Technology in Action

Chapter 7
Securing Your System:
Protecting Your Digital Data and Devices
Chapter Topics

- Cybercrime and Identity Theft
- Protecting Yourself from Computer Viruses
- Protecting Digital Assets from Hackers
- Managing Online Annoyances
- Keeping Your Data Safe
- Protecting Your Physical Computing Assets
Cybercrime and Identity Theft

- Cybercrime
- Cybercriminals
- Common types of cybercrimes
Cybercrime and Identity Theft

- Identity theft
  - Acts perpetrated by identity thieves
  - Does not have to involve the use of a computer
Cybercrime and Identity Theft

• Other methods to obtain personal information
  – Stealing purses and wallets
  – Stealing mail or looking through trash
  – Posing as bank or credit card company representative
  – Skimming devices
Cybercrime and Identity Theft

• Theft of computer equipment
  – Larceny
• Resale value is high
• Equipment sold online
Computer Viruses

• Not just limited to computers
  – Smartphones, tablets
• One of the most widespread types of cybercrimes
Computer Viruses

• Main purpose
  – Replicate themselves and copy

• Secondary objectives
  – Slow down networks
  – Display annoying messages
  – Destroy files or contents of hard drive
Computer Viruses

• Sources of virus infection
  – Downloading infected audio and video files
  – Shared flash drives
  – Downloading or executing e-mail attachments
How Viruses Spread

**STEP 1:** Virus creation

Hacker's computer

**STEP 2:** Initial virus infection

File-sharing server

**STEP 3:** Virus spreads to another computer

Bill's computer

**STEP 4:** Fred infects his cell phone

Fred's smartphone

**STEP 5:** Other computers susceptible to infection

Susan's work computer

Fred's tablet

Copyright © 2015 Pearson Education, Inc.
Major Categories of Viruses

- **Boot-sector Viruses**
  Execute when a computer boots up

- **Logic Bombs/Time Bombs**
  Execute when certain conditions or dates are reached

- **Worms**
  Spread on their own with no human interaction needed

- **Script and Macro Viruses**
  Series of commands with malicious intent

- **E-mail Viruses**
  Spread as attachments to e-mail, often using address books

- **Encryption Viruses**
  Hold files “hostage” by encrypting them; ask for ransom to unlock them
Computer Viruses:

Boot-Sector Viruses

• Replicates onto hard drive’s master boot record
• Often transmitted by a flash drive
Logic Bombs and Time Bombs

• Logic bomb
  – Triggered when certain logical conditions are met

• Time bomb
  – Triggered by passage of time
  – Activated on a specific date
Computer Viruses: Worms

- Unlike viruses, worms work independently of host file
- Goal is to spread through networks
Computer Viruses: Script and Macro Viruses

• Script
  – Series of commands (mini-program)
• Macro viruses
  – Series of short commands that automate repetitive tasks
Computer Viruses: E-Mail Viruses

- Distribute using address book in e-mail
- Melissa virus was first example
Computer Viruses:
Encryption Viruses

• Data files
  – Become unusable
Computer Viruses: Additional Virus Classifications

- Classified by methods used to avoid detection
  - Polymorphic viruses
  - Multipartite viruses
  - Stealth viruses
Computer Viruses:
Virus Symptoms

• Existing program icons or files suddenly disappear
• Unusual home page
• New toolbars
• Odd messages, pop-ups, or images
• Data files become corrupt
• Programs stop working properly
• System slows down or takes a long time to boot up
Preventing Virus Infections

• Antivirus software
  – Detects viruses and protects your computer

• Popular programs
  – Symantec
  – Kaspersky
  – AVG
  – McAfee
Preventing Virus Infections: 
Antivirus Software

• Main functions of antivirus software
  – Detection
  – Stopping virus execution
  – Preventing future infection
Preventing Virus Infections: Antivirus Software

Scan Name: Daily Hard Drive Scan

**Scan Schedule**

- **Start Time:** 4:00 AM

  - **When do you want the scan to run?**
    - Do not schedule this scan
    - Run at a specific time interval
    - Daily
    - Weekly
    - Monthly

  - **Run the scan**
    - Only at idle time
    - Only on AC power
    - Prevent standby

  This keeps the computer from entering sleep or standby mode so that the virus scan can run.

