Security Planning (Threat Modeling)

It’s easy to feel that protecting your digital security and privacy is impossible. Trying to protect yourself from all possible threats at all times is a recipe for frustration. But, do not fear! Security is a process, and through thoughtful planning, you can put together a plan that’s best for you. Security isn’t just about the tools you use or the software you download. It begins with understanding the unique threats you face and how you can counter those threats.

Consider the ways in which you make decisions in the physical world: When locking a bike or parking a car, what might you evaluate? Perhaps you think: *How visible are my valuables? How could someone get my stuff? What’s the likelihood of something happening to my valuables in this area? What is the worst that can happen, and am I okay with the decision?*

By asking yourself these types of questions, you are security planning, often referred to as “threat modeling.” By answering the following six questions, you can start to improve your security.

1. What do you want to protect?

What’s at stake for digital security is usually information: your emails, files, contacts, or text messages. You also may want to guard against someone impersonating you, such as by sending out messages from your accounts. 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.

2. Who do you want to protect it from?

Think about who might want to target you or your information. Adversaries are people or entities that pose a threat to your information. Examples of potential adversaries are your boss, law enforcement, a former partner, a business competitor, or a hacker on a public network. Make a list of who might want to get ahold of your data or communications.

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

Risk is the likelihood that a particular threat against a particular asset will actually occur. It goes hand-in-hand with capability. For example, 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 what might happen and the probability it may happen. Write down 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.

4. How bad are the consequences if you fail?

There are many ways an adversary could gain access to your data. For example, an adversary could get you to click on a malicious link sent to your email address that compromises your computer. Or more simply, it could be someone screenshotting your private DM's and using that information against you. Security planning involves understanding how bad the consequences could be if an adversary successfully gains access to one of your assets. Write down what your adversary might want to do with your private data.

5. How much trouble are you willing to go through to try to prevent potential consequences?

There is no perfect option for security. Not everyone has the same priorities or views threats in the same way. For example, an attorney representing a client in a national security case would probably be willing to go to greater lengths to protect communications about their case than a family member who regularly emails funny cat videos. Write down what options you have available to you to help mitigate your unique threats. Note if you have any financial constraints, technical constraints, or social constraints.

6. Who are your allies?

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. Open up a dialogue with others who likely share the same concerns you do. Come to some shared agreements about how to care for each other, and what information to trust each other with.

Now you can start deciding what tools you want to use to protect yourself from the threats you are taking seriously! To get started, check out EFF's Surveillance-Self Defense Guide at **ssd.eff.org.**

The Electronic Frontier Foundation is the leading nonprofit defending digital privacy, free speech, and innovation. https://eff.org