


Discovering Computers 2005 A Gateway to Information



Chapter 11 Computers and Society, Security, Privacy, and Ethics

Chapter 11 Objectives

- Describe the types of computer security risks
- Discuss the types of devices available that protect from system failure
- Identify ways to safeguard against computer viruses, worms, and Trojan horses
- Explain the options available for backing up computer resources
- Discuss techniques to prevent unauthorized computer access and use
- Identify safeguards that protect against Internet security risks
- Identify safeguards against hardware theft and vandalism
- Recognize issues related to information accuracy, rights, and conduct
- Explain the ways software manufacturers protect against software piracy
- Discuss issues surrounding information privacy
- Define encryption and explain why it is necessary
- Discuss ways to prevent health-related disorders and injuries due to computer use

Next >

Computer Security Risks

What is a computer security risk?

- Action that causes loss of or damage to computer system



p. 568 Fig. 11-1

Next >

Computer Viruses, Worms, and Trojan Horses

What are viruses, worms, and Trojan horses?

- Virus** is a potentially damaging computer program
 - Can spread and damage files
- Worm** copies itself repeatedly, using up resources and possibly shutting down computer or network
- Trojan horse** hides within or looks like legitimate program until triggered
 - Does not replicate itself on other computers
- Payload** (destructive event) that is delivered when you open file, run infected program, or boot computer with infected disk in disk drive

p. 569

Next >

Computer Viruses, Worms, and Trojan Horses

How can a virus spread through an e-mail message?

- Unscrupulous programmers create a virus program. They hide the virus in a Word document and attach the Word document to an e-mail message.
- They use the Internet to send the e-mail message to thousands of users around the world.
- Other users do not recognize the name of the sender of the e-mail message. These users do not open the e-mail message. Instead they delete the e-mail message. These users' computers are not infected with the virus.
- Some users open the attachment and their computers become infected with the virus.



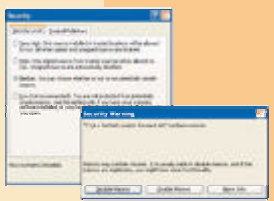
p. 570 Fig. 11-2

Next >

Computer Viruses, Worms, and Trojan Horses

How can you protect your system from a macro virus?

- Set macro security level in applications that allow you to write macros
- At medium security level, warning displays that document contains macro
 - Macros are instructions saved in an application, such as word processing or spreadsheet program



p. 571 Fig. 11-3

Next >

Computer Viruses, Worms, and Trojan Horses

What is an **antivirus program**?

- Identifies and removes computer viruses
- Most also protect against worms and Trojan horses

POPULAR ANTIVIRUS PROGRAMS

KVC Anti-Virus
Comand Antivirus
nTrend AntiVirus
F-Secure Anti-Virus
McAfee VirusScan
Norton AntiVirus
BAV AntiVirus
Trend Micro PC-cillin

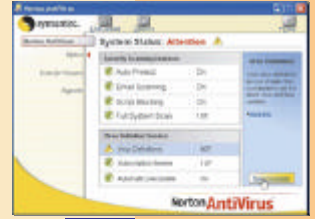
p. 571 Fig. 11-4

Next >

Computer Viruses, Worms, and Trojan Horses

What is a **virus signature**?

- Specific pattern of virus code
 - Also called **virus definition**
- Antivirus programs look for virus signatures

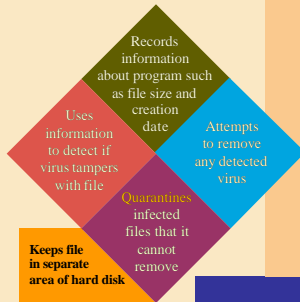


p. 572 Fig. 11-5

Next >

Computer Viruses, Worms, and Trojan Horses

How does an antivirus program **inoculate** a program file?



p. 572

Next >

Computer Viruses, Worms, and Trojan Horses

What is a **recovery disk**?

Removable disk that contains uninfected copy of key operating system commands that enables computer to restart

- Also called rescue disk

Once computer restarts, antivirus program can attempt to repair damaged files

p. 572

Next >

Computer Viruses, Worms, and Trojan Horses

What are some tips for preventing virus, worm, and Trojan horse infections?



