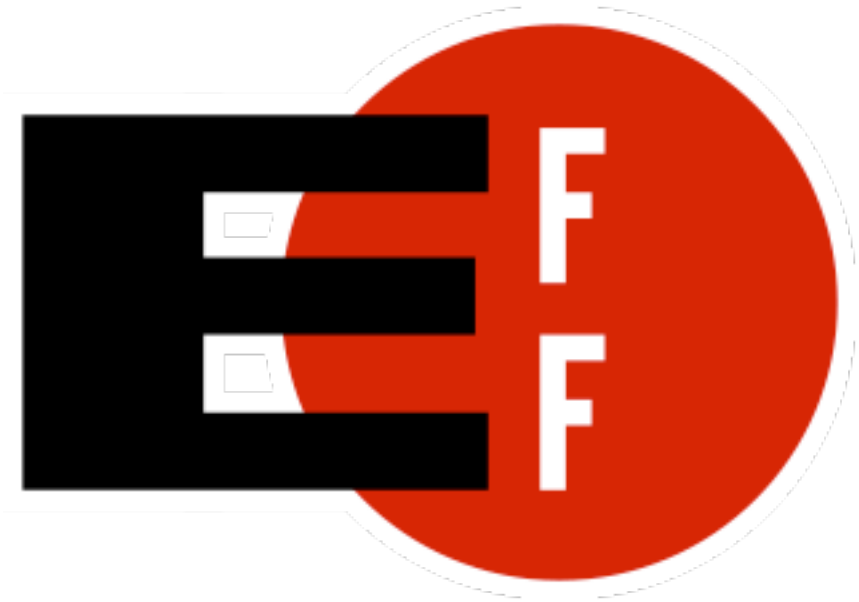
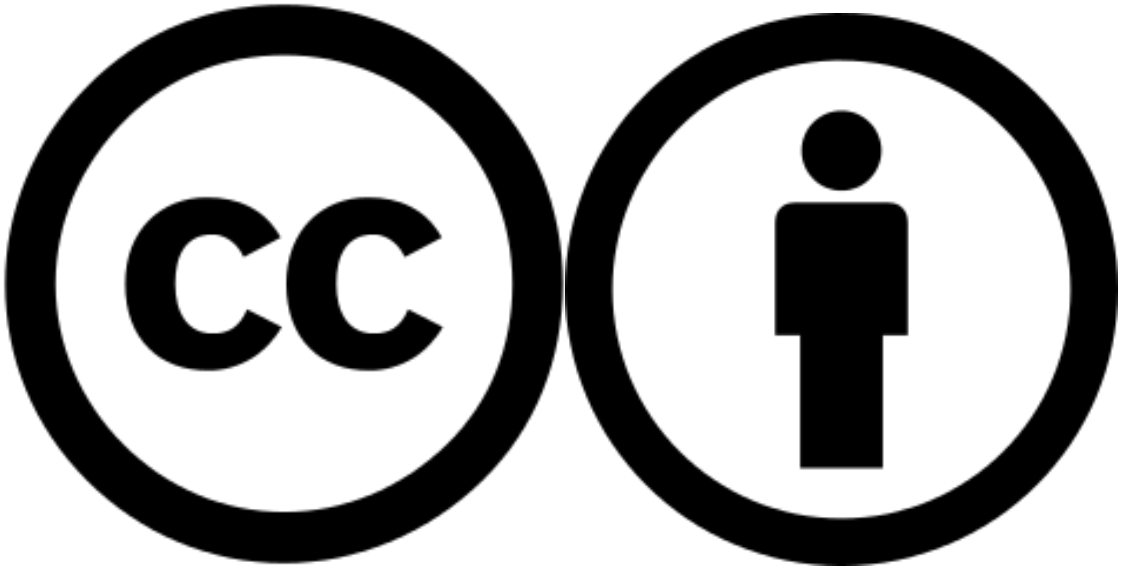
Tips, Tools, and How-To's for Safer Online Communications

Mac OSX Edition





Editor's Foreword

This edition of the Electronic Frontier Foundation's Surveillance Self-Defense Project has been arranged into a downloadable PDF version for ease of use as a printable copy to benefit Macintosh users. Many people have expressed interest into both the *why* and *how* of secured record archival, and so I think EFF's SSD helps to facilitate the remedial education that was not provided in any government school curriculum.

The intention here was to assemble the SSD into a format that could be useful to someone who doesn't yet have access to the Internet, or who would otherwise appreciate an archived version of the SSD. Screenshots from a few of the tutorials have been omitted for the sake of brevity. Minor grammatical and punctuation errors have been corrected.

It is my sincere desire that the SSD serves to increase the quality of your security culture, as it has done for mine. Please do keep in mind, though, that security culture is not just limited to cellular telephones, laptop computers, and the Internet, but also includes your home, your automobile, and your persona. I do hope the SSD helps you protect your documents through secured record archival.

Kyle Rearden
Austin, Texas
June, 2015

Table of Contents

About Surveillance Self-Defense

Who is this guide for?

Surveillance Self-Defense (SSD) is a guide to protecting yourself from electronic surveillance for people all over the world. Some aspects of this guide will be useful to people with very little technical knowledge, while others are aimed at an audience with considerable technical expertise and privacy/security trainers. We believe that everyone's threat model is unique—from activists in China to journalists in Europe to the LGBTQ community in Uganda. We believe that everyone has something to protect, whether it's from the government or parents or prying employers, stalkers, data-mining corporations, or an abusive partner.

What is this guide meant to do?

There are many privacy and security guides on the Internet that teach users to use a specific set of tools, such as password safes or VPNs or the Tor Browser Bundle. SSD includes step-by-step tutorials for installing and using a variety of privacy and security tools, but also aims to teach people how to think about online privacy and security in a sophisticated way that empowers them to choose appropriate tools and practices even as the tools and adversaries change around them. Please note that the law and technology can change quickly, and portions of SSD may become out of date.

This guide acknowledges that some especially powerful and sophisticated threats may be difficult or impossible to protect oneself against. We hope that this guide teaches users to be skeptical of sweeping claims that any particular tool offers complete security or privacy. Strong privacy and security practices are still worthwhile even if they are not guaranteed to be effective 100% of the time against every adversary. These practices increase the cost and effort of surveillance—and they may increase it to the point where an adversary feels that surveilling you is no longer worthwhile.

What are the limitations of this guide?

This guide does not address operational security or "OPSEC" in the broader sense. OPSEC is the process of protecting information about one's activities that may be important to a potential adversary. This is a process that frequently goes beyond the digital realm.

For example, people trying to have confidential meetings may have to worry about whether someone physically followed them, or whether they were observed by CCTV cameras, or whether their neighbors might have become aware of the meeting, or whether their meeting places have been bugged. Perhaps they should wonder if they are creating a suspicious pattern of activity. They may also have physical security concerns; could they

tell if someone broke into their home or tampered with their laptop? Are their confidential documents safe?

These are important and valid concerns for people with certain kinds of security needs, but they fall outside the scope of this guide.

Please use SSD as a starting point for your own research, and check for more recent facts, cases and authorities. Please note that, even if a statement made about the law is accurate, it may only be accurate in one jurisdiction (place); as well, the law may have changed, been modified or overturned by subsequent development since the entry was made. The materials in SSD are for informational purposes only and not for the purpose of providing legal advice. You should contact a lawyer licensed to practice in your jurisdiction to obtain advice with respect to any particular issue or problem.

An Introduction to Threat Modeling

There is no single solution for keeping yourself safe online. Digital security isn't about which tools you use; rather, it's about understanding the threats you face and how you can counter those threats. To become more secure, you must determine what you need to protect, and whom you need to protect it from. Threats can change depending on where you're located, what you're doing, and whom you're working with. Therefore, in order to determine what solutions will be best for you, you should conduct a threat modeling assessment.

When Conducting an Assessment, There are Five Main Questions you Should Ask Yourself:

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to try to prevent those?

When we talk about the first question, we often refer to assets, or the things that you are trying to protect. An asset is something you value and want to protect. When we are talking about digital security, the assets in question are usually information. For example, your emails, contact lists, instant messages, and files are all assets. Your devices are also assets.

Write down a list of data that you keep, where it's kept, who has access to it, and what stops others from accessing it.

In order to answer the second question, "*Who do you want to protect it from*," it's important to understand who might want to target you or your information, or who is your adversary. An adversary is any person or entity that poses a threat against an asset or assets. Examples of potential adversaries are your boss, your government, or a hacker on a public network.

Make a list of who might want to get ahold of your data or communications. It might be an individual, a government agency, or a corporation.

A threat is something bad that can happen to an asset. There are numerous ways that an adversary can threaten your data. For example, an adversary can read your private communications as they pass through the network, or they can delete or corrupt your data. An adversary could also disable your access to your own data.

The motives of adversaries differ widely, as do their attacks. A government trying to prevent the spread of a video showing police violence may be content to simply delete or reduce the availability of that video, whereas a political opponent may wish to gain access to secret content and publish it without you knowing.

Write down what your adversary might want to do with your private data.

The capability of your attacker is also an important thing to think about. For example, your mobile phone provider has access to all of your phone records and therefore has the capability to use that data against you. A hacker on an open Wi-Fi network can access your unencrypted communications. Your government might have stronger capabilities.

A final thing to consider is risk. Risk is the likelihood that a particular threat against a particular asset will actually occur, and goes hand-in-hand with capability. While your mobile phone provider has the capability to access all of your data, the risk of them posting your private data online to harm your reputation is low.

It is important to distinguish between threats and risks. While a threat is a bad thing that can happen, risk is the likelihood that the threat will occur. For instance, there is a threat that your building might collapse, but the risk of this happening is far greater in San Francisco (where earthquakes are common) than in Stockholm (where they are not).

Conducting a risk analysis is both a personal and a subjective process; not everyone has the same priorities or views threats in the same way. Many people find certain threats unacceptable no matter what the risk, because the mere presence of the threat at any likelihood is not worth the cost. In other cases, people disregard high risks because they don't view the threat as a problem.

In a military context, for example, it might be preferable for an asset to be destroyed than for it to fall into enemy hands. Conversely, in many civilian contexts, it's more important for an asset such as email service to be available than confidential.

Now, Let's Practice Threat Modeling

If you want to keep your house and possessions safe, here are a few questions you might ask:

- Should I lock my door?
- What kind of lock or locks should I invest in?
- Do I need a more advanced security system?
- What are the assets in this scenario?
    - The privacy of my home
    - The items inside my home
- What is the threat?
    - Someone could break in.

- What is the actual risk of someone breaking in? Is it likely?

Once you have asked yourself these questions, you are in a position to assess what measures to take. If your possessions are valuable, but the risk of a break-in is low, then you probably won't want to invest too much money in a lock. On the other hand, if the risk is high, you'll want to get the best locks on the market, and perhaps even add a security system.

7 Steps To Digital Security

Here are some basic tips to consider when thinking about your own digital security.

Knowledge is Power

Good security decisions can't be made without good information. Your security tradeoffs are only as good as the information you have about the value of your assets, the severity of the threats from different adversaries to those assets, and the risk of those attacks actually happening. This guide should help you gain the knowledge you need to identify the threats to your computer and communications security, and judge the risk against possible security measures. And some of this knowledge you already have: knowledge of your own situation, who might want to target you, and what resources they have. You already have more power than you think!

The Weakest Link

Think about assets as components of the system in which they are used. The security of the asset depends on the strength of all the components in the system. The old adage that "a chain is only as strong as its weakest link" applies to security too: The system as a whole is only as strong as the weakest component. For example, the best door lock is of no use if you have cheap window latches. Encrypting your email so it won't get intercepted in transit won't protect the confidentiality of that email if you store an unencrypted copy on your laptop and your laptop is stolen. That doesn't mean you have to do everything simultaneously, but it does mean that you should spend time thinking about every part of your information and computer use.

Simpler is Safer and Easier

It is generally most cost-effective and most important to protect the weakest component of the system in which an asset is used. Since the weak components are much easier to identify and understand in simple systems, you should strive to reduce the number and complexity of components in your information systems. A small number of components will also serve to reduce the number of interactions between components, which is another source of complexity, cost, and risk. That also means that the safest solution may be the least technical solution. Computers may be great for many things, but sometimes the security issues of a simple pen and notepaper can be easier to understand, and therefore easier to manage.

More Expensive Doesn't Mean More Secure

Don't assume that the most expensive security solution is the best; especially if it takes away resources needed elsewhere. Low-cost measures like shredding trash before leaving it on the curb can give you lots of bang for your security buck.

It's Okay To Trust *Someone* (But Always Know Who You're Trusting)

Computer security advice can end up sounding like you should trust absolutely no one but yourself. In the real world, you almost certainly trust plenty of people with at least *some* of your information, from your close family or companion to your doctor or lawyer. What's tricky in the digital space is understanding who you are trusting, and with what. You might deposit a list of passwords with your lawyers: but you should think about what power that might give them—or how easily they might be maliciously attacked. You might write documents in a cloud service like Dropbox or Microsoft OneDrive that are only for you: but you're also letting Dropbox and Microsoft access them, too. Online or offline, the fewer people you share a secret with, the better chance you have of keeping it secret.

There is No Perfect Security—There's Always a Trade-Off

Set security policies that are reasonable for your lifestyle, for the risks you face, and for the implementation steps you and your colleagues will take. A perfect security policy on paper won't work if it's too difficult to follow day-to-day.

What's Secure Today May Not Be Secure Tomorrow

It is also crucially important to continually re-evaluate your security practices. Just because they were secure last year or last week doesn't mean they're still secure! Keep checking sites like SSD, because we will update our advice to reflect changes in our understanding and the realities of digital security. Security is never a one-off act: it's a process.

Choosing Your Tools

All digital tools, whether they are hardware or software, should be secure. That is, they should protect you from surveillance, and stop your device from being controlled by others. Sadly, this is currently not the case. For many digital activities, you may end up needing dedicated programs or equipment intended to provide specific security features. Examples we use in this guide include software that allows you to encrypt your messages or files, like PGP.

But given the large number of companies and websites offering secure programs or hardware, how do you choose the one that's right for you?

Security is a Process, not a Purchase

The first thing to remember before changing the software you use or buying new tools is that no tool is going to give you absolute protection from surveillance in all circumstances. Using encryption software will generally make it harder for others to read your communications or rummage through your computer's files. But attacks on your digital security will always seek out the weakest element of your security practices. When you use a new secure tool, you should think about how using it might affect other ways someone could target you. For example, if you decide to use a secure texting program to talk to a contact because you know that your phone might be compromised, might the fact that you're using this program at all give an adversary a clue that you are talking about private information?

Secondly, remember your threat model. You don't need to buy some expensive encrypted phone system that claims to be “NSA-proof” if your biggest threat is physical surveillance from a private investigator with no access to internet surveillance tools. Alternatively, if you are facing a government that regularly jails dissidents *because* they use encryption tools, it may make sense to use simpler tricks—like a set of pre-arranged codes—rather than risk leaving evidence that you use encryption software on your laptop.

Given all that, here are some questions you can ask about a tool before downloading, purchasing, or using it.

How Transparent is it?

Even though digital security seems to be mostly about keeping secrets, there's a strong belief among security researchers that openness and transparency leads to more secure tools.

Much of the software used and recommended by the digital security community is free and open source, which is to say that the code that defines how it works is publicly available for others to examine, modify, and share. By being transparent about how their

program works, the creators of these tools invite others to look for security flaws, and help improve the program.

Open software provides the opportunity for better security but does not guarantee it. The open source advantage relies in part on a community of technologists actually checking the code, which for small projects (and even for popular, complex ones) may be hard to achieve. When you're considering using a tool, see if its source code is available, and whether the code has an independent security audit to confirm the quality of its security. At the very least, software or hardware should have a detailed technical explanation of how it functions, for other experts to inspect.

How Clear are its Creators About its Advantages and Disadvantages?

No software or hardware is entirely secure. Creators or sellers who are honest about the limitations of their product will give you a much stronger idea of whether their application is appropriate for you.

> *Don't trust blanket statements that say that the code is "military-grade" or "NSA-proof"; these mean nothing and give a strong warning that the creators are overconfident or unwilling to consider the possible failings in their product.*

Because attackers are always trying to discover new ways to break the security of tools, software and hardware often needs to be updated to fix new vulnerabilities. It can be a serious problem if the creators of a tool are unwilling to do this, either because they fear bad publicity, or because they have not built the infrastructure to fix problems.

You can't predict the future, but a good indicator of how toolmakers will behave in the future is their past activity. If the tool's website lists previous issues and links to regular updates and information—like specifically how long it has been since the software was last updated—you can be more confident that they will continue to provide this service in the future.

What Happens if the Creators are Compromised?

When security toolmakers build software and hardware, they (just like you) must have a clear threat model. The best creators will explicitly describe what kind of attackers they can protect you from in their documentation.

But there's one attacker that many manufacturers do not want to think about: what if they, themselves, are compromised or decide to attack their own users. For instance, a court or government may compel a company to give up personal data or create a "backdoor" that will remove all the protections their tool offers. You may want to consider the jurisdiction(s) where the creators are based. If your threat is from the government of Iran,

for example, a US-based company will be able to resist Iranian court orders, even if it must comply with US orders.

Even if a creator is able to resist government pressure, an attacker may attempt to achieve the same result by breaking into the toolmakers' own systems in order to attack its customers.
The most resilient tools are those that consider this as a possible attack, and are designed to defend against this. Look for language that asserts that a creator cannot access private data, rather than promises that a creator *will* not. Look for institutions with a reputation for fighting court orders for personal data.

Check for Recalls and Online Criticism

Of course, companies selling products and enthusiasts advertising their latest software can be misled, be misleading, or even outright lie. A product that was originally secure might be discovered to have terrible flaws in the future. Make sure you stay well-informed on the latest news about the tools that you use.

Do you Know Others who Use the Same Tool?

It's a lot of work for one person to keep up with the latest news about a tool. If you have colleagues who use a particular product or service, work with them to stay abreast on what's happening.

Products Mentioned in This Guide

We try to ensure that the software and hardware we mention in this guide complies with the criteria we've listed above: we have made a good faith effort to only list products that have a solid grounding in what we currently know about digital security, are generally transparent about their operation (and their failings), have defenses against the possibility that the creators themselves will be compromised, and are currently maintained, with a large and technically-knowledgeable user base. We believe that they have, at the time of writing, the eye of a wide audience who is examining them for flaws, and would raise concerns to the public quickly. Please understand that we do not have the resources to examine or make independent assurances about their security, we are not endorsing these products and cannot guarantee complete security.

Which Phone Should I Buy? Which Computer?

One of the most frequent questions asked of security trainers is “Should I buy Android or an iPhone?” or “Should I use a PC or a Mac?” or “What operating system should I use?” There are no simple answers to these questions. The relative safety of software and devices is constantly shifting as new flaws are discovered and old bugs are fixed.

Companies may compete with each other to provide you with better security, or they may all be under pressure from governments to weaken that security.

Some general advice is almost always true, however. When you buy a device or an operating system, keep current with its software updates. Updates will often fix security problems in older code that attacks can exploit. Older phones and operating systems are no longer supported, even for security updates. In particular, Microsoft has made it clear that Windows XP and earlier Windows versions will not receive fixes for even severe security problems. If you use XP, you cannot expect it to be secure from attackers. (The same is true for OS X before 10.7.5 or "Lion").

How Do I Protect Myself Against Malware?

Malware, short for "malicious software," is software that is used to harm computer users. It works in many different ways including, but not limited to, disrupting computer operation, gathering sensitive information, impersonating a user to send spam or fake messages, or gaining access to private computer systems. The majority of malware is criminal and is most often used to obtain banking information or login credentials for email or social media accounts. Malware is also used by governments, law enforcement agencies, and even private citizens to circumvent encryption and to spy on users. Malware has wide-range capabilities; it may allow an attacker to record from a webcam and microphone, disable the notification setting for certain anti-virus programs, record keystrokes, copy emails and other documents, steal passwords, and more.

Anti-virus Software

EFF recommends that you use anti-virus software on your computer and your smartphone, though we cannot recommend any particular anti-virus products as being superior to others. Anti-virus software can be quite effective at combatting cheap, “non targeted” malware that might be used by criminals against hundreds of targets. However anti-virus software is usually ineffective against targeted attacks, such as the ones used by Chinese government hackers to compromise the New York Times.

Indicator of Compromise

When it is not possible to detect malware using anti-virus software, it is still sometimes possible to find indicators of compromise. For example, Google will sometimes give a warning to Gmail users stating that it believes your account has been targeted by state-sponsored attackers. Additionally, you may notice a light indicating that your webcam is turned on when you have not activated it yourself (though advanced malware may be able to turn this off)—this could be another indicator of compromise. Other indicators are less obvious; you may notice your email is being accessed from an unfamiliar IP address or that your settings have been altered to send copies of all of your email to an unfamiliar email address. If you have the ability to monitor your network traffic, the timing and volume of that traffic might indicate a compromise. Another red flag would be that you might notice your computer connecting to a known Command and Control server—the computers that send commands to machines infected with malware or which receive data from infected machines.

