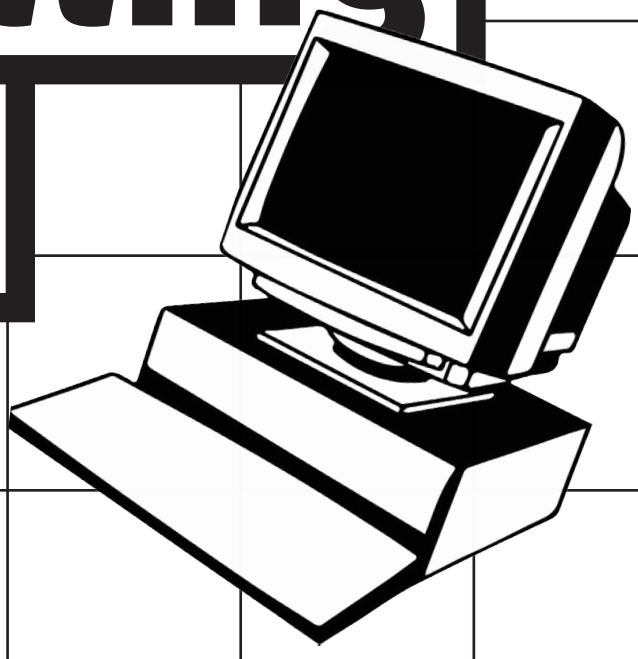
The Motherboard Guide to Not Getting Hacked



MOTHERBOARD

The Motherboard Guide to Not Getting Hacked

One of the questions we are asked most often at Motherboard is "how can I prevent myself from getting hacked?"

Because living in modern society necessitates putting an uncomfortably large amount of trust in third parties, the answer is often "not a whole lot." Take, for example, the massive Equifax hack that affected roughly half of the American population: Few people voluntarily signed up for the service, and yet their information was stolen anyway.

Hackers steal hundreds of millions of passwords in one swoop and occasionally cause large-scale blackouts. The future is probably not going to get better, with real-life disasters caused by internet-connected knick-knacks, smart home robots that could kill you, flying hacker laptops, and the dangers of hackers getting your genetic data. Meanwhile, an ever-growing and increasingly passive surveillance apparatus that has trickled down to state and local police is an ever-present threat to our digital privacy.

That doesn't mean it's hopeless out there. There are lots of things you can do to make it much more difficult for hackers or would-be surveillers to access your devices and accounts, and the aim of this guide is to give you clear, easy-to-follow steps to improve your digital security. There are, broadly speaking, two types of hacks: Those that are unpreventable by users, and those you can generally prevent. We want to help you mitigate the damage of the first and prevent the second from happening.

You, as an individual user, can't do anything to prevent your email provider, or the company that holds your financial details, from getting hacked. But you can avoid phishing attacks that will let a hacker get into your individual email account, and you can also prevent a password obtained in a larger hack from being reused on another, separate account you have.

This guide isn't comprehensive and it's not personalized; there is no such thing as "perfect security" and there are no one-size-fits all solutions. Instead, we hope this will be a jumping-off point for people looking to batten down the hatches on their digital lives.

That's why we've tried to keep this guide as accessible as possible, but if you run into any lingo you don't know, there's a glossary at the end of this guide to help out.

This guide is the work of many people on Motherboard staff both past and present, and has been vetted by several of our sources, who we owe a great debt to. Large sections of it were written by Lorenzo Franceschi-Bicchierai, Joseph Cox, Sarah Jeong, and Jason Koebler, but the tips within it have grown out of years of writing and research on digital security by dozens of reporters and infosec professionals. Consider it a forever-ongoing work-in-progress that will receive at least one big annual refresh, as well as smaller updates when major new vulnerabilities are exposed. Special thanks to Matt Mitchell of Crypto Harlem, and Eva Galperin, of the Electronic Frontier Foundation for reviewing parts of this guide.

Anyways, enough. This is the Motherboard Guide to Not Getting Hacked.

Table of Contents

04 Digital Security Basics

05 Threat Modeling
06 Software Updates
07 Passwords
08 Two-Factor Authentication

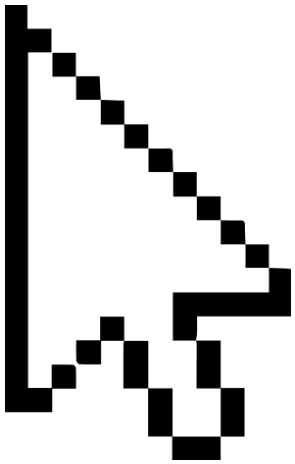
11 Mobile Security

12 Threat Modeling (Mobile edition)
12 iPhone vs Android
13 Android Security
13 SIM Card & Cell Account Security

14 Privacy, Messaging, and Avoiding State and Police Surveillance

15 Threat Modeling (Privacy and surveillance edition)
15 Signal & Messaging
16 Social Media
16 Cameras and Microphones
16 Lock Screen
16 OTR
17 Tor Browser
17 Virtual Private Networks
17 PGP
17 Email Providers and Servers
18 Hard Drive Encryption
18 Credit Cards
18 Notes for Journalists
19 The Future
20 Log Off
21 Glossary of Hacking and Cyber Terms

21 Glossary of Hacking and Cyber Terms



Digital Security Basics

Threat Modeling

Everything in this guide starts with "threat modeling," which is hacker lingo for assessing how likely it is you are going to get hacked or surveilled. When thinking about how to protect your digital communications, it is imperative that you first think about what you're protecting and who you're protecting it from. "Depends on your threat model" is a thing infosec pros say when asked questions about whether, say, Signal is the best messaging app or Tor is the most secure browser. The answer to any question about the "best" security is, essentially: "it depends."

No one security plan is identical to any other. What sort of protections you take all depend on who may try to get into your accounts, or to read your messages. The bad news is that there are no silver bullets (sorry!), but the good news is that most people have threat models in which they probably don't have to live like a paranoid recluse to be reasonably safe online.

So before doing anything else, you should consider your threat model. Basically, what are you trying to protect, and who are you trying to protect it from?

The Electronic Frontier Foundation recommends asking yourself these five questions when threat modeling:

What do you want to protect?

Who do you want to protect it from?

How likely is it that you will need to protect it?

How bad are the consequences if you fail?

How much trouble are you willing to go through in order to try to prevent those?

Is your threat an ex who might want to go through your Facebook account? Then making sure they don't know your password is a good place to start. (Don't share critical passwords with people, no matter who they are; if we're talking Netflix, make sure you never reuse that password elsewhere.) Are you trying to keep opportunistic doxers from pulling together your personal information—such as your birthday—which in turn can be used to find other details? Well, keeping an eye on what sort of stuff you publish on social media would be a good idea. And two-factor authentication (more on that below) would go a long way to thwarting more serious criminals. If you are an activist, a journalist, or otherwise have reason to fear government, state, or law enforcement actors want to hack or surveil you, the steps you must take to protect yourself are significantly different than if you're trying to keep plans for a surprise party secret from your best friend.

Overestimating your threat can be a problem too: if you start using obscure custom operating systems, virtual machines, or anything else technical when it's really not necessary (or you don't know how to use it), you're probably wasting your time and might be putting yourself at risk. At best, even the most simple tasks might take a while longer; in a worst-case scenario, you might be lulling yourself into a false sense of security with services and hardware that you don't need, while overlooking what actually matters to you and the actual threats you might be facing.

In certain places, this guide will offer specific steps to take if you have a threat model that includes sophisticated actors. But, in general, it's designed for people who want to know the basics of how to strengthen their digital security. If your threat model includes NSA hackers or other state-sponsored groups like Fancy Bear, we recommend that you speak to a trained professional about your specific situation.

Keep Your Apps Up To Date

Probably the most important and basic thing you can do to protect yourself is to update the software you use to its newest version. That means using an updated version of whatever operating system you're using, and updating all your apps and software. It also means updating the firmware on your router, connected devices, and any other gadgets you use that can connect to the internet.

Bear in mind that, on your computer, you don't necessarily have to use the latest iteration of an operating system. In some cases, even slightly older versions of operating systems get security updates. (Unfortunately, this is no longer the case with Windows XP—stop using it!) What's most important is that your OS is still receiving security updates, and that you're applying them.

So if you come away with one lesson from this guide is: update, update, update, or patch, patch, patch.

Many common cyberattacks take advantage of flaws in outdated software such as old web browsers, PDF readers, or spreadsheet and word-processing tools. By keeping everything up to date, you have a way lower chance of becoming a victim of malware, because responsible manufacturers and software developers quickly patch their products after new hacks are seen in the wild.

