous advice in this guide on locations where you might connect.

Never use your anonymous tablet at home!

Decline everything the device offers automatically, don't accept other software installations, don't send Google feedback or logs automatically, don't connect to Wi-Fi yet, and skip setting up a Google account for the time being.

## Settings

Before we do anything else, we want to make sure location tracking is turned off. You can find this under Settings > Privacy > Location. Turn it off.

Please note that throughout the tablet settings section, we will provide likely names of the settings

you should update, but these menus are specific to each device and the Android operating system version it uses. You will need to find the right settings on your own device. Use this as a guide, but use your own brain for your specific context.

Next up is to set a strong password for the device under Settings > Security > Lock Screen. Change the screen lock type to “password”, and if you have the option available, turn on “Require password to turn on.” When choosing a password, try something at least 12 characters long and unique—you will need to memorize it right now. It’s best to use a passphrase for this, consisting of multiple words, to ensure it’s difficult to guess or crack. (See discussion of diceware passphrase generation in the subsequent Passphrases section for one method of generating this type of password.) There will not be a backup for this password, so memorize it NOW.

You should also make sure that any facial recognition or fingerprint scanning settings are turned off. Look for Biometric settings under Lock Screen. Note: These are newer features that are usually associated with more expensive devices, so you might not see these on yours.

Under “Lock screen preferences,” choose “Don’t show notifications at all” on the lock screen.

Next up is to encrypt your device. How this is handled greatly depends on the Android version installed on your device. In earlier Android versions, full disk encryption could be turned on under Settings > Lock screen and security > Other security settings > Encrypt device. With newer devices, Google has shifted to a file-based encryption method that is less transparent to the user. You will need to do more research on your particular device to figure out how to enable encryption if possible. Some devices now come with encryption turned on by default, while with others, you can only do so by enabling Developer options, then turning on encryption. Please do more homework to be sure you’re updating the correct settings to encrypt your device—encryption is important!

The other thing we want to turn off is your keyboard’s predictive typing. If we don’t, the keyboard will learn your anonymous email addresses and other data you type in that could give away your identity if the tablet ever fell into the wrong hands. To address this, go to your

keyboard settings under Settings > Languages & input. The exact settings available will depend on your brand of tablet and the operating system version it uses, but you'll want to go through all keyboard settings and look for anything involving "smart typing," "predictive text," "next-word suggestions," "personalized suggestions," "share snippets," etc., and turn it off.

Depending on your need for assistive speech-to-text and text-to-speech, you should disable as many voice and Google Assistant settings as possible. The less your microphone can listen to you, the better. Along these lines, it's likely a good practice to ensure Now Playing is disabled on your device, if available on your operating-system version, since it enables the microphone to capture sound data around you, even when your device is locked.

## Passphrases

When you first connect the tablet to Wi-Fi, your first point of business should be immediately installing a password manager. This way, you can

keep track of all the various anonymous accounts and passwords you create.

Unfortunately, you can't install applications on the tablet without a Google account. (There are ways around this, but not only are they too cumbersome for this manual, they also reduce the security of your tablet. If you want to try this type of thing, search the internet for "sideload Android app.")

Go to the Play Store and you will be prompted to create a new account. When choosing a username, try creating one in another language—an easy red herring. Memorize the password for the moment. You will enter it into a password manager for safekeeping shortly.

The authors have had good luck with the Android application Keepass2Android, which is a free password manager. Other password managers are out there, and some others we know like KeePassDroid, so you can make your own decision on this. KeePass in general is an open-source standard for password managers, and Keepass2Android is a nice implementation of this standard for Android.

Install Keepass2Android from the Play Store and set a strong password for the manager. You can now store the password for the Google account you created in this password manager.

You should immediately memorize two passwords: 1. the password you use to log in to the tablet and 2. the password to unlock the password manager on the tablet.

Speaking of passwords, your passwords are likely terrible. So let's make them not terrible. This advice works for your normal life as well.

First, let's start referring to them as passphrases. Using a phrase of multiple words strung together instead of a single word will be longer and therefore stronger.

To create the passphrases you will use to unlock your device and password manager, using diceware is a great way to go. Diceware is a technique for creating passphrases that are relatively easy to memorize, yet make it nearly impossible for a computer to crack with brute-force methods.

