Telecommunications

Security, Anonymity, and Privacy

In Theory and Practise

Ver. 6.3

The Definitive Guide to Online Privacy

Prepared for CryptGnosis
https://www.cryptgnosis.com

By H.D. (Doc) Slow

CryptGnosis

CryptGnosis

https://www.cryptgnosis.com

Ordering Information:
Quantity sales. Special discounts are available on quantity purchases by corporations, associations, and others. For details, contact the publisher at the address above.

Printed in the United States of America

Version release history: 1.0 - 6.

Table of Contents

INTRODUCTION

This instructional manual is designed to give companies and individual humans the details (step-by-step) on how to remain anonymous and retain privacy and security in the digital medium. Your computers and your phones, the internet of things (IoT), etc., are the key devices that afford us the great ability to communicate, have been completely compromised allowing anyone or any agency, state sponsored or otherwise to collect vast amounts of data, personal and professional (intellectual property) on your company and/or your person. This can be as gravitas as to warrant a national security issue to the simple collection of personal data.

DISCLAIMER

The information contained in this instructional manual is intended solely to provide general information and guidance on matters of interest for the personal use of the reader, who accepts full responsibility for its use. The application and impact of laws can vary widely based on the specific facts involved. Given the changing nature of laws, rules and regulations, and the inherent hazards of electronic communication, there may be delays, omissions, or inaccuracies in information contained in this manual. Accordingly, the information in this manual is provided with the understanding that the authors and publishers are not herein engaged in rendering legal or other professional advice. As such, it should not be used as a substitute for consultation with

professional legal, or other competent security advisers.

While we have made every attempt to ensure that the information contained in this manual has been obtained from reliable sources, CryptGnosis is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this manual is provided “as is,” with no guarantee of completeness, accuracy, timeliness, or of the results obtained from the use of this information, and without warranty of any kind, express, or implied, including, but not limited to warranties of performance, merchantability, and fitness for a particular purpose. Nothing herein shall to any highly recommended extent substitute for the independent investigations and the sound technical and business judgment of the reader. In no event will CryptGnosis, or its partners, employees, or agents be liable to you or anyone else for any decision made or action taken in reliance on the information in this manual or for any consequential, special, or similar damages, even if advised of the possibility of such damages.

BASIC ANONYMITY AND PRIVACY

Even if you feel relatively certain you aren't in need of total anonymity, you're wrong. There are legal rules being thrown out the window that allow your Internet Service Provider (ISP) to collect your browsing information, and freely share it with anyone or any organisation it wishes.

Recent rulings by the FCC indicate that your Internet Service Provider (ISP) may gather this data and do with it what it wishes.

The Federal Communications Commission (FCC) voted to block one of several broadband privacy rules the agency approved last year to protect people's online activities. The new rule would have required ISPs and phone companies to take "reasonable" steps to protect customers' information from theft and data breaches, and provide notifications if they did occur.

All of the new broadband privacy rules have been opposed by the telecom industry, which said the FCC regulations would make it more difficult for ISPs to compete with companies such as Google and Facebook, which are subject to weaker privacy regulations by the FCC.

Every time you go online, you reveal a lot of information about yourself: what you browse, where you shop and what you buy, where you travel, which apps you use, and basically what you're interested in. That gives your ISP - a cable company such as Charter or Spectrum, or a telco such as AT&T or Verizon - a lot of information about you. They can track, collect, and share this data with outside companies such as marketers, or anyone else.

The regulations are supposed to mandate opt-in consent on data collection. This means that you would have to agree before an ISP could use, share, or sell your "sensitive" personal data. For regulatory purposes, the term normally covers all children's information, plus health and financial data, and Social Security numbers. But the FCC plan also pulls in web browsing and app usage histories, as well as the content of communications such as emails and texts.

The CTIA and NCTA - The Internet & Television Association - the main lobbying groups for the cable and wireless industries - as well as other groups representing ISPs and advertising companies, recently argued in a letter to Congress that the FCC rules "would create confusion and interfere with the ability of consumers to receive customised services and capabilities they enjoy and be informed of new products and discount offers."

The groups had also warned that people would be "bombarded with trivial data breach notifications" if the FCC rules were enacted.

This means is that you have no protections with regard to your ISP's data mining (collection) and distribution of your personal data. In the following procedural instruction, we

will detail all the necessary steps for derailing their intent, and ensure that you understand how to thwart their internet and telecomm data gathering practises. In somewhat lesser confidence, these procedures can, if used properly, obfuscate your identity from major state-sponsored organisations (foreign and domestic).

In this environment, how easy is it to create and maintain online accounts while preserving your anonymity — even from social media and email, and any state-sponsored agency that may request its records? There are different ways to accomplish this. If one plans on following the steps outlined here, one should make sure they understand the purpose of them, in case one needs to improvise. There is no guarantee that these techniques will protect your anonymity — there are countless ways that things can go wrong, but most of them are procedural rather than technical. The technical problems associated with maintaining anonymity are detailed further along in this document.

THREAT MODEL ASSESSMENT

Threat modeling is a process by which potential threats can be identified, enumerated, and prioritised - all from a hypothetical attacker’s point of view. The purpose of threat modeling is to provide defenders with a systematic analysis of

the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker. Threat modeling answers these questions:

- Where are the high-value assets?
- Where am I most vulnerable to attack?
- What are the most relevant threats?
- Is there an attack vector that might go unnoticed?

Before we begin, it helps to define a threat model, that is:

- What we need to protect?
- Who do we need to protect it from?
- What are their capabilities?
- What countermeasures prevent or mitigate these threats?

Since it is impossible to be completely secure all of the time, we need to prioritise our limited resources into protecting what matters the most. The most important piece of information you need to protect in this case is your real identity.

State-sponsored organisations (foreign or domestic) might launch an investigation aimed at learning your identity. It may be to retaliate against you — getting you fired, charging you with crimes, or worse. What you post on your social media

accounts might also anger armies of trolls who could threaten you, abuse you with hate speech, and try to uncover your identity.

