Module 6 of the book has given me more of an understanding of security threats on the Internet and how to prevent and combat them. I never really knew about firewalls and denial-of-service attacks, so I have gotten new information from this module. As my online accounts have been hacked, I know how scary it could be to know that hackers have access to bank account information. Fortunately, the hackers never took money out of my account and I was able to change my password before they did anything. Because of this, I believe that the information that I learned in this module is important for staying secure.

The first part of the module is about the basics of security, threats, and the different types of threats. A threat is anything that endangers an asset. Security threats come in multiple forms, with the most common being secrecy threats, integrity threats, and necessity threats. Security threats usually go after identities, files, email message, and passwords of those using the Internet. Reducing or eliminating any threat is called a countermeasure. One example of a countermeasure is a website locking an account after three password attempts. To find new ways to secure information, people study what is called cryptography. The most common method of cryptography is encryption, which is when information is coded using algorithms to produce an unreadable character string. This string is called cipher text, while unencrypted information is called plain text. Processing encrypted text so that it is readable is called decryption. The two most common types of encryption are private-key and public-key encryption. Encryption keys could be considered weak or strong depending on how long it is. Shorter keys are weaker, while longer keys are stronger. One common type of integrity threat is known as spoofing, which is when emails look like they are from a company, but are really from someone else. This email tells the receiver that their account data has been lost and needs to be verified to continue using a service. A link is sent, which asks the receiver for personal information. This is what is known as phishing. Copyrighted works could also be stolen without the publisher's permission, which is known as copyright infringement. This could be prevented by using a digital watermark. Moving onto necessity threats, the most common one is a denial-of-service (DoS) attack, which is when an attack overloads a network to make a service slow and unusable. There are also distributed denial-of-service (DDoS) attacks, which is when an attacker takes control of multiple computers and uses them to launch a DoS attack on a server. These attacking computers are called bots or zombies. A DoS filter could be used to monitor communication between a server and a router on the Internet and prevent a DoS attack. Another security issue is with identity theft, where a hacker could use the victim's personal information to buy items with their credit cards and damage the victim's credit rating.

The second half of Module 6 goes over advanced security threats on the web. It starts off with active content, which are Java and JavaScript programs that webpages use to enhance content. However, hackers could also use them to go through the victim's software and email a file to the hacker's web server. There are also programs called viruses, which is malicious software which is designed to be invisible to the victim. The most common types of viruses are malware, trojan horses, worms, adware, and spyware. These viruses could be found and deleted with an antivirus program. Web bugs, which are small hidden GIFs designed to obtain information, are also considered spyware but is not illegal. Another way of blocking a virus is by setting up a firewall, which is software that blocks traffic to and from a computer. Another countermeasure, authentication, is when the identity of a person or device is identified with certainty. This is most commonly implemented with a username and password. Since people have different passwords for most websites, they use a password manager like LastPass to keep track of them. There is also multifactor authentication, which relies on more than one factor. Other forms of authentication include digital certificates, such as digital IDs, and trust seals. Many Internet connections today are encrypted with either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Both are security protocols that use a public key to encrypt a private key and send it to the browser. These webpages start with https:// instead of http://.