Hacking is often a path of least resistance: you go after the easy, soft, targets first. For example, the hackers behind the destructive ransomware outbreak known as WannaCry hit victims who had not applied a security update that had been available for weeks. In other words, they knew they were going to get in because the victims had not changed the lock to their door even though their keys had already been made available to everyone.

Passwords

******

We all have too many passwords to remember, which is why some people just reuse the same ones over and over. Reusing passwords is bad because if, for example, a hacker gets control of your Netflix or Spotify password, they can then use it to get into your ridesharing or bank account to drain your credit card. Even though our brains aren't actually that bad at remembering passwords, it's almost impossible to remember dozens of unique, strong passwords.

The good news is that the solution to these problems is already out there: password managers. These are apps or browser extensions that keep track of passwords for you, automatically help you create good passwords, and simplify your online life. If you use a manger, all you have to remember is one password, the one that unlocks the vault of your other passwords.

That one password better be good though. Forget about capital letters, symbols, and numbers. The easiest way to make a secure master password is to make a passphrase: several random but pronounceable—and thus easier to memorize—words. For example: floodlit siesta kirk barrel amputee dice (don't use this one though, we just burned it.)

Once you have that you can use unique passwords made of a lot of characters for everything else, as long as you create them with a password manager and never reuse them. The master password is better as a passphrase because it's easier to memorize, and the other passwords don't need to be memorized because the manager will remember them.

Intuitively, you might think it's unwise to store your passwords on your computer or with a third party password manager. What if a hacker gets in? Surely it's better that I'm keeping them all in my head? Well, not really: The risk of a crook reusing a shared password that has been stolen from somewhere else is far greater than some sophisticated hacker independently targeting your database of passwords. For example, if you used the same password across different websites, and that password was stolen in the massive Yahoo! hacks (which included 3 billion people), it could easily be reused on your Gmail, Uber, Facebook, and other websites. Some password managers store your passwords encrypted in the cloud, so even if the company gets hacked, your passwords will be safe. For example, the password manager LastPass has been hacked at least twice, but no actual passwords were stolen because the company stored them securely. LastPass remains a recommended password manager despite those incidents. Again, it's all about understanding your own threat model.

So, please, use one of the many password managers out there, such as 1Password, LastPass, or KeePass. there's no reason not to do it. It will make you—and the rest of us!—safer, and it'll even make your life easier.

And if your employer asks you to change passwords periodically in the name of security, please tell them that's a terrible idea. If you use a password manager, two-factor authentication (see below), and have unique strong passwords for every account there's no need to change them all the time—unless there's a breach on the backend or your password is stolen somehow.

Two-Factor Authentication

Having unique, strong passwords is a great first step, but even those can be stolen. So for your most important accounts (think your email, your Facebook, Twitter accounts, your banking or financial accounts) you should add an extra layer of protection known as two-factor (or two-step or 2FA) authentication. A lot of services these days offer two-factor, so it doesn't hurt to turn it on in as many places as you can. See all the services that offer 2FA at twofactorauth.org.

By enabling two-factor you'll need something more than just your password to log into those accounts. Usually, it's a numerical code sent to your cellphone via text messages, or it can be a code created by a specialized app (which is great if your cellphone doesn't have coverage at the time you're logging in), or a small, physical token like a USB key (sometimes called a YubiKey, named after the most popular brand).

There's been a lot of discussion in the last year about whether text messages can be considered a safe "second factor." Activist DeRay McKesson's phone number was hijacked, meaning hackers could then have the extra security codes protecting accounts sent straight to them. And the National Institute of Standards and Technology (NIST), a part of the US government that writes guidelines on rules and measurements, including security, recently discouraged the use of SMS-based 2FA.

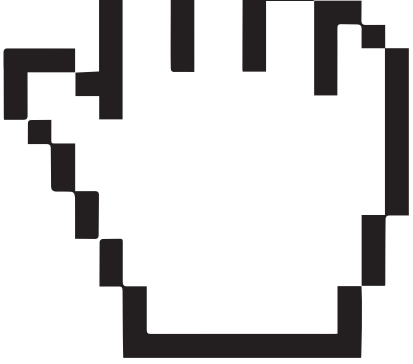
The attack on DeRay was made possible by "social engineering." In this case, a customer service rep was tricked by a criminal into making DeRay vulnerable. The attack involved getting his phone company to issue a new SIM card to the attackers, allowing them to take over his phone number. That means when they used his first factor (the password) to login to his account, the second factor code was sent directly to them. This is an increasingly common hack.

It's hard to defend against an attack like that, and it's a sad truth that there is no form of perfect security. But there are steps you can take to make these attacks harder, and we detail them below, in the mobile security section.

SMS-based two-factor can be gamed, and it's also possible to leverage vulnerabilities in the telecommunications infrastructure that carries our conversations or to use what's known as an IMSI-catcher, otherwise known as a Stingray, to sweep up your cellphone communications, including your verification texts. We don't write this to scare you, it's just worth noting that while all forms of two-factor authentication are better than nothing, you should use an authentication app or better yet a physical key if at all possible.

You should, if the website allows it, use another 2FA option that isn't SMS-based, such as an authentication app on your smartphone (for example, Google Authenticator, DUO Mobile, or Authy), or a physical token. If that option is available to you, it's a great idea to use it.

Dos & Don'ts



☑ Dos

Do use antivirus: Yes, you've heard this before. But it's still (generally) true. Antiviruses are actually, and ironically, full of security holes, but if you're not a person who's at risk of getting targeted by nation-state hackers or pretty advanced criminals, having antivirus is still a good idea. Still, antivirus software is far from a panacea, and in 2017 you need more than that to be secure. Also, be aware that antivirus software, by definition, is incredibly invasive: it needs to reach deep into your computer to be able to scan and stop malware. This reach can be abused. For example, the US government accuses Kaspersky Lab, one of the most well-known antivirus software in the world, of having passed sensitive documents from one of its customers to the Russian government.

Do use some simple security plugins: Sometimes, all a hacker needs to pwn you is to get you to the right website—one laden with malware. That's why it's worth using some simple, install-and-forget-about-it plugins such as adblockers, which protect you from malware embedded in advertising presented by the shadier sites you may wander across on the web, and sometimes even legitimate sites. (We'd naturally prefer if you whitelisted Motherboard since web ads help keep our lights on.)

Another useful plugin is HTTPS Everywhere, which forces your connection to be encrypted (when the site supports it). This won't save you if the website you're going to has malware on it, but in some cases, it helps prevent hackers from redirecting you to fake versions of that site (if there's an encrypted one available), and will generally protect against attackers trying to tamper with your connection to the legitimate one.

Do use a VPN: Virtual Private Networks are a secure channel between your computer and the internet. If you use a VPN, you first connect to the VPN, and then to the whole internet, adding a layer of security and privacy. If you're using the internet in a public space, be it a Starbucks, an airport, or even an Airbnb apartment, you are sharing it with people you don't know. And if some hacker is on your same network, they can mess up with your connection and potentially your computer. It's worth doing some research on VPNs before getting one, because some are much better than others (most of the free ones don't do a great job of protecting your privacy). We recommend Freedome, Private Internet Access, or, if you're a technical user, Algo.

Do disable macros: Hackers can use Microsoft Office macros inside documents to spread malware to your computer. It's an old trick, but it's back in vogue to spread ransomware. Disable them!

Do back up files: We're not breaking any news here, but if you're worried about hackers destroying or locking your files (such as with ransomware), then you need to back them up. Ideally, do it while you're disconnected from the network to an external hard drive so that even if you get ransomware, the backup won't get infected.