If certain state-sponsored organisations open an investigation aimed at de-anonymising you, one of the first things they'll do is simply look to social media — and every other service that they know you use — for information about your accounts. So a critically important countermeasure to take is to ensure that none of the information tied to your accounts — phone numbers, email addresses, or IP addresses you've used while logging into your accounts — lead back to you.

This is true for all accounts you create. For instance, if you supply a phone number while creating a Twitter account, the phone service provider associated with that number shouldn't have information that can lead back to you.

Another concern: State-sponsored organisations also might go undercover online and try to befriend you, to trick you into revealing details about yourself or to trick you into clicking a link to hack you. They might make use of informants in the community of people who follow you on social media as well. Organised trolls might use the same tactics.

WHO NEEDS THIS CALIBER OF ANONYMITY AND PRIVACY?

- Government Officials
- DOD Contractors
- Company employees and executives possessing intellectual property that need protection
- Company employees and executives traveling abroad
- Journalists
- Activists
- Whistle-blowers
- Celebrities
- Inventors
- Individuals in witness-protection programs

REAL WORLD SECURITY

Today's idea of computer security is but a farcical mess. Everyone is told that they can be secure if they only add-on several prophylactic applications designed to protect the flawed operating systems they are so beholden to – mainly because they have been conditioned to believe that these operating systems are their only choice. These operating systems are continuously vulnerable because of their inherently flawed architecture – and can never be protected simply by adding the defensive sheaths of third-party applications. A Catch 22. Strictly speaking, a "Catch-22" is "a problematic situation for which the only solution is denied by a circumstance inherent in the problem or by a rule." For example, losing something is typically a conventional problem;

to solve it, one looks for the lost item until one finds it. But if the thing lost is one's glasses, one can't see to look for them – it is a Catch-22. The term "Catch-22" is also used more broadly to mean a tricky problem or a no-win or absurd situation.

This, unfortunately, is the situation with ALL Microsoft Windows and Macintosh/Apple Operating Systems. These antiquated and security-less operating systems cannot be used, and need to be dispensed with if one is seeking any model of real security.

PREFERRED HARDWARE AND YOUR OPERATING SYSTEM

The very first consideration is to choose the hardware that will accommodate the operating system (OS) of choice for attaining anonymity. Our OS dictates the hardware we will choose. While there are a handful of operating systems that attempt to achieve complete anonymity, the OS we'll be using is called “Tails,” and it will be referenced throughout this document.

Tails OS should work on any reasonably recent computer, say manufactured after 2005. Here is a specific list of requirements:

- Either an internal or external DVD reader or the possibility to boot from a USB stick or SD card (micro SD preferable with or without adapter).
- Tails requires an x86 compatible processor: IBM PC compatible and others but not PowerPC nor ARM. Mac computers are IBM PC compatible since 2006.
- 2 GB of RAM to work smoothly. Tails is known to work with less memory but you might experience strange behaviours or crashes.

Tails OS documentation does not provide you with a list of hardware that works with the OS, rather it lists issues with hardware it doesn't work properly on. Please see:

https://tails.boum.org/support/known_issues/index.en.html

The hardware that we have tested extensively, and found no issues for running Tails OS is the Acer Chromebook 15 CB5-571-C1DZ (15.6-Inch Full HD IPS, 4GB RAM, 16GB SSD). It is inexpensive and just works. Plausible deniability is inherent in the system if you have a public identity associated with Google. Simply login in with your Google credentials.

https://www.amazon.com/Acer-Chromebook-CB5-571-C1DZ-15-6-Inch-Full/dp/B00TU7U4PU

PREFERRED HARDWARE MEDIUM CONTAINING THE OS

Micro SD - Better than USB - Easily concealed and disposed of.

Here is a list of known good Micro SD cards:

- Barun Electronic's Gold Flash PRO (64GB) MLC
- Memorette (memento) Standard premium (8GB) MLC
- Lexar High-Performance UHS-I cards [300x] (64GB) MLC [LSDMI64GBBNL300A]
- Lexar High-Performance UHS-I 633x MicroSD (64GB) MLC [LSDMI64GBBNL633R]
- Samsung PRO [New 2014 Series] (64GB) MLC [MB-MG64DA]
- Sony High-Speed R95 UHS-3 (64GB) MLC [SR64UXA]
- PNY Turbo Performance High Speed MicroSD (64GB) MLC [P-SDUX64U190-GE]
- Transcend Ultimate 600x UHS-1 (32GB) MLC [TS32GUSDHC10U1]

IF MEDIA SANITISATION BECOMES NECESSARY

In the best scenario, it would be wise to completely destroy your OS hardware. Since we are utilising the OS on a micro SD card, this is a rather easy task. We can quickly dispose of the micro SD card in many ways. A good shredder will do the trick (tested). Other methods, including EMP erasure, are in development stages.

WHAT IS TAILS OS?

Tails is an exclusively live system that aims to preserve your security, privacy and anonymity. It helps you to use the

Internet anonymously and circumvent censorship almost anywhere you go and on any computer, but leaves no trace unless you ask it to explicitly.

It is a complete operating system designed to be used from a DVD, USB stick, or SD card (micro preferred) independently of the computer's original operating system. It is Free software and is based on Debian GNU/Linux.

Tails comes with several built-in applications pre-configured with security in mind: web browser, instant messaging client, email client, office suite, image and sound editor, etc.

ONLINE SECURITY, ANONYMITY, AND CENSORSHIP CIRCUMVENTION: TOR

Tails relies on the Tor anonymity network to protect your privacy online:

- all software is configured to connect to the Internet through Tor.
- if an application tries to connect to the Internet directly, the connection is automatically blocked for security.

Tor is an open and distributed network that helps defend against traffic analysis (a form of network surveillance that threatens personal security and privacy, confidential business activities and relationships, and even state security).

