COURSE TECHNOLOGY
CENGAGE Learning™

Security+ Guide to Network Security Fundamentals, Fourth Edition

Chapter 2

Malware and Social Engineering Attacks

Objectives

- Describe the differences between a virus and a worm
- List the types of malware that conceals its appearance
- Identify different kinds of malware that is designed for profit
- Describe the types of social engineering psychological attacks
- Explain physical social engineering attacks

Attacks Using Malware

- Malicious software (malware)
  - Enters a computer system:
    - Without the owner’s knowledge or consent
  - Refers to a wide variety of damaging or annoying software
- Primary objectives of malware
  - Infecting systems
  - Concealing its purpose
  - Making profit

Malware That Spreads

- Viruses
  - Malicious computer code that reproduces itself on the same computer
- Virus infection methods
  - Appender infection
    - Virus appends itself to end of a file
    - Moves first three bytes of original file to virus code
    - Replaces them with a jump instruction pointing to the virus code

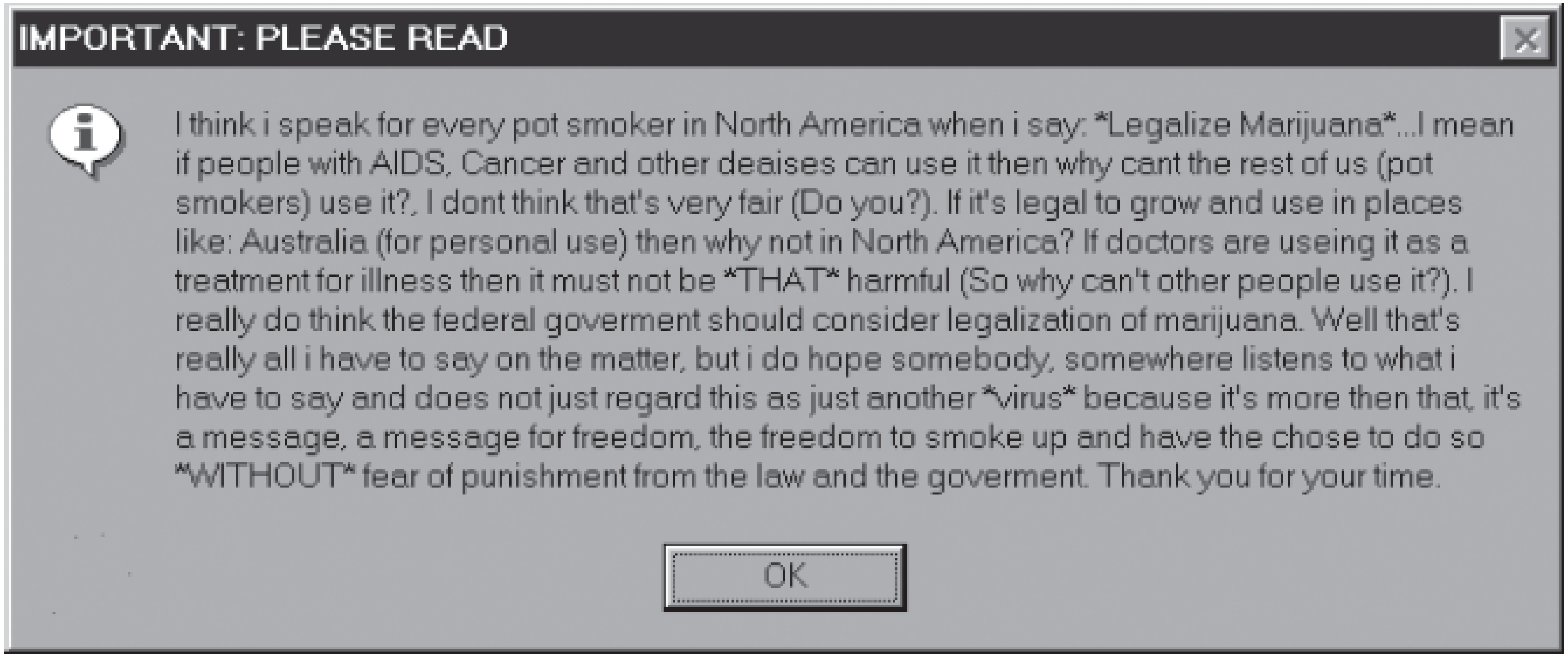
Malware That Spreads (cont'd.)

- Virus infection methods (cont'd.)
  - Swiss cheese infection
    - Viruses inject themselves into executable code
    - Original code transferred and stored inside virus code
    - Host code executes properly after the infection
  - Split infection
    - Virus splits into several parts
    - Parts placed at random positions in host program
    - Head of virus code starts at beginning of file
    - Gives control to next piece of virus code

Malware That Spreads (cont’d.)

- When infected program is launched:
  - Virus replicates itself by spreading to another file on same computer
  - Virus activates its malicious payload
- Viruses may display an annoying message:
  - Or be much more harmful
- Examples of virus actions
  - Cause a computer to repeatedly crash
  - Erase files from or reformat hard drive
  - Turn off computer’s security settings

Malware That Spreads (cont'd.)