Here are the basics. Start with a word list of approximately 8,000 words, with each word numbered from 11,111 to 66,666. You can download a word list from the Electronic Frontier Foundation here: https://www.eff.org/dice/.

Then roll 5 dice at once, giving you a random number, say 12,451. This number will correspond to a word in the list, which will be the first part of your passphrase. By repeating this process at least 6 times, you will generate a passphrase that will be nearly impossible for today's computers to crack.

An example of a passphrase that might be generated by this technique would be "AnyhowCableRemovingPunkSensuallyBlank" It consists of six individual words that combine to make one random, long, and strong passphrase.

Random words are much harder to crack than words that have connections or associations with your family, childhood, or life in general.

Make your own randomized passphrases. Make a different one for each of your devices.

# Securing Your Connection

When you normally connect to the internet via Wi-Fi, your data will pass through the Wi-Fi base station or router, the modem, Internet service provider (ISP) servers, and any other servers between your computer and the final server you are visiting. With your data going through all of these intermediaries, it could be monitored in a variety of ways. To limit the data an ISP or a strong adversary such as the NSA could capture about you, we will secure your connection to the internet.

This can done in two main ways, either with Tor or with a VPN. Please read up on both here and decide which you will primarily use for your device. The authors recommend Tor instead of a VPN service because it is stronger. Using Tor can create some hurdles. It may add some difficulty to your established habits and make browsing slower, but in return for this investment of effort, it offers better protection.

# Tor

Please refer to the previous Tor section under Tails: Amnesiac Mode for an explanation of the Tor network and browser. Here we will focus on how to user Tor on a tablet.

First you will need to install Orbot and the Tor Browser from the Google Play Store.

Orbot acts similarly to a VPN, routing traffic from other applications through the Tor network instead of directly to the internet.

When you first open Orbot, you will need to turn on “VPN Mode,” which allows traffic from all applications to flow through Tor.

To start the connection to the Tor network, tap the start button in Orbot, which is the big onion button in the center. It may take a little while to connect, but once it says “NOTICE: Bootstrapped 100%: Done” you can go back to the home screen and select the Tor Browser icon to start browsing the web anonymously.

Beware: At the time of writing, you are still required to use Orbot to connect to Tor, but eventually the connection to the Tor network will be embedded within the Tor Browser application itself. This will remove the requirement to use Orbot and perhaps render it obsolete. Check the Tor Browser application and installation instructions for updates.

Tor can also be used to visit hidden services, a.k.a. the dark web. The dark web actually consists of anonymous websites hosted on computers within the Tor network. These websites can't be accessed from the regular internet or a regular web browser; they will only work within the Tor Browser. You can always tell a site is on the dark web by the fact that the URL ends in ".onion" and has a long string of characters before it, such as http://kpvz7ki2v5agwt35.onion.

The dark web is useful in a few ways: 1. Other anonymity-focused individuals have put resources there. 2. If you want to do anything with anonymous cryptocurrencies, the dark web has lots of information available. 3. If you are trying to get information to a journalist

anonymously, the SecureDrop and GlobaLeaks services are hosted there.

SecureDrop is a project by the Freedom of the Press Foundation that enables media organizations to offer a web-based secure tool for conversations and passing of files between sources and journalists completely anonymously. Links to SecureDrop sites on the dark web hosted by news organizations can be found here: https://securedrop.org/directory.

Some good jumping-off points for trying to find websites on the dark web are 1. the onions page on Reddit (https://www.reddit.com/r/onions); 2. searching for "dark web links 2018" on Pastebin (https://pastebin.com), e.g., "The Hidden Wiki," which is a good starting point for exploration; and 3. Ahmia, a search engine for hidden services, which at the time of writing was located at http://msydqstlz2kzerdg.onion/.

Nothing on the dark web is completely straightforward, and it might feel closer to the internet in 1998 than 2018. But take your time and don't worry. Use common sense and you'll be fine exploring it.

# VPN

Virtual Private Networks (VPN) originated as a way for remote employees to securely tunnel their network connection back to their companies' headquarters. This essentially allows remote computers to connect to their organization's internal network.

VPNs became popular with internet users because they can associate your traffic with an IP address that's tied to a physical address in another city or country, obfuscating your true location. This can circumvent government firewalls and company blocks on location-locked content. With a VPN, people in the U.S. can make it look as if they are located in the U.K., for instance, to gain full access to the BBC's content.

