Unit 7: Securing Your System

Identity Theft and Hackers

9.1 Identity Theft occurs when a thief steals personal information about you and runs up debts in your name. Identity thieves can obtain information by stealing mail, searching through trash, or tricking people to reveal information over the phone or email.

9.2 White-Hat Hackers break into systems for nonmalicious reasons such as testing security to expose weakness. Black-Hat Hackers break into systems to destroy information or for illegal gain. Grey-Hat Hackers often break into systems just for the thrill or to demonstrate their powers.

9.3 Packet Analyzers (sniffers) are programs used to intercept and read data packets and they travel across a network. Trojan horses are programs that appear to be something else but are really a tool for hackers to access your computer. Backdoor programs and rootkits are also programs used by hackers. Denial-of-service attacks overwhelm computers systems with so many requests for data that legitimate users can't access the system.

Computer Viruses

9.4 A computer virus is a computer program that attaches itself to another computer programs and attempts to spread to other computers when files are exchanged. Viruses can display annoying messages, destroy your info, or corrupt your files. Symptoms of virus infection include: (1) files or app icons dissapear, (2) browser is reset to an unusual home page, (3) odd messages, pop-ups, or images are displayed, (4) data files become corrupt, and (5) Programs stop working properly.

Boot Sector Viruses copy themselves onto the master boot record of a computer and execute when the computer is started. Logic bombs and time bombs are viruses triggered by the completion of certain events or by passage of time. Worms can spread on their own without human intervention, unlike conventional viruses. Macro viruses lurk in documents
9.5 that use macros. Email viruses access the address book of a victim to spread to the victim's contacts. Encryption viruses render files unusable by compressing them with complex encryption keys. Polymorphic viruses periodically rewrite themselves to avoid detection. Stealth viruses temporarily erase their code and hide in the active memory of the computer.

Online Annoyances and Social Engineering

Malware is software that has malicious intent. Adware is software that displays sponsored advertisements in a section
9.6 of your browser window or in a pop-up box. Spyware collects information about you, without your knowledge, and transmit it to the owner of the program.

Spam is unwanted or junk email. Spim is unsolicited instant
9.7 messages, which is also a form of spam. Spam filters in e-mail systems forward junk mail to its own folder.

Cookies are small text files that some websites automatically store on your hard drive when you visit
9.8 them. Cookies are usually used to keep track of users and personalize their browsing experience.

Social Engineering is any technique that uses social skills to generate human interaction that entices individuals to reveal sensitive information.