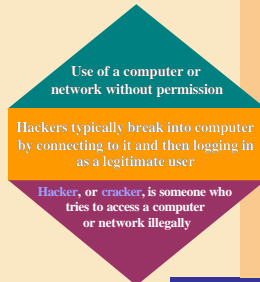
Click to view Web Link, click Chapter 11, Click Web Link from left navigation, then click Virus Horses below Chapter 11

p. 573

Next >

Unauthorized Access and Use

What is **unauthorized access** and how is it achieved?



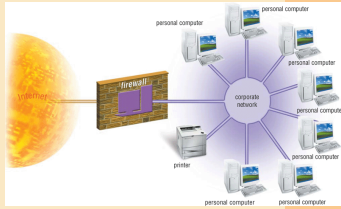
p. 573

Next >

Unauthorized Access and Use

What is a **firewall**?

- Security system consisting of hardware and/or software that prevents unauthorized network access



p. 574 Fig. 11-7

Next >

Unauthorized Access and Use

What is a **personal firewall**?

- Program that protects personal computer and its data from unauthorized intrusions
- Monitors transmissions to and from computer
- Informs you of attempted intrusion

PERSONAL FIREWALL SOFTWARE

BlackICE PC Protection
McAfee Personal Firewall Plus
Norton Personal Firewall
Sygate Personal Firewall
Tiny Personal Firewall
ZenWorks

p. 575 Fig. 11-8

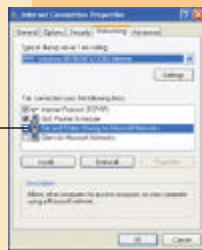
Next >

Unauthorized Access and Use

What are other ways to protect your personal computer?

- Disable file and printer sharing on Internet connection
- Use **online security service**—Web site that evaluates computer to check for Web and e-mail vulnerabilities

File and printer sharing turned off



p. 575 Fig. 11-9

Next >

Unauthorized Access and Use

How can companies protect against hackers?

Intrusion detection software analyzes network traffic, assesses system vulnerabilities, and identifies intrusions and suspicious behavior

Access control defines who can access computer and what actions they can take

Audit trail records access attempts



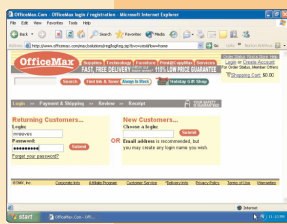
Click to view Web Link.
Click Chapter 11, Click Web Link from left navigation.
Then click Intrusion Detection Software below Chapter 11
p. 576

Next >

Unauthorized Access and Use

What is a **user name**?

- Unique combination of characters that identifies user
- **Password** is private combination of characters associated with the user name that allows access to computer resources



p. 576 Fig. 11-10

Next >

Unauthorized Access and Use

How can you make your password more secure?

- Longer passwords provide greater security

PASSWORD PROTECTION

Number of Characters	Possible Combinations	AVERAGE TIME TO DISCOVER	
		Human	Computer
1	36	3 minutes	.000033 seconds
2	1,300	3 hours	.00066 seconds
3	47,600	3 days	.02 seconds
4	1,700,000	3 months	1 second
6	80,000,000	10 years	39 seconds
10	3,700,000,000,000,000	500 million years	89 years

• Possible characters include the letters A-Z and numbers 0-9
 • Human discovery assumes 7 try every 10 seconds
 • Computer discovery assumes 1 million tries per second
 • Average time assumes the password would be discovered in approximately half the time it would take to try all possible combinations

p. 577 Fig. 11-11

Next >

Unauthorized Access and Use

What is a possessed object?

- Item that you must carry to gain access to computer or facility
- Often used with numeric password called **personal identification number (PIN)**



p. 578 Fig. 11-12

Next >

Unauthorized Access and Use

What is a **biometric device**?

- Authenticates person's identity using personal characteristic
 - Fingerprint, hand geometry, voice, signature, and iris



p. 578 Fig. 11-13

Next >

Unauthorized Access and Use

What is a callback system?