Copyright © 2015 Pearson Education, Inc.
Preventing Virus Infections: Antivirus Software

- Windows Defender is included with Windows

Copyright © 2015 Pearson Education, Inc.
Preventing Virus Infections:  
**Antivirus Software**

• If computer is infected  
  – Boot up using antivirus installation/repair disc  
• Virus is detected  
  – Research it  
  – Websites contain archives on viruses
Preventing Virus Infections:

Antivirus Software

- Smartphones and other mobile devices are susceptible to viruses
- Antivirus software for mobile devices is available
  - Trend Micro’s Mobile Security for Android
Preventing Virus Infections: Software Updates

- Drive-by downloads
- Windows operating system
  - Automatic update utility: Windows Update
Preventing Virus Infections:
Software Updates

- Default option in Windows
  - Receive updates automatically
- Other options available

![Windows Update Settings](image)
Hackers

• Types of hackers
  – White-hat or ethical hackers
  – Black-hat hackers
  – Grey-hat hackers

“Oh, we used to use a crystal ball, but hacking into your credit files is much more informative!”
Hackers:
Problems Hackers Can Cause

- Steal credit and debit card information
- Break into websites
- Capture login ID and passwords
Hackers: Problems Hackers Can Cause

• Packet analyzer (sniffer)
  – Tool used by hackers

• Firewall
  – Protection from hackers

• Data encryption
  – Excellent source of protection on wireless networks
Hackers:

Trojan Horses and Rootkits

- Trojan Horses—appear to be useful
- Rootkits
- Zombies
Hackers:
Denial-of-Service Attacks

• Legitimate users are denied access to a computer system
• System shuts down
Hackers: How Hackers Gain Computer Access

- Direct access
- Indirect access
- Logical ports
Restricting Access to Your Digital Assets

• Keep hackers out
  – Prevent them from accessing computer
  – Protect your digital information
  – Hide activities from prying eyes
Restricting Access to Your Digital Assets:

Firewalls

• Firewall – Hardware or software
• Windows and OS X include firewalls
• Security suites also include firewall software
Restricting Access to Your Digital Assets: Firewalls

Review recent messages and resolve problems

Action Center has detected one or more issues for you to review.

Security

Network firewall

Windows Firewall is actively protecting your PC.

Windows Update

Windows will automatically install updates as they become available.

Virus protection

Windows Defender is helping to protect your PC.

Spyware and unwanted software protection

Windows Defender is helping to protect your PC.

Internet security settings

All Internet security settings are set to their recommended levels.

Copyright © 2015 Pearson Education, Inc.
Restricting Access to Your Digital Assets:
How Firewalls Work

• Protect in two major ways
  – Blocking access to logical ports
  – Keeping computer’s network address secure

• Packet filtering

• Logical port blocking

• Internet Protocol address (IP address)

• Network address translation (NAT)
Restricting Access to Your Digital Assets: Knowing Your Computer Is Secure

- Websites test computer’s vulnerability
  - Gibson Research (www.grc.com)
    - ShieldsUP
    - LeakTest
- If vulnerabilities are detected:
  - Install (or reconfigure) a firewall
  - Close or restrict access to ports
## Restricting Access to Your Digital Assets: Creating Passwords