☒ Don'ts

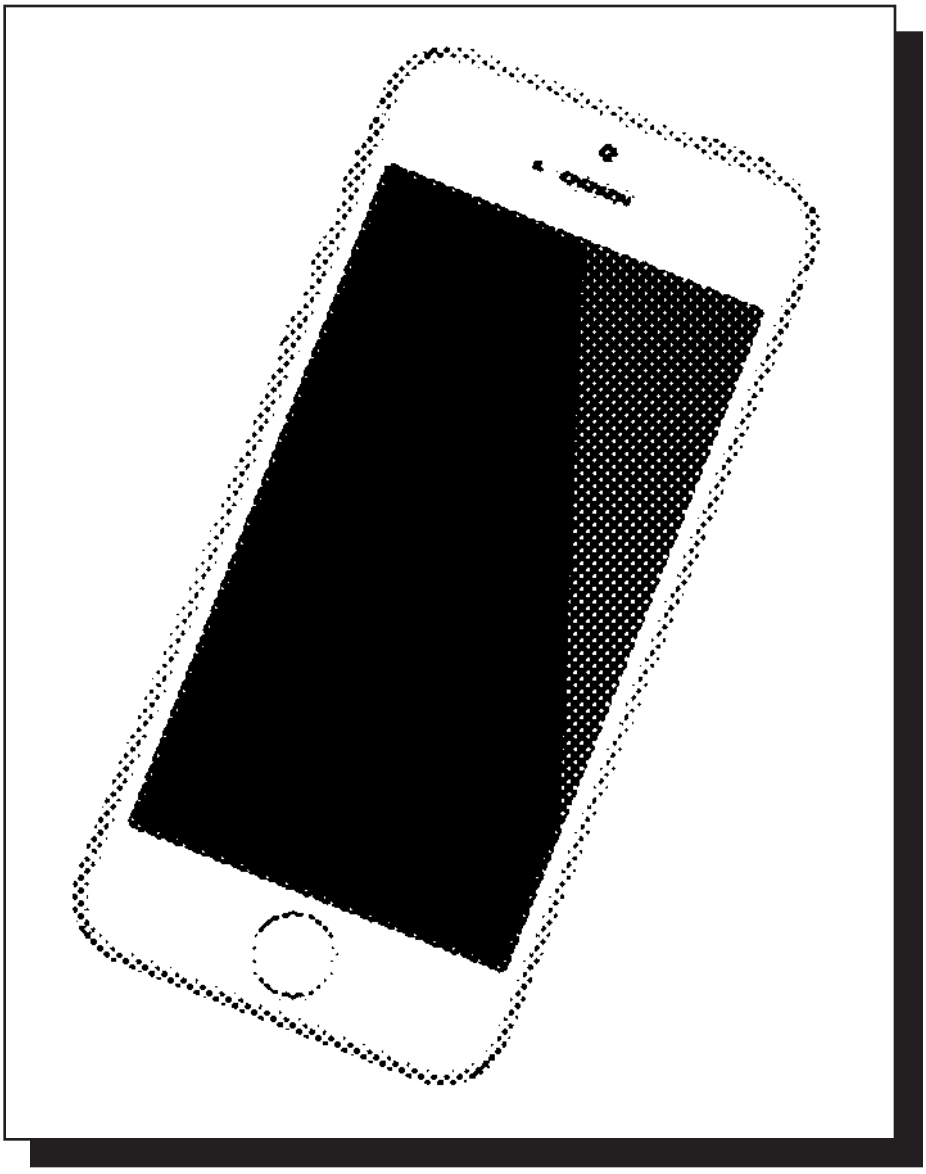
Don't use Flash: Flash is historically one of the most insecure pieces of software that's ever been on your computer. Hackers love Flash because it's had more holes than Swiss cheese. The good news is that a lot of the web has moved away from Flash so you don't really need it anymore to still enjoy a fully-featured and rich browsing experience. So consider purging it from your computer, or at least change the settings on your browser so you have to click to run Flash each time.

Don't overexpose yourself for no reason: People love to share pretty much everything about their lives on social media. But please, we beg you, don't tweet a picture of your credit card or flight's boarding pass, for example. More generally, it's a good mindset to realize that a post on social media is often a post to anyone on the internet who can be bothered to check your profile, even if it's guessing your home address through your running routes on a site like Strava, a social network for runners and cyclists.

Personal information such as your home address or high school (and the school's mascot, which is a Google away) can then be used to find more information via social engineering schemes. The more personal information an attacker has, the more likely they are to gain access to one of your accounts. With that in mind, maybe consider increasing the privacy settings on some of your accounts too.

Don't open attachments without precautions: For decades, cybercriminals have hidden malware inside attachments such as Word docs or PDFs. Antiviruses sometimes stop those threats, but it's better to just use commons sense: don't open attachments (or click on links) from people you don't know, or that you weren't expecting. And if you really want to do that, use precautions, like opening the attachments within Chrome (without downloading the files). Even better, save the file to Google Drive, and then open it within Drive, which is even safer because then the file is being opened by Google and not your computer.

Mobile Security



Mobile Security

We now live in a world where smartphones have become our primary computing devices. Not only we use cellphones more than desktop computers, but we keep them with us pretty much all the time. It goes without saying then, that hackers are targeting mobile phones more and more every day.

The good news is there are some basic steps and some precautions you can take to minimize the risks, and we're going to tell you what they are.

Mobile Threat Modeling

Most people use passcodes, passwords, or patterns to "lock" their phones. If you don't do this, you absolutely should! (Patterns are far easier to guess or "shoulder surf" than pins or passcodes, however, according to a recent study.)

One of the biggest mobile threats is someone who has physical access to your phone and can unlock it. This means your security is only as good as your passcode: If at all possible, avoid giving out your code or password, and avoid using easily guessed passcodes such as your birthday or address. Even simple passcodes and passwords are great to stop pickpockets or street thieves, but not so great if what you're worried about is an abusive partner who knows your PIN, for example.

With that in mind, here's a few basic things you can do to prevent other common threats to your cellphone.

Get an iPhone

Pretty much everyone in the world of cybersecurity—except perhaps the engineers working on Android—believes that iPhones are the most secure cellphone you can get. There are a few reasons why, but the main ones are that iOS, Apple's mobile operating system, is extremely locked down. Apps go through extensive checks before getting on the App Store, and there are extensive security measures in place, such as the fact that only code approved and digitally signed by Apple (a measure known as code-signing) and the fact that apps are limited from reaching into other apps (sandboxing). These features make it really hard for hackers to attack the most sensitive parts of the operating system. Because Apple controls the iOS infrastructure, iPhones get immediate, regular security updates and patches from Apple; critical security updates for many Android devices can take weeks or months to be pushed to users. Even the iPhone 5s, which was launched in 2013, is still supported.

So if you are paranoid, the iPhone is the most secure cellphone out of the box. But unless you have a really good reason for it, do NOT jailbreak it. While the jailbreaking movement and the hackers behind it have contributed to make the iPhone more secure, jailbreaking an iPhone at this point doesn't really provide you any feature that's worth the increased risks. In the past, hackers have been able to target at scale only jailbroken iPhones.

Nothing is unhackable though. We know some governments are armed with million-dollar hacking tools to hack iPhones, and perhaps some sophisticated criminals might have those too. Still, get an iPhone, install the updates, and don't jailbreak it and you'll probably be fine.

But I Love Android! Fine...

Android has become the most popular operating system in the world thanks to its decentralized, open-source nature and the fact that many handsets are available at prices much lower than iPhones. In some ways, this open-sourced nature was Android's original sin: Google traded control, and thus security, for market share. This way, critical security updates depend on carriers and device manufacturers, who have historically been lackadaisical about pushing them out.

The good news is that in the last two years this has improved a lot. Google has been pushing partners to give users monthly updates, and Google's own flagship devices have almost the same kind of regular support that Apple provides to iPhones, as well as some of the same security features.

So your best bet is to stick to Pixels or Nexus phones, whose security doesn't depend on anyone but Google. If you really don't want a Google phone, these cellphones have a good track record of pushing security updates, according to Google itself.

Whatever Android phone you own, be careful what apps you install. Hackers have traditionally been very successful at sneaking malicious apps on the Play Store so think twice before installing a little-known app, or double check that the app you're installing really is the one you want. Earlier this fall, a fake version of WhatsApp was installed by more than a million Android users. Also, stick to the Play Store and avoid downloading and installing apps from third-party stores, which may very well be malicious. On most Android phones, installing third-party apps is not enabled by default, leave it that way.

To protect the data on your Android phone, make sure full disk encryption is enabled. Open your Settings app, go to "Security" and click on "Encrypt Phone" if it's not enabled already. (If this doesn't work on your device, Google for instructions on your specific handset).

Finally, while not mandatory, it might be a good idea to install a mobile antivirus such as Lookout or Zips. While these can be effective against criminal's malware, they probably won't stop government hackers.

Lock Up That Sim Card

Recently we revealed that hackers had been exploiting a nasty bug on a T-Mobile website to pull the personal data of customers in an attempt to gather data that they could then use to impersonate the victims and socially engineer T-Mobile support technicians into issuing new SIM cards. These kind of attacks, known as "SIM swapping" or "SIM hijacking," allow hackers to take over your cellphone number, and in turn anything that's connected to it. SIM hijacking is what makes two-factor authentication via SMS so dangerous.

Your phone number is likely the gateway to multiple other, perhaps more sensitive, parts of your digital life: your email, your bank account, your iCloud backups.

As a consumer, you can't control the bugs that your carrier leave open for hackers. But you can make it a bit harder for hackers to impersonate you with gullible tech support employees. The solution is easy, although not that many people know about it: a secondary password or passcode that you need to provide when you call your cellphone provider. Most US carriers now offer this option.