Tor protects you by bouncing your communications around a network of relays run by volunteers all around the world: it

prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Using Tor you can:

- be anonymous online by hiding your location,
- connect to services that would be censored otherwise;
- resist attacks that block the usage of Tor using circumvention tools such as bridges.

To learn more about Tor, see the official Tor website, particularly the following pages:

Tor overview: Why we need Tor

Tor overview: How does Tor work

Who uses Tor?

Understanding and Using Tor — An Introduction for the Layman

To learn more about how Tails ensures all its network connections use Tor, see their design document.

STATELESS OPERATING SYSTEM USAGE

Using Tails on a computer doesn't alter or depend on the operating system installed on it. So you can use it in the

same way on your computer, a friend's computer, or one at your local library. After shutting down Tails, the computer will start again with its usual operating system.

Tails is configured with special care to not use the computer's hard-disks, even if there is some swap space on them. The only storage space used by Tails is in RAM, which is automatically erased when the computer shuts down. So you won't leave any trace on the computer either of the Tails system itself or what you used it for. That's why they call Tails "amnesic".

This allows you to work with sensitive documents on any computer and protects you from data recovery after shutdown. Of course, you can still explicitly save specific documents to another USB stick or external hard-disk and take them away for future use – at your own risk.

STATE-OF-THE-ART CRYPTOGRAPHIC TOOLS

Tails also comes with a selection of tools to protect your data using strong encryption:

- Encrypt your USB sticks or external hard-disks using LUKS, the Linux standard for disk-encryption.
- **Automatically use HTTPS** to encrypt all your communications to a number of major websites using HTTPS Everywhere, a Firefox extension developed by the Electronic Frontier Foundation.

Encrypt and sign your emails and documents using the *de facto* standard OpenPGP either from Tails email client, text editor or file browser.

Protect your instant messaging conversations using OTR, a cryptographic tool that provides encryption, authentication and deniability.

Securely delete your files and clean your diskspace using Nautilus Wipe.

INSTALLING AND BOOTING THE TAILS OS ON REMOVEABLE MEDIA

1. Install Tails OS **(https://tails.boum.org/)** to a USB drive or an SD card (micro SD preferably).
2. Do not use the ChromeOS.
3. Use **esc+refresh+Power** to enter dev mode
4. In recovery mode, press Ctrl+D. You'll get the message *To turn OS verification OFF, press ENTER. Your system will reboot and local data will be cleared* - hit Enter and wait. From now on you'll get a boot screen that says *OS verification is OFF* at every startup. Wait for it - after a few minutes your Chromebook will boot into developer mode.
5. Select debug mode (essential)
6. Enable usb booting: **don’t login** !; Switch to the dev console by pressing **ctrl+alt+f2**; Type **chronos**, enter the shell; Type **sudo bash** to enter root login; enter default

passwd (test0000); Then type **crossystem dev_boot_usb=1 dev_boot_legacy=1**. Then type **exit** twice to leave root and dev shell

7. Insert Tails OS USB or SD
8. Reboot
9. On boot, enter **ctrl+L** at the Chrome OS splash screen
10. Tails OS boots
11. Follow instructions
12. The end.

OBFUSCATING YOUR IP ADDRESS WITH TOR

An IP address is a set of numbers that identifies a computer, or a network of computers, on the internet. Unless you take extra steps, every website you visit can see your IP address. If you're using social media while connected to your home or office Wi-Fi network, or your phone's data plan, social media sites can tell. If they hand these IP addresses to the FBI, you will very quickly lose your anonymity.

This is where Tor comes in. Tor is a decentralised network of servers that helps people bypass internet censorship, evade internet surveillance, and access websites anonymously. If you connect to social media sites while you're using Tor Browser, they can't tell what your real IP address is — instead, they'll see the IP address of a random Tor server. Tor servers

are run by volunteers. And even if any of the servers bouncing your data around are malicious, they won't be able to learn both who you are and what you're doing.

This is the primary benefit that Tor has over Virtual Private Network, or VPN, services, which try to help users hide their IP addresses. The FBI *can* go to a VPN service to learn your real IP address (assuming the VPN keeps a record of its users' IP addresses and cooperates with these requests). This isn't true with Tor.

To get started with Tor, use the Tails OS (which has Tor built-in) or download the Tor Browser. It's a web browser, like Chrome or Firefox, but all its internet traffic gets routed over the Tor network, hiding your real IP address.

Using Tor Browser is the easiest way to get started, but it's not perfect. For instance, a hacker who knows about a vulnerability in Tor Browser can discover your real IP address by tricking you into visiting a website they control and exploiting that vulnerability — the FBI has done this in the past. For this reason, it's important to *always* immediately update Tor Browser when you get prompted.

You can also protect yourself from Tor Browser security bugs by using an operating system that's designed to protect your

anonymity, such as Tails or Qubes with Whonix. This is more work for the average user, but if you are reading this, you are not the average user. We recommend the stateless OS, Tails.

SECURING AN ANONYMOUS EMAIL ADDRESS

Before you can create nearly any account online, you need an email address. While popular email services like Gmail or Yahoo Mail let anyone make an account for free, they don't make it easy to do so anonymously. Most of them require that you verify your identity with a phone number. You can in fact do that anonymously (more on that below), but it is preferable to use an email provider that is open to give addresses to anonymous users.

One of these providers used to be SIGAINT, a darknet-only service that forced all its users to log in using Tor to read or send email. The people who ran it were anonymous and it contained ads for (sometimes very sketchy) darknet websites. Unfortunately, for reasons unknown (or known), the SIGAINT service went down recently, and there is no indication of it returning soon. Since it is down, you can try Riseup (see below) or set up a burner phone and then try ProtonMail, Gmail, or some other email service instead.

Riseup, is a technology collective that provides email,

mailing list, VPN, and other similar services to activists around the world. Accounts are free, and they don't ask for any identifying information, but you do need an invite code from a friend who already uses Riseup in order to create an account.