### Strong and Weak Password Candidates

<table>
<thead>
<tr>
<th>PASSWORD</th>
<th>RATING</th>
<th>GOOD POINTS</th>
<th>BAD POINTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joysmith1022</td>
<td>Poor</td>
<td>• Contains upper- and lowercase letters</td>
<td>• Less than 14 characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Contains letters and numbers</td>
<td>• Contains name and birth date</td>
</tr>
<tr>
<td>test44drive6car</td>
<td>Mediocre</td>
<td>• 15 characters in length</td>
<td>• Contains three words found in the dictionary</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Numbers repeated consecutively</td>
</tr>
<tr>
<td>8$RanT%5ydTtt&amp;</td>
<td>Better</td>
<td>• Good length</td>
<td>• Upper- and lowercase letters repeated consecutively</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Contains upper- and lowercase letters</td>
<td>• Still contains one dictionary word (rant)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Contains symbols</td>
<td></td>
</tr>
<tr>
<td>7R3m3mB3R$5%y38</td>
<td>Best</td>
<td>• All good points from above</td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Dictionary word (remember) has 3s instead of Es</td>
<td></td>
</tr>
</tbody>
</table>
Restricting Access to Your Digital Assets:
Creating Passwords

• Password strength tests
  – Password Meter

• Operating systems have built-in password protection (if you choose to use it)
  – Windows 8.1 offers picture passwords
Restricting Access to Your Digital Assets: Managing Your Passwords

- Password management software
- Security suites and web browsers provide password management tools
Restricting Access to Your Digital Assets: Anonymous Web Surfing: Hiding from Prying Eyes

• Browser-based privacy tools to surf the web anonymously
  – Incognito
  – Private Browsing
  – InPrivate
Restricting Access to Your Digital Assets: Anonymous Web Surfing: Hiding from Prying Eyes

• Portable privacy devices
  – Store sensitive Internet files
  – Example - Ironkey Personal Flash Drive
• Preload Linux OS on a flash drive
• Third-party software developers offer apps to enhance tablet security
  – IPVanish
Restricting Access to Your Digital Assets: Biometric Authentication Devices

- Fingerprint
- Iris pattern in eye
- Voice authentication
- Face pattern recognition
- Provide high level of security
What is cybercrime and who perpetrates it?

- Cybercrime is any type of crime perpetrated via a computer or a website.
- Major types of cybercrime are identity theft, credit card fraud, computer viruses, illegal access of computer systems, and auction fraud.
- Cybercriminals use computers, the Internet, and computer networks to commit their crimes.
What are the types of viruses from which I need to protect my computer?

• Computer viruses can be grouped into six categories:
  – boot-sector viruses
  – logic bombs and time bombs
  – worms
  – scripts and macro viruses
  – e-mail viruses
  – encryption viruses
What can I do to protect my computer from viruses?

• Install antivirus software
• Update system and application software on a regular basis
• Run a virus scan periodically
Check Your Understanding

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

• Hackers can use software to break into almost any computer connected to the Internet, unless proper precautions are taken.
• Once hackers gain access to a computer, they can potentially
  – steal personal or other important information
  – damage and destroy data
  – use the computer to attack other computers
Check Your Understanding

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

• Firewalls are software programs or hardware devices designed to keep computers safe from hackers.
• By using a personal firewall, you can close open logical ports.
• Potentially make your computer invisible to other computers on the Internet.
How do I create secure passwords and manage all of my passwords?

- Secure passwords contain a mixture of upper- and lowercase letters, numbers, and symbols and are at least 14 characters long.
- Passwords should not contain words that are in the dictionary or easy-to-guess personal information, like your pet’s name.
- Online password checkers can be used to evaluate the strength of your passwords.
- Utilities built into web browsers and Internet security software can be used to manage your passwords and alleviate the need to remember numerous complex passwords.
Check Your Understanding

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

- Browsers include tools that hide your surfing activities
- Biometric authentication devices use a physical attribute that is not easily duplicated to control access to data files or computing devices
  - Some laptops and smartphones today feature fingerprint readers and facial-recognition software to control access
Malware: Adware and Spyware

- Malware
- Three primary forms
  - Adware
  - Spyware
  - Viruses
Managing Online Annoyances:  
Malware: Adware and Spyware

• Spyware
  – Transmits information
  – Tracking cookies
  – Keystroke logger

• Windows Defender
  – Install one or two additional standalone anti-spyware programs
Managing Online Annoyances: Malware: Adware and Spyware

- Many antispyware packages are available
Managing Online Annoyances:

Spam

• Spam – junk e-mail
• Spim – unwanted instant messages
Managing Online Annoyances: Spam (cont.)