Call your provider and ask them to set this up for you. Motherboard confirmed that Sprint, T-Mobile, Verizon and U.S. Cellular all give customers this option. Verizon and U.S. Cellular have made this mandatory, according to their spokespeople. Of course, make sure you remember this phone password, or better yet, write it down in your password manager.

The Motherboard Guide to Privacy, Messaging, and Protecting Yourself From State and Law Enforcement Surveillance

In the wake of September 11th, the United States built out a massive surveillance apparatus, undermined constitutional protections, and limited possible recourse to the legal system.

Given the extraordinary capabilities of state surveillance in the US—as well as the capabilities of governments around the world—you might be feeling a little paranoid! It's not just the NSA—the FBI and even local cops have more tools at their disposal to snoop on people than ever before. And there is a terrifying breadth of passive and unexpected surveillance to worry about: Your social media accounts can be subpoenaed, your emails or calls can be scooped up in bulk collection efforts, and your cell phone metadata can be captured by Stingrays and IMSI catchers meant to target someone else.

Remember, anti-surveillance is not the cure, it's just one thing you can do to protect yourself and others. You probably aren't the most at-risk person, but that doesn't mean you shouldn't practice better security. Surveillance is a complicated thing: You can practice the best security in the world, but if you're sending messages to someone who doesn't, you can still be spied on through their device or through their communications with other people (if they discuss the information you told them, for instance).

That's why it's important that we normalize good security practices: If you don't have that much to be afraid of, it's all the more important for you to pick up some of these tools, because doing that will normalize the actions of your friends who are, say, undocumented immigrants, or engaged in activism. Trump's CIA Director thinks that using encryption "may itself be a red flag." If you have "nothing to hide," your use of encryption can actually help people at risk by obfuscating that red flag. By following this guide, you are making someone else safer. Think of it as herd immunity. The more people practice good security, the safer everyone else is.

The security tips provided earlier in this guide still apply: If you can protect yourself from getting hacked, you will have a better shot at preventing yourself from being surveilled (when it comes to surveilling iPhones, for instance governments often have few options besides hacking the devices). But tech tools don't solve all problems. Governments have a weapon in their hands that criminal hackers do not: the power of the law. Many of the tips in this section of the guide will help you not only against legal requests and government hacking, but also against anyone else who may be trying to spy on you.

You don't have to turn yourself into a security expert. Just start thinking about your risks, and don't be intimidated by the technology. Security is an ongoing process of learning. Both the threats and the tools developed to address them are constantly changing, which is one of the reasons why privacy and security advice can often seem fickle and contradictory. But the tips below are a good starting point.

Threat Modeling (privacy and surveillance edition)

Keep in mind that different tools address different problems. Without threat modelling, it's easy to feel overwhelmed by how many tools are out there. Threat modeling for surveillance is similar to threat modelling for hacking, but there are of course some nuances that vary in every situation.

It's easy for some people to say "use Signal, use Tor," and be done with it, but that doesn't work for everyone. For example, a friend used to message people about her abusive ex-partner using the built-in Words With Friends messenger, because she knew that he read her text messages and Gchat. Words With Friends does not have a particularly secure messaging system, but in this case it was a better option than Signal or Hangouts because he didn't think to read her messages on the game.

When it comes to state actors, it might be helpful to think of surveillance in two different forms: surveillance of metadata (who you are, who you're talking to, when you're talking) and surveillance of content (what you are saying). As with all things, when you dig a little deeper, it's not as simple as that. But if you're thinking about this for the first time, it's a good start.

Surveillance law is complicated, but long story short, both the law and current technological infrastructure make it easier to grab metadata than content. Metadata isn't necessarily less important or revealing than content. Say Planned Parenthood called you. Then you call your partner. Then you call your insurance. Then you call the abortion clinic. That information is going to be on your phone bill, and your telephone provider can easily give it up to the government. Your cell provider might not be recording those calls—the content is still private. But at that point, the content doesn't matter—it would be easy for someone with the metadata alone to have a reasonable idea of what your calls were about.

Start thinking about what is open and exposed, and what you can protect. Sometimes, you have to accept that there's very little you can do about a particular channel of communication. If circumstances are dire, you're going to just have to work around it.

Signal

Signal is an encrypted messaging service for smartphones and desktop computers. It is, for many—but not all—people, a good option for avoiding surveillance. Because the government has the capability to intercept electronic messages while they're being transmitted, you want to use end-to-end encryption for as many of your communications as possible.

Using Signal is easy. You can find it and install it from your phone's app store. (In the iOS App Store and the Google Play Store, it's called "Signal Private Messenger," and it's made by Open Whisper Systems.)

If you have the other person's phone number in your contacts list, you can see them in Signal, and message them or call them. As long as the other person also has Signal, the messages automatically encrypt—all the work is invisible.

It even has a desktop app, so you can use it the way that iOS/Mac OS people use iMessage on both their phones and computers. Go to the Signal.org website and download the app for your preferred operating system. Just follow the instructions—trust us, they're easy.

Signal also lets you set a timer for messages to automatically expire, thus deleting them from all devices. You can set the timer for all kinds of lengths, including very short ones. This is a great feature for journalists who are concerned about protecting their sources or their conversations with editors.

These are great features, and they're part of the reason why we recommend Signal over many other end-to-end messaging apps. iMessage and WhatsApp also use end-to-end encryption, but they both have drawbacks.

We do not recommend WhatsApp, because WhatsApp is owned by Facebook, and has been sharing user information with its parent company. While this is only metadata, it is ultimately a rollback of a privacy promise made when WhatsApp was acquired by Facebook. We think this says something negative about the overall trustworthiness of the company in coming days.

It is a very good thing that Apple encrypts iMessages end-to-end. But iMessage also backs up messages to iCloud by default, which is why you can message from all your Apple devices. This is a great and fun feature, but if you're concerned about government surveillance, remember that Apple complies with lawful government demands for data in your iCloud: "iMessage and SMS messages are backed up on iCloud for your convenience," Apple's privacy page states. You can turn this feature off, but in theory Apple could be forced to access the iMessages you've sent people who still have the feature enabled.

Signal keeps very little information. We know this, because Open Whisper Systems was subpoenaed by the government last year, and was forced to hand over information. But the information it had—by design—was pretty minimal. Signal retains phone number, account creation date, and the time of the user's last connection to Signal servers. Yes, that's still something, but as you can see, it's not very much.

There are worse products to use than iMessage and WhatsApp. For example, you absolutely should avoid using Telegram for sensitive communications. And Google can read your GChats unless you take additional steps to encrypt them end-to-end. There are several other products on the market that are decent alternatives (for example, Wire), but like WhatsApp and iMessage, they're created and maintained by for-profit companies, and we don't know how they're planning to monetize in the future. Signal is an open source, nonprofit project. That has its own drawbacks (for example, Signal is not as slick as iMessage, nor does it have the luxury of having a large security team behind it), so maybe donate money when you download it?

One thing that's worth mentioning about Signal is that it requires you to associate the device with a phone number. This means that you need to trust the people you're messaging to have your phone number (or need to jump through hoops to use Signal with a dummy phone number); there are many reasons why you might want to message people without giving them your phone number, which is one of the potential drawbacks of Signal. If this is a concern for you, consider another option.

Another thing to remember is that just because a communication is end-to-end encrypted doesn't mean it's invisible to the government. It just means the contents are encrypted between endpoints. You can see the message, your recipient can see the message. If it's intercepted in transit, it's completely garbled, and the content of your message is protected from spying eyes.

But if an "endpoint" is compromised—in other words, if your own phone is hacked or physically seized by the government, or your texting partner is screencapping your conversation—it's game over.

Encryption doesn't make it impossible for the government to snoop, it just makes it way more challenging. The point is that introducing friction into the equation does provide privacy.

Be conscious of what you post on social media

If you post publicly on social media, know that local police (and likely federal agencies as well) keep tabs on activists online. For example, Facebook, Instagram, and Twitter have all fed data to social media monitoring products that police departments used to track Black Lives Matter activists.

Even if you keep your privacy settings on lockdown, social media companies are subject to subpoenas, court orders, and data requests for your information. And often times, they'll fork over the information without ever notifying the user that it's happening. For the purposes of social media, assume that everything you post is public. This doesn't mean you should stop using social media, it just means you have to be mindful of how you use it.

If you're an activist, consider using a pseudonym for your activism. If you post online at all, take others' safety and privacy into consideration as well.

Who are you tagging into your posts? Are you adding location information? Who are you taking a picture of, and why? Be particularly careful with photos or posts about protests, rallies, or meetings. Facial recognition technology is fairly sophisticated now, so even if you leave people untagged, theoretically an algorithm could scan for and identify activists in a photograph of a rally. You can already see this at work in Facebook's tag suggestions.

