9.1.6 Malware Concern Facts

Aside from viruses, worms, and Trojan horses, there are other types of malware that can be cause for concern. These malware programs can be just as destructive, if not more than, a virus or Trojan horse. No matter the type of malware, there are multiple methods for infecting systems.

This lesson covers the following topics:

- Malware infection methods
- Additional types of malware

Malware Infection Methods

A system can be infected by malware in many ways. Some of the more common methods are:

- USB drives
- Phishing emails
- Downloading and installing from website

Additional Types of Malware

Rootkits, spyware, adware, scareware, and ransomeware are also concerns, as the follow

Type	Description
Rootkit	Rootkits are a very dangerous type of malware. The term comes from combining the words root, the equivalent of an administrator on Linux, and kit, the software being executed. A rootkit consists of different programs that give the hacker root, or administrator, access to the target machine, allowing the hacker to perform exploits such as installing keyloggers. A famous rootkit was distributed by Sony BMG (now Sony Music) in 2005. In an attempt to enforce copyright protection, Sony installed Extended Copy Protection and MediaMax CD-3 software on millions of music discs. This software prevented users from copying the CDs and also sent data to Sony about the user's actions. Unfortunately, the rootkits Sony installed also opened vulnerabilities, which other malware programs took advantage of.
Spyware	Spyware is a type of malware that is designed to collect and forward information regarding a victim's activities to someone else. While this type of malware doesn't usually cause damage to a machine, it is extremely invasive. Spyware can be especially dangerous because it can spy on everything the user is doing. People often associate spyware with web browsing activities, but spyware will also report on applications being run, instant messaging activity, and almost anything else the user does on the system.
Adware	Adware causes pop-up and pop-under advertisements on the infected system. Users often install adware as a bundle with freeware programs or when visiting a website that stealthily installs adware in the background.
Scareware	Scareware shows the user warnings about potential harm that could happen if they don't take some sort of action, such as purchasing a specific program to clean their system. If the user falls for the attack, the software that is purchased will often contain other malware, and the hacker has the user's credit card information.
Ransomware	When ransomware infects a system, it will scan the computer for user files and encrypt them. To recover the files, there are usually instructions on how to pay a ransom using cryptocurrency to receive the decryption key. There is no guarantee that the user will receive the decryption key.