Yet another option is ProtonMail — a privacy-friendly email provider based in Switzerland that asks for minimal identifying information and works well over Tor. However, to prevent abuse, they require Tor users to provide a phone number (that they promise not to store) to receive an SMS during account creation. So, if you'd like to use ProtonMail instead (or any other email service that requires a phone number when creating an account over Tor), follow the steps below to create an anonymous phone number first.

SECURING AN ANONYMOUS PHONE AND PHONE NUMBER

When attempting to create accounts online, many ask for a valid phone number for account activation. Even if you provide your (anonymous) email address, most sites won't let you create a new account without first verifying your phone number.

This is a problem, because you obviously can't use your real phone number if you want to remain anonymous. So to proceed, you need to figure out how to get a phone number that isn't

tied to your actual identity. This is a common problem when trying to stay anonymous online, so you can follow these instructions any time you need a phone number when opening an account.

There are other ways to do it, but this is a conceptually simple option: Buy a burner phone anonymously, use it to verify your new account, and then get rid of it.

Use cash, and simply buy the cheapest TracFone handset you can find (an LG 328BG "feature phone" — as in, not a smartphone) as well as 60 minutes worth of voice service - this will cost around $60.00. You might be able to find cheaper cellphone handsets if you research this further.

If you're going to get a burner phone and want to maintain your anonymity, here are some things to keep in mind:

- Buy your burner phone hardware and pre-paid service using cash. Don't use a credit card.
- When you buy service, the clerk activates your service card at the cash register. This tells the phone company (TracFone, in this case) exactly which store you bought it from, and when. Keep this in mind and consider picking a store far away from where you live — like while you're traveling in another city.
- Security cameras will probably record your face at the

store. Most stores delete old footage on a regular basis, overwriting it with new footage. If possible, wait two weeks before you start setting up and configuring accounts so that the footage is already deleted by the time anyone tries to figure out your real identity.

You can find phones and service like this at some convenience stores and pharmacies. If you need to do internet research to find a store near you that sells burner phones, use Tor Browser.

As soon as you power on your burner phone, it will connect to cell phone towers, and the phone company will know your location. So, don't activate your phone, or keep it powered on at all, at your home or office — instead, go to a public place, like a coffee shop, before activating your new phone. Keep it powered off while you're not using it.

Don't use the burner's phone number for anything at all that isn't related to this specific project. This is called compartmentalisation; if someone discovers the entire history of that phone number, they shouldn't be able to learn anything new.

Each cellphone handset has a unique identifier. So if you need a second phone number at some point in the future and you don't want it to be connected to your first phone number, you'll have to buy a second handset.

After buying phone service, you'll need to activate the phone.

This process will be different with different phone companies. TracFone requires you to activate your handset either by calling their phone number from a different phone — obviously not a good option for someone trying to remain anonymous — or by activating online at their website. **Activate your burner phone online using Tor Browser.**

Once you've activated your phone, you can use the phone's menu system to learn what your new phone number is. On the LG 328BG, press Menu, select Settings, and finally Phone Information to find it.

CREATION OF AN ANONYMOUS TWITTER ACCOUNT

Finally, armed with an email address and phone number that aren't in any way connected to your real identity, you can create a Twitter account for the dissemination of timely information.

Before making an account, grab your laptop and burner phone and go to a public location that isn't your home or office, such as a coffee shop. **Do not** power on your burner phone until you arrive. Keep in mind that this location is now tied to your burner phone, so you might really want to do this step when you're traveling in another city.

Using the Tor Browser, navigate to https://twitter.com/signup

and sign up for a new account. The new account form asks for your full name (make something up), your email address (use the anonymous one you recently created), and a password.

After clicking “Sign up,” will be prompted to enter your phone number. Type your anonymous phone number and click “Call me.” A Twitter robot will call your burner phone and read out a six-digit number, which youwill then type into the next page on Tor Browser.

With the phone number verification step complete, power off your burner phone. Once you’re sure you don’t need your burner phone anymore, get rid of it (destroy it in such a way nothing can be recovered from it).

Toward the end of the signup process, Twitter will prompt you to come up with a username. Make something up that doesn't connect it to you. After clicking through the welcome screen, login to your new anonymous account.

You will have to confirm that you are the owner via email of your anonymous email address.

You are now ready to tweet anonymously.

MAINTAINING AN ANONYMOUS TWITTER ACCOUNT

Maintaining this anonymous Twitter account for months, or years, without making ***any mistakes*** that compromise your identity is not easy. Here are some tips to achieve this:

Be careful about how you interact with people:

You should operate on a strict need-to-know basis. Don't tell ***anyone*** who doesn't need to know that you're involved with running this account. Don't brag. This is, by far, the easiest way to screw up, and for your real identity to come out: gossip.

Be careful about what privileged information you tweet. If you're part of a small group of people who have access to some information and you tweet about it, you might become a suspect when before you weren't.

If your account becomes popular, you might begin having conversations with lots of strangers on the internet. Be very careful what you say, even if you're saying it in a private message. Some of these strangers might be gaining your trust in hopes that you'll slip and tell them bits of information about your identity.

Be very careful about clicking links that people send you — they could be trying to learn your IP address, or even trying to hack your Tor Browser. Avoid clicking them at all, but if you really need to click one, first make sure

you're running the very latest version of Tor Browser and set your security slider to High.

Be conscious of your word choice. People might analyse your writing style to de-anonymise you, so you should try to write in a voice that's distinct from your own.

Compartmentalise:

Never log in from your work computer — most companies spy on their employees' computers. Use a personal computer instead. Also, avoid your work network — most companies log exactly which computers connect to their network and what they do online. Tor hides what you're doing, but the company can still tell that you're using Tor on their network.

Always use Tor Browser when using your account. Don't log in on your phone. Don't log in with any other browser. Don't even look at your anonymous Twitter account while logged in to your personal account.

When you are logged in to your anonymous account, don't follow your personal account, or the accounts of any of your friends. Don't re-tweet or like any of those tweets either. **Do not** make it obvious who your social group is.

