Chapter 1

Assessing Your Security and Privacy Needs

It seems that every day there is news of a security breach or invasion of privacy. From ransomware to widespread breaches of private data, the news is full of scare stories. Sometimes it feels like there is nothing that you as an ordinary citizen can do to protect your data—except to renounce all modern technologies and head to the hills!

Luckily, when it comes to the security of your personal and professional data, there are things you can do to reduce your risk. That's what this report is about. You can learn to see beyond the hype of media scare stories and learn what's worth paying attention to with advice from security experts.

In this report, we'll discuss answers to these questions:

- What are the best ways to back up your data?
- What's the best thing to do if your device is lost or stolen?
- How do intruders get access to your data?
- Can criminals hold your data captive and ask for ransom?
- Is your laptop's or smartphone's traffic being harvested when on public Wi-Fi?
- Should you trust a password manager?
- Is it advisable to use Touch ID or Face ID on iPhones?
- Is it a good idea to use mobile payment systems in retail stores?
- How can you make theft of your identity less likely?
- Are you giving away information for targeted advertising?
- How easy is it for anyone to see all of your search engine history?
- How can you browse the web privately and anonymously?
- What can be learned from your location history?
- How can you protect your privacy on Facebook?
- Should you use encrypted messaging and email? How?
- Is your laptop camera or microphone recording without you knowing it?
- How can you control your privacy if you use smart home devices like Amazon Alexa or Google Home?

For each question, we'll look at what security experts recommend for protecting your data. We'll also discuss the difference between threats (all the bad things that can happen) and risks (the likelihood that each threat might happen). Understanding your risks will help you create an individualized security plan for the different types of data you work with every day since not all data needs the same level of protection. I'll offer information on how to create such a plan for both your personal and your work-related data.

And finally, we'll discuss why it's important for everyone to practice good online security since what you do affects others. I'll recommend a few simple steps for getting started since it can be overwhelming to consider all of this at once. I'll end with some ideas for sharing this information with library users, along with a bibliography of resources to further your learning.

Which Advice to Trust

When reading about security threats, you'll often come across scary headlines from blogs and news sites. It's disheartening to see so many of these stories

about security threats, especially when you are busy and don't have time to learn about each risk and how it might affect you.

How do you know which advice to trust? When evaluating any security tool (such as a password manager app), I recommend looking at two sources: documentation from the vendor about its own security practices and reviews from independent security experts.

Here are some things to look for in the documentation provided with software that is designed to protect your data:

- Is it easy to move to another service if you want to leave this one? (Does it offer easy data exports, for example?)
- Does it use open standards that can be verified by independent security experts?
- Does it regularly audit its own systems for vulnerabilities?
- Does it encrypt data on your computers and mobile devices and also while the data is in transit over the internet?
- Does it keep highly sensitive data in a secure place on your own device rather than transmit it over the internet?
- Are you a paying customer of the service, or are you the data? (When the Equifax breach happened,[1] people soon remembered that our individual information was the data that was being purchased by banks and lenders. In that scenario, we are the data, not the customers.)
- Does it sell your data to others?

As for independent security experts, here are a few individuals and organizations worth following. They often write about the latest security and privacy issues on their blogs and for major media outlets:

- **Bruce Schneier** covers security issues in his blog, *Schneier on Security*. He's the chief technology officer of IBM Resilient, a fellow at Harvard's Berkman Center, and a board member of the Electronic Frontier Foundation. He's an internationally recognized expert on security and the author of many books and academic papers on security topics.
- **Brian Krebs** maintains his blog, *Krebs on Security*. He's a journalist and investigative reporter known for his coverage of cybercriminals.
- **EFF** (Electronic Frontier Foundation), a nonprofit that defends digital privacy, free speech, and innovation.
- **EPIC** (Electronic Privacy Information Center), a public interest research center in Washington, DC, that works to bring public attention to privacy and civil liberties issues.

Schneier on Security
https://www.schneier.com

Krebs on Security
https://krebsonsecurity.com

EFF
https://eff.org

EPIC
https://epic.org

When you see a scary headline about the latest security breach, it's a good idea to look for commentary about it on the blogs of these experts. They will often bring a balanced view of what has happened and offer recommendations on what to do about it. Of course, there are other experts, but these are the ones I have found to be most consistently useful and trustworthy.

Building Your Threat Model

One piece of advice from the EFF that I have found very helpful is to build your own "threat model."[2] This is a plan you can create that helps you decide what level of security you will need for each different type of data you work with.

When working with data, EFF recommends you ask yourself the following questions:

1. What do I want to protect?
2. Who do I want to protect it from?
3. How bad are the consequences if I fail?
4. How likely is it that I will need to protect it?
5. How much trouble am I willing to go through to try to prevent potential consequences?[2]

Threats are any potential harm to the security and privacy of your data. A risk, on the other hand, is the likelihood that a potential threat will happen. You'll start to realize that for some of your data, the likelihood of something bad happening is small or the outcome of the worst-case scenario is not important to you. Since each kind of protection that you implement has a cost in lost time, money, or inconvenience, it's a good idea to be selective about which of your collections of data need strong locks and which don't. You already do the same in the physical world when deciding where to put locks or alarms and where not to.

- **When it comes to question 1, "What do I want to protect?"** make a list of the data you keep, where you store it, who has access to it, and what you already do to keep it safe.

- **For question 2, "Who do I want to protect it from?"** make a list of who might want to get access to each type of information you deal with. This could include individuals or groups, criminals or not, who may benefit in some way from accessing your data.
- **For question 3, "How bad are the consequences if I fail?"** write down what your adversaries might do with your private data. This could be anything from your internet provider selling your browsing history, to advertisers, to a criminal hacker using your credit card to make purchases.
- **For question 4, "How likely is it that I will need to protect it?"** for each threat, write down whether it's worth putting a lot of effort into protecting the data or not. This is somewhat subjective because everyone has different tolerances for risk. But it's usually fairly obvious which items are extremely unlikely to happen or which outcomes would not be so serious if they did happen.
- **For question 5, "How much trouble am I willing to go through to try to prevent potential consequences?"** write down which options you have available to help protect against each threat. If you don't have an answer, mark these threats with a question mark for now. After reading this report, you can come back to them and choose which security or privacy tool fits each need. Sometimes financial, technical, or social reasons (such as budgetary limitations) make it difficult to implement certain choices. It's a good idea to make note of those too.

As your situation changes over time, these risks and threats may also change. It's a good idea to create a new threat model each calendar year.[3]

Notes

1. Allen St. John, "Equifax Data Breach: What Consumers Need to Know," Consumer Reports, September 21, 2017, https://www.consumerreports.org/privacy/what-consumers-need-to-know-about-the-equifax-data-breach/.
2. For complete details, see the Electronic Frontier Foundation, "Assessing Your Risks," Surveillance Self-Defense, last reviewed September 7, 2017, https://ssd.eff.org/en/module/assessing-your-risks.
3. Ibid.