User connects to computer only after the computer calls that user back at a previously established telephone number

Some networks utilize callback systems as an access control method to authenticate remote or mobile users

Callback systems work best for users who regularly work at the same remote location, such as at home or branch office

p. 579

Next >

Hardware Theft and Vandalism

What are **hardware theft** and **hardware vandalism**?

- **Hardware theft** is act of stealing computer equipment
 - Cables sometimes used to lock equipment
 - Some notebook computers use passwords, possessed objects, and biometrics as security methods
 - For PDAs, you can password-protect the device
- **Hardware vandalism** is act of defacing or destroying computer equipment



p. 579 Fig. 11-14

Next >

Software Theft

What is **software theft**?

Act of stealing or illegally copying software or intentionally erasing programs

Software piracy is illegal duplication of copyrighted software



Click to view Web Link.
click Chapter 11, Click Web Link
from left navigation.
Then click Software Piracy below
Chapter 11

p. 580

Next >

Software Theft

What is a **license agreement**?

- Right to use software
- **Single-user license agreement** allows user to install software on one computer, make backup copy, and sell software after removing from computer



p. 580 Fig. 11-15

Next >

Software Theft

What are some other safeguards against software theft?

Product activation allows user to input product identification number online or by phone and receive unique installation identification number

Business Software Alliance (BSA) promotes better understanding of software piracy problems

Click to view Web Link, click Chapter 11, Click Web Link from left navigation, then click Business Software Alliance below Chapter 11 p. 581

Next >

Information Theft

What is **encryption**?

- > Safeguards against **information theft**
- > Process of converting plaintext (readable data) into ciphertext (unreadable characters)
- > Encryption key (formula) often uses more than one method
- > To read the data, the recipient must **decrypt**, or decipher, the data

SAMPLE ENCRYPTION METHODS

Name	Method	Plaintext	Ciphertext	Explanation
Transposition	Switch the order of characters	MESSAGE	EMSSAGE	Adjacent characters swapped
Substitution	Replace characters with other characters	MESSAGE	DRADYU	Each letter replaced with another
Expansion	Insert characters between existing characters	MESSAGE	MEASSEES	Letter E inserted before each character
Compression	Remove characters and shift others over	MESSAGE	MEASSES	Every third letter removed (E, L, S, E)

Click to view Web Link, click Chapter 11, Click Web Link from left navigation, then click Encryption below Chapter 11 p. 582 Fig. 11-16

Next >

Information Theft

What does an encrypted file look like?

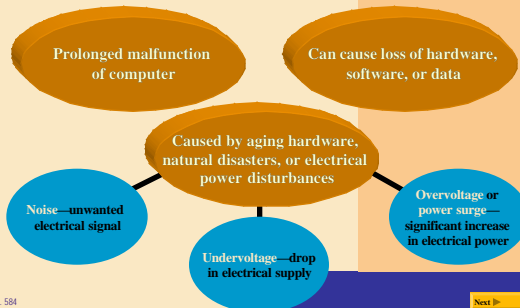


p. 583 Fig. 11-17

Next >

System Failure

What is a system failure?



p. 584

Next >

System Failure

What is a **surge protector**?

- > Protects computer and equipment from electrical power disturbances
- > **Uninterruptible power supply (UPS)** is surge protector that provides power during power loss

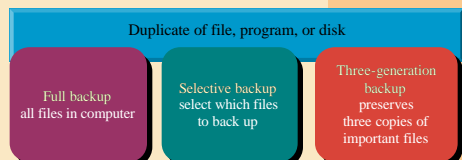


Click to view Web Link, click Chapter 11, Click Web Link from left navigation, then click Uninterruptible Power Supply below Chapter 11 p. 584 Figs. 11-18–11-19

Next >

Backing Up – The Ultimate Safeguard

What is a **backup**?



In case of system failure or corrupted files, restore files by copying to original location

p. 586

Next >

Internet Security Risks

What is a denial of service attack?