When you take a picture of someone at a protest, make sure that they consent, and that they know the implications of having a photo of themselves out there.

Beware of device cameras and microphones

Do you live around any cameras? If you use internet-connected security cameras inside your home, or have a webcam running, don't leave these things unsecured. Make sure that you've changed any passwords from the default that they shipped with, and cover them when you're not using them.

If you have a laptop or a smartphone, use a sticker to cover the front-facing camera. You don't have to stop Facetiming and taking selfies, you just want to cover things up so no one's looking at you when you don't want them to. The Electronic Frontier Foundation sells removable laptop cover stickers (five for $5) that won't leave a residue on your camera, so you can take it on and off whenever you need it. Consider buying several and giving them to friends who might be shorter on cash.

Finally, there is absolutely no way to make sure your microphone is not recording. If you're concerned about being wiretapped, consider turning off your phone and putting it in the microwave (temporarily, with the microwave off), or leaving your phone in the other room. Turning your phone off alone does not necessarily protect you! And consider leaving all your devices outside of the bedroom when you have sex with your partner.

In 2012, Khadija Ismayilova, an Azeri journalist, was blackmailed with a surreptitiously filmed sex tape. The blackmailer told Ismayilova to stop publishing articles critical of the government, or else have her tape released. (Ismayilova went public, and the tape was posted on the internet.) In 2015, the Azerbaijan government sentenced her to seven and a half years in prison on tax evasion charges. She is currently out on probation.

Governments at home and abroad have used sex to blackmail dissenters. Be aware of that, and protect your privacy.

Protect your devices with a lock screen

Put a password/passcode on your phone and your computer. Don't rely on your thumbprint alone. The police are more likely to be able to legally compel you to use your fingerprint to open up your phone. You may have a stronger constitutional right not to speak your password.

Use OTR for chatting (if you have to)

It's best to use Signal for desktop when chatting with people. But here's another option that's particularly useful for journalists.

Close your Gmail window and use OTR (Off The Record) instead to chat. Keep in mind that you can only use OTR if the other person is also using OTR*.

You can use your Gmail account as your chat ID. So what's going on is that you're engaging in Gchat, but with a layer of encryption on top. Open up a chat window and click the lock icon to begin encryption. And make sure you tweak your settings so that you're not retaining chat logs during encrypted conversations.

Again, end-to-end only goes so far. If the other person is logging your conversations, it might not matter that you went this far. If you're concerned, ask your friend to stop logging.

**Mac users can install Adium, PC (and Linux) users will have to install Pidgin and the OTR plugin.*

Install the Tor Browser

Tor—which takes its name from an acronym for "The Onion Router"—scrambles your internet traffic by routing it through several layers of computers. This way, when you access a website, it can't tell where you're connecting from. The easiest way to use Tor is just to install the Tor Browser. It's just like Firefox or Chrome or Internet Explorer, just a lot slower because of the privacy it provides.

Using Tor for everything will give you a big privacy boost, but it's a bit unwieldy. Don't, for instance, try to stream Netflix over Tor.

Evaluate your needs and figure out how much Tor you need in your life. Always remember that your IP address (which can give away where you are, and therefore, who you might be) is laid bare if you aren't using it.

There are four reasons why you might want to use Tor.

You're trying to keep your identity hidden.
You use a lot of public WiFi.
You're trying to get around government censorship.
You are protecting the other people who use Tor.

If you're an activist who is trying to hide their identity, you need Tor to mask your IP address. This is a limited use case scenario. For example, it's self-defeating for me to open up Tor, log into my public Twitter account, and tweet, "What up, everyone, I'm tweeting from the Vice Media offices in New York City." I am giving away all the information that Tor is masking for me—because when it comes down to it, in that use case scenario, I was never planning on keeping it private.

If you connect to a lot of public Wi-Fi (think Starbucks, a hotel, or the airport), though, you should use Tor. It provides similar benefits as VPNs , but without many of the drawbacks of a VPN (see the next section for a discussion of that).

If the United States begins to censor parts of the web, as many other governments do, Tor might be able to help you get around that. Tor certainly helps people connecting to the internet from other countries that practice internet censorship.

Finally, the thing about Tor is that the more people use it, the less trackable everyone else is. When a lot of random, unaffiliated people from all over the world use it, it becomes stronger and stronger. If you take the time to use Tor every day, you are helping people who really do need it.

A couple caveats, here: Tor is not bulletproof. The government has been known to hack groups of users on Tor, just like it's been known to hack VPN users en masse. Tor, by itself, does not make it more unlikely for you to get hacked. Tor is for privacy, not security. And Tor is designed to make it hard to log your traffic, not impossible, so there's always a risk that you aren't being hidden.

The computers that make up the Tor network—the ones that your traffic bounces through—are run by volunteers, institutions, and organizations all over the world, some of whom face legal risks for doing so. They are not supposed to log the traffic that goes through them, but because it's a volunteer network, some might. The risk is mitigated by the fact that each node only sees a snapshot of the traffic running through it, and nobody has access to both the user's IP and their unencrypted traffic. A bad actor would have to run a very large number of Tor nodes to start logging meaningful traffic—which would be difficult—and the Tor project monitors for behavior that suggests anybody might be doing that.

Ultimately, for the purposes of state surveillance, Tor is better than a VPN, and a VPN is better than nothing.

It's not clear whether Tor will continue to exist into the future. Tor is run partly through grants from the government. (Like many cutting edge technologies, Tor was originally developed by the US military.) It's possible Tor will lose most of its funding in the very near-term. Consider donating to the Tor Project.

Virtual Private Networks

When it comes to state surveillance, VPNs won't help much. A VPN will obscure your IP address, but when it comes to state surveillance, VPNs can be subpoenaed for user information that may ultimately identify you. For example, many VPN companies keep logs on what IP addresses log on when and what sites are accessed—which can end up pinpointing you, especially if you used your credit card to pay for a VPN subscription.

Some VPN companies claim not to log user information. You need to evaluate how much you trust these companies, and make that decision for yourself. If what you're concerned about is government surveillance, our recommendation is that you stick with Tor.

PGP (probably isn't worth the trouble)

The only reliable way to encrypt your email is PGP—also known as Pretty Good Privacy. However, PGP is incredibly obnoxious to use. Even PGP's creator Phil Zimmermann has stopped using it, since he can't use it on his phone. The problem isn't just that you have to figure out PGP, everyone you talk to also has to figure it out. Telling someone to download Signal is a lot easier than walking them through public/private key encryption. This is where your threat model comes in handy, to help figure out if PGP is actually worth it to you.

If you absolutely must use encrypted email, this guide to PGP might be helpful. It's tricky, so you might want to go to a crypto party and have an activist or technologist help you set it up.

Don't run your own email server

If 2016 did anything, it convinced everyone not to run their own private email server.

It's true that Google and other companies have to comply with court orders for your information, including your emails. But on the other hand, Google knows how to run email servers way better than you do. Email servers are hard! Just ask Hillary Clinton.

If you are encrypting email, Google can only hand over the metadata (who's sending to whom and subject headers). Since encrypting email is a huge pain, try to keep all your sensitive stuff away from email, and in end-to-end encrypted channels instead. Don't abandon your third-party email account, just be aware that the government can get at what's inside.

Encrypt your hard drive

Good news: this isn't as hard as it used to be!

Full-disk encryption means that once your device is locked (when it's off, or when it's on but showing a lock screen), the contents of your hard drive can't be accessed without your password/key.

A lot of smartphones come with full disk encryption built in. If you own an iPhone with a recently updated operating system (like, in the last three years, really), just slap a passcode on that sucker and you're golden.

If you own an Android phone, it might already be encrypted by default (Google Pixel is). But chances are, it's not. There isn't an up-to-date guide on turning on encryption on all Android devices, so you're going to have to poke around yourself, or ask a friend. And if you own a Windows phone, god help you, because we can't.

As for computers, things are again, much easier than they used to be. Use your operating system's full disk encryption option instead. For MacBooks running Lion or newer, just turn on FileVault.

Windows, on the other hand, is a lot more complicated. First off, some users have encryption by default. Some more users can turn it on, but it's kind of a pain. And if you're using Microsoft's Bitlocker, you're going to have to fiddle with some additional settings to make it more secure. Apple doesn't retain the capability of unlocking your devices. Famously, if the government goes to Apple, Apple can't just decrypt your phone for the feds, not without coming up with a hack that will affect every iPhone in the world. But Microsoft isn't doing quite the same thing—in some cases they use what's known as "key escrow," meaning they can decrypt your machine—so you have to take additional steps (outlined in this article) to get that same level of protection.