How can Attackers use Malware to Target me?

The best way to deal with a malware attack is to avoid getting infected in the first place. This can be a difficult feat if your adversary has access to zero day attacks—attacks that exploit a previously-unknown vulnerability in a computer application. Think of your computer as a fortress; a zero day would be a hidden secret entrance that you do not know about, but which an attacker has discovered. You cannot protect yourself against a secret entrance you don't even know exists. Governments and law enforcement agencies stockpile zero day exploits for use in targeted malware attacks. Criminals and other actors may also have access to zero day exploits that they may use to covertly install malware on your computer. But zero day exploits are expensive to buy and costly to re-use (once you use the secret tunnel to break into the fortress, it increases the chances that other people may find it). It is much more common for an attacker to trick you into installing the malware yourself.

There are many ways in which an attacker might try to trick you into installing malware on your computer. They may disguise the payload as a link to a website, a document, PDF, or even a program designed to help secure your computer. You may be targeted via email (which may look as if it's coming from someone you know), via a message on Skype or Twitter, or even via a link posted to your Facebook page. The more targeted the attack, the more care the attacker will take in making it tempting for you to download the malware.

For example, in Syria, pro-Assad hackers targeted members of the opposition with malware hidden in fake revolutionary documents and a fake anti-hacking tool. Iranians have been targeted using malware hidden in a popular censorship-circumvention program. And in Morocco, activists were targeted with malware hidden in a document made to look as if it had been sent by an Al-Jazeera reporter, promising information about a political scandal.

The best way to avoid being infected with this kind of targeted malware is to avoid opening the documents and installing the malware in the first place. People with more computer and technical expertise will have somewhat better instincts about what might be malware and what might not be, but well-targeted attacks can be very convincing. If you are using Gmail, opening suspicious attachments in Google Drive rather than downloading them may protect your computer from infection. Using a less common computing platform, like Ubuntu or ChromeOS, significantly improves your odds against many malware delivery tricks, but will not protect against the most sophisticated adversaries.

Another thing you can do to protect your computer against malware is to *always make sure you are running the latest version of your software and downloading the latest security patches*. As new vulnerabilities are discovered in software, companies can fix those problems and offer that fix as a software update, but you will not reap the benefits of their work unless you install the update on your computer. It is a common belief that if

you are running an unregistered copy of Windows, you cannot or should not accept security updates. This is not true.

What Should I do if I Find Malware on my Computer?

> *If you do find malware on your computer, **unplug your computer from the Internet and stop using it immediately**. Every keystroke you make may be being sent to an attacker. You may wish to take your computer to a security expert, who may be able to discover more details about the malware. If you've found the malware, removing it does not guarantee the security of your computer. Some malware gives the attacker the ability to execute arbitrary code on the infected computer—and there is no guarantee that the attacker has not installed additional malicious software while in control of your machine.*

Log into a computer you believe is safe and *change your passwords;* every password that you typed on your computer while it was infected should now be considered to be compromised.

You may wish to reinstall the operating system on your computer in order to remove the malware. This will remove most malware, but some especially sophisticated malware may persist. If you have some idea of when your computer was infected, you may reinstall files from before that date. *Reinstalling files from after the date of infection may re-infect your computer.*

Keeping Your Data Safe

One of the greatest challenges of defending your data from those who might want it is the sheer size of the information you store or carry, and the ease by which it can be taken from you. Many of us carry entire histories of our contacts, our communications, and our current documents on laptops, or even mobile phones. That data can include confidential information of dozens, even thousands, of people. A phone or laptop can be stolen, or copied in seconds.

The United States is just one of many countries that seizes and copies data at borders. Data can be taken from you at roadblocks, grabbed from you in the street, or burgled from your house.

Just as you can keep your communications safer with encryption, you can also make it harder for those who physically steal data to unlock its secrets. Computers and mobile phones can be locked by passwords, PINs or gestures, but these locks do not help protect data if the device itself is seized. It's relatively simple to bypass these locks, because your data is stored in an easily readable form within the device. All an attacker needs to do is to access the storage directly, and the data can be copied or examined without knowing your password.

> *If you use encryption, your adversary needs not just your device, but also your password to unscramble the encrypted data—there's no shortcut.*

It's safest and easiest to encrypt all of your data, not just a few folders. Most computers and smartphones offer complete, full-disk encryption as an option. Android offers it under its "Security" settings, Apple devices such as the iPhone and iPad describe it as "Data Protection" and turn it on if you set a passcode. On computer running Windows Pro, it's known as "BitLocker." If you have the standard version of Windows, you can use a free program called DiskCryptor (see our guide "How to Encrypt your Windows Device"). On Macs it's called "FileVault." On Linux distributions, full-disk encryption is usually offered when you first set up your system.

Whatever your device calls it, encryption is only as good as your password. If your attacker has your device, they have all the time in the world to try out new passwords. Forensic software can try millions of passwords a second. That means that a four number pin is unlikely to protect your data for very long at all, and even a long password may merely slow down your attacker. A really strong password under these conditions should be over fifteen characters long.

Most of us are not realistically going to learn and enter such passphrases on our phones or mobile devices. So while encryption can be useful to prevent casual access, you should preserve truly confidential data by keeping it hidden from physical access by attackers, or cordoned away on a much more secure machine.

Create a Secure Machine

Maintaining a secure environment can be hard work. At best, you have to change passwords, habits, and perhaps the software you use on your main computer or device. At worst, you have to constantly think about whether you're leaking confidential information or using unsafe practices. Even when you know the problems, some solutions may be out of your hands. Other people might require you to continue unsafe digital security practices even after you have explained the dangers. For instance, work colleagues might want you to continue to open email attachments from them, even though you know your attackers could impersonate them and send you malware. Or you may be concerned that your main computer has already been compromised.

One strategy to consider is cordoning off valuable data and communications onto a more secure computer. Use that machine only occasionally, and when you do, consciously take much more care over your actions. If you need to open attachments, or use insecure software, do it on another machine.

> *If you're setting up a secure machine, what extra steps can you take to make it secure?*

You can almost certainly keep the device in a more physically safe place: somewhere where you are able to tell if it has been tampered with, such as a locked cabinet.

You can install a privacy- and security-focused operating system like Tails. You might not be able (or want) to use an open source operating system in your everyday work, but if you just need to store, edit and write confidential emails or instant messages from this secure device, Tails will work well, and defaults to high security settings.

An extra, secure computer may not be as expensive an option as you think. A computer that is seldom used, and only runs a few programs, does not need to be particularly fast or new. You can buy an older netbook for a fraction of the price of a modern laptop or phone. Older machines also have the advantage that secure software like Tails may be more likely to work with them than newer models.

You can use the secure machine to keep the primary copy of confidential data. A secure machine can be valuable in cordoning off private data in this way, but you should also consider a couple of extra risks it might create. If you concentrate your most treasured information onto this one computer, it may make it more of an obvious target. Keep it well hidden, don't discuss its location, and don't neglect to encrypt the computer's drive with a strong password, so that if it is stolen, the data will remain unreadable without the password safe.

Another risk is the danger that destroying this one machine will destroy your only copy of the data.

If your adversary would benefit from you losing all your data, don't keep it in just one place, no matter how secure. Encrypt a copy and keep it somewhere else.

The highest level of protection from Internet attacks or online surveillance is, not surprisingly, not connecting to the Internet at all. You could make sure your secure computer never connects to a local network or Wifi, and only copy files onto the machine using physical media, like DVDs or USB drives. In network security, this is known as having an "air gap" between the computer and the rest of the world. Not many people go this far, but it can be an option if you want to keep data that is rarely accessed but you never want to lose. Examples might be an encryption key you only use for important messages (like "My other encryption keys are now insecure"), a list of passwords or instructions for other people to find if you are unavailable, or a backup copy of someone else's private data that has been entrusted to you. In most of these cases, you might want to consider just having a hidden storage device, rather than a full computer. An encrypted USB key kept safely hidden is probably as useful (or as useless) as a complete computer unplugged from the Internet.

If you do use the secure device to connect to the Internet, you might choose not to log in or use your usual accounts. Create separate web or email accounts that you use for communications from this device, and use Tor to keep your IP address hidden from those services. If someone is choosing to specifically target your identity with malware, or is only intercepting your communications, separate accounts and Tor can help break the link between your identity, and this particular machine.

A variation on the idea of a secure machine is to have an insecure machine: a device that you only use when you are going into dangerous places or need to try a risky operation. Many journalists and activists, for instance, take a minimal netbook with them when they travel. This computer does not have any of their documents, usual contact or email information on it, and so is less of a loss if it is confiscated or scanned. You can apply the same strategy to mobile phones. If you usually use a smartphone, consider buying a cheap throwaway or burner phone when travelling or for specific communications.

Creating Strong Passwords

Because remembering many different passwords is difficult, people often reuse a small number of passwords across many different accounts, sites, and services. Today, users are constantly being asked to come up with new passwords—many people end up reusing the same password dozens or even hundreds of times.

Reusing passwords is an exceptionally bad security practice, because if an attacker gets hold of one password, she will often try using that password on various accounts belonging to the same person. If that person has reused the same password several times, the attacker will be able to access multiple accounts. That means a given password *may be only as secure as the least secure service where it's been used*.

Avoiding password reuse is a valuable security precaution, but you won't be able to remember all your passwords if each one is different. Fortunately, there are software tools to help with this—a password manager (also called a password safe) is a software application that helps store a large number of passwords safely. This makes it practical to avoid using the same password in multiple contexts. The password manager protects all of your passwords with a single master password (or, ideally a passphrase—*see discussion below*) so you only have to remember one thing. People who use a password manager no longer actually know the passwords for their different accounts; the password manager can handle the entire process of creating and remembering the passwords for them.

For example, KeePassX is an open source, free password safe that you keep on your desktop. *It's important to note that if you're using KeePassX, it will not automatically save changes and additions. This means that if it crashes after you've added some passwords, you can lose them forever. You can change this in the settings.*

Using a password manager also helps you choose strong passwords that are hard for an attacker to guess. This is important too; too often computer users choose short, simple passwords that an attacker can easily guess, including "password1," "12345," a birthdate, or a friend's, spouse's, or pet's name. A password manager can help you create and use a random password without pattern or structure—one that won't be guessable. For example, a password manager is able to choose passwords like "vAeJZ!Q3p$Kdkz/CRHzj0v7," which a human being would be unlikely to remember—or guess. Don't worry; the password manager can remember these for you!

Syncing Your Passwords Across Multiple Devices

You may use your passwords on more than one device, such as your computer and your smart phone. Many password managers have a password-synchronizing feature built in. When you sync your password file, it will be up to date on all of your devices, so that if

you've added a new account on your computer, you will still be able to log into it from your phone. Other password managers will offer to store your passwords "in the cloud," which is to say, they will store your passwords encrypted on a remote server, and when you need them on a laptop or mobile, they will retrieve and decrypt them for you automatically. Password managers that use their own servers to store or help synchronize your passwords are more convenient, but the trade-off is that they are slightly more vulnerable to attack. If you just keep your passwords on your computer, then someone who can take over your computer may be able to get hold of them. If you keep them in the cloud, your attacker may target that also. It's not usually a compromise you need to worry about unless your attacker has legal powers over the password manager company or is known for targeting companies or internet traffic. If you use a cloud service, the password manager company may also know what services you use, when, and where from.

Choosing Strong Passwords

There are a few passwords that do need to be memorized and that need to be particularly strong: those that ultimately lock your own data with cryptography. That includes, at least, passwords for your device, encryption like full-disk encryption, and the master password for your password manager.

Computers are now fast enough to quickly guess passwords shorter than ten or so characters. That means short passwords of any kind, even totally random ones like nQ\m=8*x or !s7e&nUY or gaG5^bG, *are not strong enough for use with encryption today*.

There are several ways to create a strong and memorable passphrase; the most straightforward and sure-fire method is Arnold Reinhold's "Diceware."

Reinhold's method involves rolling physical dice to randomly choose several words from a word list; together, these words will form your passphrase. For disk encryption (and password safe), we recommend selecting a minimum of six words.

> *Try making a password using Reinhold's "Diceware" method.*

When you use a password manager, the security of your passwords and your master password is only as strong as the security of the computer where the password manager is installed and used. If your computer or device is compromised and spyware is installed, the spyware can watch you type your master password and could steal the contents of the password safe. So it's still very important to keep your computer and other devices clean of malicious software when using a password manager.

A Word About “Security Questions”

Be aware of the “security questions” (such as “What is your mother’s maiden name?” or "What was your first pet's name?") that websites use to confirm your identity if you do forget your password. Honest answers to many security questions are publicly discoverable facts that a determined adversary can easily find, and therefore bypass your password entirely. For instance, US vice-presidential candidate Sarah Palin had her Yahoo! account hacked this way. Instead, give fictional answers that, like your password, no one knows but you. For example, if the password question asks you your pet’s name, you may have posted photos to photo sharing sites with captions such as “Here is a photo of my cute cat, Spot!” Instead of using “Spot” as your password recovery answer, you might choose “Rumplestiltskin.” *Do not use the same passwords or security question answers for multiple accounts on different websites or services*. You should store your fictional answers in your password safe, too.

Think of sites where you’ve used security questions. Consider checking your settings and changing your responses.

Remember to keep a backup of your password safe! If you lose your password safe in a crash (or if you have your devices taken away from you), it may be hard to recover your passwords. Password safe programs will usually have a way to make a separate backup, or you can use your regular backup program.

You can usually reset your passwords by asking services to send you a password recovery email to your registered email address. For that reason, you may want to memorize the passphrase to this email account also. If you do that, then you will have a way of resetting passwords without depending on your password safe.

Multi-factor Authentication and One-time Passwords

Many services and software tools let you use two-factor authentication, also called two-step authentication or two-step login. Here the idea is that in order to log in, you need to be in possession of a certain physical object: usually a mobile phone, but, in some versions, a special device called a security token. Using two-factor authentication ensures that even if your password for the service is hacked or stolen, the thief won't be able to log in unless they also have possession or control of a second device and the special codes that only it can create.

Typically, this means that a thief or hacker would have to control both your laptop and your phone before they have full access to your accounts.

Because this can only be set up with the cooperation of the service operator, there is no way to do this by yourself if you're using a service that doesn't offer it.

Two-factor authentication using a mobile phone can be done in two ways: the service can send you an SMS text message to your phone whenever you try to log in (providing an extra security code that you need to type in), or your phone can run an authenticator application that generates security codes from inside the phone itself. This will help protect your account in situations where an attacker has your password but does not have physical access to your mobile phone.

Some services, such as Google, also allow you to generate a list of one-time passwords, also called single-use passwords. These are meant to be printed or written down on paper and carried with you (although in some cases it might be possible to memorize a small number of them). Each of these passwords works only once, so if one is stolen by spyware when you enter it, the thief won't be able to use it for anything in the future.

If you or your organization run your own communications infrastructure, such as your own e-mail servers, there's freely available software that can be used to enable two-factor authentication for accessing your systems. Ask your systems administrators to look for software offering implementations of the open standard “Time-Based One-Time Passwords” or RFC 6238.

Threats of Physical Harm or Imprisonment

Finally, understand that there is always one way that attackers can obtain your password: They can directly threaten you with physical harm or detention. If you fear this may be a possibility, consider ways in which you can hide the existence of the data or device you are password-protecting, rather than trust that you will never hand over the password. One possibility is to maintain at least one account that contains largely unimportant information, whose password you can divulge quickly.

If you have good reason to believe that someone may threaten you for your passwords, it's good to make sure your devices are configured so that it won't be obvious that the account you are revealing is not the “real” one. Is your real account shown in your computer's login screen, or automatically displayed when you open a browser? If so, you may need to reconfigure things to make your account less obvious.

In some jurisdictions, such as the United States or Belgium, you may be able to legally challenge a demand for your password. In other jurisdictions, such as the United Kingdom or India, local laws allow the government to demand disclosure. EFF has detailed information for anyone travelling across U.S. borders who wishes to protect their data on their digital devices in our Defending Privacy at the U.S. Border guide.

Please note that intentional destruction of evidence or obstruction of an investigation can be charged as a separate crime, often with very serious consequences. In some cases, this can be easier for the government to prove and allow for more substantial punishments than the alleged crime originally being investigated.

Things to Consider When Crossing the US Border

Planning on crossing the border into the United States anytime soon? Did you know that the government has the right to, without a warrant, search travelers at the border—including when they land at international airports—as part of its traditional power to control the flow of items into the country? (Note that although some of the same legal justifications exist for searches of those leaving the US and that such searches are possible, travelers are not routinely searched on their way out of the country.)

For a more in depth treatment of this issue, check out EFF's guide, Defending Privacy at the US Border

In the Meantime, Here are Some Things to Keep in Mind When Crossing the US Border:

- Have you backed up your devices? This may help in case one or more of your devices is seized. You can use an online backup service or an external hard drive, though we don't recommend carrying both your laptop and your backup hard drive at the same time.
- Do you need to be carrying so much data? We suggest minimizing the amount of data you are carrying over the border. Consider traveling with a "clean" laptop, and note that simply dragging files to your trash doesn't delete them completely. Make sure you securely delete your files.
- Are your devices encrypted? We recommend full-disk encryption on your devices (laptops, mobile phones, etc.) and choosing secure passphrases. If a border agent asks for your passphrase, you do not have to comply. Only a judge can force you to reveal such information. However, refusal to comply could bear consequences: for noncitizens, you may be refused entry into the country; for citizens, you may be detained until the border patrol decides what to do, which may include seizing your computer, phone, camera, USB sticks, etc.
- When you enter a new country, consider purchasing a temporary phone and transferring your SIM card over or getting a new number. This phone will carry far less data than your normal phone.
- When dealing with border guards, remember these three things: *Be courteous, do not lie*, and *do not* physically interfere with the agent's search.

What Is Encryption?

Encryption is the mathematical science of codes, ciphers, and secret messages. Throughout history, people have used encryption to send messages to each other that (hopefully) couldn't be read by anyone besides the intended recipient.

Today, we have computers that are capable of performing encryption for us. Digital encryption technology has expanded beyond simple secret messages; today, encryption can be used for more elaborate purposes, for example to verify the author of messages or to browse the Web anonymously with Tor.

Under some circumstances, encryption can be fairly automatic and simple. But there are ways encryption can go wrong, and the more you understand it, the safer you will be against such situations.

Three Concepts to Understand in Encryption

Private and Public Keys

One of the most important concepts to understand in encryption is a key. Common types of encryption include a private key, which is kept secret on your computer and lets you read messages that are intended only for you. A private key also lets you place unforgeable digital signatures on messages you send to other people. A public key is a file that you can give to others or publish that allows people to communicate with you in secret, and check signatures from you. Private and public keys come in matched pairs, like the halves of a rock that has been split into two perfectly matching pieces, but they are not the same.

Security Certificates

Another extremely valuable concept to understand is a security certificate. The Web browser on your computer can make encrypted connections to sites using HTTPS. When they do that, they examine certificates to check the public keys of domain names—(like www.google.com, www.amazon.com, or ssd.eff.org). Certificates are one way of trying to determine if you know the right public key for a person or website, so that you can communicate securely with them.

From time to time, you will see certificate-related error messages on the Web. Most commonly, this is because a hotel or cafe network is trying to break your secret communications with the website. It is also common to see an error because of a bureaucratic mistake in the system of certificates. But occasionally, it is because a hacker, thief, police agency, or spy agency is breaking the encrypted connection.

Unfortunately, it is extremely difficult to tell the difference between these cases. This means you should never click past a certificate warning if it relates to a site where you have an account, or are reading any sensitive information.

Key Fingerprints

The word "fingerprint" means lots of different things in the field of computer security. One use of the term is a "key fingerprint," a string of characters like "342e 2309 bd20 0912 ff10 6c63 2192 1928" that should allow you to uniquely and securely check that someone on the Internet is using the right private key. If you check that someone's key fingerprint is correct, that gives you a higher degree of certainty that it's really them. But it's not perfect, because if the keys are copied or stolen someone else would be able to use the same fingerprint.

Key Verification

When encryption is used properly, your communications or information should only be readable by you and the person or people you're communicating with. End-to-end encryption protects your data from surveillance by third parties, but if you're unsure about the identity of the person you're talking to, its usefulness is limited. That's where key verification comes in. By verifying public keys, you and the person with whom you're communicating add another layer of protection to your conversation by confirming each other's identities, allowing you to be that much more certain that you're talking to the right person.

Key verification is a common feature of protocols that use end-to-end encryption, such as PGP and OTR. To verify keys without the risk of interference, it's advisable to use a secondary method of communicating other than the one you're going to be encrypting; this is called out-of-band verification. For example, if you are verifying your OTR fingerprints, you might email your fingerprints to one another. In that example, email would be the secondary communications channel.