• To avoid spam:
  – Use a separate e-mail address for filling out online forms
  – Use a spam filter
Managing Online Annoyances: Spam

- Other ways to prevent spam
  - Read website privacy policies
  - Don’t give the site permission to pass on your e-mail address
  - Don’t reply to spam
  - Subscribe to an e-mail forwarding service
Managing Online Annoyances:
Cookies

• Provide websites with information about browsing habits
• Don’t search for personal information
• Only collect information you supply when filling out forms
• Some sites sell the information
• Pose no security threat
# Keeping Your Data Safe: Protecting Your Personal Information

## Internet Information-Sharing Precautions

### Information Identity Thieves Crave

- Social Security Number
- Full Date of Birth
- Phone Number
- Street Address

Never make this information visible on websites!

### Other Sensitive Information

- Full Legal Name
- E-mail Address
- Zip Code
- Gender
- School or Workplace

Only reveal this information to people you know—don’t make it visible to everyone!
Keeping Your Data Safe: 
Backing Up Your Data

• How might I lose data?
  – Unauthorized access
  – Tampering
  – Destruction (accidental or intentional)

• Backups
  – Copies of data used to replace originals
Keeping Your Data Safe: Backing Up Your Data

Files to Back Up

- **Program files**: Installation files for productivity software (i.e., Microsoft Office)
- **Data files**: Files you create (term papers, spreadsheets, etc.)

Types of Backups

- **Incremental (partial)**: Only backs up files that have changed
- **Image (system)**: Snapshot of your entire computer, including system software

Where to Store Backup Files

- Online (in the cloud)
- External hard drives
- Network-attached storage devices or home servers
Keeping Your Data Safe:  
Backing Up Your Data

• Options for backing up files
  – Incremental backup (partial backup)
  – Image backup (system backup)
## Keeping Your Data Safe: Backing Up Your Data

### A Comparison of Typical Data Backup Locations

<table>
<thead>
<tr>
<th>BACKUP LOCATION</th>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Online (in the Cloud)</strong></td>
<td>• Files stored at a secure, remote location</td>
<td>• Most free storage sites don’t provide enough space for image backups</td>
</tr>
<tr>
<td></td>
<td>• Files/backups accessible anywhere through a browser</td>
<td></td>
</tr>
<tr>
<td><img src="image1.png" alt="Cloud icon" /></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>External Hard Drive</strong></td>
<td>• Inexpensive, one-time cost</td>
<td>• Could be destroyed in one event (fire/flood) with your computer</td>
</tr>
<tr>
<td></td>
<td>• Fast backups with USB 3.0 devices connected directly to your computer</td>
<td>• Can be stolen</td>
</tr>
<tr>
<td><img src="image2.png" alt="External Hard Drive icon" /></td>
<td></td>
<td>• Slightly more difficult to back up multiple computers with one device</td>
</tr>
<tr>
<td><strong>Network-Attached Storage (NAS) Device and Home Server</strong></td>
<td>• Makes backups much easier for multiple computing devices</td>
<td>• More expensive than a stand-alone external hard drive</td>
</tr>
<tr>
<td><img src="image3.png" alt="NAS icon" /></td>
<td></td>
<td>• Could be destroyed in one event (fire/flood) with your computer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Can be stolen</td>
</tr>
</tbody>
</table>
Keeping Your Data Safe: Backing Up Your Data

