Risk Assessment (Threat Modeling)

Because resistance *isn't* futile

EFF One-Pager
Revised 6.24.19

Learn more:
ssd.eff.org/en/module/assessing-your-risks

Support our work on Surveillance Self Defense:
eff.org/donate

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! Through thoughtful planning, you can assess what tools and practices are right for you.

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, and what am I trying to protect? How could they access 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? How much inconvenience am I willing to go through?*

By asking yourself this series of questions, you are *threat modeling*. The first step to good security is doing a threat modeling assessment. By answering the following five threat modeling 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: for example, your emails, files, contacts, and 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, your government, a persistent harasser, or a hacker on a public network. Make a list of who might want to get ahold of your data or communications.

EFF

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

The capabilities of your attacker are also an important thing to think about. For example, your mobile phone provider has access to all your phone records and therefore has the capability to use that data against you. A hacker on an open Wi-Fi network can access your unencrypted communications. Your government likely has stronger capabilities. Risk is the likelihood that a particular threat against a particular asset will occur. Moreover, risk goes hand-in-hand capability. For example, your mobile phone provider has the capability to access all your data. Yet, the risk of them posting your private data online to harm your reputation is low. For the list of adversaries you've written down, rate both the risk that they will attack you and their capability, i.e. how likely it is that they would be successful.

4. How bad are the consequences if you fail?

There are many ways that an adversary can threaten your data. For example, an adversary can read your private communications as they pass through the network. Or they can delete or corrupt your data. An adversary could also disable your access to your own data. The motives of adversaries differ widely, as do their attacks. A corporation trying to track your shopping habits may be content to simply sell that information to another corporation or use it for marketing purposes, whereas a government may wish to gain access to communications in order to harass, arrest, or even kill political activists. 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?

Answering this question requires doing the risk analysis in question three. 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 that case, such as using encrypted email, than a mother who regularly emails her daughter funny cat videos. In a military context, it might be preferable for information to be destroyed than for it to fall into enemy hands, while in many civilian contexts, it's more important for an asset such as email service to be available than for it to be confidential. Ask yourself 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.

*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**. Surveillance Self-Defense (SSD) is a guide to protecting yourself from electronic surveillance for people all over the world. Some aspects of this guide will be useful to people with very little technical knowledge, while others are aimed at an audience with considerable technical expertise and privacy/security trainers. SSD includes step-by-step tutorials for installing and using a variety of privacy and security tools, but also aims to teach people how to think about online privacy and security in a sophisticated way that empowers them to choose appropriate tools and practices even as the tools and adversaries change around them.*