You may need to resort to using VeraCrypt. A lot of older guides will say to use TrueCrypt, regardless of operating system. This is now outdated advice. VeraCrypt used to be TrueCrypt, and the story of why it's not any more is a convoluted crypto soap opera with plot holes the size of Mars, and it is frankly outside the scope of this guide. Long story short, there's nothing wrong with VeraCrypt as far as the experts can tell, but if you have the option, use the full disk encryption that your operating system already provided.

If you use Linux, your distro probably supports encryption out of the box. Follow the instructions while installing.

If you're a journalist, know the risk of hanging onto your notes

Want to protect your sources? Your notes, your Slack chats, your Gchats, your Google Drive, your Dropbox, your recorded interviews, your transcripts, and your texts can all end up in court. Depending on what kind of court case it is, it might not matter that it's encrypted.

Don't wait until a lawsuit is imminent to delete all your stuff. That might be illegal, and you might be risking going to jail. Every situation is different: your notes might be necessary to get you out of trouble. So if you're the type to hoard notes, know the risk, talk to a lawyer, and act responsibly.

Credit Cards

Know that credit card companies never stand up to the government. If you pay for anything using your credit card, know that the government can get that information pretty easily. And remember that once your identity touches something, there's a chain that the government can follow all the way back.

For example, if you get a prepaid Visa gift card using your personal credit card, and pay a VPN company with that, the government can just go backwards through the chain and find your personal credit card, and then you. If you pay a VPN company with Bitcoin, but you bought the Bitcoin through a Bitcoin exchange using your personal credit card, that's traceable as well.

This applies to anything else you use money for, like buying domains or cheap, pay-as-you-go phones, known as burners. Practically speaking, there's not a lot you can do about this. It's one of the reasons why we recommend Tor instead of a VPN service.

It's also one of the reasons why it's so hard to get a burner phone that's really a burner. (How are you going to pay for continuing phone service without linking your name to it?) There is no easy answer here. We're not going to pretend to be able to give good advice in this instance. If you find yourself in a situation where your life depends on staying anonymous, you're going to need a lot more help than any internet guide.

One more thing: For now, organizations like the ACLU and NAACP have a constitutional right to resist giving up the names of donors. But your credit card or PayPal might betray you anyways. This doesn't mean you shouldn't donate to organizations that resist oppression and fight for civil rights and civil liberties. Rather, it makes it all the more important that you do. The more ordinary people do so, the more that individual donors are protected from scrutiny and suspicion.

We don't know what the future holds

Which brings us to our next point: we don't know what the future holds. This guide was written with the current technical and legal capabilities of the United States government in mind. But that might all change in the future. Strong encryption might become illegal. The United States might begin to practice internet censorship the way that China and other countries do. The government might institute a National ID policy for getting online, making it near-impossible to post anonymously.

These things are harder to enforce and implement, so they're not likely to happen quickly.

It's also not infeasible that the government pressures app stores to take down Signal and other end-to-end encryption applications. This guide might be only be so good for so long. That's all the more reason to become proactive against surveillance now, and to keep adapting to changing circumstances.

Meet in person

Many public places have cameras, some spots are wired with microphones. And there's always the possibility that you are being individually targeted for surveillance. But ultimately, it's a lot harder to surveil someone in person than to collect the electronic communications of many people at the same time.

Take a break from the wired world and meet people in person. If you stay out of earshot, you won't be overheard, and your words will melt into the air, unsurveilled and unrecorded.

And besides, if you're reading this guide, chances are that you really need a hug right now.

So meet up with your friends, verify your Signal keys, and give each other a big hug. Because you're probably both scared, and you need each other more than you need any of this technology.

Go Out There And Be Safe

That is all for now. Again, this is just meant to be a basic guide for average computer users. So if you're a human rights activist working in a dangerous country or a war zone, or an organization building IT infrastructure on the fly, this is certainly not enough, and you'll need more precautions.

But these are common sense essential tips that everyone should know about.

Of course, some readers will leap at the chance to point out everything that may have been missing from this guide, and we'd like to hear your feedback. Security is a constantly changing world, and what's good advice today might not be good advice tomorrow, so our goal is to keep this guide updated somewhat regularly, so, please, do reach out if you think we have something wrong or missing something.

And remember, always be vigilant!

Glossary of Hacking and Cyber Terms

One of the challenges of writing—and reading—about hacking is that it's a world full of jargon and technical terms. It's our job as journalists to translate this lingo and make it understandable to the average reader.

Still, accuracy is important and sometimes you have to use the right terms. To help you navigate this guide, we thought this glossary—which includes some concepts and terms not raised elsewhere in the guide—would help.

Attribution: Attribution is the process of establishing who is behind a hack. Often, attribution is the most difficult part of responding to a major breach since experienced hackers may hide behind layers of online services that mask their true location and identity. Many incidents, such as the Sony hack, may never produce any satisfactory attribution.

Backdoor: Entering a protected system using a password can be described as going through the front door. Companies may build "backdoors" into their systems, however, so that developers can bypass authentication and dive right into the program. Backdoors are usually secret, but may be exploited by hackers if they are revealed or discovered.

Black hat: A black hat hacker is someone who hacks for personal gain and/or who engages in illicit and unsanctioned activities. As opposed to white hack hackers (see below), who traditionally hack in order to alert companies and improve services, black hat hackers may instead sell the weaknesses they discover to other hackers or use them.

Botnet: Is your computer part of a botnet? It could be, and you might not know it. Botnets, or zombie armies, are networks of computers controlled by an attacker. Having control over hundreds or thousands of computers lets bad actors perform certain types of cyberattacks, such as a DDoS (see below). Buying thousands of computers wouldn't be economical, however, so hackers deploy malware to infect random computers that are connected to the internet. If your computer gets infected, your machine might be stealthily performing a hacker's bidding in the background without you ever noticing.

Brute force: A brute force attack is arguably the least sophisticated way of breaking into a password-protected system, short of simply obtaining the password itself. A brute force attack will usually consist of an automated process of trial-and-error to guess the correct passphrase. Most modern encryption systems use different methods for slowing down brute force attacks, making it hard or impossible to try all combinations in a reasonable amount of time.

Bug: You've probably heard of this one. A bug is a flaw or error in a software program. Some are harmless or merely annoying, but some can be exploited by hackers. That's why many companies have started using bug bounty programs to pay anyone who spots a bug before the bad guys do.

Cracking: A general term to describe breaking into a security system, usually for nefarious purposes. According to the New Hacker's Dictionary published by MIT Press, the words "hacking" and "hacker" (see below) in mainstream parlance have come to subsume the words "cracking" and "cracker," and that's misleading. Hackers are tinkerers; they're not necessarily bad guys. Crackers are malicious. At the same time, you'll see cracking used to refer to breaking, say, digital copyright protections—which many people feel is a just and worthy cause—and in other contexts, such as penetration testing (see below), without the negative connotation.

Crypto: Short for cryptography, the science of secret communication or the procedures and processes for hiding data and messages with encryption (see below).

Chip-off: A chip-off attack requires the hacker to physically remove memory storage chips in a device so that information can be scraped from them using specialized software. This attack has been used by law enforcement to break into PGP-protected Blackberry phones.

Dark web: The dark web is made up of sites that are not indexed by Google and are only accessible through specialty networks such as Tor (see below). Often, the dark web is used by website operators who want to remain anonymous. Everything on the dark web is on the deep web, but not everything on the deep web is on the dark web.

DDoS: This type of cyberattack has become popular in recent years because it's relatively easy to execute and its effects are obvious immediately. DDoS stands for Distributed Denial of Service Attack, which means an attacker is using a number of computers to flood the target with data or requests for data. This causes the target—usually a website—to slow down or become unavailable. Attackers may also use the simpler Denial of Service attack, which is launched from one computer.

Deep web: This term and "dark web" or "dark net" are sometimes used interchangeably, though they shouldn't be. The deep web is the part of the internet that is not indexed by search engines. That includes password-protected pages, paywalled sites, encrypted networks, and databases—lots of boring stuff.

DEF CON: One of the most famous hacking conferences in the US and the world, which started in 1992 and takes place every summer in Las Vegas.

Digital Certificate: A digital passport or stamp of approval that proves the identity of a person, website or service on the internet. In more technical terms, a digital certificate proves that someone is in possession of a certain cryptographic key that, traditionally, can't be forged. Some of the most common digital certificates are those of websites, which ensure your connection to them is properly encrypted. These get displayed on your browser as a green padlock.

