Threat Modeling:

BECAUSE RESISTANCE ACTUALLY *ISN'T* FUTILE

It's easy to succumb to privacy nihilism. That's the idea that digital security and privacy are simply impossible. But that's simply wrong.

It *is* true that trying to protect yourself from 100% of the threats you face 100% of the time is a recipe for failure. But perfection is not the goal of digital security. Each person is faced with different threats—potential events that could undermine your efforts to defend your data. By determining what you need to protect and whom you need to protect it from, you can figure out how to counter the threats to your data.

The first step to good security is doing a threat modeling assessment.

By answering these five questions, you can start to improve your security:

- **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?**

1. What do you want to protect?

When we are talking about digital security, what's at stake is usually information, for example, your emails, files, and text messages. You also may want to guard against someone impersonating you, say by sending out emails from your account.

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?

In order to answer this question, 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, or a hacker on a public network.

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

Continued

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

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

Risk is the likelihood that a particular threat against a particular asset will occur, and 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.

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 numerous ways that an adversary can threaten your data. For example, an adversary can read your private communications as they pass through the network, or they can delete or corrupt your data. An adversary could also disable your access to your own data.

The motives of adversaries differ widely, as do their attacks. A 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 in order 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.