I think i speak for every pot smoker in North America when i say: *Legalize Marijuana*...I mean if people with AIDS, Cancer and other deaises can use it then why cant the rest of us (pot smokers) use it?, I dont think that's very fair (Do you?). If it's legal to grow and use in places like: Australia (for personal use) then why not in North America? If doctors are useing it as a treatment for illness then it must not be *THAT* harmful (So why can't other people use it?). I really do think the federal goverment should consider legalization of marijuana. Well that's really all i have to say on the matter, but i do hope somebody, somewhere listens to what i have to say and does not just regard this as just another *virus* because it's more then that, it's a message, a message for freedom, the freedom to smoke up and have the chose to do so *WITHOUT* fear of punishment from the law and the goverment. Thank you for your time.

Figure 2-4 Annoying virus message
© Cengage Learning 2012

Malware That Spreads (cont’d.)

- Virus cannot automatically spread to another computer
  - Relies on user action to spread
- Viruses are attached to files
- Viruses are spread by transferring infected files

Malware That Spreads (cont’d.)

- Types of computer viruses
  - Program
    - Infects executable files
  - Macro
    - Executes a script
  - Resident
    - Virus infects files opened by user or operating system

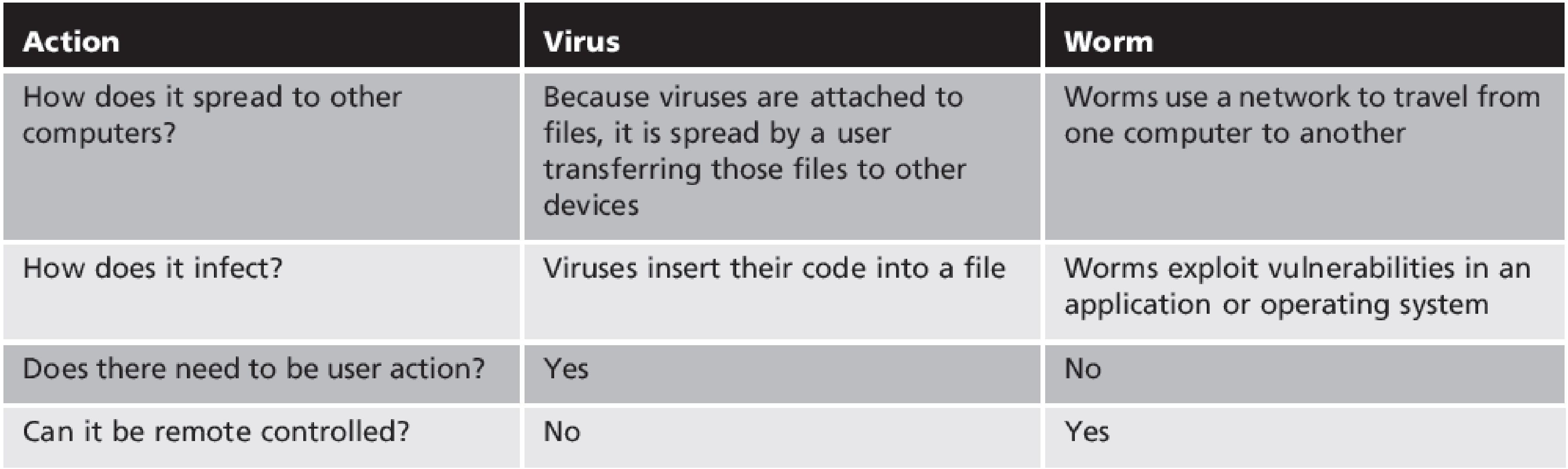
Malware That Spreads (cont'd.)

- Types of computer viruses (cont'd.)
  - Boot virus
    - Infects the Master Boot Record
  - Companion virus
    - Adds malicious copycat program to operating system

Malware That Spreads (cont'd.)

- Worm
  - Malicious program
  - Exploits application or operating system vulnerability
  - Sends copies of itself to other network devices
- Worms may:
  - Consume resources *or*
  - Leave behind a payload to harm infected systems
- Examples of worm actions
  - Deleting computer files
  - Allowing remote control of a computer by an attacker

Malware That Spreads (cont'd.)



Action	Virus	Worm
How does it spread to other computers?	Because viruses are attached to files, it is spread by a user transferring those files to other devices	Worms use a network to travel from one computer to another
How does it infect?	Viruses insert their code into a file	Worms exploit vulnerabilities in an application or operating system
Does there need to be user action?	Yes	No
Can it be remote controlled?	No	Yes

Table 2-1 Difference between viruses and worms

Malware That Conceals

- Trojans
  - Program that does something other than advertised
  - Typically executable programs
    - Contain hidden code that launches an attack
  - Sometimes made to appear as data file
  - Example
    - User downloads “free calendar program”
    - Program scans system for credit card numbers and passwords
    - Transmits information to attacker through network

Malware That Conceals (cont'd.)