Also called DoS attack

Hacker uses unsuspecting computer, called **zombie**, to execute attack on other systems

Distributed DoS (DDoS) attack is more devastating DoS attack in which multiple computers attack multiple networks

Computer Emergency Response Team Coordination Center (CERT/CC) assists with DDoS attacks



Click to view Web Link
click Chapter 11, Click Web Link
from left navigation,
then click Emergency Response
Team Coordination Center
below Chapter 11
p. 587

Next >

Internet Security Risks

How do Web browsers provide secure data transmission?

Many Web browsers use encryption

Secure site is Web site that uses encryption to secure data

Digital certificate is notice that guarantees Web site is legitimate

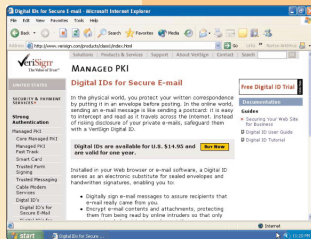
p. 587

Next >

Internet Security Risks

What is a certificate authority (CA)?

- Authorized person or company that issues and verifies digital certificates
- Users apply for digital certificate from CA



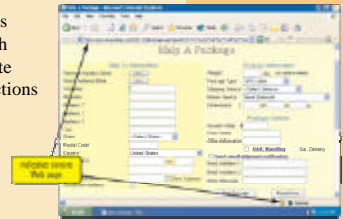
p. 588 Fig. 11-20

Next >

Internet Security Risks

What is Secure Sockets Layer (SSL)?

- Provides encryption of all data that passes between client and Internet server
 - Web addresses beginning with “https” indicate secure connections



p. 588 Fig. 11-21

Next >

Internet Security Risks

What are methods for securing e-mail messages?

Pretty Good Privacy (PGP) is popular e-mail encryption program

Digital signature is encrypted code attached to e-mail message to verify identity of sender

Freeware for personal, non-commercial use



Click to view Web Link
click Chapter 11, Click Web Link from left navigation,
then click PGP below Chapter 11
p. 588

Next >

Ethics and Society

What are **computer ethics**?

Moral guidelines that govern use of computers and information systems

Unauthorized use of computers and networks

Software theft

Information accuracy

Intellectual property rights—rights to which creators are entitled for their work

Codes of conduct

Information privacy



Click to view Web Link
click Chapter 11, Click Web Link from left navigation,
then click Intellectual Property Rights below Chapter 11
p. 589

Next >

Ethics and Society

What is an IT code of conduct?

- Written guideline that helps determine whether computer action is ethical
- Employers can distribute to employees

IT CODE OF CONDUCT

1. Computers may not be used to harm other people.
2. Employees may not interfere with others' computer work.
3. Employees may not messle in others' computer files.
4. Computers may not be used to cheat.
5. Computers may not be used to steal files without authorization.
6. Employees may not copy or use software illegally.
7. Employees may not use others' computer resources without authorization.
8. Employees may not use others' intellectual property as their own.
9. Employees should consider the social impact of programs and systems they design.
10. Employees always should use computers in a way that demonstrates consideration and respect for fellow humans.

p. 591 Fig. 11-24

Next >

Information Privacy

What is information privacy?

Right of individuals and companies to restrict collection and use of information about them

Difficult to maintain today because data is stored online

Employee monitoring is using computers to observe employee computer use

Legal for employers to use monitoring software programs

Click to view video

p. 591 and 597

Next >

Information Privacy

What are some ways to safeguard personal information?

Fill in necessary information on rebate, warranty, and registration forms

Install a cookie manager to filter cookies

Sign up for e-mail filtering through your Internet service provider or use an antisppam program, such as Brightmail

Avoid shopping club and buyers cards

Clear your history file when you are finished browsing

Set up a free e-mail account; use this e-mail address for merchant forms

Do not reply to spam for any reason

Inform merchants that you do not want them to distribute your personal information

Turn off file and print sharing on your Internet connection

Surf the Web anonymously with a program such as Freedom Web Secure or through an anonymous Web site such as Anonymizer.com

Limit the amount of information you provide to Web sites; fill in only required information

Install a personal firewall

p. 592

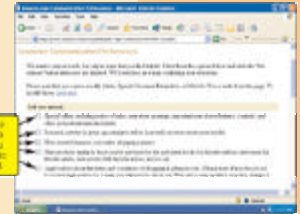
Next >

Information Privacy

What is an electronic profile?

