HOW DO I MAKE MY OWN SECURITY PLAN?

When building a security plan answer these six questions:

What do I want to protect?

An “asset” is something you value and want to protect. In the context of digital security, an asset is usually some kind of information. For example it could be your emails, contact lists, direct messages, location, or other documents. Your devices themselves may also be assets.

Who do I want to protect it from?

To answer this question, it’s important to identify who might want to target you or your information. A person or entity that poses a threat to your assets is an “adversary .” Examples of potential adversaries are your boss, law enforcement, your former partner, your business competition, your government, or a hacker on a public network. It could even include people you would otherwise trust who might accidentally compromise your assets by being careless with their own security plans.

How bad are the consequences if I fail?

Security planning involves understanding how bad the consequences could be if an adversary successfully gains access to one of your assets. To determine this, you should consider the capability of your adversary. For example, your mobile phone provider has access to all your phone records. Your government might have stronger capabilities.

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

It is important to distinguish between what might happen and the probability it may happen. 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).

Assessing risks is both a personal and a subjective process. Many people find certain threats unacceptable no matter the likelihood they will occur 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.

How much trouble am I willing to go through to try to prevent potential consequences?

There is no perfect option for security. Not everyone has the same priorities, concerns, or access to resources. Your risk assessment will allow you to plan the right strategy for you, balancing convenience, cost, and privacy.

Who are my allies?

As we’ve indicated several times throughout this guide—digital privacy and security is a team sport that’s best applied with the help of others. This is not just because there is power in numbers, but because your privacy and security overlap with others in your life. If a threat affects you, it could also affect them, and vice versa.

Consider who you extend that trust to. For example, consider if someone may be an "insider threat," a person in your trusted network who could betray your security in one way or another. But don’t let the fear of an insider threat discourage you from making connections with others. Rather, use it as a guide to urge you to plan carefully and make sure others in your circles are taking their security seriously as well.

SURVEILLANCE SELF-DEFENSE

7 STEPS TO DIGITAL SECURITY + SECURITY PLAN

LEARN MORE ABOUT THESE STEPS HERE:

Digital security is as much of a mindset as it is a toolkit, and there are concepts to consider regardless of whether you’re first getting started or you’re a seasoned veteran. Before you start seeking out solutions, take a minute to step back and consider the whole picture of what you’re trying to accomplish.

1. KNOWLEDGE IS POWER

Good security decisions begin with proper knowledge about your own situation. To start, ask yourself the following questions:

* What do I want to protect?
* Who do I want to protect it from?
* How likely is it that I’ll need to protect it?
* How bad are the consequences if it doesn’t work out?
* How much trouble am I willing to go through to try to prevent potential consequences?

Once you answer these questions you can better assess your digital security needs and create a security plan (sometimes called a threat model). You already have more power than you think!

2. THE WEAKEST LINK

The old adage that “a chain is only as strong as its weakest link” applies to security too. For example, the best door lock is worthless if you have cheap window latches. Similarly, using an encrypted chat app to share personal photos won’t protect the confidentiality of those photos if you store unencrypted copies on your laptop and your laptop is stolen. Think about every part of your information and computer use and try to identify any weak links in your digital security practices.

3. SIMPLER IS SAFER AND EASIER

Some people are tempted by every shiny, new security solution they hear about. But soon they find themselves using so many tools, and trying so many things, that they can’t keep them all straight. Having a complex security system makes it harder to identify the weak links. So, keep it simple. Sometimes the safest solution may be the least technical solution. Computers can be great for many things, but sometimes the security issues of a simple pen and paper can be easier to understand, and therefore easier to manage

4. MORE EXPENSIVE DOES NOT 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.

5. IT’S OK TO TRUST SOMEONE (BUT ALWAYS KNOW WHO YOU ARE 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 partner to your doctor or lawyer. What’s tricky in the digital space is understanding who you are trusting, and with what. You might give a list of passwords to your lawyers, but you should think about what power that might give them or how easily a bad actor could then access your passwords. You might save documents in a cloud service like Dropbox or Google that are only for you, but you’re also letting Dropbox and Google access them too.

6. THERE IS NO ONE PERFECT SECURITY PLAN

Make a security plan that works for you, and for the risks you face. A perfect security plan on paper won’t work if it’s too difficult to follow day-to-day.

7. WHAT’S SECURE TODAY MAY NOT BE SECURE TOMORROW

It is 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 an eye on big security news when you can (most people don’t need to overdo this: think “huge data breach of an important piece of software like a password manager " type of news that’s so important that it reaches big tech-focused media outlets like Wired or The Verge, or even The New York Times or The Washington Post, not "this specific exploit targets a specific CPU"), and check sites like SSD, because we update our advice to reflect changes in our understanding and the realities of digital security. Remember: effective security is a continual process.