Chapter 6 was entirely about online security. The chapter first reviewed the three different types of security threats: secrecy, integrity, and necessity. This was completely new information to me. I also learned about encryption and how public and private keys work. I was actually curious about keys beforehand; for I had heard of keys being used for encryption in the past, but I never understood quite how they functioned until reading this chapter. The text also reviewed the different types of threats, such as malware, phishing scams, spoofing, and trojans. I was a bit more familiar with these just from my general internet experience, but the book expanded upon my knowledge about these threats.

In addition, this chapter discussed how identity theft happens and what to do to prevent and mitigate it. It also elaborated on DDoS attacks and how exactly they work – I had heard of DDoS attacks before but didn't know about how they functioned. The chapter also reviewed antimalware software, web bug blocking, and finally digital certificates. The last of which, I was actually very interested to learn more about, as – just like encryption keys – I knew that they existed, but never knew how they worked, until now.