Module 7 of the book is mainly about wireless networks, how they evolved through the years, and how they work. It also goes into network security and how to secure networks. Having an interest in how technology evolved, I was interested throughout the first section. There were also some parts that I never knew before, such as the different types of networks and the security risks for smartphones. I believe that this information is important to know because security is overall a very important topic when it comes to networks.

The first part of Module 7 goes over the evolution of wireless networks. It was not until 1978 that wireless connections first came out as a voice-only network. This was called a 1G wireless network. Eventually, 2G came out, which was slightly faster and supported text messages. Then, as smartphones became more common, networks switched to 3G, which was fast enough to use the internet on. Eventually, starting in 2010, 4G was rolled out, which had more support for multitasking. Today, much faster 5G networks are starting to replace 4G networks. As time goes on, newer, faster networks will come out and replace the older networks. When it comes to computers, most use wireless local area networks (WLAN) networks. The most common type of WLAN is Wi-Fi, which consists of a hotspot, or area of network coverage, that multiple computers connect to. There are also four main WLAN standards and the main differences between these standards are the radio frequency that they transmit at, the transfer rate of data, and the range they operate at. The closer a device is to an access point, the faster the transfer rate is. Another less common type of WLAN is a wireless mesh network, which, instead of using a router, uses several wireless nodes that connect to each other. The second most common type of network is a personal area network (PAN), in which personal devices are connected to each other. Bluetooth is the most popular type of PAN and, unlike a WLAN, it does not need a router or nodes, as it uses radio waves to connect devices. There are also wireless wide area networks (WWAN), which makes it possible for the Internet to be accessed from anywhere in its area. WWANs also use Long Term Evolution (LTE), which provides faster wireless connections to a large area. Until recently, most cellular carriers used 4G LTE networks. Ending the first half, the module goes over the Internet of Things (IoT), which uses machines manufactured with embedded sensors that collect and transmit data using wireless network connections so that data could be acted upon by a person or machine.

The second half of Module 7 goes over the several different wireless security concerns and several ways to overcome those security concerns. The first way to overcome these concerns is with wireless encryption. The most common type of wireless encryption is Wired Equivalent Privacy (WEP), which is a security protocol that encrypts wireless data with a 64 or 128-bit key called a passphrase entered by the user. Passphrases could only contain letters from A to F and numbers from 0 to 9. There is also Wi-Fi Protected Access (WPA), which uses a pre-shared key to encrypt data and encrypts data with different keys. WEP and WPA could be used together, but all devices in a network would have to be able to use WPA. Every network card uses a unique code called a Media Access Control (MAC) address to identify it on a network. This number allows certain devices to be kicked out of a wireless network and for people to filter devices based on a MAC address. Every router has a service set identifier (SSID), which is a name up to 32 characters given to a wireless network. Even though these security features are effective at protecting wireless networks, there are also over-the-shoulder attacks, evil twin attacks, and man-in-the-middle attacks. There are also security concerns with Bluetooth, with the most common security concerns being bluejacking, bluesnarfing, and bluebugging. One way to prevent these is to disable Bluetooth when not using it, also known as undiscoverable mode. On smartphones, viruses are less common unless an iPhone is jailbroken or an Android device is rooted. This allows more apps to be installed, but also allows more viruses to enter the device. A few guidelines to keep wireless devices safe is to keep them updated with the latest operating system, backup files frequently, lock the device with a password, and disable autoconnect, which lets the device connect to a network automatically.