Be careful about uploading photos for tweets or your profile. Photos often contain metadata that could be used to lead back to you. Screenshots don't though, so one easy way to remove metadata from a photo is to take a

screenshot of it.

Many successful Twitter accounts have a team of people who run them instead of a single individual. If you're part of such a team, or thinking of sharing access to your existing account with someone new:

- Only invite people who you know and trust.
- Come up with a set of operational security rules — like the rules listed above — and make sure that everyone involved understands them and is compliant.
- Come up with a secure communication channel as a team, and only discuss the Twitter account using this channel, or in person. There are many different technologies you could use, all with different trade-offs, but one option is to use the encrypted messaging app Signal: Create a Signal group (with an innocuous name) and set your messages to automatically disappear after a short time - five minutes.
- Instead of just tweeting when you come up with ideas, edit each other's tweets. This will both improve the quality of the tweets and could help defeat style analysis, since you'll end up with a shared voice.

And finally, keep in mind that after all this, Twitter can always kick you off for their own reasons. And if your account gets hacked and the email address associated with it is changed, you'll have no way to recover it.

YOUR OS DOES NOT PROTECT AGAINST COMPROMISED HARDWARE

If the computer has been compromised by someone having physical access to it and who installed untrusted pieces of hardware (like a keylogger), then it might be unsafe to use Tails. If you think that the computer that you are using is not trustworthy, for example when using a public computer in a library, everything that you type might be recorded by a hardware keylogger. If you want to maintain security in such an untrusted environment, it is highly suggested you use the built-in **Florence** virtual keyboard to protect you against a hardware keylogger when typing passwords and sensitive text. To display the virtual keyboard, click on the keyboard icon in the notification area.

NOTE: There is currently no virtual keyboard in Tails Greeter, so a hardware keylogger could record your persistent volume passphrase or administration password.

YOUR OS CAN BE COMPROMISED IF INSTALLED OR PLUGGED IN UNTRUSTED SYSTEMS

When starting your computer on Tails, it cannot be compromised by a virus in your usual operating system, but:

Tails should be installed from a trusted system. Otherwise

it might be corrupted during installation.

Plugging your Tails device in a compromised operating system might corrupt your Tails installation, and destroy the protection that Tails provides. Only use your Tails device to start Tails.

See the corresponding FAQ.

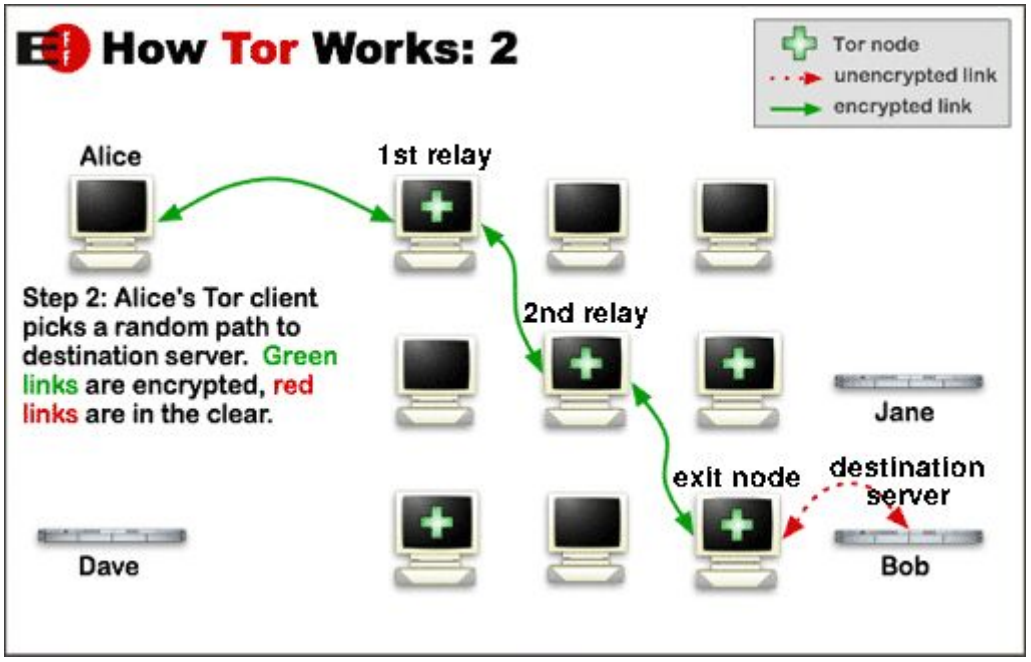
YOUR OS DOES NOT PROTECT AGAINST BIOS OR FIRMWARE ATTACKS

It is also impossible for Tails to protect against attacks made through the BIOS or other firmware embedded in the computer. These are not managed or provided by the operating system directly, and no operating system can protect against such attacks.

See for example, this attack on BIOS by LegbaCore.

TOR IS ABOUT HIDING YOUR LOCATION, NOT ABOUT ENCRYPTING YOUR COMMUNICATION.

Instead of taking a direct route from source to destination, communications using the Tor network take a random pathway through several Tor relays that cover your tracks. So no observer at any single point can tell where the data came from or where it's going.



The last relay on this circuit, called the exit node, is the one that establishes the actual connection to the destination server. As Tor does not, and by design cannot, encrypt the traffic between an exit node and the destination server, **any exit node is in a position to capture any traffic passing through it**. See Tor FAQ: Can exit nodes eavesdrop on communications?.

For example, in 2007, a security researcher intercepted thousands of private email messages sent by foreign embassies and human rights groups around the world by spying on the connections coming out of an exit node he was running. See Wired: Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise.

TO PROTECT YOURSELF FROM SUCH ATTACKS YOU SHOULD USE END-TO-END ENCRYPTION.

Tails includes many tools to help you using strong encryption while browsing, sending email or chatting, as presented on their about page.