This isn't a foolproof system, mostly because you need to trust your VPN not to reveal your information to other parties. In essence, with a VPN, you shift trust in your internet connection from your internet service provider to the VPN provider. The advantage of a VPN is that the VPN will encrypt all of the information from your

computer until it reaches the VPN's server. This makes it harder for those in physical proximity to you (e.g., others in your Wi-Fi café) or those who might intercept traffic at a country-level internet gateway (e.g., the government of another country) to gain access to your data.

Choosing a VPN provider is a difficult task. Try an internet search for "VPN." The results can be confusing. A vast array of services are available, each with its own pros and cons. Look through review sites to do due diligence. This article is a good resource: https://torrentfreak.com/vpn-services-keep-anonymous-2018/

The authors have had good luck with the VPN service provider Private Internet Access (PIA). One particularly great feature of this service is that it can be paid for anonymously with a Starbucks gift card. Other brands of gift cards are also accepted, but we have had good luck with Starbucks, because it is so ubiquitous and easy to visit at random locations.

To set up PIA, go to https://www.privateinternetaccess.com and scroll down until you see the option to "Pay anonymously with

many major brand gift cards." Then enter a new anonymous email address you created for just this service and the number of the Starbucks gift card you purchased with cash at a random location.

PIA will then email your username and password to the anonymous address you entered. Download the VPN by Private Internet Access application from the Google Play Store and log in with the provided username and password. Store this username and password in your password manager for safekeeping.

Now, any time you connect to a Wi-Fi network, you should immediately open the PIA app and connect to its network. By default, PIA is configured so that all of your applications' traffic runs through the PIA VPN system. In effect, you now have better encryption when using Wi-Fi.

While you're using the VPN, use a privacy-focused browser such as the DuckDuckGo Privacy Browser, instead of the Google Chrome browser that comes packaged with the tablet. This will leave fewer traces and won't connect your browsing to the Google email identity created to configure the tablet.

# Pseudonymous Chats

Now that you can do research anonymously online, the next thing you might want to do is communicate with someone pseudonymously.

Before creating any accounts, make sure you are doing it from an anonymous web access point like a computer library, an anonymous tablet, or using Tails on your laptop. Lots of messaging systems are available for pseudonymous communication, but let's start by thinking about ways you might be identified first.

## Communication Style

When writing emails or messages, do not refer to yourself or provide details about yourself unless necessary. The less information you include, the better. Remember you are trying to be anonymous, or at least pseudonymous—you don't want anyone to know your true identity.

Be careful how you write, particularly with regard to the language you use. Stylometry can be

used to compare language usage from multiple sources to determine how likely a writing sample is to have been written by a particular person. Everyone has their own writing style, and this can be analyzed and detected using algorithms. So be careful about your phrases and constructions.

Why should you be careful about how you write? Take the last paragraph as an example. The first sentence of the previous paragraph contains “particularly with regard to.” This can be a hallmark of a writing style, and it would be better if it were changed. One way to do this is by passing the text through a language translation program and back again.

Here is the previous paragraph again, but translated into Korean, Arabic, Bosnian, then finally English once more.

> Be careful how you write, especially with the language you use. You can use stylesheets to compare the use of languages from different sources to determine the possibilities that the author created for a particular person. Everyone has his own writing style, and can be analyzed and discovered using

> algorithms. So be careful with phrases and structure.

The translated paragraph isn't perfect—notably, it leaves out the word "stylometry"—but it gets the point across. Consider translation as a form of obfuscation for your communication to protect your identity.

## Email Accounts

A new email address should be created whenever you are going to register with a website or communicate with someone. This way, if one account is compromised, it won't affect your other accounts.

In terms of which email provider to use, there are many, but we have a soft spot in our hearts for ProtonMail. It was created by former scientists at CERN and MIT and has end-to-end email encryption built in by default.

Riseup is the other provider we tend to use. Its set of tools for email, chat, and document collaboration is supported by a community of

activists. Riseup requires that new users apply to use its services (which can take a while) or have a referral code (which can be hard to obtain if you don't know the right person), though, so in this manual we will focus on using ProtonMail.