Encryption: The process of scrambling data or messages making it unreadable and secret. The opposite is decryption, the decoding of the message. Both encryption and decryption are functions of cryptography. Encryption is used by individuals as well as corporations and in digital security for consumer products.

End-to-end encryption: A particular type of encryption where a message or data gets scrambled or encrypted on one end, for example your computer or phone, and get decrypted on the other end, such as someone else's computer. The data is scrambled in a way that, at least in theory, only the sender and receiver—and no one else—can read it.

Evil maid attack: As the name probably suggests, an evil maid attack is a hack that requires physical access to a computer—the kind of access an evil maid might have while tidying his or her employer's office, for example. By having physical access, a hacker can install software to track your use and gain a doorway even to encrypted information.

Exploit: An exploit is a way or process to take advantage of a bug or vulnerability in a computer or application. Not all bugs lead to exploits. Think of it this way: If your door was faulty, it could be simply that it makes a weird sound when you open it, or that its lock can be picked. Both are flaws but only one can help a burglar get in. The way the criminal picks the lock would be the exploit.

Forensics: On CSI, forensic investigations involve a series of methodical steps in order to establish what happened during a crime. When it comes to a hack, however, investigators are looking for digital fingerprints instead of physical ones. This process usually involves trying to retrieve messages or other information from a device—perhaps a phone, a desktop computer or a server—used, or abused, by a suspected criminal.

GCHQ: The UK's equivalent of the US' National Security Agency. GCHQ, or Government Communications Headquarters, focuses on foreign intelligence, especially around terrorism threats and cybersecurity. It also investigates the digital child pornography trade. "As these adversaries work in secret, so too must GCHQ," the organization says on its website. "We cannot reveal publicly everything that we do, but we remain fully accountable."

Hacker: This term has become—wrongly—synonymous with someone who breaks into systems or hacks things illegally. Originally, hackers were simply tinkerers, or people who enjoyed "exploring the details of programmable systems and how to stretch their capabilities," as the MIT New Hacker's Dictionary puts it. Hackers can now be used to refer to both the good guys, also known as white hat hackers, who play and tinker with systems with no malicious intent (and actually often with the intent of finding flaws so they can be fixed), and cybercriminals, or "black hat" hackers, or "crackers."

Hacktivist: A "hacktivist" is someone who uses their hacking skills for political ends. A hacktivist's actions may be small, such as defacing the public website of a security agency or other government department, or large, such as stealing sensitive government information and distributing it to citizens. One often-cited example of a hacktivist group is Anonymous.

Hashing: Say you have a piece of text that should remain secret, like a password. You could store the text in a secret folder on your machine, but if anyone gained access to it you'd be in trouble. To keep the password a secret, you could also "hash" it with a program that executes a function resulting in garbled text representing the original information. This abstract representation is called a hash. Companies may store passwords or facial recognition data with hashes to improve their security.

HTTPS/SSL/TLS: Stands for Hypertext Transfer Protocol, with the "S" for "Secure." The Hypertext Transfer Protocol (HTTP) is the basic framework that controls how data is transferred across the web, while HTTPS adds a layer of encryption that protects your connection to the most important sites in your daily browsing—your bank, your email provider, and social network. HTTPS uses the protocols SSL and TLS to not only protect your connection, but also to prove the identity of the site, so that when you type https://gmail.com you can be confident you're really connecting to Google and not an imposter site.

Infosec: An abbreviation of "Information Security." It's the inside baseball term for what's more commonly known as cybersecurity, a term that irks most people who prefer infosec.

Jailbreak: Circumventing the security of a device, like an iPhone or a PlayStation, to remove a manufacturer's restrictions, generally with the goal to make it run software from non-official sources.

Keys: Modern cryptography uses digital "keys". In the case of PGP encryption, a public key is used to encrypt, or "lock," messages and a secret key is used to decrypt, or "unlock", them. In other systems, there may only be one secret key that is shared by all parties. In either case, if an attacker gains control of the key that does the unlocking, they may have a good chance at gaining access to.

Lulz: An internet-speak variation on "lol" (short for "laughing out loud") employed regularly among the black hat hacker set, typically to justify a hack or leak done at the expense of another person or entity. Sample use: y did i leak all contracts and employee info linked to Sketchy Company X? for teh lulz

Malware: Stands for "malicious software." It simply refers to any kind of a malicious program or software, designed to damage or hack its target. Viruses, worms, Trojan horses, ransomware, spyware, adware and more are malware.

Man-in-the-middle: A Man-in-the-Middle or MitM is a common attack where someone surreptitiously puts themselves between two parties, impersonating them. This allows the malicious attacker to intercept and potentially alter their communication. With this type of attack, one can just passively listen in, relaying messages and data between the two parties, or even alter and manipulate the data flow.

Metadata: Metadata is simply data about data. If you were to send an email, for example, the text you type to your friend will be the content of the message, but the address you used to send it, the address you sent it to, and the time you sent it would all be metadata. This may sound innocuous, but with enough sources of metadata—for example, geolocation information from a photo posted to social media—it can be trivial to piece together someone's identity or location.

NIST: The National Institute of Standards and Technology is an arm of the US Department of Commerce dedicated to science and metrics that support industrial innovation. The NIST is responsible for developing information security standards for use by the federal government, and therefore it's often cited as an authority on which encryption methods are rigorous enough to use given modern threats.

Nonce: A portmanteau of number and once, nonce literally means "a number only used once." It's a string of numbers generated by a system to identify a user for a one-time-use session or specific task. After that session, or a set period of time, the number isn't used again.

OpSec: OpSec is short for operational security, and it's all about keeping information secret, online and off. Originally a military term, OpSec is a practice and in some ways a philosophy that begins with identifying what information needs to be kept secret, and whom you're trying to keep it a secret from. "Good" OpSec will flow from there, and may include everything from passing messages on Post-Its instead of emails to using digital encryption. In other words: Loose tweets destroy fleets.

OTR: What do you do if you want to have an encrypted conversation, but it needs to happen fast? OTR, or Off-the-Record, is a protocol for encrypting instant messages end-to-end. Unlike PGP, which is generally used for email and so each conversant has one public and one private key in their possession, OTR uses a single temporary key for every conversation, which makes it more secure if an attacker hacks into your computer and gets a hold of the keys. OTR is also generally easier to use than PGP.

Password managers: Using the same, crummy password for all of your logins—from your bank account, to Seamless, to your Tinder profile—is a bad idea. All a hacker needs to do is get access to one account to break into them all. But memorizing a unique string of characters for every platform is daunting. Enter the password manager: software that keeps track of your various passwords for you, and can even auto-generate super complicated and long passwords for you. All you need to remember is your master password to log into the manager and access all your many different logins.

Penetration testing or pentesting: If you set up a security system for your home, or your office, or your factory, you'd want to be sure it was safe from attackers, right? One way to test a system's security is to employ people—pentesters—to purposely hack it in order to identify weak points. Pentesting is related to red teaming, although it may be done in a more structured, less aggressive way.

PGP: "Pretty Good Privacy" is a method of encrypting data, generally emails, so that anyone intercepting them will only see garbled text. PGP uses asymmetric cryptography, which means that the person sending a message uses a "public" encryption key to scramble it, and the recipient uses a secret "private" key to decode it. Despite being more than two decades old, PGP is still a formidable method of encryption, although it can be notoriously difficult to use in practice, even for experienced users.

Phishing: Phishing is really more of a form of social engineering than hacking or cracking. In a phishing scheme, an attacker typically reaches out to a victim in order to extract specific information that can be used in a later attack. That may mean posing as customer support from Google, Facebook, or the victim's cell phone carrier, for example, and asking the victim to click on a malicious link—or simply asking the victim to send back information, such as a password, in an email. Attackers usually blast out phishing attempts by the thousands, but sometimes employ more targeted attacks, known as spearphishing (see below).

Plaintext: Exactly what it sounds like—text that has not been garbled with encryption. This definition would be considered plaintext. You may also hear plaintext being referred to as "cleartext," since it refers to text that is being kept out in the open, or "in the clear." Companies with very poor security may store user passwords in plaintext, even if the folder they're in is encrypted, just waiting for a hacker to steal.

Pwned: Pwned is computer nerd jargon (or "leetspeak") for the verb "own." In the video game world, a player that beat another player can say that he pwned him. Among hackers, the term has a similar meaning, only instead of beating someone in a game, a hacker that has gained access to another user's computer can say that he pwned him. For example, the website "Have I Been Pwned?" will tell you if your online accounts have been compromised in the past.

RAT: RAT stands for Remote Access Tool or Remote Access Trojan. RATs are really scary when used as malware. An attacker who successfully installs a RAT on your computer can gain full control of your machine. There is also a legitimate business in RATs for people who want to access their office computer from home, and so on. The worst part about RATs? Many malicious ones are available in the internet's underground for sale or even for free, so attackers can be pretty unskilled and still use this sophisticated tool.

