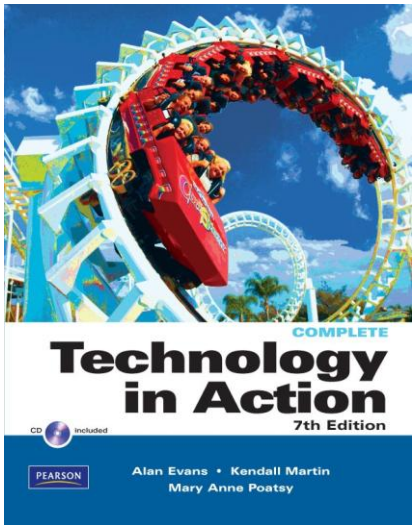


Technology in Action

Chapter 9

Digital Lifestyle: Protecting Digital Data and Devices

Chapter Topics

- Computer virus types
- Protecting computers from viruses
- Hackers
- Firewalls
- Passwords and password management

Chapter Topics

- Biometrics
- Spyware and spam
- Backup methods
- Protecting physical assets

Computer Threats

- Cybercrimes are criminal acts conducted by cybercriminals through the use of computers
- Computer users need to protect themselves from becoming victims of cybercriminals

Types of Cybercrime

- Fraud-related (58 percent of cybercrime)
  - Auction fraud
  - Nondelivery of ordered items
  - Credit and debit card fraud
- Non-fraud-related
  - Computer intrusions
  - Unsolicited e-mail
  - Child pornography

Computer Threats: Viruses

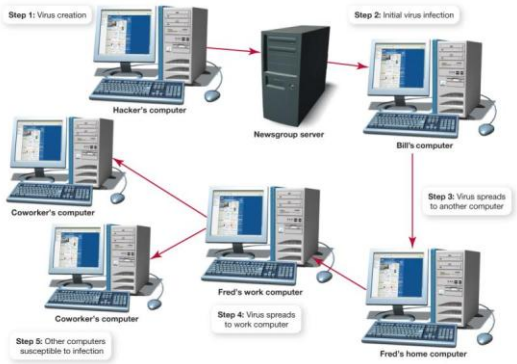
- Virus: A program that attaches itself to another program and spreads itself to other computers
- Viruses are hidden within the code of a host program

What Viruses Do

- Replicate themselves
  - Slow down networks
- Secondary objectives
  - Display annoying messages
  - Delete files on the hard drive
  - Change computer settings

How Does a Computer Catch a Virus?

- Viruses copy themselves and infect a file on your computer
- Spread by
  - Sharing disks or flash drives
  - Opening an e-mail attachment
  - Downloading infected audio or video files



Types of Viruses

- Boot-sector viruses
  - Replicate themselves in the boot sector of the hard drive
- Logic bombs
  - Activate when certain conditions are met
- Time bombs
  - Triggered by the passage of time or on a certain date
- Worms
  - Travel between systems through networks

Types of Viruses

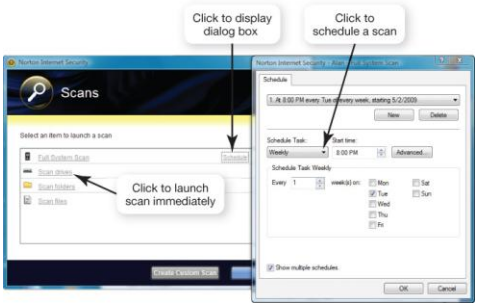
- Script viruses
  - Hidden on Web pages as miniprograms
- Macro viruses
  - Attached to documents
- E-mail viruses
  - Use e-mail address books to distribute themselves
- Encryption viruses
  - Compress files using a complex encryption key

Virus Classifications

- Polymorphic viruses
  - Periodically rewrite themselves to avoid detection
- Multipartite viruses
  - Infect multiple file types
- Stealth viruses
  - Erase their code from the hard drive and reside in the active memory

Antivirus Software

- Programs designed to detect viruses
  - Scan files looking for virus signatures (unique code)
  - Provide options for deleting or fixing infected files
  - Inoculate files against further infection
- Needs to be updated frequently



Dealing with an Infected Computer

1. Boot computer with antivirus DVD/CD in DVD drive.
2. Run directly from DVD/CD.
3. Allow software to delete or quarantine infected files.
4. Research viruses found to ensure further manual steps are not needed.