YOUR OS MAKES IT CLEAR THAT YOU ARE USING TOR AND PROBABLY TAILS

Your Internet Service Provider (ISP) or your local network administrator can see that you're connecting to a Tor relay, and not a normal web server for example. Using Tor bridges in certain conditions can help you hide the fact that you are using Tor.

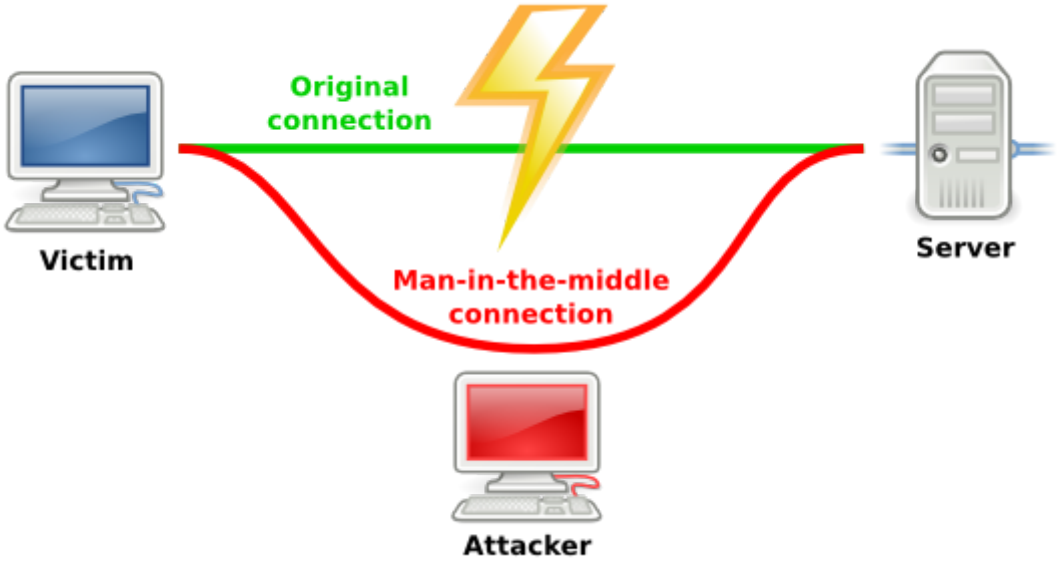
The destination server that you are contacting through Tor can know whether your communication comes from a Tor exit node by consulting the publicly available list of exit nodes that might contact it. For example using the Tor Bulk Exit List tool from the Tor Project.

So using Tails doesn't make you look like any random Internet user. The anonymity provided by Tor and Tails works by trying to make all of their users look the same so it's not possible to identify who is who amongst them.

See also Can I hide the fact that I am using Tails?

MAN-IN-THE-MIDDLE ATTACKS

A man-in-the-middle attack (MitM) is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.



While using Tor, man-in-the-middle attacks can still happen between the exit node and the destination server. The exit node itself can also act as a man-in-the-middle. For an example of such an attack see MW-Blog: TOR exit-node doing MITM attacks.

Again, to protect yourself from such attacks you should use end-to-end encryption and while doing so taking extra care at verifying the server authenticity.

Usually, this is automatically done throught SSL certificates checked by your browser against a given set of recognised certificate authorities). If you get a security exception message, you might be the victim of a man-in-the-middle attack and should not bypass the warning unless you have another trusted way of checking the certificate's fingerprint with the people running the service.

But, on top of that, the certificate authorities model of trust on the Internet is susceptible to various methods of compromise.

For example, on March 15, 2011, Comodo, one of the major SSL certificates authorities, reported that a user account with an affiliate registration authority had been compromised. It was then used to create a new user account that issued nine certificate signing requests for seven domains: mail.google.com, login.live.com, www.google.com, login.yahoo.com (three certificates), login.skype.com, addons.mozilla.org, and global trustee. See Comodo: The Recent RA Compromise.

Later in 2011, DigiNotar, a Dutch SSL certificate company, incorrectly issued certificates to a malicious party or parties. Later on, it came to light that they were apparently compromised months before, perhaps as far back as May of 2009, or even earlier. Rogue certificates were issued for domains such as google.com, mozilla.org, torproject.org, login.yahoo.com and many more. See The Tor Project: The DigiNotar Debacle, and what you should do about it.

This still leaves open the possibility of a man-in-the-middle attack even when your browser is trusting an HTTPS connection.

On one hand, by providing anonymity, Tor makes it more difficult to perform a man-in-the-middle attack targeted at **one specific person** with the blessing of a rogue SSL certificate. But on the other hand, Tor makes it easier for people or organisations running exit nodes to perform large scale MitM attempts, or attacks targeted at **a specific server**, and especially those among its users who happen to use Tor.

Quoted from Wikipedia: Man-in-the-middle attack, Wikipedia: Comodo Group#Certificate hacking and Tor Project: Detecting Certificate Authority compromises and web browser collusion.

CONFIRMATION ATTACKS

The Tor design doesn't try to protect against an attacker who

can see or measure both traffic going into the Tor network and also traffic coming out of the Tor network. That's because if you can see both flows, some simple statistics let you decide whether they match up.

That could also be the case if your ISP (or your local network administrator) and the ISP of the destination server (or the destination server itself) cooperate to attack you.

Tor tries to protect against traffic analysis, where an attacker tries to learn whom to investigate, but Tor can't protect against traffic confirmation (also known as end-to-end correlation), where an attacker tries to confirm a hypothesis by monitoring the right locations in the network and then doing the math.

Quoted from Tor Project: "One cell is enough to break Tor's anonymity".

YOUR OS DOESN'T ENCRYPT YOUR DOCUMENTS BY DEFAULT

The documents that you save on external storage devices will not be encrypted by default, except in the encrypted persistent volume. But Tails provides you with tools to encrypt your documents, such as GnuPG, or encrypt your storage devices, such as LUKS.

It is also likely that the files you may create will contain evidence that they were created using Tails.

If you need to access the local hard-disks of the computer you are using, be conscious that you might then leave trace of your activities with Tails on it.