Install the ProtonMail application from the Google Play Store or go to https://protonmail.com. Follow the Sign Up prompts to create a new account. The system will attempt to confirm that you are an actual human, not a spambot trying to create random accounts. Typically a captcha is used to confirm your humanity, but sometimes if you are connecting to the site using Tor or a VPN, the captcha method will generally not be available.

If you do not see an option to use a captcha, try connecting from a different Wi-Fi location or from a different VPN server or different Tor route. Do not use text verification to verify your humanity.

Whenever you create a new email account, memorize the username and password (if you are a genius), or better yet, store it in your password manager.

Do not cross-contaminate your email accounts. Use one email account per service or per conversation. Keep your accounts compartmentalized, so that if one is compromised, the others will not be.

## Instant Messengers

Aside from email, some other options are possible to communicate pseudonymously and securely online. A growing list of instant messenger applications claim to be private and secure, including iMessage, Google Hangouts, WhatsApp, Telegram, Wickr, Signal, Threema, and Peerio. For a number of years, the authors have been closely following the development of these sorts of secure messaging applications, and they currently make use of Wire and Signal for both pseudonymous and everyday communications.

Of course, the reader is encouraged to do more research and make their own choices about what messenger applications they choose.

Like most messenger applications, Wire and Signal can only be used when both people are using the same app.

A few reasons why we like Signal and Wire:

- Both are open-source and have had their code bases audited by third parties.

- Both limit log retention (how long they keep any records that your device connected to their servers). This makes it harder for others even with judicial approval to find your identity or access your message metadata.

- Both have privacy-focused features like "disappearing messages," which enables messages to delete themselves after they have been delivered.

- Both strip the metadata and location out of photos when they are sent, limiting ways extra tracking information could inadvertently slip through.

- Both offer encrypted voice communication, meaning you can make calls through these applications and no one can snoop on what you are saying through your connection.

Between the two services, we prefer Wire.

## Wire

Wire only requires an email address to sign up, not a phone number. It is very easy to create an anonymous email address, but quite difficult to create and maintain a phone number completely anonymously. Even if you were to use a burner phone, it would still ping cell towers whenever it is turned on. If someone knew your phone number from Signal, they could potentially use it to track your present location and past locations.

Along similar lines, Wire can be installed on a tablet, whereas Signal cannot.

The use of email addresses to sign up also makes it easy to have multiple accounts with Wire. This can allow you to further compartmentalize your identities and anonymous activities.

In terms of legal protections, the company behind Wire is located in privacy-friendly Switzerland, with servers in Ireland and Germany. This potentially makes it harder for anyone to legally requisition data Wire might have stored in connection to your

accounts. Your messages are stored in encrypted form on the servers and can be decrypted only by the recipient of the message, not by the company.

Before launching Wire or any messaging application, make sure you are connected to a VPN or Tor. To get started, sign up for an account with an anonymous email address. Make sure you use “timed messages,” a.k.a. notes that auto-destroy after one reads them.

## Signal

To use Signal, we need an anonymous phone number. To do that in a secure way, we will actually use two anonymous phones: one smartphone that has never been registered and doesn’t have a SIM card and one simple flip phone that will be registered anonymously. The flip phone will only be used to receive one verification text from the Signal servers, then never used again, except to keep the phone number active.

Acquiring a phone number anonymously can be difficult in some countries, but it is surprisingly easy in the U.S. Pay-as-you-go services such

as Boost Mobile, Cricket Wireless, or Tracfone support this. You can buy phones and SIM cards for these services from big-box stores such as Best Buy, Walmart, or Target. Again, make sure when buying that you are as anonymous as possible, using all of the tips we have already discussed. The phone's serial number and IMEI number will be registered at the time and location it is sold to you. So wear a disguise, pay cash, and don't bring your regular phone!

Once you have bought your two prepaid phones anonymously, one smartphone and one flip phone, you should go to a place that is not your home or anywhere you normally go. That way, when you register the flip phone, your initial location transmitted to the phone-company servers will not be associated with you.

The process for registration usually involves going to the carrier's website and using a prepaid top-up card to pay for the service. At this point, you will likely have to enter the phone's IMEI number (this can be found under the battery) and the SIM card's ICCID number. Remember to do this all from an anonymous browser, as detailed previously.

Once you have a working flip phone, take the smartphone and configure it similarly to the anonymous tablet, making sure you immediately disable any location services in the phone settings. This will disable all GPS and location data that might be determined via one's Wi-Fi connection.