Verifying Keys Out-of-band

There are several ways to do this. If it can be arranged safely and is convenient, it is ideal to verify keys face-to-face. This is often done at key-signing parties or amongst colleagues.

If you cannot meet face-to-face, you can contact your correspondent through a means of communication other than the one for which you're trying to verify keys. For example, if you're trying to verify PGP keys with someone, you could use the telephone or an OTR chat to do so.

Regardless of the program that you use, you will always be able to locate both your key and the key of the your communication partner.

Although the method of locating your key varies by program, the method of verifying keys remains approximately the same. You can either read your key's fingerprint aloud (if you are face-to-face or using the telephone) or you can copy and paste it into a communications program, but whichever you choose, *it is imperative that you check every single letter and numeral*.

> *Tip: Try verifying keys with one of your friends. To learn how to verify keys in a specific program, visit that program's how-to guide.*

Communicating with Others

Telecommunication networks and the Internet have made communicating with people easier than ever, but have also made surveillance more prevalent than it has ever been in human history. Without taking extra steps to protect your privacy, every phone call, text message, email, instant message, voice over IP (VoIP) call, video chat, and social media message may be vulnerable to eavesdroppers.

Often the safest way to communicate with others is in person, without computers or phones being involved at all. Because this isn't always possible, the next best thing is to use end-to-end encryption while communicating over a network if you need to protect the content of your communications.

How Does End-to-End Encryption Work?

When two people want to communicate securely (for example, Akiko and Boris) they must each generate crypto keys. Before Akiko sends a message to Boris she encrypts it to Boris's key so that only Boris can decrypt it. Then she sends the already-encrypted message across the Internet. If anyone is eavesdropping on Akiko and Boris—even if they have access to the service that Akiko is using to send this message (such as her email account)—they will only see the encrypted data and will be unable read the message. When Boris receives it, he must use his key to decrypt it into a readable message.

End-to-end encryption involves some effort, but it's the only way that users can verify the security of their communications without having to trust the platform that they're both using. Some services, such as Skype, have claimed to offer end-to-end encryption when it appears that they actually don't. For end-to-end encryption to be secure, users must be able to verify that the crypto key they're encrypting messages to belongs to the people they believe they do. If communications software doesn't have this ability built-in, then any encryption that it might be using can be intercepted by the service provider itself, for instance if a government compels it to.

You can read Freedom of the Press Foundation's whitepaper, Encryption Works for detailed instructions on using end-to-end encryption to protect instant messages and email. Be sure to check out the following SSD module as well:

- How to: Use OTR for Mac

Voice Calls

When you make a call from a landline or a mobile phone, your call is not end-to-end encrypted. If you're using a mobile phone, your call may be (weakly) encrypted between your handset and the cell phone towers. However as your conversation travels through the phone network, it's vulnerable to interception by your phone company and, by extension, any governments or organizations that have power over your phone company. The easiest way to ensure you have end-to-end encryption on voice conversations is to use VoIP instead.

> *Beware! Most popular VoIP providers, such as Skype and Google Hangouts, offer transport encryption so that eavesdroppers cannot listen in, but* ***the providers themselves are still potentially able to listen in****. Depending on your threat model, this may or may not be a problem.*

Some services that offer end-to-end encrypted VoIP calls include:

- Ostel
- RedPhone
- Silent Phone
- Signal

In order to have end-to-end encrypted VoIP conversations, both parties must be using the same (or compatible) software.

Text Messages

Standard text (SMS) messages do not offer end-to-end encryption. If you want to send encrypted messages on your phone, consider using encrypted instant messaging software instead of text messages.

Some end-to-end encrypted instant messaging services use their own protocol. So, for instance, users of TextSecure and Signal on Android and iOS can chat securely with others who use those programs. ChatSecure is a mobile app that encrypts conversations with OTR on any network that uses XMPP, which means you can choose from a range of independent instant messaging services.

Instant Messages

Off-the-Record (OTR) is an end-to-end encryption protocol for real-time text conversations that can be used on top of a variety of services.

Some tools that incorporate OTR with instant messaging include:

- Adium (for OS X)
- ChatSecure (for iPhone and Android)

Email

Most email providers give you a way of accessing your email using a web browser, such as Firefox or Chrome. Of these providers, most of them provide support for HTTPS, or transport-layer encryption. You can tell that your email provider supports HTTPS if you log in to your webmail and the URL at the top of your browser begins with the letters HTTPS instead of HTTP (for example: https://mail.google.com).

If your email provider supports HTTPS, but does not do so by default, try replacing HTTP with HTTPS in the URL and refresh the page. If you'd like to make sure that you are always using HTTPS on sites where it is available, download the HTTPS Everywhere browser add-on for Firefox or Chrome.

Some webmail providers that use HTTPS by default include:

- Gmail
- Riseup
- Yahoo

Some webmail providers that give you the option of choosing to use HTTPS by default by selecting it in your settings. The most popular service that still does this is Hotmail.

What does transport-layer encryption do and why might you need it? HTTPS, also referred to as SSL or TLS, encrypts your communications so that it cannot be read by other people on your network. This can include the other people using the same Wi-Fi in an airport or at a café, the other people at your office or school, the administrators at your ISP, malicious hackers, governments, or law enforcement officials. Communications sent over your web browser, including the web pages that you visit and the content of your emails, blog posts, and messages, using HTTP rather than HTTPS are trivial for an attacker to intercept and read.

HTTPS is the most basic level of encryption for your web browsing that we recommend for everybody. It is as basic as putting on your seat belt when you drive.

But there are some things that HTTPS does not do. When you send email using HTTPS, your email provider still gets an unencrypted copy of your communication. Governments and law enforcement may be able to access this data with a warrant. In the United States, most email providers have a policy that says they will tell you when you have received a government request for your user data as long as they are legally allowed to do so, but these policies are strictly voluntary, and in many cases providers are legally prevented from informing their users of requests for data. Some email providers, such as Google, Yahoo, and Microsoft, publish transparency reports, detailing the number of government

requests for user data they receive, which countries make the requests, and how often the company has complied by turning over data.

> *If your threat model includes a government or law enforcement, or you have some other reason for wanting to make sure that your email provider is not able to turn over the contents of your email communications to a third party, you may want to consider using end-to-end encryption for your email communications.*

PGP (or Pretty Good Privacy) is the standard for end-to-end encryption of your email. Used correctly, it offers very strong protections for your communications. For detailed instructions on how to install and use PGP encryption for your email, see:

- How to: Use PGP for Mac OS X

What End-To-End Encryption Does Not Do

End-to-end encryption only protects the content of your communication, not the fact of the communication itself. It does not protect your metadata—which is everything else, including the subject line of your email, or who you are communicating with and when.

> *Metadata can provide extremely revealing information about you even when the content of your communication remains secret.*

Metadata about your phone calls can give away some very intimate and sensitive information. For example:

- They know you rang a phone sex service at 2:24 am and spoke for 18 minutes, but they don't know what you talked about.
- They know you called the suicide prevention hotline from the Golden Gate Bridge, but the topic of the call remains a secret.
- They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour, but they don't know what was discussed.
- They know you received a call from the local NRA office while it was having a campaign against gun legislation, and then called your senators and congressional representatives immediately after, but the content of those calls remains safe from government intrusion.
- They know you called a gynecologist, spoke for a half hour, and then called the local Planned Parenthood's number later that day, but nobody knows what you spoke about.

If you are calling from a cell phone, *information about your location is metadata*. In 2009, Green Party politician Malte Spitz sued Deutsche Telekom to force them to hand over six months of Spitz's phone data, which he made available to a German newspaper. The resulting visualization showed a detailed history of Spitz's movements.

Protecting your metadata will require you to use other tools, such as Tor, at the same time as end-to-end encryption.

For an example of how Tor and HTTPS work together to protect the contents of your communications and your metadata from a variety of potential attackers, you may wish to take a look at this explanation.

Choosing the VPN That's Right for You

What's a VPN? VPN stands for "Virtual Private Network." It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network—benefiting from the functionality, security, and management policies of the private network.

What is a VPN Good For?

You can use a VPN to connect to the corporate intranet at your office while you're traveling abroad, while you are at home, or any other time you are out of the office.

You can also use a commercial VPN to encrypt your data as it travels over a public network, such as the Wi-Fi in an Internet café or a hotel.

You can use a commercial VPN to circumvent Internet censorship on a network that blocks certain sites or services. For example, some Chinese users use commercial VPNs to access websites blocked by the Great Firewall.

You can also connect to your home network by running your own VPN service, using open source software such as OpenVPN.

What Doesn't a VPN Do?

A VPN protects your Internet traffic from surveillance on the public network, but it *does not protect your data from people on the private network you're using*. If you are using a corporate VPN, then whoever runs the corporate network will see your traffic. If you are using a commercial VPN, whoever runs the service will be able to see your traffic.

The manager of your corporate or commercial VPN may also be subject to pressure from governments or law enforcement to turn over information about the data you have sent over the network. You should review your VPN provider's privacy policy for information about the circumstances under which your VPN provider may turn your data over to governments or law enforcement.

You should also take note of the countries in which the VPN provider does business. The provider will be subject to the laws in those countries, which may include both legal requests for your information from that government, and other countries with whom it has a legal assistance treaty. In some cases, the laws will allow for requests without notice to you or an opportunity to contest the request.

Most commercial VPNs will require you to pay using a credit card, which includes information about you that you may not want to divulge to your VPN provider. If you would like to keep your credit card number from your commercial VPN provider, you may wish to use a VPN provider that accepts Bitcoin, or use temporary or disposable credit card numbers. Also, please note that the VPN provider may still collect your IP address when you use their service, which can be used to identify you, even if you use an alternative payment method. If you would like to hide your IP address from your VPN provider, you may wish to use Tor when connecting to your VPN.

An Introduction to Public Key Cryptography and PGP

PGP stands for Pretty Good Privacy. It's actually *very* good privacy. If used correctly, it can protect the contents of your messages, text, and even files from being understood even by well-funded government surveillance programs. When Edward Snowden says "encryption works," it's PGP and its related software that he is talking about. It should be noted that it's not unheard of for governments to steal private keys off of particular people's computers (by taking the computers away, or by putting malware on them using physical access or with phishing attacks), which undoes the protection and even allows for reading old mail. This is comparable to saying that you might have an unpickable lock on your door, but somebody might still be able to pickpocket you in the street for your key, then copy it and sneak it back into your pocket—and hence get into your house without even picking the lock.

Unfortunately, PGP is also pretty bad at being easy to understand, or use. The strong encryption that PGP uses—public key encryption—is ingenious, but hard to wrap your head around. PGP software itself has been around since 1991, which makes it the same vintage as the early versions of Microsoft Windows, and its appearance hasn't changed much since then.

The good news is that there are many programs available now which can hide the ancient design of PGP and make it somewhat easier to use, especially when it comes to encrypting and authenticating email—the main use of PGP. We've included guides to installing and operating this software elsewhere.

Before you play around with PGP or other programs that use it, though, it's worth spending a few minutes understanding the basics of public key encryption: what it can do for you, what it can't do, and when you should use it.

A Tale of Two Keys

When we use encryption to fight surveillance, here's what we're trying to do:

We take a clearly readable message like "hello mum." We encrypt that into a coded message that is incomprehensible to anyone looking at it ("OhsieW5ge+osh1aehah6," say). We send that encrypted message over the Internet, where it can be read by lots of people, but hopefully not understood by any of them. Then, when it arrives at its destination, our intended recipient, and only our intended recipient, has some way of decrypting it back into the original message.

How does our recipient know how to decode the message, when nobody else can? It must be because they know some extra information that nobody else knows. Let's call this the decoding key, because it *unlocks* the message inside the code.

How does the recipient know this key? Mostly, it's because the sender has previously told them the key, whether it's “try holding the message up in a mirror” or “take each letter and convert it to the next letter in the alphabet.” There's a problem with this strategy though. If you're worried about being spied upon when you send your coded message, how do you send the recipient the key without someone spying on *that* conversation too? There's no point sending an ingeniously encrypted message if your attacker already knows the key to decoding it. And if you have a secret way to send decoding keys, why don't you just use that for all your secret messages?

Public-key cryptography has a neat solution for this. Each person in a conversation has a way of creating two keys. One is their private key, which they keep to themselves and never let anyone else know. The other is a public key, which they hand out to anyone who wants to communicate with them. It doesn't matter who can see the public key. You can put it online where everyone can see it.

The “keys” themselves are, at heart, actually very large numbers, with certain mathematical properties. The public key and private key are connected. If you encode something using the public key, then someone else can decode it with its matching private key.

Let's see how that might work. You want to send a secret message to Aarav. Aarav has a private key, but like a good public key encryption user, he has put its connected public key on his web page. You download the public key, encrypt the message using it, and send it to him. He can decode it, because he has the corresponding private key – but nobody else can.

Sign of the Times

Public key cryptography gets rid of the problem of smuggling the decoding key to the person you want to send a message to, because that person already *has* the key. You just need to get hold of the matching public, encoding key, which the recipient can hand out to everyone, including spies. Because it's only useful for encoding a message, it is useless for anyone trying to decode the message.

But there's more! If you encode a message with a certain public key, it can only be decoded by the matching private key. But the opposite is also true. If you encode a message with a certain private key, it can only be decoded by its matching public key.

Why would this be useful? At first glance, there doesn't seem to be any advantage to making a secret message with your private key that everyone in the world (or at least, everyone who has your public key) can crack. But suppose I wrote a message that said “I

promise to pay Aazul $100," and then turned it into a secret message using my private key. Anyone could decode that message—but only one person could have written it: the person who has my private key. If I've done a good job keeping my private key safe, that means me, and only me. In effect, by encoding it with my private key, I've made sure that it could only have come from me. In other words, I've done the same thing with this digital message as we do when we *sign* a message in the real world.

Signing also makes messages tamper-proof. If someone tried to change that "I promise to pay Aazul $100" into "I promise to pay Bob $100," they would not be able to re-sign it using my private key. So a signed message is guaranteed to originate from a certain source, and not be messed with in transit.

So public key cryptography lets you encrypt and send messages safely to anyone whose public key you know. If others know your public key, they can send you messages, which only you can decode. And if people know your public key, you can sign messages so that those people will know they could only have come from you. And if you know someone else's public key, you can decode a message signed by them, and know that it only came from them.

It should be clear by now that public key cryptography becomes more useful, the more people know your public key. It should also be apparent that you need to keep your private key very safe. If someone else gets a copy of your private key, they can pretend to be you, and sign messages claiming that they were written by you. PGP has a feature that lets you "revoke" a private key, and warn people it's no longer trustable, but it's not a great solution. The most important part of using a public key cryptography system is to guard your private key very carefully.

How PGP Works

Pretty Good Privacy is mostly concerned with the minutiae of creating and using public and private keys. You can create a public/private key pair with it, protect the private key with a password, and use it and your public key to sign and encrypt text. It will also let you download other people's public keys, and upload your public keys to "public key servers," which are repositories where other people can find your key. See our guides to installing PGP-compatible software in your email software.

> *If there's one thing you need to take away from this overview, it's this: you should keep your private key stored somewhere safe, and protected with a long password. You can give your public key to anyone you want to communicate with you, or who wants to learn whether a message truly came from you.*

Advanced PGP: The Web of Trust

You may have spotted a potential flaw in how public key cryptography works. Suppose I started distributing a public key that I say belongs to Barack Obama. If people believed me, they might start sending secret messages to Barack, encrypted using the key. Or they might believe anything signed with that key is a sworn statement of Barack. This is quite rare, and yet it has actually happened to some people in real life, including to some of the authors of this document—some people writing to them have been fooled! (We don't know for sure in these instances whether or not some of the people who make the fake keys were really able to intercept the messages in transit and read them, or whether it was the equivalent of a prank to make it more inconvenient for people to have a secure conversation.)

Another sneaky attack is for an attacker to sit between two people talking online, eavesdropping on their entire conversation, and occasionally inserting the attackers own misleading messages into the conversation. Thanks to the design of the Internet as a system that ferries messages across many different computers and private parties, this attack is entirely possible. Under these conditions (called a “man-in-the-middle attack”), exchanging keys without prior agreement can get very risky. “Here's my key,” announces a person who sounds like Barack Obama, and sends you a public key file. But what's to say someone didn't wait until that moment, jam the transmission of Obama's key, and then insert his or her own?

How do we prove that a certain key really does belong to a certain person? One way is to get the key from them directly, but that's not much better than our original challenge of getting a secret key without someone spotting us. Still, people do exchange public keys when they meet, privately and at public cryptoparties.

PGP has a slightly better solution called the “web of trust.” In the web of trust, if I believe a key belongs to a certain person, I can sign that key, and then upload the key (and the signature) to the public key servers. These key servers will then pass out the signed keys to anyone who asks for them.

Roughly speaking, the more people who I trust that have signed a key, the more likely it is that I will believe that key really belongs to who it claims. PGP lets you sign other people's keys, and also lets you trust other signers, so that if they sign a key, your software will automatically believe that key is valid.

The web of trust comes with its own challenges, and organizations like EFF are currently investigating better solutions. But for now, if you want an alternative to handing keys to one another in person, using the web of trust and the public key server network are your best option.

Metadata: What PGP Can't Do

PGP is all about making sure the contents of a message are secret, genuine, and untampered with. But that's not the only privacy concern you might have. As we've noted, information *about* your messages can be as revealing as their contents (See "metadata"). If you're exchanging PGP messages with a known dissident in your country, you may be in danger for simply communicating with them, even without those messages being decoded. Indeed, in some countries you can face imprisonment simply for refusing to decode encrypted messages.

> *PGP does nothing to disguise who you are talking to, or that you are using PGP to do so. Indeed, if you upload your public key onto the keyservers, or sign other people's keys, you're effectively showing the world what key is yours, and who you know.*

You don't have to do that. You can keep your PGP public key quiet, and only give it to people you feel safe with, and tell them not to upload it to the public keyservers. You don't need to attach your name to a key.

Disguising that you are communicating with a particular person is more difficult. One way to do this is for both of you to use anonymous email accounts, and access them using Tor. If you do this, PGP will still be useful, both for keeping your email messages private from others, and proving to each other that the messages have not been tampered with.

Protecting Yourself on Social Networks

Social networking sites are some of the most popular websites and tools we use on the Internet. Facebook, Google+, and Twitter have hundreds of millions of users each.

Social networks are often built on the idea of sharing posts, photographs, and personal information. Yet they have also become forums for organizing and speech—much of which relies on privacy and pseudonymity. Thus, the following questions are important to consider when using social networks: How can I interact with these sites while protecting myself? My basic privacy? My identity? My contacts and associations? What information do I want keep private and who do I want to keep it private from?

Depending on your circumstances, you may need to protect yourself against the social media site itself, against other users of the site, or both.

Here are some tips to keep in mind when you're setting up your account:

Registering for a Social Media Site

- Do you want to use your real name? Some social media sites have so-called "real name policies," but these have become more lax over time. If you do not want to use your real name when registering for a social media site, do not.
- When you register, don't provide more information than is necessary. If you are concerned with hiding your identity, *use a separate email address*. Be aware that your IP address may be logged at registration.
- *Choose a strong password* and, if possible, enable two-factor authentication.
- Beware of password recovery questions whose answers can be mined from your social media details. For example: "What city were you born in?" or "What is the name of your pet?" You may want to choose password recovery answers that are false. One good way to remember the answers to password recovery questions, should you choose to use false answers for added security, is to note your chosen answers in a password safe.

Check the Social Media Site's Privacy Policy

Remember that information stored by third parties is subject to their own policies and may be used for commercial purposes or shared with other companies, for example, marketing firms. We know that reading privacy policies is a near-impossible task, but you may want to take a look at sections on how your data is used, when it is shared with other parties, and how the service responds to law enforcement requests.

Social networking sites, usually for-profit businesses, often collect sensitive information beyond what you explicitly input—where you are, what interests and advertisements you react to, what other sites you've visited (e.g. through "Like" buttons). It can be helpful to block third-party cookies and use tracker-blocking browser extensions to make sure extraneous information isn't being passively transmitted to third parties.

Some social networking sites, like Facebook and Twitter, have business relationships with data brokers in order to target advertisements more effectively. EFF has guides that walk you through how to opt-out of these tracking schemes:

- How to opt-out of Facebook's data broker relationships
- How to opt-out of Twitter's data broker relationships

Change Your Privacy Settings

Specifically, change the default settings. For example, do you want to share your posts with the public, or only with a specific group of people? Should people be able to find you using your email address or phone number? Do you want your location shared automatically?

- How to change your Facebook privacy settings

Remember, privacy settings are subject to change. Sometimes, these privacy settings get stronger and more granular; sometimes not. Be sure to pay attention to these changes closely to see if any information that was once private will be shared, or if any additional settings will allow you to take more control of your privacy.