Prevent Instant Messaging Viruses

- Allow contact from Buddy or Friends List users only.
- Never automatically accept transfers of data.
- Avoid using instant messaging programs on public computers.

Other Ways to Protect Your System

- Keep your antivirus and operating system (OS) software up to date
- Load security patches as soon as they are available
- Enable automatic updates

Hackers

- Anyone who unlawfully accesses a computer system
- Types of hackers
  - White hat
  - Black hat
  - Script kiddies

17

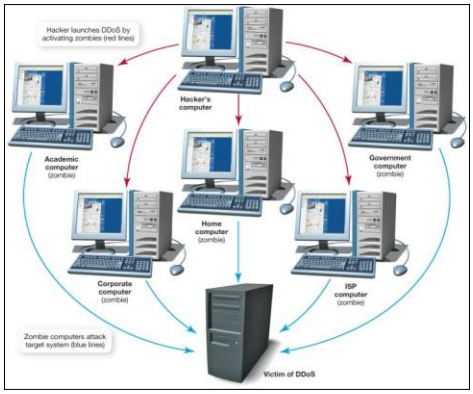
What Hackers Steal

- Hackers try to steal data stored on hard drives:
  - Credit card numbers
  - Bank account numbers
- Also can steal information through packet sniffing
- Use information to commit identity theft

18

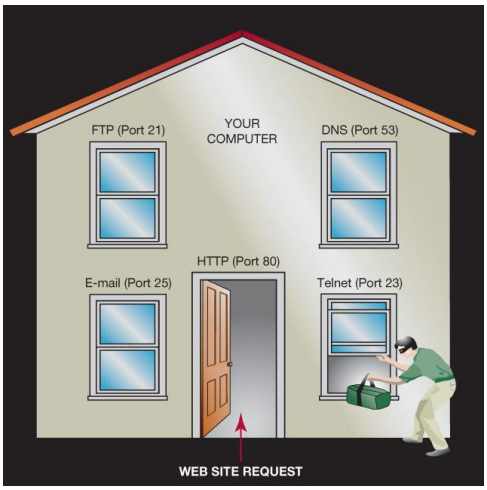
How Computers Are Attacked

- Trojan horse
- Backdoor program
  - Zombies
- Denial of service attacks (DoS)
- Distributed denial of service attacks (DDoS)



How Hackers Gain Access

- Direct access
  - Hacking software
- Indirect access
  - Internet connection
  - Logical ports



Firewalls

- Software programs or hardware designed to close logical ports to invaders
  - A software firewall is built into Windows 7
  - Other software firewalls are available from vendors
  - Network routers can contain a hardware firewall
- Firewalls are critical if you have an always-on broadband connection
- Test your computer's vulnerability

Bluetooth Attacks

- Bluesnarfing
  - Exploits flaw in access software to steal information contained on the device
- Bluebugging
  - Hacker takes control of the device
- Make your device invisible

Wireless Networks on the Road

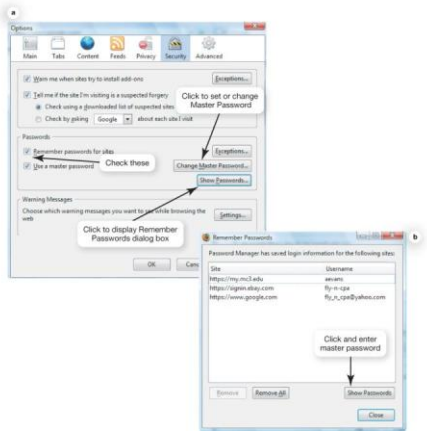
- Beware
  - "Evil twins"
  - Free Internet access in paid locations
- Protect yourself
  - Check with authorized personnel for official name of hot spot
  - Do not use free access from unknown sources

Passwords

- Create a strong password
  - At least 14 characters, including numbers, symbols, and upper- and lowercase letters
  - Not a single word or a word from a dictionary
  - Not easily associated with you (birthday, name of pet, nickname)
  - Use different passwords for different sites
  - Do not tell anyone or write down password
  - Change password regularly (every month)

Password Managers

- Remember all your different passwords
- Built into
  - Operating systems
  - Web browsers
  - Some security packages



