Tia chapter 9

cybercrimeis any criminal action perpetrated primarily through the use of a computer

cybercriminalsindividuals who use computers, networks, and the internet to perpetrate crime

Internet Crime Complaint Center (IC3)a partnership between the FBI and the National WHite Collar Crime Center

identity theftoccurs when a thief steals your name, address, SSN, birth date, bank account, and credit card information and runs up debts in your name

The Federal Trade CommissionWho identified these other methods that theives could use to obtain information?
-stealing purses and wallets
-stealing mail
posing as bank or credit card company reps

virusa computer program that attatches itself to another computer program and attempts to spread to other computers when files are excahnged

hostWhat is the program that the virus attatches itself to?

they are engineered to evade detectionwhy are computer viruses threatening?

to replicate itself and copy its code into as many other host files as possiblewhat is a computer virus's main purpose?

boot-sector virusreplicates itself into a hard drive's master boot record master boot recorda program that executes whenever a computer boots up, ensuring the virus will be loaded into memory immediately

by a flash drive left in a USB portHow are most boot-sector viruses transmitted?

logic bombis a vrius that is triggered when certain logical conditions are met- such as opening a file or starting a program

time bomba virus that is triggered by the passage of time or on a certain date

Michelangelo virusa famous time bomb that was set to trigger every year on March 6

BlackWorm virusa time bomb that spreads through email attachments

wormtake advantage of file transport methods like emails or network connects to spread

viruusWhat requires human interaction to spread?

wormDoes a virus or a worm work more independently?

scripta seriees of commands that is executed without your knowledge
-used to perfor useful, legitimate functions on web sites, like collecting name and address information

macro virusa virus that attaches itself to a documet that uses macros

macroa short series of commands that usually automates repetitive tasks e-mail virusesuse the address book in the victim's email system to distribute the virus

-once the infected document is opened it triggers the virus

Melissa virusWhat was the first practical example of an e-mail virus?

encrytion viruseswhen they infect your computer they run a program that searches for common types of data files and compresses them using a complex encryption key that renders your files unusable.

-then you get a message that asks you to send money to an account

polymorphic viruschanges its own code or periodically rewrites itself to avoid detection

multipartite virusdesigned to infect multiple file types in an effort to fool the antivirus software that is looking for it

stealth virustemporarily erase their code from the files where they reside and then hide in the active memory of the computer

-existing programs icons suddenly disappear

-if you start a browser and it take you to an unusual home page

-odd messages pop up

-data files become corrupt

-programs stop working

-your system slows downWhat are some of the ways you know your computer can be infected with a virus?

antivirus softwareis specifically designed to detect viruses and protect your computer and files from harm

virus signaturea portion of the virus code that is unique to a particular computer virus

quarantining-antivirus software scans files when theyre opened or executed
-if it detects a virus signature it stops the execution of the file
-it also places the virus in a secure area on your hard drive.

inoculationthe antivirus software records key attributes about files on your computer and keeps these statistics in a safe place on your hard drive

drive-by downloads-viruses on websites
-is common and affects almost 1 in 1000 web pages

hackermost commonly defined as anyone who unlawfully breaks into a computer system

white-hat hackershackers who break into systems for non-malicious reasons

black-hat hackersthe more villainous hackers

gray-hat hackers-cross between white and black
-they will often illegally break into systems merely to flaunt their expertise

packetdata travels through the internet in small pieces called this

IP addresshow are the packets identified?

packet analyzer (sniffer)a computer program deployed by hackers that looks at each packet as it travels on the internet

Trojan horsea program that appears to be something useful or desirable but while it runs does something malicious in the background without your knowledge

backdoor program or rootkitsare programs that allow hackers to gain access to your computer and take almost complete control of it without your knowledge

zombiea computer that a hacker controls in this manner
-used to launch denial-of-service attacks on other computer

denial-of-service (DoS) attacklegitimate users are denied access to a computer system because a hacker is repeatedly making requests of that computer system through a computer he or she has taken over as a zombie

distributed denial-of-service (DDoS) attackwhich launches DoS attacks from more than one zombie at the same time

botnetis a large group of software programs that runs autonomously on zombie computers

logical portsare virtual communications gateways or paths that allow a computer to organize requests for information

SMTPthe protocol used for sending email on the internet firewalla software program or hardware device designed to protect computers from hackers

personal firewalla firewall specifically designed for home networks

-blocking access to logical ports
-keeping your computer's network address secureHow do firewalls protect you?

packet filteringfirewalls filter out packets sent to specific logical ports

logical port blockingfirewals can be configured to ignore requests that originate from the internet asking for access to these ports

internet protocol address (IP address)unique address code

network address translation (NAT)assign internal IP addresses on a network

trueVirus and hacking attacks against Linux are far less likely than attacks against Windows

biometric authentication devicea device that reads a unique personal characteristic such as a fingerprint or the iris pattern in your eye and converts its pattern to a digital code

malwareis software that has a malicious intent

adware
spywarre
virusesWhat the three primary forms of malware?

adwareis software that displays sponsored advertisements in a section of your browser window or as a pop-up ad box

spywareis an unwanted piggyback program that usually downloads with other software you want to install from the Internet
-it runs in the background of your system

keystroke logger (keylogger)monitors keystrokes with the intent of stealing passwords, login IDs, or credit card information

spamunwanted or junk email

spimunsolicited instant messages and are a form of spam

spam filterscan catch as much as 95% of spam by checking incoming e-mail subject headers and senders' addresses against databases of known spam

cookiessmall text files that some web sites automatically store on your computer's hard drive when you visit them

unauthorized access
tampering
destructionWhat are the three major threats your data on your computer faces?

backupsare copies of files that you can use to replace the originals if they are lost or damanged

program fileis used to install software and usually comes on DVDs or is downloaded from the Internet data filea file you have created or purched

-include files such as research papers, spreadsheets, music files, movies, etc

image backupWhat would you perform in order to back up all files on your computer?

incremental backupinvolveds backing up only files that have changed or been created since the last backup was performed

image backupmeans that all system, application, and data files are backed up

incremental backupsWhat is the more efficient backup?

social engineeringany technique that uses social skills to generate human interaction that entices individuals to reveal sensitive information

pretextinginvolves creating a scenario that sounds legitimate enough that someone will trust you

phishinglures Internet users to reveal personal information such as credit card numbers, SSN, or other sensitive information that can lead to identity theft

pharmingwhen malicious code is planted on your computer that alters your browser's ability to find web addresses.

scarewarea type of malware that is downloaded onto your computer and tries to convince you that your computer is infect with a virus or other type of malware.

hoaxan attempt to make someone believe something that is untrue.

urban legendwhen hoaxes become so well known and they are accepted by society as true events even though they are false

surge protectoris a device that protects your computer against power surges

Metal-oxide varistorsbleed off excess current during minor surges and feed it to the ground wire

whole house surge protectorfunction like other surge protectors but they protect all electrical devices in the house

uninterruptible power supply (UPS)a device that contains surge protection equipment and a large battery
-when power is interrupted, the UPS continues to send power to the attached computer from its battery