Your Social Graph

Remember that you're not the only person who can give away potentially sensitive data about yourself**.** Your friends can tag you in photos, report your location, and make their connections to you public in a variety of ways. You may have the option of untagging yourself from these posts, but privacy does not work retroactively. You may want to talk to your friends about what you do and do not feel comfortable having them share about you in public.

The Problem with Mobile Phones

Mobile phones have become ubiquitous and basic communications tools—now used not only for phone calls, but also for accessing the Internet, sending text messages, and documenting the world.

Unfortunately, mobile phones were not designed for privacy and security. Not only do they do a poor job of protecting your communications, they also expose you to new kinds of surveillance risks—especially location tracking. Most mobile phones give the user much less control than a personal desktop or laptop computer would; it's harder to replace the operating system, harder to investigate malware attacks, harder to remove or replace undesirable bundled software, and harder to prevent parties like the mobile operator from monitoring how you use the device. What's more, the device maker may declare your device obsolete and stop providing you with software updates, including security fixes; if this happens, you may not have anywhere else to turn for these fixes.

Some of these problems can be addressed by using third-party privacy software—but some of them can't. Here, we'll describe some of the ways that phones can aid surveillance and undermine their users' privacy.

Location Tracking

The deepest privacy threat from mobile phones—yet one that is often completely invisible—is the way that they announce your whereabouts all day (and all night) long through the signals they broadcast. There are at least four ways that an individual phone's location can be tracked by others.

1. Mobile Signal Tracking — Towers

In all modern mobile networks, the operator can calculate where a particular subscriber's phone is located whenever the phone is powered on and registered with the network. The ability to do this results from the way the mobile network is built, and is commonly called triangulation.

One way the operator can do this is to observe the signal strength that different towers observe from a particular subscriber's mobile phone, and then calculate where that phone must be located in order to account for these observations. The accuracy with which the operator can figure out a subscriber's location varies depending on many factors, including the technology the operator uses and how many cell towers they have in an area. Very often, it is accurate to about the level of a city block, but in some systems it can be more accurate.

There is no way to hide from this kind of tracking as long as your mobile phone is powered on and transmitting signals to an operator's network. Although normally only the mobile operator itself can perform this kind of tracking, a government could force the operator to turn over location data about a user (in real-time or as a matter of historical record). In 2010, a German privacy advocate named Malte Spitz used privacy laws to get his mobile operator to turn over the records that it had about his records; he chose to publish them as an educational resource so that other people could understand how mobile operators can monitor users this way. (You can visit here to see what the operator knew about him.) The possibility of government access to this sort of data is not theoretical: it is already being widely used by law enforcement agencies in countries like the United States.

Another related kind of government request is called a tower dump; in this case, a government asks a mobile operator for a list of *all of the mobile devices* that were present in a certain area at a certain time. This could be used to investigate a crime, or to find out who was present at a particular protest. (Reportedly, the Ukrainian government used a tower dump for this purpose in 2014, to make a list of all of the people whose mobile phones were present at an anti-government protest.)

Carriers also exchange data with one another about the location from which a device is currently connecting. This data is frequently somewhat less precise than tracking data that aggregates multiple towers' observations, but it can still be used as the basis for services that track an individual device—including commercial services that query these records to find where an individual phone is currently connecting to the mobile network, and make the results available to governmental or private customers. (The *Washington Post* reported on how readily available this tracking information has become.) Unlike the previous tracking methods, this tracking does not involve forcing carriers to turn over user data; instead, this technique uses location data that has been made available on a commercial basis.

2. Mobile Signal Tracking — IMSI Catcher

A government or another technically sophisticated organization can also collect location data directly, such as with an IMSI catcher (a portable fake cell phone tower that pretends to be a real one, in order to "catch" particular users' mobile phones and detect their physical presence and/or spy on their communications). IMSI refers to the International Mobile Subscriber Identity number that identifies a particular subscriber's SIM card, though an IMSI catcher may target a device using other properties of the device as well.

The IMSI catcher needs to be taken to a particular location in order to find or monitor devices at that location. Currently there is no reliable defense against all IMSI catchers. (Some apps claim to detect their presence, but this detection is imperfect.) On devices that permit it, it could be helpful to disable 2G support (so that the device can connect only to 3G and 4G networks) and to disable roaming if you don't expect to be traveling outside of your home carrier's service area. These measures can protect against certain kinds of IMSI catchers.

3. Wi-Fi and Bluetooth Tracking

Modern smartphones have other radio transmitters in addition to the mobile network interface. They usually also have Wi-Fi and Bluetooth support. These signals are transmitted with less power than a mobile signal and can normally be received only within a short range (such as within the same room or the same building), although sometimes using a sophisticated antenna allows these signals to be detected from unexpectedly long distances; in a 2007 demonstration, an expert in Venezuela received a Wi-Fi signal at a distance of 382 km or 237 mi, under rural conditions with little radio interference. Both of these kinds of wireless signals include a unique serial number for the device, called a MAC address, which can be seen by anybody who can receive the signal. The device manufacturer chooses this address at the time the device is created and it cannot be changed using the software that comes with current smartphones.

Unfortunately, the MAC address can be observed in wireless signals even if a device is not actively connected to a particular wireless network, or even if it is not actively transmitting data. Whenever Wi-Fi is turned on on a typical smartphone, the smartphone will transmit occasional signals that include the MAC address and thus let others nearby recognize that that particular device is present. This has been used for commercial tracking applications, for example to let shopkeepers determine statistics about how often particular customers visit and how long they spend in the shop. As of 2014, smartphone manufacturers have started to recognize that this kind of tracking is problematic, but it may not be fixed in every device for years—if ever.

In comparison to GSM monitoring, these forms of tracking are not necessarily as useful for government surveillance. This is because they work best at short distances and require prior knowledge or observation to determine what MAC address is built into a particular person's device. However, these forms of tracking can be a highly accurate way to tell when a person enters and leaves a building. Turning off Wi-Fi and Bluetooth on a smartphone can prevent this type of tracking, although this can be inconvenient for users who want to use these technologies frequently.

Wi-Fi network operators can also see the MAC address of every device that joins their network, which means that they can recognize particular devices over time, and tell whether you are the same person who joined the network in the past (even if you don't type your name or e-mail address anywhere or sign in to any services).

On a few devices, it is physically possible to change the MAC address so that other people can't recognize your Wi-Fi device as easily over time; on these devices, with the right software and configuration, it would be possible to choose a new and different MAC address every day, for example. On smartphones, this commonly requires special software such as a MAC address-changing app. Currently, this option is not available for the majority of smartphone models.

4. Location Information Leaks From Apps and Web Browsing

Modern smartphones provide ways for the phone to determine its own location, often using GPS and sometimes using other services provided by location companies (which usually ask the company to guess the phone's location based on a list of cell phone towers and/or Wi-Fi networks that the phone can see from where it is). Apps can ask the phone for this location information and use it to provide services that are based on location, such as maps that show you your position on the map.

Some of these apps will then transmit your location over the network to a service provider, which, in turn, provides a way for other people to track you. (The app developers might not have been motivated by the desire to track users, but they might still end up with the ability to do that, and they might end up revealing location information about their users to governments or hackers.) Some smartphones will give you some kind of control over whether apps can find out your physical location; a good privacy practice is to try to restrict which apps can see this information, and at a minimum to make sure that your location is only shared with apps that you trust and that have a good reason to know where you are.

In each case, location tracking is not only about finding where someone is right now, like in an exciting movie chase scene where agents are pursuing someone through the streets. It can also be about answering questions about people's historical activities and also about their beliefs, participation in events, and personal relationships. For example, location tracking could be used to try to find out whether certain people are in a romantic relationship, to find out who attended a particular meeting or who was at a particular protest, or to try and identify a journalist's confidential source.

The *Washington Post* reported in December 2013 on NSA location-tracking tools that collect massive amounts of information "on the whereabouts of cellphones around the world," mainly by tapping phone companies' infrastructure to observe which towers particular phones connect to when. A tool called CO-TRAVELER uses this data to find relationships between different people's movements (to figure out which people's devices seem to be traveling together, as well as whether one person appears to be following another).

Turning Phones off

There's a widespread concern that phones can be used to monitor people even when not actively being used to make a call. As a result, people having a sensitive conversation are sometimes told to turn their phones off entirely, or even to remove the batteries from their phones.

The recommendation to remove the battery seems to be focused mainly on the existence of malware that makes the phone appear to turn off upon request (finally showing only a

blank screen), while really remaining powered on and able to monitor conversations or invisibly place or receive a call. Thus, users could be tricked into thinking they had successfully turned off their phones when they actually hadn't. Such malware does exist, at least for some devices, though we have little information about how well it works or how widely it has been used.

Turning phones off has its own potential disadvantage: if many people at one location all do it at the same time, it's a sign to the mobile carriers that they all thought something merited turning their phones off. (That “something” might be the start of a film in a movie theater, or the departure of a plane at an airport, but it might also be a sensitive meeting or conversation.) An alternative that might give less information away is to leave everybody's phone in another room where the phones' microphones wouldn't be able to overhear the conversations.

Burner Phones

Phones that are used temporarily and then discarded are often referred to as burner phones or burners. People who are trying to avoid government surveillance sometimes try to change phones (and phone numbers) frequently to make it more difficult to recognize their communications. They will need to use prepaid phones (not associated with a personal credit card or bank account) and ensure that the phones and SIM cards were not registered with their identity; in some countries these steps are straightforward, while in others there may be legal or practical obstacles to obtaining anonymous mobile phone service.

There are a number of limitations to this technique.

> *First, merely swapping SIM cards or moving a SIM card from one device to another offers minimal protection, because the mobile network observes both the SIM card and device together. In other words, the network operator knows the history of which SIM cards have been used in which devices, and can track either individually or both together. Second, governments have been developing mobile location analysis techniques where location tracking can be used to generate leads or hypotheses about whether multiple devices actually belong to the same person.*

There are many ways this can be done. For example, an analyst could check whether two devices tended to move together, or whether, even if they were in use at different times, they tended to be carried in the same physical locations.

A further problem for the successful anonymous use of telephone services is that people's calling patterns tend to be extremely distinctive. For example, you might habitually call your family members and your work colleagues. Even though each of these people receive calls from a wide range of people, you're likely the only person in the world who commonly calls both of them from the same number. So even if you suddenly changed

your number, if you then resumed the same patterns in the calls you made or received, it would be straightforward to determine which new number was yours. Remember that this inference isn't made based only on the fact that you called one particular number, but rather on the uniqueness of the combination of all the numbers that you called. (Indeed, *The Intercept* reported that a secret U.S. government system called PROTON does exactly this, using phone records to recognize people who placed phone calls in a "similar manner to a specific target" from new phone numbers.) An additional example can be found in the Hemisphere FOIA document. The document describes the Hemisphere database (a massive database of historical call records) and how the people who run it have a feature that can link burner phones by following the similarity of their call patterns. The document refers to burner phones as "dropped phones" because their user will "drop" one and start using another one—but the database analytics algorithms can draw the connection between one phone and another when this happens, so long as both were used to make or receive calls to similar sets of phone numbers.

Together, these facts mean that effective use of burner phones to hide from government surveillance requires, at a minimum: not reusing either SIM cards or devices; not carrying different devices together; not creating a physical association between the places where different devices are used; and not calling or being called by the same people when using different devices. (This isn't necessarily a complete list; for example, we haven't considered the risk of physical surveillance of the place where the phone was sold, or the places where it's used, or the possibility of software to recognize a particular person's voice as an automated method for determining who is speaking through a particular phone.)

A Note About GPS

The Global Positioning System (GPS) lets devices anywhere in the world figure out their own locations quickly and accurately. GPS works based on analyzing signals from satellites that are operated by the U.S. government as a public service for everyone. It's a common misconception that these satellites somehow watch GPS users or know where the GPS users are. In fact, the GPS satellites only transmit signals; the satellites don't receive or observe anything from your phone, and the satellites and GPS system operators do not know where any particular user or device is located, or even how many people are using the system.

This is possible because the individual GPS receivers (like those inside smartphones) calculate *their own positions* by determining how long it took the radio signals from different satellites to arrive.

So, why do we speak of "GPS tracking"? Usually, this tracking is done by apps running on a smartphone. They ask the phone's operating system for its location (determined via GPS). Then the apps are able to transmit this information to someone else over the Internet. There are also tiny GPS-receiving devices that can be surreptitiously hidden in someone's possessions or attached to a vehicle; those receivers determine their own

location and then actively retransmit it over a network, usually the mobile phone network.

Spying on Mobile Communications

Mobile phone networks were not originally designed to use technical means to protect subscribers' calls against eavesdropping. That meant that anybody with the right kind of radio receiver could listen in on the calls.

The situation is somewhat better today, but sometimes only slightly. Encryption technologies have been added to mobile communications standards to try to prevent eavesdropping. But many of these technologies have been poorly designed (sometimes deliberately, due to government pressure not to use strong encryption!). They have been unevenly deployed, so they might be available on one carrier but not another, or in one country but not another, and have sometimes been implemented incorrectly. For example, in some countries carriers do not enable encryption at all, or they use obsolete technical standards. This means it is often still possible for someone with the right kind of radio receiver to intercept calls and text messages as they're transmitted over the air.

Even when the best industry standards are being used—as they are in some countries and on some mobile carriers—there are still people who can listen in. At a minimum, the mobile operators themselves have the ability to intercept and record all of the data about who called or texted whom, when, and what they said. This information might be available to local or foreign governments through official or informal arrangements. In some cases, foreign governments have also hacked mobile operators' systems in order to get secret access to users' data. Also, IMSI catchers (described above) can be used by someone physically nearby you. These can trick your phone into using their fake "tower" instead of your mobile operator's legitimate infrastructure, in which case the person operating the IMSI catcher may be able to intercept your communications.

The safest practice is to assume that traditional calls and SMS text messages have not been secured against eavesdropping or recording. Even though the technical details vary significantly from place to place and system to system, the technical protections are often weak and can be bypassed in many situations. *See Communicating with Others to learn how to text and talk more securely.*

The situation can be different when you are using secure communications apps to communicate (whether by voice or text), because these apps can apply encryption to protect your communications. This encryption can be stronger and can provide more meaningful protections. The level of protection that you get from using secure communications apps to communicate depends significantly on which apps you use and how they work. One important question is whether a communications app uses end-to-end encryption to protect your communications and whether there's any way for the app developer to undo or bypass the encryption.

Infecting Phones with Malware

Phones can get viruses and other kinds of malware (malicious software), either because the user was tricked into installing malicious software, or because someone was able to hack into the device using a security flaw in the existing device software. As with other kinds of computing device, the malicious software can then spy on the device's user.

For example, malicious software on a mobile phone could read private data on the device (like stored text messages or photos). It could also activate the device's sensors (such as microphone, camera, GPS) to find where the phone is or to monitor the environment, even turning the phone into a bug.

This technique has been used by some governments to spy on people through their own phones, and has created anxiety about having sensitive conversations when mobile phones are present in the room. Some people respond to this possibility by moving mobile phones into another room when having a sensitive conversation, or by powering them off. (Governments themselves often forbid people, even government employees, from bringing personal cell phones into certain sensitive facilities—mainly based on the concern that the phones could be infected with software to make them record conversations.)

A further concern is that malicious software could theoretically make a phone pretend to power off, while secretly remaining turned on (and showing a black screen, so that the user wrongly believes that the phone is turned off). This concern has led to some people physically removing the batteries from their devices when having very sensitive conversations.

As we discussed above, precautions based on powering off phones could be noticed by a mobile operator; for example, if ten people all travel to the same building and then all switch off their phones at the same time, the mobile operator, or somebody examining its records, might conclude that those people were all at the same meeting and that the participants regarded it as sensitive. This would be harder to detect if the participants had instead left their phones at home or at the office.

Forensic Analysis of Seized Phones

There is a well-developed specialty of forensic analysis of mobile devices. An expert analyst will connect a seized device to a special machine, which reads out data stored inside the device, including records of previous activity, phone calls, and text messages. The forensic analysis may be able to recover records that the user couldn't normally see or access, such as deleted text messages, which can be undeleted. Usually forensic analysis can bypass simple forms of screen locking.

There are many smartphone apps and software features that try to inhibit or prevent forensic analysis of certain data and records, or to encrypt data to make it unreadable to

an analyst. In addition, there is remote wipe software, which allows the phone owner or someone designated by the owner to tell the phone to erase certain data on request.

This software can be useful to protect against data being obtained if your phone is taken by criminals. However, please note that intentional destruction of evidence or obstruction of an investigation can be charged as a separate crime, often with very serious consequences. In some cases, this can be easier for the government to prove and allow for more substantial punishments that the alleged crime originally being investigated.

Computer Analysis of Patterns of Phone use

Governments have also become interested in analyzing data about many users' phones by computer in order to find certain patterns automatically. These patterns could allow a government analyst to find cases in which people used their phones in an unusual way, such as taking particular privacy precautions.

A few examples of things that a government might try to figure out from data analysis: automatically figuring out whether people know each other; detecting when one person uses multiple phones, or switches phones; detecting when groups of people are traveling together or regularly meeting one another; detecting when groups of people use their phones in unusual or suspicious ways; identifying the confidential sources of a journalist.

Attending Protests (United States)

With the proliferation of personal technologies, protesters of all political persuasions are increasingly documenting their protests—and encounters with the police—using electronic devices like cameras and mobile phones. In some cases, getting that one shot of the riot police coming right at you posted somewhere on the Internet is an exceptionally powerful act and can draw vital attention to your cause.

The following are useful tips for you to remember if you find yourself at a protest and are concerned about protecting your electronic devices if or when you're questioned, detained, or arrested by police. Remember that these tips are general guidelines, so if you have specific concerns, please talk to an attorney.

Protect your Phone Before you Protest

Think carefully about what's on your phone before bringing it to a protest.

Your phone contains a wealth of private data, which can include your list of contacts, the people you have recently called, your text messages and email, photos and video, GPS location data, your web browsing history and passwords or active logins, and the contents of your email and social media accounts. Through stored passwords, access to the device can allow someone to obtain yet even more information on remote servers.

The United States Supreme Court recently held that the police are required to get a warrant to obtain this information when someone is arrested, but the exact limits of that ruling are still being examined. In addition, sometimes law enforcement will seek to seize a phone because they believe it contains evidence of a crime (such as photos you may have taken of the protest), or as part of a vehicle search. They can then later get a warrant to examine the phone that they've already seized.

To protect your rights, you may want to harden your existing phone against searches. You should also consider bringing a throwaway or alternate phone to the protest that does not contain sensitive data, which you've never used to log in to your communications or social media accounts, and which you would not mind losing or parting with for a while. If you have a lot of sensitive or personal information on your phone, the latter might be a better option.

Password-protection and encryption options: Always password-protect your phone. Be aware that merely password-protecting or locking your phone is *not* an effective barrier to expert forensic analysis. Android and iPhone both provide options for full-disk encryption on their operating systems, and you should use them, though the safest option remains leaving the phone elsewhere.

One problem with mobile phone encryption is that on Android the same password is used for disk encryption and screen unlocking. This was a bad design, because it forces the user to either select a too-weak password for the encryption, or to type a too-long and inconvenient password for the screen. The best compromise may be 8-12 fairly random characters that are nonetheless easy to type quickly on your particular device. Or if you have root access to your Android phone and know how to use a shell, read here. *(See also "Communicating with Others" for details on how to encrypt text and voice calls.)*

Back up your data: It's important that you frequently back up the data stored on your phone, especially if your device lands into the hands of a police officer. You may not get your phone back for a while (if at all) and it is possible that its contents may be deleted, whether intentional or not. While we believe it would be improper for the police to delete your information, there's a chance it could happen.

> *For similar reasons, consider writing one important, but non-incriminating phone number on your body with a permanent marker in case you lose your phone, but are permitted to make a call.*

Cell site location information: If you take your mobile phone with you to a protest, it makes it easy for the government to figure out that you are there by seeking the information from your provider. (We believe that the law requires the government obtain an individualized warrant to obtain location information, but the government disagrees). If you need to keep the fact of your participation in a protest from the government do not take your mobile phone with you. If you absolutely must bring a mobile phone with you, try to bring one that is not registered in your name.

You may not be able to reach colleagues if you are detained. You may want to plan a pre-arranged call after the protest with a friend—if they don't hear from you, they can assume you've been arrested.

You're at the Protest – now What?

Maintain control over your phone: Maintaining control might mean keeping your phone on you at all times, or handing it over to a trusted friend if you are engaging in action that you think might lead to your arrest.

Consider taking pictures and video: Just knowing that there are cameras documenting the event can be enough to discourage police misconduct during the protest. EFF believes that you have the First Amendment right to document public protests, including police action. However, please understand that the police may disagree, citing various local and state laws. If you plan to record audio, you should review this helpful guide, the Reporter's Committee for Freedom of the Press' Can We Tape?.

