Chapter 6 is about Internet Security. With so much personal information being spread across many different websites it is imperative to have some understanding of basic Internet security. In fact, no matter how you protect yourself, there are always ways to improve. Personally, I make sure to use anti-virus software and multi-factor authentication, which isn’t a whole lot, but has served me well as a basic Internet user. I also use a password program that stores and suggests strong passwords, and periodically suggests they be changed when they have been used for too long. This chapter goes into the two types of security, being physical and logical, and covers other topics such as what types of security threats exist and how to protect yourself from them.

Physical security pertains to the actual hardware and the personal habits of users that leave them open to security threats. For instance, do you leave your computer logged in and unattended? Do you leave flash drives and hard drives out in the open where people could take them? These are just some examples of what the authors mean by physical security whereas logical security pertains to the way that you protect yourself using the operating system or software. For instance, using a strong password prevents people from having easy access to your user profile. Whereas encrypting a drive to store sensitive documents is another example of logical security that prevents data leaks and other potentially devasting consequences.

Hackers and other Internet criminals have devised clever ways of getting personal information from people. One such method is phishing. Phishing is when a user receives and email or text message from someone, usually claiming to be someone else, either outright asking for information or getting your information through familiar looking, but fake, webpages designed to capture your credentials. This is one reason why it is important to never open links from people you don’t know, and even if you know them, it is important to verify that this person or institution is legitimate by calling them and making sure it is actually them. Another threat comes from virus infected attachments in emails. Once a virus makes its way into your operating system, whatever information you have stored becomes vulnerable. So, another tip the authors stress is to never open email attachments from people or institutions you don’t know before verifying with the actual entity that it is in fact legitimate.

Overall, this chapter describes security threats and the countermeasures that users can take to prevent the potentially devastating consequences that comes from exploited vulnerabilities. Every Internet user should already be familiar with some of these concepts to avoid encountering viruses identity theft. Even though good anti-virus software and other security measures can cost money it is worth it in my opinion, because it can potentially save a lot of money and stress in the event of a data breach.