YOUR OS DOESN'T CLEAR THE METADATA OF YOUR DOCUMENTS FOR YOU

Numerous files formats store hidden data or metadata inside of the files. Word processing or PDF files could store the name of the author, the date and time of creation of the file, and sometimes even parts of the editing history of the file, depending on the file format and the software used.

Image file formats, like TIFF of JPEG, probably take the prise for most hidden data. These files, created by digital cameras or mobile phones, contain a metadata format called EXIF which can include the date, time and sometimes the GPS coordinates when the picture was taken, the brand and serial number of the device which took it, as well as a thumbnail of the original image. Image processing software tends to keep this metadata intact. The internet is full of cropped or blurred images in which the included EXIF thumbnail still shows the original picture.

Tails doesn't clear the metadata of your files for you. Yet. Still it's in Tails' design goal to help you do that. For example, Tails already comes with the Metadata anonymisation toolkit (MAT).

YOUR OS DOESN'T ENCRYPT THE "SUBJECT:" AND OTHER HEADERS OF YOUR ENCRYPTED EMAIL MESSAGES

Please note also, that the "Subject:" as well as the rest of the header lines of your OpenPGP encrypted email messages are not encrypted. This is not a bug of Tails or the OpenPGP protocol; it's due to backwards compatibility with the original SMTP protocol. Unfortunately no RFC standard exists yet for "Subject:" line encryption.

TOR DOESN'T PROTECT YOU FROM A GLOBAL ADVERSARY

A global passive adversary would be a person or an entity able to monitor at the same time the traffic between all the computers in a network. By studying, for example, the timing and volume patterns of the different communications across the network, it would be statistically possible to identify Tor circuits and thus match Tor users and destination servers.

It is part of Tor's initial trade-off not to address such a threat in order to create a low-latency communication service usable for web browsing, Internet chat, or SSH connections.

For more information see the Tor design paper, "Tor Project: The Second-Generation Onion Router", specifically, "Part 3. Design goals and assumptions."

TAILS DOESN'T MAGICALLY SEPARATE YOUR DIFFERENT CONTEXTUAL IDENTITIES

It is usually not advisable to use the same Tails session to perform two tasks or endorse two contextual identities that you really want to keep separate from one another. For example hiding your location to check your email and anonymously publishing a document.

Firstly, because Tor tends to reuse the same circuits, for example, within the same browsing session. Since the exit node of a circuit knows both the destination server (and possibly the content of the communication if it's not encrypted) and the address of the previous relay it received the communication from, it makes it easier to correlate several browsing requests as part of a same circuit and possibly made by the same user. If you are facing a global adversary as described above, it might then also be in a position to do this correlation.

Secondly, in case of a security hole or an error in using Tails or one of its applications, information about your

session could be leaked. That could reveal that the same person was behind the various actions made during the session.

The solution to both threats is to shutdown and restart Tails every time you're using a new identity, if you really want to isolate them better.

As explained in the documentation about Tor Browser, its **New identity** feature is not a perfect solution to separate different contextual identities. And, as explained in the FAQ, Tails does not provide a global New Identity feature. **SHUTDOWN AND RESTART TAILS.**

Or, the solution provided in this document is to use your Google identity which is the default boot option. This will be your public identity. You will simply boot into your ChromeOS, login with your Google credentials, and you are golden. Never mix identities - it is always one or the other, or simply, just the other.

THE PROBLEM WITH MULTI-FACTOR AUTHENTICATION

As previously stated, multifactor authentication is essential for enterprise and individual security. But how does multi-factor auth work with the anonymity model we are trying to achieve? If we are to work with two-factor auth in the usual way - having a code sent to our phone - be it our

standard phone or even the throw-away, we become completely vulnerable to tracking once again. But, there is a way - albeit somewhat complicated - to get around this and still have confidence in our security and anonymity.

One would need to set up a tor server specifically designed to sync with an external device such as a fob that generates a six or more digit pseudo-random number for multi-factor auth. This regenerates a new number every 30 or less seconds. All of this would have to be kept in total secrecy, and distribution of the key-generating fobs that sync with this server must be done in total secrecy. That secret distribution can be achieved in many ways, and it is paramount to maintaining anonymity. In the instance of the infeasibility to achieve this secret distribution channel, the use of extremely strong passwords in single-factor auth is a more acceptable alternative - which will be detailed in the next section of this document.

Note: If you are simply using Tails OS to obfuscate your traffic so that your ISP cannot collect data from you, using an authenticator like Google's will not reveal any specific identity or location information about you, as nothing is actually sent to your phone - the auth app functions just like an auth fob.

IS THERE NO USER-FRIENDLY SCREENLOCK AS OF YET IN TAILS OS?

While the implementation of a user-friendly screen-lock supposedly has yet to be perfectly implemented in Tails OS, it's on the list. There are ways to install such a beast, but currently it remains complicated and un-user-friendly, and it isn't necessary.

The reality is that it does work in Tails. The shortcut is actually **Super+L** (Super is the GNOME name for the magnifying glass key on the Chromebook). Unfortunately, it does not actually lock the screen by default. It just goes into a full screen window that can just be scrolled out of the way. In order for it to be password protected, you need to set an administration password in the Tails OS Greeter. Screen-lock then works perfectly.

TAILS DOESN'T MAKE YOUR LOUSY PASSWORDS STRONGER

Tor allows you to be anonymous online; Tails allows you to leave no trace on the computer you're using. But again, **neither or both are magic spells for computer security**.