If you want to keep your identity and location secret, make sure to strip all metadata off of your photos before you post them.

In other circumstances, metadata can be useful for demonstrating the credibility of evidence collected at a protest. The Guardian Project makes a tool called InformaCam that allows you to store metadata along with including information about the user's current GPS coordinates, altitude, compass bearing, light meter readings, the signatures of neighboring devices, cell towers, and WiFi networks; and serves to shed light on the exact circumstances and contexts under which the digital image was taken.

If you take photos or video, the police may also seek to seize your phone to obtain the material as evidence. If you are engaged in journalism, you may be able to assert the reporter's privilege to protect your unpublished material. The RCFP has a guide explaining the Reporter's Privilege in various states.

If you are concerned about being identified, cover your face so that you cannot be identified from photos. Masks may get you into trouble in some locations due to anti-mask laws.

Help! Help! I'm Being Arrested

> *Remember that you have a right to remain silent—about your phone and anything else.*

If questioned by police, you can politely but firmly ask to speak to your attorney and politely but firmly request that all further questioning stop until your attorney is present. It is best to say nothing at all until you have a chance to talk to a lawyer. However, if you do decide to answer questions, be sure to tell the truth. It is likely a crime to lie to a police officer and you may find yourself in more trouble for lying to law enforcement than for whatever it was they wanted on your computer.

If the police ask to see your phone, you can tell them you do not consent to the search of the device. They might still be able to search your phone with a warrant after they arrest you, but at least it's clear that you did not give them permission to do so.

If the police ask for the password to your electronic device (or ask you to unlock it), you can politely refuse to provide it and *ask to speak to your lawyer*. If the police ask if a phone is yours, you can tell them that it is lawfully in your possession without admitting or denying ownership or control. Every arrest situation is different, and you will need an attorney to help you sort through your particular circumstance.

Ask your attorney about the Fifth Amendment, which protects you from being forced to give the government self-incriminating testimony. If turning over an encryption key or password triggers this right, not even a court can force you to divulge the information. If turning over an encryption key or password will reveal to the government information it does not have (such as demonstrating that you have control over files on a computer), there is a strong argument that the Fifth Amendment protects you. If, however, turning

over passwords and encryption keys will not result in a "testimonial act," for instance demonstrating that you have control over the data, then the Fifth Amendment may not protect you. Your
attorney can help you figure out how this applies in a particular situation.

And just because the police cannot compel you to give up your password, doesn't mean that they can't pressure you. The police may detain you and you may go to jail rather than being immediately released if they think you're refusing to be cooperative. You will need to decide whether to comply.

The Police Have my Phone, How do I Get it Back?

If your phone or electronic device was illegally seized, and is not promptly returned when you are released, you can have your attorney file a motion with the court to have your property returned. If the police believe that evidence of a crime was found on your electronic device, including in your photos or videos, the police can keep it as evidence. They may also attempt to make you forfeit your electronic device, but you can challenge that in court.

Cell phones and other electronic devices are an essential component of 21st century protests. Everyone in the United States, both citizens and non-citizens, can and should exercise their First Amendment right to free speech and assembly, and hopefully the above tips can be a useful guide for you to intelligently manage the risks to your property and privacy.

How to: Delete Your Data Securely on Mac OS X

Most of us think that a file on our computer is deleted once we put the file in our computer's trash folder and empty the trash; in reality, deleting the file does not completely erase it. When one does this, the computer just makes the file invisible to the user and marks the part of the disk that the file was stored on as "available"—meaning that your operating system can now write over the file with new data. Therefore, it may be weeks, months, or even years before that file is overwritten with a new one. Until this happens, that "deleted" file is still on your disk; it's just invisible to normal operations. And with a little work and the right tools (such as "undelete" software or forensic methods), you can even still retrieve the "deleted" file. The bottom line is that computers normally don't "delete" files; they just allow the space those files take up to be overwritten by something else some time in the future.

The best way to delete a file forever, then, is to make sure it gets overwritten immediately, in a way that makes it difficult to retrieve what used to be written there. Your operating system probably already has software that can do this for you—software that can overwrite all of the "empty" space on your disk with gibberish and thereby protect the confidentiality of deleted data.

Note that securely deleting data from solid state drives (SSDs), USB flash drives, and SD cards is very hard! The instructions below apply *only* to traditional disk drives, and *not* to SSDs, which are becoming standard in modern laptops, USB keys/USB thumb drives, or SD cards/flash memory cards.

This is because these types or drives use a technique called wear leveling. (You can read more about why this causes problems for secure deletion here.)

If you're using an SSD or a USB flash drive, you can jump to the section below.

Secure Deletion on Mac OS X

On OS X 10.4 and above, you can securely delete files by moving them to the Trash, and then selecting Finder > Secure Empty Trash.

Ensuring Previously Deleted Data Cannot be Recovered

Apple's advice on preventing forensic undeletion on Mac OS X is as follows:

To prevent the recovery of files you've deleted, open Disk Utility (in Applications/Utilities), choose Help > Disk Utility Help, and search for help on erasing free disk space.

A Warning About the Limitations of Secure Deletion Tools

First, remember that the advice above only deletes files on the disk of the computer you're using. None of the tools above will delete backups that were made to somewhere else on your computer, another disk or USB drive, a "Time Machine," on an email server, or in the cloud. In order to securely delete a file, you must delete *every copy* of that file, *everywhere it was stored or sent*. Additionally, once a file is stored in the cloud (e.g. via Dropbox or some other file-sharing service) then there's usually no way to guarantee that it will be deleted forever.

Unfortunately, there's also another limitation to secure deletion tools. Even if you follow the advice above and you've deleted all copies of a file, there is a chance that certain traces of deleted files may persist on your computer, not because the files themselves haven't been properly deleted, but because some part of the operating system or some other program keeps a deliberate record of them.

There are many ways in which this could occur, but two examples should suffice to convey the possibility. On Windows or Mac OS, a copy of Microsoft Office may retain a reference to the name of a file in the "Recent Documents" menu, even if the file has been deleted (Office might sometimes even keep temporary files containing the contents of the file). On a Linux or other *nix system, OpenOffice may keep as many records as Microsoft Office, and a user's shell history file may contain commands that include the file's name, even though the file has been securely deleted. In practice, there may be dozens of programs that behave like this.

It's hard to know how to respond to this problem. It is safe to assume that even if a file has been securely deleted, its name will probably continue to exist for some time on your computer. Overwriting the entire disk is the only way to be 100% sure the name is gone. Some of you may be wondering, "Could I search the raw data on the disk to see if there are any copies of the data anywhere?" The answer is yes and no. Searching the disk (e.g. by using a command like `grep -ab /dev/` on Linux) will tell you if the data is present in plaintext, but it won't tell you if some program has compressed or otherwise coded references to it. Also be careful that the search itself does not leave a record! The probability that the file's contents may persist is lower, but not impossible. Overwriting the entire disk and installing a fresh operating system is the only way to be 100% certain that records of a file have been erased.

Secure Deletion When Discarding Old Hardware

If you want to finally throw a piece of hardware away or sell it on eBay, you'll want to make sure no one can retrieve your data from it. Studies have repeatedly found that computer owners usually fail to do this—hard drives are often resold chock-full of highly

sensitive information. So, before selling or recycling a computer, be sure to overwrite its storage media with gibberish first. And even if you're not getting rid of it right away, if you have a computer that has reached the end of its life and is no longer in use, it's also safer to wipe the hard drive before stashing the machine in a corner or a closet. Darik's Boot and Nuke is a tool designed for this purpose, and there are a variety of tutorials on how to use it across the web, (including here).

Some full-disk encryption software has the ability to destroy the master key, rendering a hard drive's encrypted contents permanently incomprehensible. Since the key is a tiny amount of data and can be destroyed almost instantaneously, this represents a much faster alternative to overwriting with software like Darik's Boot and Nuke, which can be quite time-consuming for larger drives. However, this option is only feasible if the hard drive was always encrypted. If you weren't using full-disk encryption ahead of time, you'll need to overwrite the whole drive before getting rid of it.

Discarding CD-ROMS

When it comes to CD-ROMs, you should do the same thing you do with paper—shred them. There are inexpensive shredders that will chew up CD-ROMs. Never just toss a CD-ROM out in the garbage unless you're absolutely sure there's nothing sensitive on it.

Secure Deletion on Solid-state Disks (SSDs), USB Flash Drives, and SD Cards

Unfortunately due to the way SSDs, USB flash drives, and SD cards work, it is difficult, if not impossible, to securely delete both individual files and free space. As a result your best bet in terms of protection is to use encryption—that way, even if the file is still on the disk, it will at least look like gibberish to anyone who gets ahold of it and can't force you to decrypt it. At this point in time, we cannot provide a good general procedure that will definitely remove your data from an SSD. If you want to know *why* it's so hard to delete data, read on.

As we mentioned above, SSDs and USB flash drives use a technique called wear leveling. At a high level, wear leveling works as follows. The space on every disk is divided into blocks, kind of like the pages in a book. When a file is written to disk, it's assigned to a certain block or set of blocks (pages). If you wanted to overwrite the file then all you would have to do is tell the disk to overwrite those blocks. But in SSDs and USB drives, erasing and re-writing the same block can wear it out. Each block can only be erased and rewritten a limited number of times before that block just won't work anymore (the same way if you keep writing and erasing with a pencil and paper, eventually the paper might rip and be useless). To counteract this, SSDs and USB drives will try to make sure that the amount of times each block has been erased and rewritten is about the same, so that the drive will last as long as possible (thus the term wear leveling). As a side effect, sometimes instead of erasing and writing the block a file was

originally stored on, the drive will instead leave that block alone, mark it as invalid, and just write the modified file to a different block. This is kind of like leaving the page in the book unchanged, writing the modified file on a different page, and then just updating the book's table of contents to point to the new page. All of this occurs at a very low level in the electronics of the disk, so the operating system doesn't even realize it's happened. This means, however, that even if you try to overwrite a file, there's no guarantee the drive will actually overwrite it—and that's why secure deletion with SSDs is so much harder.

How to: Use KeePassX

KeePassX is a password safe—a program you can use to store all your passwords for various websites and services. A password safe is a great tool because it allows you to use different difficult-to-guess passwords for all your services, without needing to remember them. Instead, you only need to remember one master password that allows you to decrypt a database of all your passwords. Password safes are convenient and allow you to organize all of your passwords in one location.

> *It should be noted that using a password safe creates a single point of failure and establishes an obvious target for bad actors or adversaries. Research has suggested that many commonly used passwords safes have vulnerabilities, so use caution when determining whether or not this is the right tool for you.*

Download location:

- For Windows/Mac: https://www.keepassx.org/downloads
- For Linux: via your distro's normal software distribution channels (i.e. Software Manager or Synaptic)

Computer requirements: Windows 2000 or higher, Mac OS X 10.4-10.9, Linux (most distros)

Versions used in this guide: KeePassX 0.4.3 (KeePassX is a cross-platform version of the Windows-only KeePass program.)

License: FOSS (primarily GPLv2)

Other Reading: https://www.keepassx.org/forum/

Level: Beginner

Time required: 5 minutes to setup, a lifetime of blissful strong password usage after that.

How KeePassX works

KeePassX works with files called password databases, which are exactly what they sound like—files that store a database of all your passwords. These databases are encrypted when they're stored on your computer's hard disk, so if your computer is off and someone steals it they won't be able to read your passwords.

Password databases can be encrypted via three methods: using a master password, using a keyfile, or both. Let's look at the pros and cons of each.

Using a Master Password

A master password acts like a key—in order to open the password database, you need the correct master password. Without it, nobody can see what's inside the password database. There are a few things to keep in mind when using a master password to secure your password database.

- *This password will decrypt all of your passwords, so it needs to be strong!* That means it shouldn't be something easy to guess, and it should also be long—the longer the better! Also, the longer it is, the less you need to worry about having special characters or capitals or numbers. A password that is only made up of six random words (in all lower case, with spaces in between) can be harder to break than a 12-character password made up of upper and lower case letters, numbers, and symbols.
- *You need to be able to remember this password!* Since this one password will allow access to all your other passwords, you need to be able to make sure you can remember it without writing it down. This is another reason to use something like Diceware—you can use regular words that are easy to remember, instead of trying to remember unnatural combinations of symbols and capital letters.

Using a Keyfile

Alternatively, you can use a keyfile to encrypt your password database. A keyfile acts the same way a password would—every time you want to decrypt your password database you will need to provide that keyfile to KeePassX. A keyfile should be stored on a USB drive or some other portable media, and only inserted into your computer when you want to open your password database. The benefit of this is that even if somebody gets access to your computer's hard disk (and thus your password database) they still won't be able to decrypt it without the keyfile stored in the external media. (Additionally, a keyfile can be much harder for an adversary to guess than a normal password.) The downside is that any time you want to access your password database, you'll need to have that external media handy (and if you lose it or it gets damaged, then you won't be able to open your password database).

Using a keyfile instead of a password is the closest thing to having an actual physical key to open your password database—all you need to do is insert your USB drive, select the keyfile, and presto! If you do choose to use a keyfile instead of a master password, though, make sure your USB drive is stored somewhere safe—*anyone who finds it will be able to open your password database*.

Using Both

The most secure method for encrypting your password database is to use both a master password and a keyfile. This way, your ability to decrypt your password database depends on *what you know* (your master password) and *what you have* (your keyfile)—and any malicious entity who wants to get access to your passwords will need both. (With that said, keep in mind your threat model—for most home users who just want to store their passwords, a strong master password should be sufficient. But if you're worried about protecting against state-level actors with access to huge computational resources, then the more security the better.)

Now that you understand how KeePassX works, let's get started with actually using it!

Getting Started with KeePassX

Once you've installed KeePassX, go ahead and launch it. Once it's started, select "New Database" from the File menu. A dialog will pop up which will ask you to enter a master password and/or use a keyfile. Select the appropriate checkbox(es) based on your choice. Note that if you want to see the password you're typing in (instead of obscuring it with dots) you can click the button with the "eye" to the right. Also note that you can use any existing file as a keyfile—an image of your cat for example, could be used as a keyfile. You'll just need to make sure the file you choose never gets modified, because if its contents are changed then it will no longer work for decrypting your password database. Also be aware that sometimes opening a file in another program can be enough to modify it; the best practice is to not open the file except to unlock KeePassX. (It is safe to move or rename the keyfile, though.)

Once you've successfully initialized your password database, you should save it by choosing "Save Database" from the File menu (Note that if you want, you can move the password database file later to wherever you like on your hard disk, or move it to other computers—you'll still be able to open it using KeePassX and the password/keyfile you specified before).

Organizing Passwords

KeePassX allows you to organize passwords into "Groups," which are basically just folders. You can create, delete, or edit Groups or Subgroups by going to the "Groups" menu in the menubar, or by right-clicking on a Group in the left-hand pane of the KeePassX window. Grouping passwords doesn't affect any of the functionality of KeePassX—it's just a handy organizational tool.

Storing/generating/editing Passwords

To create a new password or store a password you already have, right-click on the Group in which you want to store the password, and choose "Add New Entry" (you can also choose "Entries > Add New Entry" from the menubar). For basic password usage, do the following:

- Enter a descriptive title you can use to recognize this password entry in the "Title" field.
- Enter the username associated with this password entry in the "Username" field. (This can be blank if there is no username.)
- Enter your password in the "Password" field. If you're creating a new password (i.e. if you're signing up for a new website and you want to create a new, unique, random password) click the "Gen" button to the right. This will pop up a password generator dialog which you can use to generate a random password. There are several options in this dialog, including what sorts of characters to include and how long to make the password.
    - Note that if you generate a random password, it's not necessary that you remember (or even know!) what that password is! KeePassX stores it for you, and any time you need it you'll be able to copy/paste it into the appropriate program. This is the whole point of a password safe—you can use different long random passwords for *each* website/service, without even knowing what the passwords are!
    - Because of this, you should make the password as long as the service will allow and use as many different types of characters as possible.
    - Once you're satisfied with the options, click "Generate" in the lower right to generate the password, and then click "OK." The generated random password will automatically be entered in the "Password" and "Repeat" fields for you. (If you're not generating a random password, then you'll need to enter your chosen password again in the "Repeat" field.)
- Finally, click OK. Your password is now stored in your password database. To make sure the changes are saved, be sure to save the edited password database by going to "File > Save Database." (Alternatively, if you made a mistake, you can close and then re-open the database file and all changes will be lost.)

If you ever need to change/edit the stored password, you can just choose the Group it's in and then double-click on its title in the right-hand pane, and the "New Entry" dialog will pop up again.

Normal Use

In order to use an entry in your password database, simply right-click on the entry and choose "Copy Username to Clipboard" or "Copy Password to Clipboard," and then go to the window/website where you want to enter your username/password, and simply paste in the appropriate field (Instead of right-clicking on the entry, you can also double-click

on the username or password of the entry you want, and the username or password will be automatically copied to your clipboard).

Advanced Use

One of the most useful features of KeePassX is that it can automatically type in usernames and passwords for you into other programs when you press a special combination of keys on your keyboard. Note that although this feature is only available under Linux, other password safes like KeePass (on which KeePassX was based) support this feature on other operating systems, and it works similarly.

To enable this feature, do the following.

1. *Choose your global hotkey*. Choose "Settings" from the "Extras" menu, and then choose "Advanced" in the pane on the left. Click inside the "Global Auto-Type Shortcut" field, and then press the shortcut-key combination you wish to use. (For example, press and hold Ctrl, Alt, and Shift, and then hit "p." You can use any key combination you like, but you'll want to make sure that it doesn't conflict with hotkeys other applications use, so try to stay away from things like Ctrl+X or Alt+F4.) Once you're satisfied, click "OK."
2. *Setup auto-type for a specific password*. Make sure that you have the window open where you'll want to enter the password. Then go to KeePassX, find the entry for which you want to enable auto-type, and double-click on the entry's title to open up the "New Entry" dialog.
3. Click the "Tools" button in the bottom left, and select "Auto-Type: Select target window." In the dialog that pops up, expand the drop-down box and choose the title of the window in which you want the username and password to be entered. Click OK, and then click OK again.

Test it out! Now in order to autotype your username and password, go to the window/website where you want KeePassX to autotype your username/password for you. Make sure your cursor is in the text box for your username, and then hit the combination of keys you chose above for the global hotkey. As long as KeePassX is open (even if it's minimized or not focused) your username and password should automatically be entered.

Note that depending on how the website/window is set up, this feature may not work 100% correctly right off the bat. (It might enter the username but not the password, for example.) You can troubleshoot and customize this feature, though—for more information we recommend looking at the KeePass documentation here. (Although there are some differences between KeePass and KeePassX, that page should be enough to guide you in the right direction.)

It is recommended that you use a key combination that is difficult to hit accidentally. You don't want to accidentally paste your bank account password into a Facebook post!

Other Features

You can search your database by typing something in the search box (the text box in the toolbar of the main KeePassX window) and hitting enter.

You can also sort your entries by clicking on the column header in the main window.

You can also "lock" KeePassX by choosing "File > Lock Workspace," so that you can leave KeePassX open, but have it ask for your master password (and/or keyfile) before you can access your password database again. You can also have KeePassX automatically lock itself after a certain period of inactivity. This can prevent someone from accessing your passwords if you step away from your computer. To enable this feature, choose "Extras > Settings" from the menu and click on the security options. Then check the box that says "Lock database after inactivity of {number} seconds."

KeePassX can also store more than just usernames and passwords. For example, you can create entries to store important things like account numbers, or product keys, or serial numbers, or anything else. There's no requirement that the data you put in the "Password" field actually has to be a password. It can be anything you want—just input what you want to store in the "Password" field instead of an actual password (and leave the "Username" field blank if there's no username) and KeePassX will safely and securely remember it for you.

KeePassX is easy to use, robust software, and we recommend exploring the program to learn all of the useful things it can do.

How to: Circumvent Online Censorship

This is a short overview to circumventing online censorship, but is by no means comprehensive. For a more in-depth guide on how to circumvent online censorship, check out FLOSS Manuals' guide, Bypassing Censorship.

Many governments, companies, schools, and public access points use software to prevent Internet users from accessing certain websites and Internet services. This is called Internet filtering or blocking and is a form of censorship. Content filtering comes in different forms. Sometimes entire websites are blocked, sometimes individual web pages, and sometimes content is blocked based on keywords contained in it. One country might block Facebook entirely, or only block particular Facebook group pages—or it might block any page or web search with the words "falun gong" in it.

Regardless of how content is filtered or blocked, you can almost always get the information you need by using a circumvention tool. Circumvention tools usually work by diverting your web or other traffic through another computer, so that it bypasses the machines conducting the censorship. An intermediary service through which you channel your communications in this process is called a proxy.

Circumvention tools *do not* necessarily provide additional security or anonymity, even those that promise privacy or security, even ones that have terms like "anonymizer" in their names.