- Data collected when you fill out form on Web
- Merchants sell your electronic profile
- Often you can specify whether you want personal information distributed

Learning about online users' interests and behavior can be used to create a profile of the user. This profile can be sold to other companies.



p. 592 Fig. 11-26

Next >

Information Privacy

What is a cookie?



Click to view Web Link, click Chapter 11, Click Web Link from left navigation, then click Cookies below Chapter 11

p. 593

Next >

Information Privacy

How do cookies work?

Step 1. When you type the Web address of Web site in your browser window, browser program searches your hard disk for a cookie associated with Web site.



Step 2. If browser finds a cookie, it sends information in cookie file to Web site.

Step 3. If Web site does not receive cookie information, and is expecting it, Web site creates an identification number for you in its database and sends that number to your browser. Browser in turn creates a cookie file based on that number and stores cookie file on your hard disk. Web site now can update information in cookie files whenever you access the site.



p. 594 Fig. 11-27

Next >

Information Privacy

What is a cookie manager?

- Software program that selectively blocks cookies

COOKIE MANAGER

Application Name	Tracking
AdBlock Plus	Blocks advertising and tracking
EPN Privacy & Control Wizard	Asks to install cookies, blocks otherwise. Also view and advertisements, disable pop-up windows
Cookie Controler	View, edit, and delete cookies
Cookie Guardian	Asks to install cookies by Web site - lets you manage cookies on number (tracking, advertising, etc. etc.)
CookieSight	Allows you to block or allow cookies and advertising based on their domain names
Cookiecutter, NICE	Deletes cookies, also can delete cache, history files, and other browsing files
WebCrawler	Blocks advertising banners and associated cookies
Webcam Shield	Deletes cache, history, and cookie files

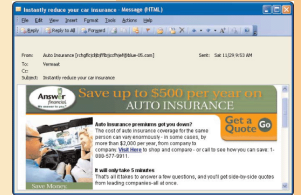
p. 594 Fig. 11-28

Next >

Information Privacy

What are spyware and spam?

- Spyware is program placed on computer without user's knowledge
 - Secretly collects information about user
- Spam is unsolicited e-mail message sent to many recipients

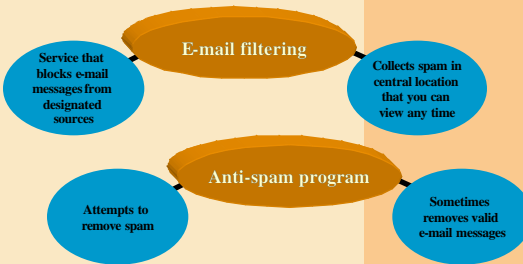


p. 595 Fig. 11-29

Next >

Information Privacy

How can you control spam?



p. 595

Next >

Information Privacy

What privacy laws have been enacted?

Date	Law	Purpose
2001	Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act	Gives law enforcement the right to monitor people's activities, including Web and e-mail habits.
1998	Digital Millennium Copyright Act (DMCA)	Makes it illegal to circumvent anti-piracy schemes in commercial software; outlaws sale of devices that copy software illegally.
1997	No Electronic Theft (NET) Act	Closes a narrow loophole in the law that allowed people to give away copyrighted material (such as software) on the Internet without legal repercussions.
1996	National Information Infrastructure Protection Act	Penalizes theft of information across state lines, threats against networks, and computer system trespassing.
1994	Computer Abuse Amendments Act	Amends 1984 act to outlaw transmission of harmful computer code such as viruses.
1992	Cable Act	Extends the privacy of the Cable Communications Policy Act of 1984 to include cellular and other wireless services.
1991	Telephone Consumer Protection Act	Restricts activities of telemarketers.
1988	Computer Matching and Privacy Protection Act	Regulates the use of government data to determine the eligibility of individuals for federal benefits.
1988	Video Privacy Protection Act	Forbids retailers from releasing or selling video-rental records without customer consent or a court order.

p. 596 Fig. 11-30

Next >

Information Privacy

What privacy laws have been enacted? (cont'd)