If you use weak passwords, they can be guessed by brute-force attacks with or without Tails in the same way. To know if your passwords are weak and learn good practices to create better password, you can read Wikipedia: Weak Passwords.
From the wiki,

Password policies should suggest these memory techniques to assist remembering passwords:

mnemonic passwords: Users should develop mnemonic phrases and use them to generate high-entropy (more or less random) passwords which are nevertheless relatively easy for the user to remember. For instance, the first letter of each word in a memorable phrase. Silly ones are possibly more memorable. Another way to make random-appearing passwords more memorable is to use random words (see diceware) or syllables instead of randomly chosen letters.

after-the-fact mnemonics: After the password has been established, invent a mnemonic that fits. It does not have to be reasonable or sensible, only memorable. This allows passwords to be random.

visual representations of passwords: a password is memorised based on a sequence of keys pressed, not the values of the keys themselves, e.g. a sequence !qAsdE#2 represents a rhomboid on a US keyboard. The method to produce such passwords is called PsychoPass, however such spatially patterned passwords are relatively weak and should be avoided.

password patterns: Any pattern in a password makes guessing (automated or not) easier and

reduces an attacker's work factor.

For example, passwords of the following case-insensitive form: consonant, vowel, consonant, consonant, vowel, consonant, number, number (for example *pinray45*) are called Environ passwords. The pattern of alternating vowel and consonant characters was intended to make passwords more likely to be pronounceable and thus more memorable. Unfortunately, such patterns severely reduce the password's information entropy, making brute force password attacks considerably more efficient. In the UK in October 2005, employees of the British government were advised to use passwords in this form.

TOR EXIT NODES CAN EAVESDROP ON COMMUNICATIONS

When looking at how Tor works, we've looked at the various types of nodes that make up the Tor network. However, we haven't detailed the *exit nodes*. Exit nodes are the final link in a Tor "circuit", or path from the client to the server. Since exit nodes send data to the final destination, they can see the data as if it had just left the device.

This visibility puts quite a bit of trust in exit nodes and, for the most part, they tend to act responsibly. However, this

isn’t always the case.

TRAFFIC SNIFFING

Tor exit nodes can be the definition of a man-in-the-middle (MitM). This means that **any** unencrypted protocols (e.g. FTP, HTTP, SMTP, etc.) can be seen by the exit node operator. This includes things like usernames, passwords, session cookies, or even file uploads/downloads.

> **To be clear:** Tor exit nodes can see traffic as if it were just leaving your device.

The unfortunate part about this is that there is nothing (aside from using encrypted protocols… more on this later) we can do about this. Sniffing is a completely passive operation, so the only protection is to be aware of the risks and avoid passing any sensitive data over Tor unencrypted.

Let’s take a look at just a few of the ways your traffic can be modified:

SSL MITM & SSLSTRIP

SSL rains on our parade if we’re trying to cause havoc for our users. Fortunately for those who would be attackers, many sites have issues that allow them to force the user through

unencrypted connections. Examples include redirects from HTTP to HTTPS, including HTTP content on an HTTPS site, and more.

An example of a tool to take advantage of this is called sslstrip. All we have to do is proxy the traffic leaving our exit node through sslstrip and it's game over in many scenarios.

Of course, if we want to be less sneaky, we can just straight up terminate the SSL connections with a self-signed cert. Then we have insight into all the SSL traffic crossing our exit node.

HOOKING BROWSERS WITH BEEF

Now that we have insight into more traffic than before, we can start doing some damage. One example of this would be to use the BeEF framework to automatically "hook" browsers so they are under our control. Then, we can leverage Metasploit's "browser autopwn" function to compromise the end host and drop a reverse shell. Game over (This can't happen through Tails).

BACKDOOR BINARIES

Let's say that we see binaries being downloaded through our exit nodes. These can be full software downloads, or even updates to existing software that's happening in the

background that the user isn't even aware of.

All we have to do to transparently backdoor binaries would be to proxy the Tor traffic through something like The Backdoor Factory. Then, as the software is executed, the end host is compromised. Game over (This also can't happen through Tails).

EXIT MAPS

While most Tor exit nodes (from what we can tell) play nice, it's not terribly uncommon to find some that don't. Remember all those theoretical attacks we just talked about? They actually happened.

Fortunately, the Tor Project thought of this and designed a safeguard to prevent bad exits from being used by clients. This comes in the form of a flag in the consensus. Not surprisingly, the flag is called BadExit.

To address the problem of hunting down bad exit nodes, a slick system called exitmap was created.

Exitmap works like this:

    For each exit node:

        Run Python module (file upload/download, login, etc.)

        Record the results

Exitmap leverages the awesome Stem library to do most of the heavy lifting for building circuits to each exit node. Pretty basic, but effective.

Back in 2013, exitmap was created as part of the Spoiled Onions project. The authors of the paper found 65 exit nodes that were tampering with traffic. This shows that, while the problem isn't rampant "(there were about 1000 exit nodes when they wrote the paper), it's bad enough to warrant a sheriff to make sure exits are playing nice, which is why exitmap is still up, running, and actively maintained."

In another example, a researcher basically set up a fake login page and logged in through every exit node (similar to exitmap). Then, the HTTP logs were watched for any further login attempts. Multiple nodes tried to break in to the site using the same credentials the author used.

ENFORCE ENCRYPTION

It's important to note that this isn't just Tor's problem. There are a substantial number of hops along any given path, including the normal path between you, your ISP, and the funny cat picture you're trying to look at. All it takes is one operator with malicious intent to cause serious harm.

The best thing you can do is to enforce encryption wherever possible. If the traffic can't be seen, it can't (feasibly) be modified. (HTTPS Everywhere)

Finally, keep in mind this is just an example of what happens when Tor operators act irresponsibly. This is **not** the norm. In fact, a vast majority of exit node operators take their role very seriously and deserve a major "thank you" for all the risk they assume to keep information flowing freely.

THE INTERNET OF THINGS - DON'T

Here's a link to a list of IoT devices. **DO NOT USE ANY** IoT devices, period. You will be tracked.

http://iotlist.co/

TAILS AND THIS DOCUMENT ARE A WORK IN PROGRESS

Tails, as well as all the software it includes, are continuously being developed and may contain programming errors or security holes. As well, this is a living document and will be updated on a regular basis as needed.

CONCLUSION

As of the latest update, this information can be dependably relied upon to offer you the best security, anonymity, and privacy to date. It is tested and true. Good luck.