There are different ways of circumventing Internet censorship, some of which provide additional layers of security. The tool that is most appropriate for you depends on your threat model.

> *If you're not sure what your threat model is, start here.*

Basic Techniques

HTTPS is the secure version of the HTTP protocol used to access websites. Sometimes a censor will block the insecure version of a site only, allowing you to access that site simply by entering the version of the domain that starts with HTTPS. This is particularly useful if the filtering you're experiencing is based on keywords or only blocks individual web pages. HTTPS stops censors from reading your web traffic, so they cannot tell what keywords are being sent, or which individual web page you are visiting (*censors can still see the domain names of all websites you visit*).

If you suspect this type of simple blocking, try entering https:// before the domain in place of http://.

Try EFF's HTTPS Everywhere plug-in to automatically turn on HTTPS for those sites that support it.

Another way that you may be able to circumvent basic censorship techniques is by trying an alternate domain name or URL. For example, instead of visiting http://twitter.com, you might visit http://m.twitter.com, the mobile version of the site. Censors that block websites or web pages usually work from a blacklist of banned websites, so anything that is not on that blacklist will get through. They might not know of all the variations of a particular website's domain name—especially if the site knows it is blocked and registers more than one name.

Web-based Proxies

A web-based proxy (such as http://proxy.org/) is a good way of circumventing censorship. In order to use a web-based proxy, all you need to do is enter the filtered address that you wish to use; the proxy will then display the requested content.

Web-based proxies a good way to quickly access blocked websites, but often don't provide any security and will be a poor choice if your threat model includes someone monitoring your internet connection. Additionally, they will not help you to use other blocked non-webpage services such as your instant messaging program. Finally, web-based proxies themselves pose a privacy risk for many users, depending on their threat model, since the proxy will have a complete record of everything you do online.

Encrypted Proxies

There are numerous proxy tools that utilize encryption, providing an additional layer of security, as well as the ability to bypass filtering. Although the connection is encrypted, the tool provider may have your personal data, meaning that these tools do not provide anonymity. They are, however, more secure than a plain web-based proxy.

The simplest form of an encrypted web proxy is one that starts with "https"—this will use the encryption usually provided by secure websites. Ironically, in the process, the owners of these proxies will get to see the data you send to and from other secure websites, so be cautious.

Other tools use a hybrid approach—they act like a proxy, but contain elements of the encrypted services listed below. Examples of these tools include Ultrasurf and Psiphon.

Virtual Private Networks

A Virtual Private Network (VPN) encrypts and sends all Internet data between your computer and another computer. This computer could belong to a commercial or

nonprofit VPN service, your company, or a trusted contact. Once a VPN service is correctly configured, you can use it to access webpages, e-mail, instant messaging, VoIP and any other Internet service. A VPN protects your traffic from being intercepted locally, but your VPN provider can keep logs of your traffic (websites you access, and when you access them) or even provide a third party with the ability to snoop directly on your web browsing. Depending on your threat model, the possibility of a government listening in on your VPN connection or obtaining the logs may be a significant risk and, for some users, could outweigh the short-term benefits of using a VPN.

For information about specific VPN services, click here. Disclaimer: some VPNs with exemplary privacy policies could well be run by devious people. Do not use a VPN that you do not trust.

Tor

Tor is free and open-source software that is intended to provide you with anonymity, but which also allows you to circumvent censorship. When you use Tor, the information you transmit is safer because your traffic is bounced around a distributed network of servers, called onion routers. This could provide anonymity, since the computer with which you're communicating will never see your IP address, but instead will see the IP address of the last Tor router through which your traffic traveled.

When used with a couple of optional features (bridges and obfsproxy) Tor is the gold standard for secure censorship circumvention against a local state, since it will both bypass almost all national censorship, and if properly configured, protect your identity from an adversary listening in on your country's networks. It can be slow and hard to use, however.

To learn how to use Tor, click here

How to: Use Tor on Mac OS X

This guide outlines how to use the Tor Browser Bundle on OS X.

> **Computer requirements**: An internet connection, a computer running a recent version of Mac OS X
>
> **Versions used in this guide**: OS X; OS X 10.9.5; Tor Browser Bundle 4.0.8
>
> **License**: Free Software; mix of Free Software licenses
>
> **Other reading**: https://tor.stackexchange.com/
>
> **Level**: Beginner-Intermediate
>
> **Time required**: 15-30 minutes

What is Tor?

Tor is a volunteer-run service that provides both privacy and anonymity online by masking who you are and where you are connecting. The service also protects you from the Tor network itself.

For people who might need occasional anonymity and privacy when accessing websites, Tor Browser provides a quick and easy way to use the Tor network.

The easiest way to use the Tor network is to use the Tor Browser Bundle, which combines a web browser, the Tor software, and other helpful software that will give you a way of more securely accessing the web.

> *The Tor Browser works just like other web browsers, except that it sends your communications through Tor, making it harder for people who are monitoring you to know exactly what you're doing online, and harder for people monitoring the sites you use to know where you're connecting from. Keep in mind that only activities you do inside of Tor Browser itself will be anonymized. Having Tor Browser installed on your computer does not make things you do on the same computer using other software (such as your regular web browser) anonymous.*

Getting Tor Browser Bundle

Open a browser like Mozilla Firefox or Safari and type: https://www.torproject.org/download/download-easy.html.en in the URL bar. If you are

using a search engine to look for the Tor Browser Bundle, make sure that the URL is correct.

Click the big purple download button to get the installation program for Tor Browser Bundle.

The website will have detected your operating system and you'll get the correct file for OS X. If this fails you can click the link to the side of the purple button to download to the correct version.

If you are using Safari, the Tor Browser Bundle will start to download. In Firefox you will be asked whether you wish to open or save the file. It is always best to save the file, so click the Save button. This example shows Tor Browser Bundle Version 4.0.8, which was the most current version at the time this guide was published. There may be a more recent version available for download by the time you read this.

Installing Tor Browser Bundle

After the download is complete, you might get an option to open the folder where the file was downloaded to. The default location is the Downloads folder. Double-click on the file Torbrowser-4.0.8-osx32_en-US.dmg

A window will open asking you to install Tor Browser Bundle by dragging it to your applications folder. You may do so now.

Tor Browser is now installed in your applications folder.

Using Tor Browser Bundle

To open Tor Browser for the first time, locate it in the finder or in launchpad on newer versions of OS X.

After clicking on the Tor Browser icon, a window will open with a warning about the origin of the software. You should always take these warnings seriously and make sure you trust the software you want to install and that you got an authentic copy from the official site over a secure connection. Since you know what you want, and you know where to get the software, and the download was from the Tor Project's secure HTTPS site, click Open.

The first time Tor Browser starts, you'll get a window that allows you to modify some settings if necessary. You might have to come back and change some configuration settings, but go ahead and connect to the Tor network by clicking the Connect button.

After clicking “Connect,” a new window will open with a green bar that will get longer as the Tor software starts up.

The first time Tor Browser starts it might take a bit longer than usual; within a few minutes Tor Browser should be ready and a web browser will open congratulating you.

You can verify that you are connected to the Tor network by visiting check.torproject.org. If you are connected the website it will say “Congratulations. This browser is configured to use Tor.”

Browsing with Tor is different in some ways from the normal browsing experience. We recommended reading the tips for properly browsing with Tor and retaining your anonymity.

You are now ready to browse the internet anonymously with Tor.

How to: Use PGP for Mac OS X

Download Location: GPG Suite; Mozilla Thunderbird; Enigmail

Computer requirements: An internet connection, a computer running Mac OS X, an email account

Versions used in this guide: GPG Suite Beta 4, Mozilla Thunderbird 31.2.0, Enigmail 1.7.2

License: Free Software; mix of Free Software licenses

Other reading: https://gpgtools.tenderapp.com

Level: Beginner-Intermediate

Time required: 30-60 minutes

Pretty Good Privacy (PGP) is a way to protect your email communications from being read by anyone except their intended recipients. It can protect against companies, governments, or criminals spying on your Internet connection, and, to a lesser extent, it can save your email from being read if the computer on which they are stored is stolen or broken into.

It can also be used to prove that an email came from a particular person, instead of being a fake message sent by another sender (it is otherwise very easy for email to be fabricated). Both of these are important defenses if you're being targeted for surveillance or misinformation.

To use PGP, you will need to install some extra software that will work with your current email program. You will also need to create a private key, which you will keep private. The private key is what you will use to decrypt emails sent to you, and to digitally sign emails that you send to show they truly came from you. Finally, you'll learn how to distribute your public key—a small chunk of information that others will need to know before they can send you encrypted mail, and that they can use to verify emails you send.

This guide will show you how to use PGP with an Apple Mac (but not iPad or iPhone), with either the Mac's built-in Mail program, or with Mozilla Thunderbird, a popular alternative email program.

You can't currently use PGP directly with a web email service like Gmail, Hotmail, Yahoo! Mail, or Outlook Live. You can still use your webmail address; you'll just have to configure it with the Mail or Thunderbird programs on your computer.

Note that both ends of the email conversation need to be using PGP-compatible software for it to work.

People will normally use this only on their own personal devices, not on shared devices. Fortunately, PGP is available for most desktop computers and mobile devices, and you can point them to these guides to help them set up their own version. This guide is for Mac users.

Installing GPGTools on your Mac

PGP is an open standard, which means that more than one piece of software can use it. The software we're going to use for PGP is called the GPG Suite, from GPG Tools, because it works on Macs, is free for anyone to use, and it's open source: the underlying source code is available for anyone to check for bugs and backdoors.

Once the GPG Suite is installed, you can set up your keys for the first time, and then enable PGP on Apple Mail and, optionally, Thunderbird.

Step 1: Install the program

First, go to https://www.gpgtools.org/ in your browser and choose "Download GPG Suite."

You'll end up with a disk image that you can click on to install the software. If you're not accustomed to installing third-party software on your computer, ask a nearby Mac expert – this is a step most techies can help you with, even if they don't know PGP or encryption.

Clicking on install will give you a list of tools that will be added to your computer.

What exactly am I installing here?

These are tools will mostly work behind the scenes so that more than one program on your Mac can use PGP. Think of them as programs that other programs can use, rather than applications that you will use directly. GPGMail lets Apple Mail send and read PGP emails, GPG Keychain Access lets you keep your private and public keys in the same manner as you can save other passwords on your Mac. GPGServices optionally adds a feature to OS X to let you use PGP directly in programs other than email (for instance, in a word processor). GPGPreferences is for changing PGP settings in Apple's preferences. Finally, MacGPG2 is the basic tool that any program needs to use to do encryption or signing.

In October 2014, the GPG Tools team announced that they would soon be charging for GPGMail, the part of their package that lets you use GPG with Apple's Mail application. This tutorial is about using GPG with Thunderbird, so it doesn't use that component. You can just use the zero-cost part of the GPG Suite. In addition, all of these tools are "free software" in the FLOSS sense that you are still allowed to freely examine, edit and redistribute GPG Mail's underlying source code. For more information, see GPG Tools' own FAQ on their decision.

Click "Continue" to install GPG Suite.

When the installation is complete, open GPG Keychain (found in your applications folder) if it doesn't automatically open and prompt you to generate your PGP keys after installation. Click "New" to generate your PGP keys.

Step 2: Create your PGP key

Sometimes when you install new software, your computer will pester you with questions that have no obvious answer, without actually giving you any advice on how to reply. This is one of those times.

It's important to spend a little time thinking about the answers you'll give here, because changing your PGP key details can be difficult later, and if you've chosen to publish your key somewhere, you won't be able to unpublish it. (There are still thousands of old public keys from the 1990's floating around, with the names and old email addresses of the people who made them back then.)

PGP keys contain a name and an email address that link the key to you. The email address will be one of the ways others can discover which key to use when they are encrypting a message to you.

When should I not put my real name or email address on my PGP key? When shouldn't I upload my key?

For most people, it makes sense to add a real email address to your key, and upload it to the public keyservers – it's how people will match the right key to you. They can send you an email directly, and know it will be encrypted with the right key, and when they receive a signed email from you, the digital signature will be marked with your name.

For some people, though, it will not make sense to add your real name to your key, for instance if your threat model means that having your identity publicly attached to your key (and the linked email address) is not a good idea. Edward Snowden communicated with journalists using PGP and an anonymous email address before he revealed his identity; his PGP key certainly wasn't marked with his name.

> *Uploading your key is normal practice, but it can reveal that you're using encryption, even if you don't use your own name. Also, as we'll see, others might upload your key and associate their own key with it, implying that you and they have a connection. That can be harmful if you are communicating and don't want people to know it. It can also be troublesome if you're not communicating, but your attacker wants people to think that you are associated.*

Here's a rough guideline: if you're thinking about using a pseudonym generally, use that pseudonym (and alternative email) when labeling your key. If you are in a more dangerous environment, when you don't want people to know you're using PGP at all, or know who you are communicating with, don't upload your key to the public keyservers – and make sure the small group of people you're communicating with know not to upload your key either. There are other ways of verifying keys that don't rely on them being available on the public key server – see Key Verification.

Click the "Upload public key after generation" box if you'd like to let others find your key quickly so that they can send you encrypted messages. It's like adding your phone number to a public phone directory: you don't need it, but it's convenient for others.

Before generating the key, expand "Advanced options." You can leave the comment blank, and leave the key type "RSA and RSA (default)." But make sure to change the Length field to 4096.

> *Your key will expire at a certain time; when that happens, other people will stop using it entirely for new emails to you, though you might not get any warning or explanation about why. So, you may want to mark your calendar and pay attention to this issue a month or so before the expiration date.*

It's possible to extend the lifetime of an existing key by giving it a new, later expiration date, or it's possible to replace it with a new key by creating a fresh one from scratch. Both processes might require contacting people who email you and making sure that they get the updated key; current software isn't very good at automating this. So make a reminder for yourself; if you don't think you'll be able to manage it, you can consider setting the key so that it never expires, though in that case other people might try to use it when contacting you far in the future even if you no longer have the private key or no longer use PGP.

When you're ready, click the "Generate key" button.

Your computer will start generating both your public and private key. It shouldn't take any more than a couple of minutes to finish (it takes a while because to create your keys, your computer needs to gather random numbers. Think of it as your computer throwing a pair of dice many, many, many times.)

When you're done generating your key, you'll see it key listed in GPG Keychain Access. You can double-click on your key to see information about it, including its "fingerprint"—a unique way to identify your PGP key (see Key Verification).

Now is a good time to generate a revocation certificate.

> *In the future, if you ever worry that your private key has been copied by someone, you accidentally delete or lose your private key, or you forget your passphrase, you can tell everyone it has been revoked, or cancelled, by using a revocation certificate.*

It's better to create one now, because you need the private key and passphrase to create a revocation certificate. If you leave it until later, you might lose one or the other, and then it will be too late. So create a certificate by clicking on your key, choosing the "Key" menu entry, and then "Create Revocation Certificate." You'll be prompted for somewhere to save the file. You might want to keep it with a backup copy of the key (see next step).

Step 3: Back up your PGP key

If you lose access to your private key, you won't be able to decrypt any incoming PGP mail, or your old mail. On the other hand, you want to keep your private key as securely as you can.

You might want to save a backup copy to a USB key, which you keep safely hidden. You will only need it if you lose your original key, but for safety you will want to keep it out of the hands of your potential attackers.

Is everything lost if my attackers get hold of my PGP private key?

What if you get your Mac stolen, or your backup key is taken from you? Does that mean your PGP messages are vulnerable? No: if you've chosen a good passphrase and nobody has been able to learn what it is, you should still be mostly protected. To be safe, you may want to revoke your old key, and create a new PGP key. This won't stop your old key from being able to decrypt your old email, but it will discourage other people from using the old key for their new emails to you.

To backup your key, open GPG Keychain Access. Select your key, and click "Export" in the toolbar. Put your USB drive into the machine, and choose it in the "Where" part of the "Save As..." dialog. Check the "Allow secret key export" checkbox.

Configuring Apple Mail

When you first open Apple Mail, you'll see a first run wizard that helps you set up your email address. Fill out your name, email address, and your email password and click "Create."

Mail Account Setup Wizard

If you use popular free email services like Gmail, Mail should be able to automatically detect your email settings when you click Continue. If it doesn't, you may need to manually configure your IMAP and SMTP settings. Talk to the company you use for email, or ask someone technical who is familiar with your email provider (so, an IT person at work, or a technical friend who uses the same ISP as you. They don't need to know about PGP, but you can ask them “Can you set up Apple Mail for me?”).

Mail Account Setup Auto-detect

When you're composing a new message, there are two icons just beneath the Subject field. There's a padlock (encrypt email) and a star (digitally sign email). If the padlock is closed it means this email will be encrypted, and if the star has a check in it, it means this email will be digitally signed.

Sending PGP Signed or Encrypted Email

You can always sign your email, even if the recipient doesn’t use PGP. Because digitally signing emails requires your secret key, Mail will pop up a window asking for your passphrase when you first sign an email.

You can only encrypt emails if the person you’re emailing uses PGP and you have that person’s public key. If the encryption padlock icon is unlocked and greyed out so you can't click on it, this means you first need to import the recipient's public key. Either ask them to send it to you, or use the GPG Keychain Access app to find the key to from a public keyserver.

To be absolutely safe, you'll need to verify the keys you get from the keyserver or your colleague. See our section on Verifying Keys.

Using PGP with Mozilla Thunderbird

This walkthrough shows how to use GPG with the free, open source, Thunderbird mail client from Mozilla, together with the Enigmail plugin for email encryption.

First, download Thunderbird from from https://www.mozilla.org/thunderbird, mount the disk image as you did with GPG Tools, and drag the Thunderbird into Applications.

When you open it for the first time it will ask if you want to set it as your default email client. Go ahead and click "Set as Default."

Then you will see the first run wizard. To set up your existing email address, click "Skip this and use my existing email." Then enter your name, email address, and the password to your email account.

If you use popular free email services like Gmail, Thunderbird should be able to automatically detect your email settings when you click Continue. If it doesn't, you may need to manually configure your IMAP and SMTP settings—ask your ISP, or a technical friend who knows about setting up email, to help. Sometimes, Thunderbird can just guess the correct settings.

> *If you use two-factor authentication with Google (and depending on your threat model you probably should!) you cannot use your standard Gmail password with Thunderbird. Instead, you will need to create a new application-specific password for Thunderbird to access your Gmail account. See Google's own guide for doing this.*

After you're done configuring Thunderbird to check your email, click "Done." Then click on "Inbox" in the top left to load your emails.

Now that you've installed and configured Thunderbird to work with your email, you need to install Enigmail, the GPG add-on for Thunderbird. In Thunderbird, click the menu icon in the top-right, and choose Add-ons.

Search for "enigmail" in the search box in the top right.

Click the Install button next to the Enigmail extension to download and install Enigmail. When it's done, click "Restart Now" to restart Thunderbird.

The first time you run Thunderbird with Enigmail enabled it opens the OpenPGP Setup Wizard. Click "Cancel." We will manually configure Enigmail instead.

Click the menu button, hover over Preferences, and choose Account Settings.

Go to the OpenPGP Security tab. Make sure "Enable OpenPGP support (Enigmail) for this identity" is checked. "Use specific OpenPGP key ID" should be selected, and if your key isn't already selected you can click "Select Key" to select it.

You should also check "Sign non-encrypted message by default," "Sign encrypted messages by default," and "Use PGP/MIME by default," but not (for most people) "Encrypt messages by default."

If most of the people that you email use PGP (or you would like to encourage them to do so), you may wish to encrypt by default. It would be ideal to encrypt all the emails you

send, but that is not always possible. Remember that you can only send encrypted email to other people who use PGP, and you need to have their public keys in your keychain. For most people, manually choosing to encrypt each email you send will probably work best.

Then click "OK" to save all of the settings.

Congratulations, you now have Thunderbird and Enigmail set up! Here are a couple of quick pointers:

- You can click the menu button, hover over OpenPGP, and open Key Management to see the PGP key manager that's build-in to Enigmail. It's very similar to GPG Keychain Access, and it's your choice which you use.
- When you're composing a new message, there are two icons in the bottom right corner of the window: a pen (digitally sign email) and a key (encrypt email). If the icons are gold it means they are selected, and if they're silver it means they're not selected. Click on them to toggle signing and encrypting the email you're writing.

How to: Use OTR for Mac

Download Location: https://adium.im/

Computer requirements (Adium 1.5 or later): Mac OS X 10.6.8 or newer, an Apple-branded Macintosh computer.

Version used in this guide: Adium 1.5.9

License: GNU GPL

Other reading: https://pressfreedomfoundation.org/encryption-works; https://adium.im/help/

Level: Beginner-Intermediate

Time required: 15-20 minutes

Adium is a free and open source instant messaging client for OS X that allows you to chat with individuals across multiple chat protocols, including Google Hangouts, Yahoo! Messenger, Facebook chat, Windows Live Messenger, AIM, ICQ, and XMPP.