Date	Law	Purpose
1986	Electronic Communications Privacy Act (ECPA)	Provides the same right of privacy protection for the postal delivery service and telephone companies to the new forms of electronic communications, such as voice mail, e-mail, and cellular telephones.
1984	Cable Communications Policy Act	Regulates disclosure of cable television subscriber records.
1984	Computer Fraud and Abuse Act	Outlaws unauthorized access of federal government computers.
1978	Right to Financial Privacy Act	Strictly outlines procedures federal agencies must follow when looking at customer records in banks.
1974	Privacy Act	Forbids federal agencies from allowing information to be used for a reason other than that for which it was collected.
1974	Family Educational Rights and Privacy Act	Gives students and parents access to school records and limits disclosure of records to unauthorized parties.
1970	Fair Credit Reporting Act	Prohibits credit reporting agencies from releasing credit information to unauthorized people and allows consumers to review their own credit records.

p. 596 Fig. 11-30

Next >

Information Privacy

What is content filtering?

- Process of restricting access to certain material
- Internet Content Rating Association (ICRA) provides rating system of Web content
- Web filtering software restricts access to specified sites



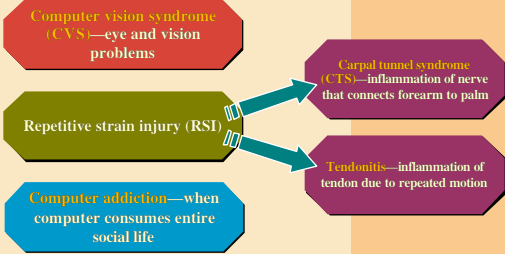
Click to view Web Link, click Chapter 11, Click Web Link from left navigation, then click Internet Content Rating Association below Chapter 11

p. 597 Fig. 11-31

Next >

Health Concerns of Computer Use

What are some health concerns of computer use?



p. 598, 599, and 601

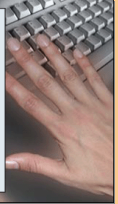
Next >

Health Concerns of Computer Use

What precautions can prevent tendonitis or carpal tunnel syndrome?

- > Take frequent breaks during computer session
- > Use wrist rest
- > Exercise hands and arms
- > Minimize number of times you switch between mouse and keyboard

Spread fingers apart for several seconds while keeping wrists straight. Gently push back fingers and then thumb. Dangle arms loosely at sides and then shake arms and hands.



p. 599 Fig. 11-32

Next >

Health Concerns of Computer Use

How can you ease eyestrain when working at the computer?

Every 20 to 30 minutes, take an eye break.

- Look into the distance and focus on an object for 20 to 30 seconds.
- Roll your eyes in a complete circle.
- Close your eyes and rest them for at least one minute.

blink your eyes every five seconds

Place your display device about an arm's length away from your eyes with the top of the screen at eye level or below.

Use large fonts.

If you wear glasses, ask your doctor about computer glasses.

Adjust the lighting.

p. 599 Fig. 11-33

Next >

Health Concerns of Computer Use

What is ergonomics?

- > Applied science devoted to comfort, efficiency, and safety in



Click to view video

p. 600 Fig. 11-34

Next >

Health Concerns of Computer Use

What is green computing?

- > Reducing electricity and environmental waste while using computer

1. Use computers and devices that comply with the ENERGY STAR program.
2. Do not leave the computer running overnight.
3. Turn off the monitor, printer, and other devices when not in use.
4. Use paperless methods to communicate.
5. Recycle paper.
6. Buy recycled paper.
7. Recycle toner cartridges.
8. Recycle old computers and printers.
9. Telecommute (saves gas).



Click to view Web Link, click Chapter 11, Click Web Link from left navigation, then click Green Computing below Chapter 11.

p. 601 Fig. 11-35

Next >

Summary of Computers and Society, Security, Privacy, and Ethics

Potential computer risks

Safeguards that schools, business, and individuals can implement to minimize these risks

Internet security risks and safeguards

Ethical issues surrounding information accuracy, intellectual property rights, codes of conduct, and information privacy

Computer-related health issues, their preventions, and ways to keep the environment healthy

Chapter 11 Complete