25

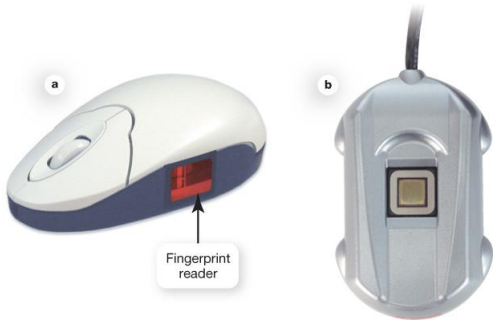
Anonymous Web Surfing

- Public computers
  - Shared computers risk subsequent user viewing your data
  - Might already have viruses or hacking tools installed
- Portable privacy devices
- Linux OS on a flash drive

26

Biometric Authentication Devices

- Read unique personal characteristics
  - Fingerprint
  - Iris patterns
  - Voice patterns
  - Face patterns



Malware

- Software that has a malicious intent
  - Grayware (nondestructive)
    - Adware
    - Spyware
  - Viruses (destructive)

SPAM or SPIM

- SPAM: Unwanted or junk e-mail
  - To avoid SPAM
    - Create free Web-based e-mail account for filling out online forms or making online purchases
    - Use a spam filter
    - *Do not* try to "unsubscribe" from spam e-mails
    - Use an e-mail forwarding service
- SPIM: Unsolicited instant messages

Cookies

- A Web site assigns an ID number to your computer, stored in a cookie file
- Each time you log in to the site, it notes the visit and keeps track of it in a database
- Provide info about browsing habits
- Identify user preferences
- Pose some privacy risks, but low security threat

Backing Up Your Data

- Backup
  - A copy of a file that can be used to replace the original
- Types of files to back up
  - Program
  - Data
- Backup routine
  - Frequency
  - Changed files

Backing Up Your Data

- Software programs for easy backup
  - Schedule automatic backups
  - Can back up files, folders, or entire drives
  - Back up to USB device, CD, or DVD
- Entire system backup software
  - Takes an image of the entire system
  - Stores on a separate hard drive
  - In case of failure, a new drive is inserted

Backing Up Your Data

- Store backups offsite
- Online backups
  - Store backup files on Internet servers
  - Fees for the service

Social Engineering

- Uses social skills to generate human interaction to entice individuals to reveal sensitive information
  - Usually does not use a computer or face-to-face interaction
  - Pretexting

Phishing and Pharming

- Phishing
  - Uses e-mail to lure user to fake Web sites
  - Tricks user into revealing private data
- Pharming
  - Malicious code changes Web browser's ability to find Web addresses

Hoaxes

- An attempt to make someone believe something that is untrue
  - Target large audiences
  - Practical joke, agents of social change, or time wasters
  - Mostly e-mail

Protect Physical Assets

- Environmental factors
  - Avoid
    - Sudden movement
    - Excessive heat or cold
    - Dust
    - Food and liquids
  - Use padded case for notebooks

Power Surges

- Occur when electrical current is supplied in excess of normal voltage (120 volts in the United States)
- Caused by:
  - Old or faulty wiring
  - Downed power lines
  - Malfunctions at electric substations
  - Lightning strikes
- Use surge protectors

Deterring Theft

- Alarms
- Locks and surrounds
- Software alerts

Chapter 9 Summary Questions

- From which types of viruses do I need to protect my computer?

Chapter 9 Summary Questions

- What can I do to protect my computer from viruses?

Chapter 9 Summary Questions

- How can hackers attack my computing devices, and what harm can they cause?

Chapter 9 Summary Questions

- What is a firewall, and how does it keep my computer safe from hackers?

Chapter 9 Summary Questions

- How do I create secure passwords and manage all of my passwords?

Chapter 9 Summary Questions

- How can I surf the Internet anonymously and use biometric authentication devices to protect my data?

Chapter 9 Summary Questions

- How do I manage online annoyances such as spyware and spam?

Chapter 9 Summary Questions

- What data do I need to back up, and what are the best methods for doing so?

Chapter 9 Summary Questions

- What is social engineering, and how do I avoid falling prey to phishing and hoaxes?

Chapter 9 Summary Questions

- How do I protect my physical computing assets from environmental hazards, power surges, and theft?