OTR (Off-the-record) is a protocol that allows people to have confidential conversations using the messaging tools they're already familiar with. This should not be confused with Google's "Off the record," which merely disables chat logging, and does not have encryption or verification capabilities. For Mac users, OTR comes built-in with the Adium client.

OTR employs end-to-end encryption. This means that you can use it to have conversations over services like Google Hangouts or Facebook without those companies ever having access to the contents of the conversations. This is different from the way in which Google and AOL use the term "off the record" to mean that a conversation is not being logged; that option does not encrypt your conversation.

Why Should I Use Adium + OTR?

When you have a chat conversation using Google Hangouts or Facebook chat on the Google or Facebook websites, that chat is encrypted using HTTPS, which means the content of your chat is protected from hackers and other third parties while it's in transit. It is *not*, however, protected from Google or Facebook, which have the keys to your conversations and can hand them over to authorities.

After you have installed Adium, you can sign in to it using multiple accounts at the same time. For example, you could use Google Hangouts, Facebook, and XMPP simultaneously. Adium also allows you to chat using these tools without OTR. Since OTR *only works if both people are using it*, this means that even if the other person does not have it installed, you can still chat with them using Adium.

Adium also allows you to do out-of-band verification to make sure that you're talking to the person you think you're talking to and you are not being subject to a man-in-the-middle attack. For every conversation, there is an option that will show you the key fingerprints it has for you and the person with whom you are chatting. A "key fingerprint" is a string of characters like "342e 2309 bd20 0912 ff10 6c63 2192 1928," that's used to verify a longer public key. Exchange your fingerprints through another communications channel, such as Twitter DM or email, to make sure that no one is interfering with your conversation.

Limitations: When Should I Not Use Adium + OTR?

Technologists have a term to describe when a program or technology might be vulnerable to external attack: they say it has a large "attack surface." Adium has a large attack surface. It is a complex program, which has not been written with security as a top priority. It almost certainly has bugs, some of which might be used by governments or even big companies to break into computers that are using it. Using Adium to encrypt your conversations is a great defense against the kind of untargeted dragnet surveillance that is used to spy on everyone's Internet conversations, but if you think you will be personally targeted by a well-resourced attacker (like a nation-state), you should consider stronger precautions, such as PGP-encrypted email.

Installing Adium + OTR On Your Mac

Step 1: Install the program

First, go to https://adium.im/ in your browser. Choose "Download Adium 1.5.9." The file will download as a .dmg, or disk image, and will probably be saved to your "downloads" folder.

Double-click on the file.

Move the Adium icon into the "Applications" folder to install the program. Once the program is installed, look for it in your Applications folder and double-click to open it.

Step 2: Set up your account(s)

First, you will need to decide what chat tools or protocols you want to use with Adium. The setup process is similar, but not identical, for each type of tool. You will need to

know your account name for each tool or protocol, as well as your password for each account.

To set up an account, go to the Adium menu at the top of your screen and click "Adium" and then "Preferences." This will open a window with another menu at the top. Select "Accounts," then click the "+" sign at the bottom of the window. You will see a menu.

Select the program that you wish to sign in to. From here, you will be prompted either to enter your username and password, or to use Adium's authorization tool to sign in to your account. Follow Adium's instructions carefully.

How to Initiate an OTR Chat

Once you have signed in to one or more of your accounts, you can start using OTR.

> *Remember: In order to have a conversation using OTR, both people need to be using a chat program that supports OTR.*

Step 1: Initiate an OTR Chat

First, identify someone who is using OTR, and initiate a conversation with them in Adium by double-clicking on their name. Once you have opened the chat window, you will see a small, open lock in the upper left-hand corner of the chat window. Click on the lock and select "Initiate Encrypted OTR Chat."

Step 2: Verify Your Connection

Once you have initiated the chat and the other person has accepted the invitation, you will see the lock icon close; this is how you know that your chat is now encrypted (congratulations!) – But wait, there's still another step!

At this time, you have initiated an unverified, encrypted chat. This means that while your communications are encrypted, you have not yet determined and verified the identity of the person you are chatting with. Unless you are in the same room and can see each other's screens, it is important that you verify each other's identities. For more information, read the module on Key Verification.

To verify another user's identity using Adium, click again on the lock, and select "Verify." You will be shown a window that displays both your key and the key of the other user. Some versions of Adium only support manual fingerprint verification. This means that, using some method, you and the person with whom you're chatting will need to check to make sure that the keys that you are being shown by Adium match precisely.

The easiest way to do this is to read them aloud to one another in person, but that's not always possible. There are different ways to accomplish this with varying degrees of trustworthiness. For example, you can read your keys aloud to one another on the phone if you recognize each other's voices or send them using another verified method of communication such as PGP. Some people publicize their key on their website, Twitter account, or business card.

> *The most important thing is that you verify that every single letter and digit matches perfectly.*

Step 3: Disable Logging

Now that you have initiated an encrypted chat and verified your chat partner's identity, there's one more thing you need to do. Unfortunately, Adium logs your OTR-encrypted chats by default, saving them to your hard drive. This means that, despite the fact that they're encrypted, they are being saved in plain text on your hard drive.

To disable logging, click "Adium" in the menu at the top of your screen, then "Preferences." In the new window, select "General" and then disable "Log messages" and "Log OTR-secured chats."

Also, when Adium displays notifications of new messages, the contents of those messages may be logged by the OS X Notification Center. This means that while Adium leaves no trace of your communications on your own computer or your correspondent's, either your or their computer's version of OS X may preserve a record. To prevent this, you may want to disable notifications.

To do this, select "Events" in the Preferences window, and look for any entries that say "Display a notification." For each entry, expand it by clicking the gray triangle, and then click the newly-exposed line that say "Display a notification," then click the minus icon ("-") at the lower left to remove that line." If you are worried about records left on your computer, you should also turn on full-disk encryption, which will help protect this data from being obtained by a third party without your password.

How to: Encrypt Your iPhone

If you have an iPhone 3GS or later, an iPod touch 3rd generation or later, or any iPad, you can protect the contents of your device using encryption. That means that if someone gets physical access to your device, they will also need your passcode to decrypt what's stored on it, including contacts, instant messages or texts, call logs and email.

In fact, most modern Apple devices encrypt their contents by default, with various levels of protection. But to protect yourself from someone obtaining your data by physically stealing your device, you need to tie that encryption to a passphrase or code that only you know.

On devices running iOS 4–iOS 7, you can do this by going to the General settings, and choosing Passcode (or iTouch & Passcode). As for iOS 8, Passcode has its own section in the Settings app. Follow the prompts to create a passcode. You should set the "Require passcode" option to "Immediately," so that your device isn't unlocked when you are not using it. Disable Simple Passcode so that you can use a code that's longer than 4 digits.

> *If you choose a passcode that's all-numeric, you will still get a numeric keypad when you need to unlock your phone, which may be easier than typing a set of letters and symbols on a tiny virtual keyboard. You should still try to keep your passcode long even though Apple's hardware is designed to slow down password-cracking tools. Try creating a passcode that is more than 6 digits.*

Once you've set a passcode, scroll down to the bottom of the Passcode settings page. You should see a message that says "Data protection enabled." This means that the device's encryption is now tied to your passcode, and that most data on your phone will need that code to unlock it.

Here are some other iOS features you should think about using if you're dealing with private data:

- iTunes has an option to backup your device onto your computer. If you choose the "Encrypt backup" option on the Summary tab of your device in iTunes, iTunes will backup more confidential information (such as Wifi passwords and email passwords), but will encrypt it all before saving it onto your computer. Be sure to keep the password you use here safe: restoring from backups is a rare event, but extra painful if you cannot remember the password to unlock the backup in an emergency.
- If you back up to Apple's iCloud, you should use a long passphrase to protect the data, and keep that passphrase safe. While Apple encrypts most data in its backups, it may be possible for the company to obtain access for law enforcement

purposes (especially Email and Notes, which at time of writing are stored unencrypted).

- If you turn on data protection as described above, you will also be able to delete your data on your device securely and quickly. In the Passcode settings, you can set your device to wipe all its data after ten failed attempts to guess your passphrase.
- According to Apple's old Law Enforcement Guide, "Apple can extract certain categories of active data from passcode locked iOS devices. Specifically, the user generated active files on an iOS device that are contained in Apple's native apps and for which the data is not encrypted using the passcode ("user generated active files"), can be extracted and provided to law enforcement on external media. Apple can perform this data extraction process on iOS devices running iOS 4 or more recent versions of iOS. Please note the only categories of user generated active files that can be provided to law enforcement, pursuant to a valid search warrant, are: SMS, photos, videos, contacts, audio recording, and call history. Apple cannot provide: email, calendar entries, or any third-party App data."

The above information applies only to iOS devices running versions of iOS prior to 8.0.

- Now, Apple states that "On devices running iOS 8, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. … Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."

REMEMBER: While Apple will be unable to extract data directly off a phone, if the device is set to sync with iCloud, or backup to a computer, much of the same data will indeed be accessible to law enforcement. Under most circumstances, iOS encryption is only effective when a device has been fully powered down (or freshly-rebooted, without being unlocked). Some attackers might be able to take valuable data from your device's memory when it's turned on. (They might even be able to take the data when it has just been turned off). Keep this in mind and, if possible, try to make sure your device is powered off (or rebooted and not unlocked) if you believe it's likely to be seized or stolen.

- If you are concerned about your device getting lost or stolen, you can also set up your Apple device so that it can be erased remotely, using the "Find My iPhone" feature. Note that this will allow Apple to remotely request the location of your device at any time. You should balance the benefit of deleting data if you lose control of your device, with the risk of revealing your own position. (Mobile phones transmit this information to telephone companies as a matter of course; WiFi devices like iPads and the iPod Touch do not.)

How to: Use Signal – Private Messenger

Signal – Private Messenger is a free and open source software application for iPhone that employs end-to-end encryption, allowing users to send end-to-end encrypted group, text, picture, and video messages and have encrypted phone conversations between Signal users on iPhone and TextSecure or RedPhone users on Android. Although Signal uses telephone numbers as contacts, calls and messages actually use your data connection; therefore both parties to the conversation must have Internet access on their mobile devices. Due to this, Signal users don't incur SMS and MMS fees.

Download Location: The app can be downloaded from the Apple App Store

System requirements: Requires iOS 7.0 or later. Compatible with iPhone, iPad, and iPod touch.

Version used in this guide: Signal – Private Messenger 2.0.1

License: GPLv3

Other reading:

- https://whispersystems.org/blog/signal/
- http://support.whispersystems.org/

Level: Beginner-Intermediate

Time required: 15-20 minutes

Installing Signal – Private Messenger on your iPhone

Step 1: Download and Install Signal – Private Messenger

On your iOS device, enter the App Store and search for "Signal." Select the app "Signal – Private Messenger" by Open Whisper Systems.

Click to download the app and accept the iTunes Store Terms & Conditions by selecting "Accept." The app will download and install automatically. Click "Open" to launch the app.

Step 2: Register and Verify your Phone Number

Enter your mobile phone number and click “Verify This Device.” In order to verify your phone number, you will be sent an SMS text with a six-digit code; enter the code in the space provided. If you are unable to receive SMS texts, you have the option of receiving a phone call to verify your phone number. Click “Submit Verification Code.”

Using Signal

In order to use Signal, the person that you are calling must have either Signal or TextSecure or RedPhone (for Android devices) installed. If you try to call or send a message to someone using the Signal app and they do not have any of the aforementioned apps installed, the app will ask if you would like to invite them via SMS, but it will not allow you to complete your call or send a message to them from inside the app.

To get started, click the "+" button.

You’ll see a list of your contacts that have already installed Signal, TextSecure, or RedPhone. You have the choice to either call them or send them a message.

How to Initiate an Encrypted Call

To initiate an encrypted call to a contact, click on the phone icon next to the contact's name.

Once a call is established, both parties to the call will be shown a random pair of words. This word pair will allow you to verify your identity and keys with the other user—also known as key verification.

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

How to Send an Encrypted Message

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

You can send an encrypted group message by navigating to your list of contacts, clicking on the group chat icon in the upper right-hand corner, and creating a new group.

Using this app can help to keep your communications safer since everything sent via Signal - Private Messenger is always end-to-end encrypted.

How to: Install and Use ChatSecure

Download location: https://chatsecure.org ; can also be downloaded from the Apple App store or the Google Play store.

System requirements: iOS 6.0, Android (varies)

Version used in this guide: 2.2.4 (iPhone), 13.1.2 (Android)

License: Apple, GPLv3; Android, Apache 2.0

Other reading: https://guardianproject.info/apps/chatsecure/

Level: Beginner-Intermediate

Time required: 5-10 minutes

ChatSecure is a free mobile phone application for iPhone and Android devices that allows users to communicate with off the record instant messaging. ChatSecure allows users to send instant messages and chats using a cell phone, instead of with a traditional desktop or laptop computer. It's compatible with iPhone and Android phones.

ChatSecure supports OTR encryption over XMPP. All messages sent via ChatSecure are completely private, so long as the person you are chatting with is also using an OTR compatible instant messaging client like ChatSecure, Adium, Pidgin, or Jitsi. The app's capabilities allow it to deliver audio messages, photos, files, or text.

When you send messages using ChatSecure, they are not stored on the phone system's memory. ChatSecure used with the privacy plugin Orbot should be able to bypass most firewalls, network restrictions, and blacklists. The app can manage multiple accounts, so you can chat with your Facebook friends, Google contacts, or other privacy conscious users that use an instant messaging program that supports OTR encryption.

How to Install and Configure ChatSecure

1. Download and Install ChatSecure

Visit the Apple App Store or Google Play store and search for ChatSecure by The Guardian Project. Select "Install" and accept the Terms of Service by clicking "Accept." The app will download and install automatically.

2. Open the App and Set Your Password

When you open the app you will be promoted to set a password. You will be prompted to create a passphrase in order to locally encrypt your data. If you choose to do this, your data will be encrypted in transit, as well as encrypted locally on your phone.

If you choose to skip this step, your messages will still be encrypted in transit, but will not be protected on your device. For more information on selecting a strong passphrase, see our module on Passwords.

3. Configure Your Accounts

You can add a variety of different accounts your ChatSecure app. To add GoogleTalk or Google Hangouts, choose "Google." To add any XMPP or Jabber messaging service, choose "Jabber (XMPP)." To add your Facebook account, also choose "Jabber (XMPP)."

Once you've added your account, type in your username (or email address) and your password to sign in. Your contacts should load automatically.

To add a second or third account, click on the "accounts" tab in the menu. In the upper right hand corner, click on the "+" sign. You can either choose to add an existing account or create a new account.

How to Use ChatSecure

1. Sign in to Your Accounts

To sign in to your account, click on the "accounts" tab in the menu and turn on the accounts you wish to use. Once you sign in, anyone can connect with you from a mobile or desktop instant messaging application.

2. Start End-to-end Encryption

Once you've started a chat with someone, click on the unlocked lock icon on the top menu bar of the display. Choose "Start Encryption." If the person you are chatting with has an OTR compatible instant messaging system, then you will have the option to verify your (and their) fingerprint.

ChatSecure offers three ways to verify OTR fingerprints, but if you're chatting with someone over a desktop instant messenger and not with ChatSecure, the best way to verify an OTR fingerprint is by communicating through another channel. You can resend your fingerprint over an SMS (TextSecure), say it over the phone if you recognize one

another's voices, use PGP email, or verify in person. Click on “manual verification” and ChatSecure will display your and your friend's fingerprints. If you can confirm that you both have the same information, you can click “verify.”

ChatSecure supports manual verification or verification by scanning the other user’s barcode (QR). If you are in the same room as the other person, you can easily scan the barcode on their phone or read your keys aloud to one another.

3. Understand Your Options

- Just like a desktop instant messaging service, ChatSecure gives you the option to appear offline, busy, idle, or away. To change this setting click on your name at the top of your friends list.
- ChatSecure also allows you to initiate group chats and add new contacts, both of which can be done from the main menu. (Note that group chats *cannot be secured* like one-on-one chats due to limitations of the OTR protocol.)
- The app supports multimedia messaging, can take pictures, and can send photos and files securely if your friend is also using end-to-end encryption and you are able to verify her identity.
- ChatSecure gives you the option to create a new XMPP or Jabber messaging account that supports OTR encryption. If you don't already use XMPP messaging, this is a great opportunity to create one and experiment with non-proprietary messaging.

Glossary

Adversary
Your adversary is the person or organization attempting to undermine your security goals. Adversaries can be different, depending on the situation. For instance, you may worry about criminals spying on the network at a cafe, or your classmates at a school. Often the adversary is hypothetical.

Air gap
A computer or network that is physically isolated from all other networks, including the Internet, is said to be air-gapped.

Anti-virus
Software that attempts to protect a device from being taken over by malicious software (or “malware"). "Viruses' were some of the first and most prevalent forms of malware; they were named viruses to reflect the way they would spread from device to device. These days most antivirus software concentrate on warning you if you look to be downloading a suspicious fiile from an external source, and examining files on your computer to see if they match the software's idea of what malware looks like.

Anti-virus software can only recognise malware if it is substantially similar to samples that the anti-virus developer has already analysed. This makes it far less effective at combating targeted malware designed to infiltrate a particular community or person, rather than more widespread strains of malware. Some advanced malware can also actively attack or conceal itself from antivirus software.

Asset
In threat modeling, any piece of data or a device that needs to be protected.

Attack
In computer security, an attack is a method that can be used to compromise security, or its actual use. An attacker is the person or organization using an attack. An attack method is sometimes called an "exploit."

Burner phone
A phone that is not connected to your identity, is only used for a small set of calls or activities, and can be discarded if and when it is suspected of being tracked or compromised. Burner phones are often pre-paid mobile phones bought with cash.

Capability
The capability of an attacker (in the sense we use it in this guide) is what it is able to do to achieve its aims. For example, a country's security services might have the capability to listen to telephone calls while a neighbor may have the capability to watch you from their window. To say that an attacker “has" a capability does not

mean that they will necessarily use that capability. It does mean that you should consider and prepare for the possibility.

Command line tool

The "command line" is an ancient way of giving a computer a series of small, self-contained orders (think of those science fiction movies where teenage geniuses type long strings of green text onto black screens). To use a command line tool, the user types a command into a window called a terminal emulator, hits the return or enter key, and then receives a textual response in the same window. Windows, Linux and Apple desktop computers still let you run software using this interface, and even some mobile phones can do the same with the right app. The command line can be used to run software pre-packaged with your operating system. Some downloadable programs, especially technical utilities, use the command line instead of a more familiar "icons and buttons" user interface. The command line needn't be scary, but it does require you to type in exactly the right set of letters and numbers to get the correct result, and it's often unclear what to do if the responses don't match your expectations.

Commercial VPN

A commercial Virtual Private Network is a private service that offers to securely relay your Internet communications via their own network. The advantage of this is that all of the data you send and receive is hidden from local networks, so it is safer from nearby criminals, or untrusted local ISPs or cybercafes. A VPN may be hosted in a foreign country, which is useful both for protecting communications from a local government, and bypassing national censorship. The down side is that most of the traffic is decrypted at the commercial VPN's end. That means you need to trust the commercial VPN (and the country where it is located) not to snoop on your traffic.

Cookies

Cookies are a web technology that let websites recognize your browser. Cookies were originally designed to allow sites to offer online shopping carts, save preferences or keep you logged on to a site. They also enable tracking and profiling so sites can recognize you and learn more about where you go, which devices you use, and what you are interested in – even if you don't have an account with that site, or aren't logged in.

Corporate Intranet

Companies and other large institutions will usually have some services (email, web, and access to files and printers for instance) that are accessible from within their own local network, but not from outside on the wider Internet. Most companies take this as being sufficient security to protect their internal documents, but this means that any attack that can connect to the intranet can access or interfere with all the information being kept locally. An example of such an attack is tricking an employee to install malware on their laptop.

To allow employees to access the intranet via the wider Internet, companies will often provide their own Virtual Private Network (VPN) which creates a secure connection to the inside of the intranet from anywhere in the world.

Cryptography
The art of designing secret codes or ciphers that let you send and receive messages to a recipient without others being able to understand the message.

Decrypt
Make a secret message or data intelligible. The idea behind encryption is to make messages that can only be decrypted by the person or people who are meant to receive them.

Distributed Denial of Service attack
A method for taking a website or other Internet service offline, by co-ordinating many different computers to request or send data to it simultaneously. Usually the computers used to conduct such an attack are remotely controlled by criminals, who have taken over the machines by breaking into them, or infecting them with malware.

Domain name
The address, in words, of a website or Internet service; for example: ssd.eff.org

Encryption
A process that takes a message and makes it unreadable except to a person who knows how to "decrypt" it back into a readable form.

Encryption key
An encryption key is a piece of information that is used to convert a message into an unreadable form. In some cases, you need the same encryption key to decode the message. In others, the encryption key and decryption key are different.