- Windows 8 includes backup utilities – use them!
Social Engineering

- Human interaction to learn information
- Pretexting – creating scenarios that sound legitimate, but aren’t
  - Fake phone call
Social Engineering: Phishing and Pharming

• Phishing
  – Luring people into revealing information

• Pharming
  – Malicious code planted in browser software to gather information
Social Engineering: Phishing and Pharming

• Guidelines to avoid schemes
  – Never reply directly to e-mails asking for personal information
  – Don’t click on links in e-mails
  – Never give personal information over the Internet unless the site is secure
  – Use phishing filters
  – Use Internet security software
Social Engineering: Scareware

- Type of malware
- Attempts to convince you something is wrong…and to pay money to fix it!
Protecting Your Physical Computing Assets:

Environmental Factors

• Level surfaces
• Protective cases
• Don’t leave in a car in extreme temperatures
• Chill mats
• Keep intake vent unblocked
• Keep room clean
• Don’t eat or drink near your computer
Protecting Your Physical Computing Assets: Power Surges

• Power surges
  – Old or faulty wiring
  – Downed power lines
  – Malfunctions at electric company substations
  – Lightning strikes

• Surge protector
  – Replace every two – three years
  – Use with all devices that have solid-state components
Protecting Your Physical Computing Assets: Deterring Theft

• Security concerns with mobile devices
  – Keeping them from being stolen
  – Keeping data secure in case they are stolen
  – Finding a device if it is stolen
  – Remotely recovering and wiping data off a stolen device
Protecting Your Physical Computing Assets: Keep Them Safe: Alarms

• Motion alarm software
  – LAlarm: free software for laptops
  – SuperAlarm and Alarmomatic
Protecting Your Physical Computing Assets:
Keeping Mobile Device Data Secure

• Encrypt data on your mobile device
  – Transform data using an algorithm that can only be unlocked by a secure code (or key)
  – Safe: an app that provides 256-bit encryption
  – SensiGuard and SafeHouse
Protecting Your Physical Computing Assets:
Software Alerts and Data Wipes

• Theft-tracking software
  – Computrace LoJack for Laptops
  – PC PhoneHome
  – MacPhoneHome

• Remote recovery and deletion of files
  – LoJack for Laptops
Protecting Your Physical Computing Assets: Software Alerts and Data Wipes

- Find my iPhone (or iPad)
Protecting Your Computing Assets: Summary

Computer Security Checklist

Virus and Spyware Protection
- Is antivirus and anti-spyware software installed on all your devices?
- Is the antivirus and anti-spyware software configured to update itself automatically and regularly?
- Is the software set to scan your device on a regular basis (at least weekly) for viruses and spyware?

Firewall
- Do all your computers and tablets have firewall software installed and activated before connecting to the Internet?
- Is your router also able to function as a hardware firewall?
- Have you tested your firewall security by using the free software available at grc.com?

Software Updates
- Have you configured your operating systems (Windows, OS X, iOS) to install new software patches and updates automatically?
- Is other software installed on your device, such as Microsoft Office or productivity apps, configured for automatic updates?
- Is the web browser you're using the latest version?

Protecting Your Devices
- Are all computing devices protected from electrical surges?
- Do your mobile devices have alarms or tracking software installed on them?
Check Your Understanding

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

• Installing anti-malware software tools helps to prevent, detect, and/or reduce spam, adware, and spyware
Check Your Understanding

9. What data do I need to back up, and what are the best methods for doing so?
Check Your Understanding

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

• Social engineering schemes use human interaction, deception, and trickery to fool people into revealing sensitive information

• To avoid phishing schemes
  – Never reply directly to any e-mail asking you for personal information
  – Don’t click on a link in an e-mail to go to a website
Check Your Understanding

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

• Clean environment
• No extreme temperatures
• Use surge protectors
• Install antitheft software on mobile devices
  – Should include the ability to wipe data remotely