Never put a SIM card in the smartphone and always keep Airplane Mode turned on when using it. This will block your phone's baseband processor from communicating with your cellular provider. You can still turn on Wi-Fi with airplane mode on.

Set up Tor or a VPN and a password manager on the smartphone, then install Signal from the Google Play Store. Be sure to use Tor or a VPN when you sign up for Signal to obfuscate the IP address from which your account is created. Use the phone number of the anonymous flip phone to register Signal. A verification text message will be sent to the flip phone, which you will enter on the smartphone to complete your Signal installation.

Your Signal account will only be secure as long as you control the phone number associated

with it. Because the phone number you're using here is associated with a prepaid phone, if you do not keep it active, your number will be forfeited and someone else could take over your Signal account. So you must abide by the carrier's rules for keeping your phone number active. This usually involves keeping your bill paid and turning the flip phone on monthly (not from your house). When you aren't adding credit to your phone account, be sure to keep the battery removed from the phone.

Please note that at the time of writing, Signal could not be installed on a tablet. It is not available. If it does become an option in the future, it would be better to use a tablet than a smartphone. Smartphones still have a baseband processor that could potentially be a vector for attack.

One of the reasons why privacy advocates appreciate Signal is that it doesn't store any more information on its servers than is absolutely necessary. In terms of log files, the company only keeps the date of the first time you signed up and the date you last connected. Many companies can claim that they don't store or hold

onto your data, but these types of claims are very hard to confirm.

In the case of Signal, this extra care around data retention has been tested through subpoenas of user information by the U.S. government. Legally, Signal has to provide all of the information it had available for a particular account to the government. But as the released documents showed, Signal had virtually no information or logs to hand over. Looking at past government data requests is a great way to verify companies' privacy claims. This confirmation of Signal's stance as a company to protect its users makes it a strong choice for privacy.

# Good Luck.

This isn't easy.

There is no single approach to staying under the radar. It takes commitment and consistency.

Anonymity is a state of mind and one that you can practice just by going to the store and trying not to be seen by cameras.

Try using cash more often.

Can you keep accounts compartmentalized?

You should start to practice this new way of thinking and viewing the world daily. That is the only way to make sure that you are prepared.

# Social Contract

In writing this manual, the authors seek to provide information to others, such that they can be better protected. We have sought to overcome bias and endeavored to be a reliable source.

The reader therefore needs to be able to assume and trust that the information provided here is accurate and reliable, and if it's followed, it will not compromise the reader's livelihood. The following is a social contract that is derived from the Tails Social Contract. That, in turn, was derived from the social contracts of Tor and Debian (the operating system Tails is based on).

Here are our commitments to you, the reader.

## 1. By creating this manual, we have tried to provide usable information on tools, techniques, and systems to be anonymous, private, and secure.

The authors believe that privacy, the free exchange of ideas, and equal access to information are essential to free and open societies. Through the techniques and best practices here described, we provide means that empower all people to protect and advance these ideals.

## 2. Open and transparent information are keys to our success.

When possible, all reasoning for what is written has been included and references have been linked for further explanation.

## 3. Our tools are free to access, use, adapt, and distribute.

This information in this manual can be reused, shared, modified, and distributed in any way you the reader see fit. This work is licensed under the Creative Commons Attribution 4.0 International

license:
https://creativecommons.org/licenses/by/4.0/

### 4. We will never intentionally harm our readers.

We will always do our best to provide the most accurate information. We will never willingly include false or misleading information. We will be upfront about the known issues with the tools, techniques, and best practices included.

### 5. We give the reader the means to decide how much they can rely on the information provided.

We encourage readers to inform themselves and decide whether the tools and techniques included here are suitable for their use case and how much they can trust us.

We encourage readers to do more research and consult third-party documentation and other opinions to make informed decisions and engage in a learning process about the tools and techniques covered in this manual.

# Revision History

**v1.0: November 13, 2018**
Initial release of this document.

**v1.1: January 8, 2019**

- Grammar updates for clarity.
- Added torrentfreak.com link to the VPN section.

With this manual you may find a copy of the Tails operating system. Enjoy.

Fira Sans and Fira Mono are the fonts used throughout this manual and are from Mozilla. We like Mozilla.