End-to-end encryption
End-to-end encryption ensures that a message is turned into a secret message by its original sender, and decoded only by its final recipient. Other forms of encryption may depend on encryption performed by third-parties. That means that those parties have to be trusted with the original text. End-to-end encryption is generally regarded as safer, because it reduces the number of parties who might be able to interfere or break the encryption.

File system
Where data is stored, usually locally, on your computer or other device. File systems are usually where personal documents and notes are stored for easy access.

File Transfer Protocol (FTP server)
An old method for copying files from a local computer to a remote one, or vice versa. The job of FTP programs (and the FTP servers that stored the files) have mostly been

replaced by web browsers and web servers, or file synchronising programs like Dropbox.

Fingerprint
The keys of public key cryptography are very large numbers, sometimes a thousand or more digits long. A fingerprint is a much smaller number or set of numbers and letters that can be used as a unique name for that key, without having to list all of the key's digits. So, for instance, if you and a friend wished to make sure you both had the same key, you could either spend a long time reading off all the hundreds of digits in the key, or you could each calculate your key's fingerprint and compare those instead. The fingerprints presented by cryptographic software usually consist of around 40 letters and numbers. If you carefully check that a fingerprint has the right value, you should be safe against impersonation using a fake key. Some software tools may offer more convenient alternative ways to verify a friend's key, but some form of verification needs to happen to prevent communications providers from easily being able to listen in.

Firewall
A tool that protects a computer from unwanted connections to or from local networks and the Internet. A firewall might have rules that forbid outgoing email, or connections to certain websites. Firewalls can be used as a first line of defense to protect a device from unexpected interference. Or they can be used to prevent users from using the Internet in certain ways.

Forward Secrecy
A property of a secure messaging system which ensures that your past communications can remain secure even if one of the private keys is stolen later. For HTTPS websites, forward secrecy is an important protection against adversaries like intelligence agencies which may record large amounts of traffic and use a stolen key to decrypt it. For instant messaging and chat systems, forward secrecy is necessary to ensure that deleted messages are really deleted, but you will also need to either disabled logging or securely delete past messages.

Free, libre and open source software
Open source software, or free software, is software that can be distributed freely in a form that lets others modify it and rebuild it from scratch. While it is known as “free software”, it's not necessarily free as in zero-cost: FLOSS programmers can ask for donations, or charge for support or for copies. Linux is an example of a free, open source program, as are Firefox and Tor.

Full disk encryption
If you're planning on securing data on your local device, you could choose to just encrypt a few key files, or you could encrypt everything on the computer. “Full disk encryption” is the term for encrypting everything. It's usually safer (and often easier) to use full disk encryption than to manage just a few individually encrypted files. If you try to encrypt just individual files, your computer might make temporary

unencrypted copies of those files without you noticing. And some software might keep some unencrypted records about your use of your computer. Apple's OS X, Linux and high-end
versions of Windows all have built-in full disk encryption, but it is usually not turned on by default.

HTTPS
If you've ever seen a web address spelled out as "http://www.example.com/", you'll recognize the "http" bit of this term. HTTP (hypertext transfer protocol) is the way a web browser on your machine talks to a remote web server. Unfortunately, standard http sends text insecurely across the Internet. HTTPS (the S stands for "secure") uses encryption to better protect the data you send to websites, and the information they return to you, from prying eyes.

IMAP settings
IMAP is the way that many email programs communicate with services that send, receive and store your email. By changing the IMAP settings on your email program, you can choose to load email from different servers or set the level of security and encryption used to transfer the mail across the Internet to you.

Indicators of compromise
Clues that show that your device may have been broken into or tampered with.

Internet filtering
Filtering is the politer term for blocking or censoring Internet traffic.

IP address
A device on the Internet needs its own address to receive data, just like a home or business needs a street address to receive physical mail. This address is its IP (Internet Protocol) address. When you connect to a web site or other server online, you usually reveal your own IP address. This doesn't necessarily reveal either your identity (it's hard to map an IP address to a real address or a particular computer). An IP address can give away some information about you, however, such as your rough location or the name of your Internet Service Provider. Services like Tor let you hide your IP address, which helps give you anonymity online.

Key
In cryptography, a piece of data which gives you the capability to encrypt or decrypt a message.

Key pair
To receive encrypted messages using public key cryptography (and to reliably inform others that a message genuinely came from you), you need to create two keys. One, the private key, you keep secret. The other, the public key, you can let anyone see. The two keys are connected mathematically, and are often collectively known as a "keypair".

Key verification
In public key cryptography, each person has a set of keys. To send a message securely to a particular person, you encrypt your message using their public key. An attacker may be able to trick you into using their key, which means that they will be able to read your message, instead of the intended recipient. That means that you have to verify that a key is being used by a particular person. Key verification is any way that lets you match a key to a person.

Key-signing party
When you're using public key encryption, it's important to be sure that the key you use to encrypt a message really belongs to the recipient (see key verification). PGP makes this a little easier by having a way to tell others "I believe this key belongs to this person -- and if you trust me, you should believe that too." Telling the world that you trust someone's key is called "signing their key": it means anyone who uses that key can see you vouched for it. To encourage everyone to check and sign each others keys, PGP users organize key-signing parties. They're almost, but not quite, as exciting as they sound.

Keylogger
A malicious program or device that records everything you type into a device, including passwords and other personal details, allowing others to secretly collect that information. (The "key" in keylogger refers to the keys you have on your keyboard.) Keyloggers are often malware that users have been tricked into downloading and running, or occasionally physical hardware secretly plugged into a keyboard or device.

Keyring
If you use public key cryptography, you'll need to keep track of many keys: your secret, private key, your public key, and the public keys of everyone you communicate with. The collection of these keys is often referred to as your keyring.

Malware
Malware is short for malicious software: programs that are designed to conduct unwanted actions on your device. Computer viruses are malware. So are programs that steal passwords, secretly record you, or delete your data.

Man-in-the-middle attack
Suppose you believe you were speaking to your friend, Bahram, via encrypted instant messager. To check it's really him, you ask him to tell you the city where you first met. "Istanbul" comes the reply. That's correct! Unfortunately, without you or Bahram knowing, someone else online has been intercepting all your communications. When you first connected to Bahram, you actually connected to this person, and she, in turn, connected to Bahram. When you think you are asking Bahram a question, she receives your message, relays the question to Bahram, receives his answer back , and then sends it to you. Even though you think you are

communicating securely with Bahram, you are, in fact, only communicating securely with the spy, who is also communicating securely to Bahram! This is the man-in-the-middle attack. Men-in-the-middle can spy on communications or even insert false or misleading messages into your communications. Security-focused internet communications software needs to defend against the man-in-the-middle attack to be safe against attackers who have control of any part of the Internet between two communicators.

Master password
A password used to unlock a store of other passwords or other ways to unlock programs or messages. You should make a master password as strong as you can.

Metadata
Metadata (or "data about data") is everything about a piece of information, apart from the information itself. So the content of a message is not metadata, but who sent it, when, where from, and to whom, are all examples of metadata. Legal systems often protect content more than metadata: for instance, in the United States, law enforcement needs a warrant to listen to a person's telephone calls, but claims the right to obtain the list of who you have called far more easily. However, metadata can often reveal a great deal, and will often need to be protected as carefully as the data it describes.

Off-the-Record (OTR)
Instant messaging systems are often unencrypted. OTR is a way of adding encryption to them, so that you can keep using familiar networks like Facebook chat, Google Chat or Hangouts, or Microsoft Messenger, but with your messages more resistant to surveillance.

One-time password
Passwords are usually semi-permanent: once you set them up, you can keep using them until you manually change or reset them. One-time passwords only work once. Some one-time password systems work by having a tool or program that can create many different one-time passwords, that you use in turn. This is useful if you're afraid that there may be a key-logger on a system where you have to type in a password.

Operating system
A program that runs all the other programs on a computer. Windows, Android and Apple's OS X and iOS are all examples of operating systems.

Out-of-band verification
"Out-of-band" means any way of communicating outside of the current method. Verifying the identity of the person you're talking to over an insecure communication system often requires communicating out-of-band via another method that is less vulnerable to the same kind of attack. So, for instance, you might check that you are using someone's correct public key by talking to them in person, before using it to encrypt your email.

Passive adversary
A passive adversary is one that can listen to your communications, but cannot directly tamper with them.

Passphrase
A passphrase is a kind of password. We use "passphrase" to convey the idea that a password which is a single word is far too short to protect you and a longer phrase is much better. The webcomic XKCD has a good explanation. http://xkcd.com/936/

Password manager
A tool that can encrypt and store your passwords using a single master password making it practical to use many different passwords on different sites and services without having to memorize them.

PGP
PGP or Pretty Good Privacy was one of the first popular implementations of public key cryptography. Phil Zimmermann, its creator, wrote the program in 1991 to help activists and others protect their communications. He was formally investigated by the US government when the program spread outside the United States. At the time, exporting tools that included strong public key encryption was a violation of US law.

PGP continues to exist as a commercial software product. A free implementation of the same underlying standard that PGP uses called GnuPG (or GPG) is also available. Because both use the same interchangeable approach, people will refer to using a “PGP key” or sending a “PGP message”, even if they are using GnuPG.

Protocol
A communications protocol is a way of sending data between programs or computers. Software programs that use the same protocol can talk to each other: so web browsers and web servers speak the same protocol, called "http". Some protocols use encryption to protect their contents. The secure version of the http protocol is called "https". Another example of an encrypted protocol used by many different programs is OTR (Off-the-Record), a protocol for secure instant messaging.

Public key encryption
Traditional encryption systems use the same secret, or key, to encrypt and decrypt a message. So if I encrypted a file with the password "bluetonicmonster", you would need both the file and the secret "bluetonicmonster" to decode it. Public key encryption uses two keys: one to encrypt, and other to decrypt. This has all kinds of useful consequences. For one, it means that you can hand out the key to encrypt messages to you, and as long as you keep the other key secret, anyone with that key can talk to you securely. The key you hand out widely is known as the "public key": hence the name of the technique. Public key encryption is used to encrypt email and files by Pretty Good Privacy (PGP), OTR for instant messaging, and SSL/TLS for web browsing.

Public key servers

If you plan to send a secure message to someone who uses public key cryptography like PGP, you need to know what key to use to encrypt your message. Public key servers act as a phonebook for such keys, allowing software to use an email address, name, or key fingerprint to search for a full key and download it. There are many PGP public key servers, but they usually share their key collections with each other. Keyservers can't verify whether the keys they publish are genuine or forgeries. Anyone can upload a key to a public key server—in anyone's name. That means that a key connected to a person's name or email on a keyserver might not be their real key. In order to check the authenticity of a key, you need to check its signatures, or confirm its fingerprint with the original user in a trustworthy way.

PGP allows you to sign other people's keys, which is a way of using your own key to assert that a certain key is the right one to use to contact another person. This is meant to provide a way of distinguishing between genuine and fake keys; if people sign the right keys for people they know and communicate with, others can use those signatures to confirm that the genuine keys are genuine. When you download a key from a key server, it may include signatures from other people who affirm that it's the right one. If you know those people and know that you have the right key for them, you can have more confidence in the newly downloaded key. This verification process is also called the web of trust. Its advantage is that it's decentralized and not controlled by any authority, so you don't have to believe a certain company or government about which keys to use when writing to new people. Instead, you can believe your own social networks. One important disadvantage of the web of trust is that publishing signatures for other people's keys tells the whole world who your contacts are; it creates public evidence that you know particular people. Also, using the web of trust correctly requires a good deal of time and attention, and some communities rarely or never participate.

Revocation certificate

What happens if you lose access to a secret key, or it stops being secret? A revocation certificate is a file that you can generate that announces that you no longer trust that key. You generate it when you still have the secret key, and keep it for any future disaster.

Risk analysis

In computer security, risk analysis is calculating the chance that threats might succeed, so you know how much effort to spend defending against them. There may be many different ways that you might lose control or access to your data, but some of them are less likely than others. Assessing risk means deciding which threats you are going to take seriously, and which may be too rare or too harmless (or too difficult to combat) to worry about. See threat modeling.

Secure Sockets Layer (SSL)
The technology that permits you to maintain a secure, encrypted connection between your computer and some of the websites and Internet services that you visit. When you are connected to a website through SSL, the address of the website will begin with HTTPS rather than HTTP.

Security certificate
A security certificate is a kind of private key used to prevent man-in-the-middle attacks. A site that has access to the certificate can prove to remote systems that it has the certificate, and at the same time demonstrate that no other system without that certificate is tampering with the communication.

Security question
To supplement passwords, some systems use "security questions". These are queries to which only you are supposed to know the answer. The problem with security questions is that they are really just extra passwords that have potentially guessable answers. We recommend you treat them as any other password: create a long, novel, random, phrase to answer them, and record that somewhere safe. So the next time your bank asks you your mother's maiden name, you should be ready to answer "Correct Battery Horse Staple" or similar.

SIM card
A small, removable card that can be inserted into a mobile phone in order to provide service with a particular mobile phone company. SIM (subscriber identity module) cards can also store phone numbers and text messages.

SMTP settings
SMTP is one method for sending mail between computers. You can configure most email programs to encrypt messages between your e-mail software and the email server by changing your programs' SMTP settings (as long as your email service supports it)

Solid State Drive (SSD)
Historically, computers stored data on rotating magnetic discs. Mobile devices and increasing numbers of personal computers now store permanent data on non-moving drives. These SSD drives are currently more expensive, but much faster than magnetic storage. Unfortunately, it can be more difficult to reliably and permanently remove data from SSD drives.

SSH
SSH (or Secure SHell) is a method for letting you securely control a remote computer via a command line interface. One of the features of the SSH protocol is that as well as sending commands, you can also use it to securely relay Internet traffic between two computers. To set up an ssh link, the remote system needs to operate as a ssh server, and your local machine need an ssh client program.

Terminal
In ancient computer history, a terminal was a dedicated system of keyboard and screen that connected a user to a server. These days, it's more likely to be a program that allows you to talk to computers (either local or remote) over the command line.

Threat
In computer security, a threat is a potential event that could undermine your efforts to defend your data. Threats can be intentional (conceived by attackers), or they could be accidental (you might leave your computer turned on and unguarded).

Threat model
A way of narrowly thinking about the sorts of protection you want for your data. It's impossible to protect against every kind of trick or attacker, so you should concentrate on which people might want your data, what they might want from it, and how they might get it. Coming up with a set of possible attacks you plan to protect against is called threat modeling. Once you have a threat model, you can conduct a risk analysis.

Throwaway address
An email address you use once, and never again. Used to sign up to Internet services without revealing an email address connected to your identity.

Traffic-blocking browser extension
When you visit a website, your browser sends some information to that site's operators -- your IP address, other information about your computer, and cookies that link you to previous visits using that browser, for instance. If the website includes images and content taken from other web servers, that same information is sent to other websites as part of downloading or viewing the page. Advertising networks, analytics providers, and other data collectors may gather information from you in this way.
You can install additional software that runs alongside your browser and will limit how much information is leaked to third-parties in this way. The most well-known examples are programs that block advertisements. EFF offers a tool called Privacy Badger which is another traffic-blocking extension.

Transport encryption
Encrypting data as it travels across the network, so that others spying on the network cannot read it.

Two-factor authentication
"Something you know, and something you have." Login systems that require only a username and password risk being broken when someone else can obtain (or guess) those pieces of information. Services that offer two-factor authentication also require you to provide a separate confirmation that you are who you say you are. The second factor could be a one-off secret code, a number generated by a program running on a mobile device, or a device that you carry and that you can use to confirm who you

are. Companies like banks, and major internet services like Google, Paypal and Twitter now offer two-factor authentication.

Undelete software

Most devices let you delete data from them; For instance, you can drag a file to the Trash icon, or press delete in a photo album. But deletion does not always mean that the original data is gone. Undelete programs are applications that can be used by the device's owner, or others with access to the device, to restore some data. Undelete programs are useful for those who accidentally delete their own data, and to those whose data might have been sabotaged, such as a photographer who has been compelled to remove images from their camera. However, those same programs can be a threat to anyone who wants to permanently erase confidential data. See How to Delete Your Data Securely for advice on wiping data, and how undelete programs work on modern devices.

Virtual Private Network

A virtual private network is a method for connecting your computer securely to the network of an organization on the other side of the Internet. When you use a VPN, all of your computer's Internet communications is packaged together, encrypted and then relayed to this other organization, where it is decrypted, unpacked, and then sent on to its destination. To the organization's network, or any other computer on the wider Internet, it looks like your computer's request is coming from inside the organization, not from your location.
VPNs are used by businesses to provide secure access to internal resources (like file servers or printers). They are also used by individuals to bypass local censorship, or defeat local surveillance.

Voice over IP (VoIP)

Any technology that allows you to use the Internet for voice communication with other VoIP users or receive telephone calls over the Internet.

Wear leveling

Some forms of digital storage, like the flash memory used in solid-state drives (SSD) and USB sticks, can wear out if overwritten many times. Wear leveling is a method that spreads the writing of data evenly across all of the media to prevent one part of it being overwritten too many times. Its benefit is that it can make devices last longer. The danger for security-conscious users is that wear leveling interferes with secure erase programs, which deliberately try to overwrite sensitive files with junk data in order to permanently erase them. Rather than trusting secure erase programs with files stored on SSD or USB flash drives, it can be better to use full-disk encryption. Encryption avoids the difficulty of secure erasing by making any file on the drive difficult to recover without the correct passphrase.

Web browser
The program you use to view web sites. Firefox, Safari, Internet Explorer and Chrome are all web browsers. Smartphones have a built-in web browser app for the same purpose.

Web-based proxy
A website that lets its users access other, blocked or censored websites. Generally, the web proxy will let you type a web address (or URL) onto a web page, and then redisplay that web address on the proxy page. Easier to use than most other censorship-circumventing services.

XMPP
A open standard for instant messages - Google uses XMPP for Google Talk; Facebook used to offer it, but stopped. Non-corporate independent instant messaging services will usually use XMPP. Services like WhatsApp have their own, closed and secret protocol.

Zero day
A flaw in a piece of software or hardware that was previously unknown to the maker of the product. Until the manufacturers hear of the flaw and fix it, attackers can use it for their own purposes.

Credits

Many thanks to all of those who have written, translated, and given feedback on Surveillance Self-Defense. As always, the errors are ours, the bug fixes theirs.

Content contributors/translators:

- Abed W. Ayyad
- Julie Schwietert Collazo
- Ahmad Gharbeia
- Amr Gharbeia
- Eman AlTamimi
- Vitaliy Grishenko
- Keylingo Translations
- Nighat Dad
- Sobia Ghazal
- Ali Kamran
- Samir Nassar
- Anas Qtiesh
- Ramy Raoof
- Carlos Wertheman
- Abdullah Aloglu
- Ahmet Sabancı
- Viet Tan

External reviewers and other assistance:

- Tarek Amr
- Mytili Bala
- Ruben Bloemgarten
- Wojtek Bogusz
- Griffin Boyce
- Jon Camfield
- Endalkachew Chala
- Sacha Costanza-Chock and the 2014 students of MIT's Civic Media: Collaborative Design Studio
- Marianne Diaz
- Allen Gunn and all the attendees and organizers at the 2014 New York Privacy Sprint
- Paulina Haduong
- Nadia Heninger
- Becky Hurwitz
- Ramzi Jaber
- Fieke Jansen
- Oktavia Jonsdottir
- Marta M. Kanashiro
- Emi Kane
- Michael Khoo
- Jeremie Leclanche
- Tom Lowenthal
- Wei-Wei Lu
- Moxie Marlinspike
- Andre Meister
- Dan Meredith
- Henrique Parra
- Jennie Phillips
- Enrique Piracaes
- Ali Ravi
- Karen Reilly
- Garrett Robinson
- Runa Sandvik
- Bruce Schneier
- Samantha Majerus and the SSD team at Spitfire Strategies
- Katarzyna Szymielewicz
- Trevor Timm
- Marek Tuszynski
- Dmitri Vitaliev
- Chris Walker
- Carol Waters

EFF would like to thank all those who worked on the documentation, quality assurance, and online support for the tools and services mentioned in this guide.

Team SSD at EFF included:

- Mark Burdett
- Nate Cardozo
- Kim Carlson
- Hugh D'Andrade
- Peter Eckersley
- Eva Galperin
- Jeremy Gillula
- April Glaser
- Starchy Grant
- Max Hunter
- Rebecca Jeschke
- Adi Kamdar
- Danny O'Brien
- Matt Olenick (Mirabot)
- Kurt Opsahl
- Katitza Rodríguez
- Squiggy Rubio (Mirabot)
- Seth Schoen
- Jillian C. York

Special thanks to EFFers emeriti: Dan Auerbach, Kevin Bankston, Micah Lee, Chris Palmer, and Yan Zhu for showing us the way.

SSD was funded with the generous support of the Ford Foundation.