Ransomware: Ransomware is a type of malware that locks your computer and won't let you access your files. You'll see a message that tells you how much the ransom is and where to send payment, usually requested in bitcoin, in order to get your files back. This is a good racket for hackers, which is why many consider it now an "epidemic," as people typically are willing to pay a few hundred bucks in order to recover their machine. It's not just individuals, either. In early 2016, the Hollywood Presbyterian Medical Center in Los Angeles paid around $17,000 after being hit by a ransomware attack.

Rainbow table: A rainbow table is a complex technique that allows hackers to simplify the process of guessing what passwords hide behind a "hash" (see above).

Red team: To ensure the security of their computer systems and to suss out any unknown vulnerabilities, companies may hire hackers who organize into a "red team" in order to run oppositional attacks against the system and attempt to completely take it over. In these cases, being hacked is a good thing because organizations may fix vulnerabilities before someone who's not on their payroll does. Red teaming is a general concept that is employed across many sectors, including military strategy.

Root: In most computers, "root" is the common name given to the most fundamental (and thus most powerful) level of access in the system, or is the name for the account that has those privileges. That means the "root" can install applications, delete and create files. If a hacker "gains root," they can do whatever they want on the computer or system they compromised. This is the holy grail of hacking.

Rootkit: A rootkit is a particular type of malware that lives deep in your system and is activated each time you boot it up, even before your operating system starts. This makes rootkits hard to detect, persistent, and able to capture practically all data on the infected computer.

Salting: When protecting passwords or text, "hashing" (see above) is a fundamental process that turns the plaintext into garbled text. To make hashing even more effective, companies or individuals can add an extra series of random bytes, known as a "salt," to the password before the hashing process. This adds an extra layer of protection.

Script kiddies: This is a derisive term for someone who has a little bit of computer savvy and who's only able to use off-the-shelf software to do things like knock websites offline or sniff passwords over an unprotected Wi-Fi access point. This is basically a term to discredit someone who claims to be a skilled hacker.

Shodan: It's been called "hacker's Google," and a "terrifying" search engine. Think of it as a Google, but for connected devices rather than websites. Using Shodan you can find unprotected webcams, baby monitors, printers, medical devices, gas pumps, and even wind turbines. While that's sounds terrifying, Shodan's value is precisely that it helps researchers find these devices and alert their owners so they can secure them.

Signature: Another function of PGP, besides encrypting messages, is the ability to "sign" messages with your secret encryption key. Since this key is only known to one person and is stored on their own computer and nowhere else, cryptographic signatures are supposed to verify that the person who you think you're talking to actually is that person. This is a good way to prove that you really are who you claim to be on the internet.

Side channel attack: Your computer's hardware is always emitting a steady stream of barely-perceptible electrical signals. A side-channel attack seeks to identify patterns in these signals in order to find out what kind of computations the machine is doing. For example, a hacker "listening in" to your hard drive whirring away while generating a secret encryption key may be able to reconstruct that key, effectively stealing it, without your knowledge.

Sniffing: Sniffing is a way of intercepting data sent over a network without being detected, using special sniffer software. Once the data is collected, a hacker can sift through it to get useful information, like passwords. It's considered a particularly dangerous hack because it's hard to detect and can be performed from inside or outside a network.

Social engineering: Not all hacks are carried out by staring at a Matrix-like screen of green text. Sometimes, gaining entry to a secure system is as easy as placing a phone call or sending an email and pretending to be somebody else—namely, somebody who regularly has access to said system but forgot their password that day. Phishing (see above) attacks include aspects of social engineering, because they involve convincing somebody of an email sender's legitimacy before anything else.

Spearphishing: Phishing and spearphishing are often used interchangeably, but the latter is a more tailored, targeted form of phishing (see above), where hackers try to trick victims into clicking on malicious links or attachments pretending to be a close acquaintance, rather than a more generic sender, such as a social network or corporation. When done well, spearphishing can be extremely effective and powerful. As a noted security expert says, "give a man a 0day and he'll have access for a day, teach a man to phish and he'll have access for life."

Spoofing: Hackers can trick people into falling for a phishing attack (see above) by forging their email address, for example, making it look like the address of someone the target knows. That's spoofing. It can also be used in telephone scams, or to create a fake website address.

Spyware: A specific type of malware of malicious software designed to spy, monitor, and potentially steal data from the target.

State actor: State actors are hackers or groups of hackers who are backed by a government, which may be the US, Russia, or China. These hackers are often the most formidable, since they have the virtually unlimited legal and financial resources of a nation-state to back them up. Think, for example, of the NSA. Sometimes, however, state actors can also be a group of hackers who receive tacit (or at least hidden from the public) support from their governments, such as the Syrian Electronic Army.

Threat model: Imagine a game of chess. It's your turn and you're thinking about all the possible moves your opponent could make, as many turns ahead as you can. Have you left your queen unprotected? Is your king being worked into a corner checkmate? That kind of thinking is what security researchers do when designing a threat model. It's a catch-all term used to describe the capabilities of the enemy you want to guard against, and your own vulnerabilities. Are you an activist attempting to guard against a state-sponsored hacking team? Your threat model better be pretty robust. Just shoring up the network at your log cabin in the middle of nowhere? Maybe not as much cause to worry.

Token: A small physical device that allows its owner to log in or authenticate into a service. Tokens serve as an extra layer of security on top of a password, for example. The idea is that even if the password or key gets stolen, the hacker would need the actual physical token to abuse it.

Tor: Tor is short for The Onion Router. Originally developed by the United States Naval Research Laboratory, it's now used by bad guys (hackers, pedophiles) and good guys (activists, journalists) to anonymize their activities online. The basic idea is that there is a network of computers around the world—some operated by universities, some by individuals, some by the government—that will route your traffic in byzantine ways in order to disguise your true location. The Tor network is this collection of volunteer-run computers. The Tor Project is the nonprofit that maintains the Tor software. The Tor browser is the free piece of software that lets you use Tor. Tor hidden services are websites that can only be accessed through Tor.

Tails: Tails stands for The Amnesic Incognito Live System. If you're really, really serious about digital security, this is the operating system endorsed by Edward Snowden. Tails is an amnesic system, which means your computer remembers nothing; it's like a fresh machine every time you boot up. The software is free and open source. While it's well-regarded, security flaws have been found.

Verification (dump): The process by which reporters and security researchers go through hacked data and make sure it's legitimate. This process is important to make sure the data is authentic, and the claims of anonymous hackers are true, and not just an attempt to get some notoriety or make some money scamming people on the dark web.

VPN: VPN stands for Virtual Private Network. VPNs use encryption to create a private and secure channel to connect to the internet when you're on a network you don't trust (say a Starbucks, or an Airbnb WiFi). Think of a VPN as a tunnel from you to your destination, dug under the regular internet. VPNs allow employees to connect to their employer's network remotely, and also help regular people protect their connection. VPNs also allow users to bounce off servers in other parts of the world, allowing them to look like they're connecting from there. This gives them the chance to circumvent censorship, such as China's Great Firewall, or view Netflix's US offerings while in Canada. There are endless VPNs, making it almost impossible to decide which ones are the best.

Virus: A computer virus is a type of malware that typically is embedded and hidden in a program or file. Unlike a worm (see below), it needs human action to spread (such as a human forwarding a virus-infected attachment, or downloading a malicious program.) Viruses can infect computers and steal data, delete data, encrypt it or mess with it in just about any other way.

Vuln: Abbreviation for "vulnerability." Another way to refer to bugs or software flaws that can be exploited by hackers.

Warez: Pronounced like the contraction for "where is" (where's), warez refers to pirated software that's typically distributed via technologies like BitTorrent and Usenet. Warez is sometimes laden with malware, taking advantage of people's desire for free software.

White hat: A white hat hacker is someone who hacks with the goal of fixing and protecting systems. As opposed to black hat hackers (see above), instead of taking advantage of their hacks or the bugs they find to make money illegally, they alert the companies and even help them fix the problem.

Worm: A specific type of malware that propagates and replicates itself automatically, spreading from computer to computer. The internet's history is littered with worms, from the Morris worm, the first of its kind, and the famous Samy worm, which infected more than a million people on MySpace.

Zero-day: A zero-day or "0day" is a bug that's unknown to the software vendor, or at least it's not patched yet. The name comes from the notion that there have been zero days between the discovery of the bug or flaw and the first attack taking advantage of it. Zero-days are the most prized bugs and exploits for hackers because a fix has yet to be deployed for them, so they're almost guaranteed to work.