- Rootkits
  - Software tools used by an attacker to hide actions or presence of other types of malicious software
  - Hide or remove traces of log-in records, log entries
  - May alter or replace operating system files with modified versions:
    - Specifically designed to ignore malicious activity

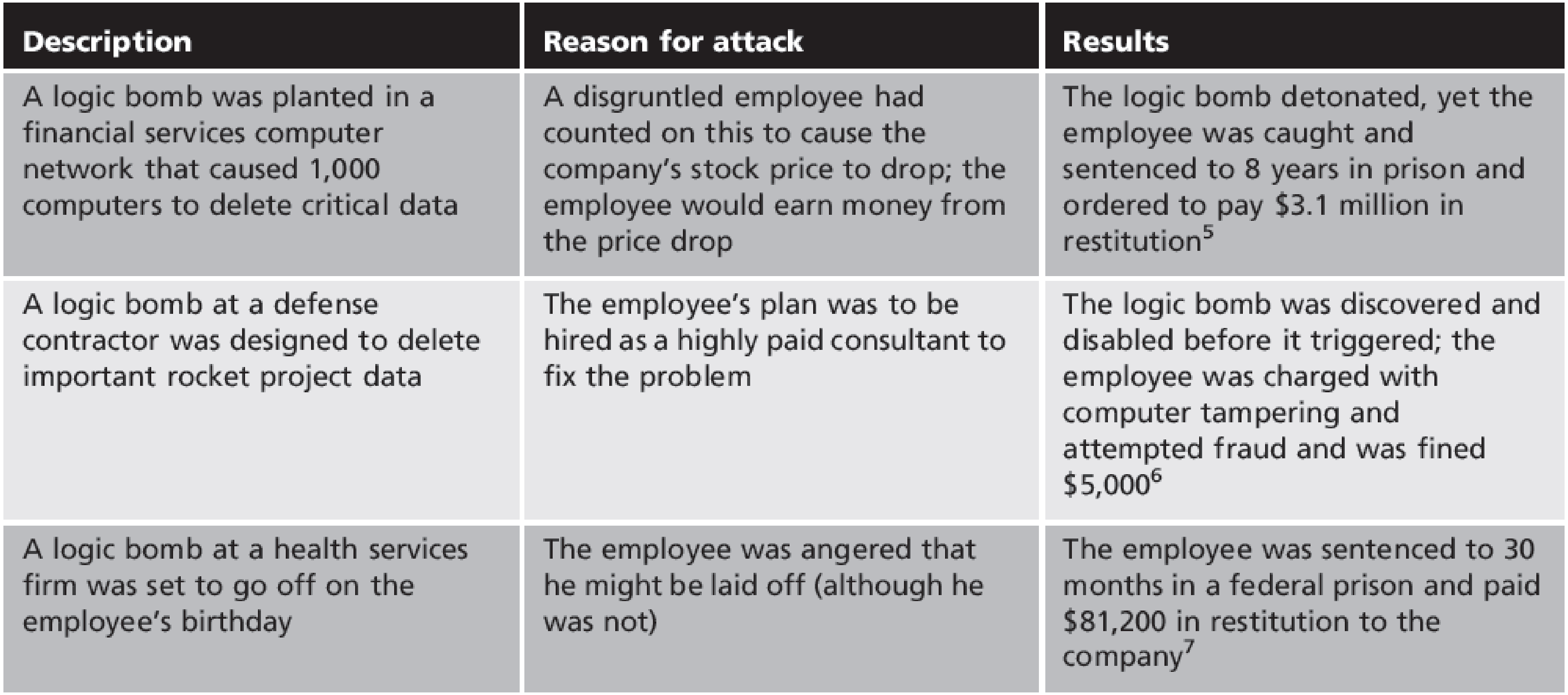
Malware That Conceals (cont'd.)

- Rootkits can be detected using programs that compare file contents with original files
- Rootkits that operate at operating system's lower levels:
  - May be difficult to detect
- Removal of a rootkit can be difficult
  - Rootkit must be erased
  - Original operating system files must be restored
  - Reformat hard drive and reinstall operating system

Malware That Conceals (cont'd.)

- Logic bomb
  - Computer code that lies dormant
    - Triggered by a specific logical event
    - Then performs malicious activities
  - Difficult to detect before it is triggered
- Backdoor
  - Software code that circumvents normal security to give program access
  - Common practice by developers
    - Intent is to remove backdoors in final application

Malware That Conceals (cont'd.)



Description	Reason for attack	Results
A logic bomb was planted in a financial services computer network that caused 1,000 computers to delete critical data	A disgruntled employee had counted on this to cause the company's stock price to drop; the employee would earn money from the price drop	The logic bomb detonated, yet the employee was caught and sentenced to 8 years in prison and ordered to pay $3.1 million in restitution[5]
A logic bomb at a defense contractor was designed to delete important rocket project data	The employee's plan was to be hired as a highly paid consultant to fix the problem	The logic bomb was discovered and disabled before it triggered; the employee was charged with computer tampering and attempted fraud and was fined $5,000[6]
A logic bomb at a health services firm was set to go off on the employee's birthday	The employee was angered that he might be laid off (although he was not)	The employee was sentenced to 30 months in a federal prison and paid $81,200 in restitution to the company[7]

Table 2-2 Famous logic bombs

Malware That Profits

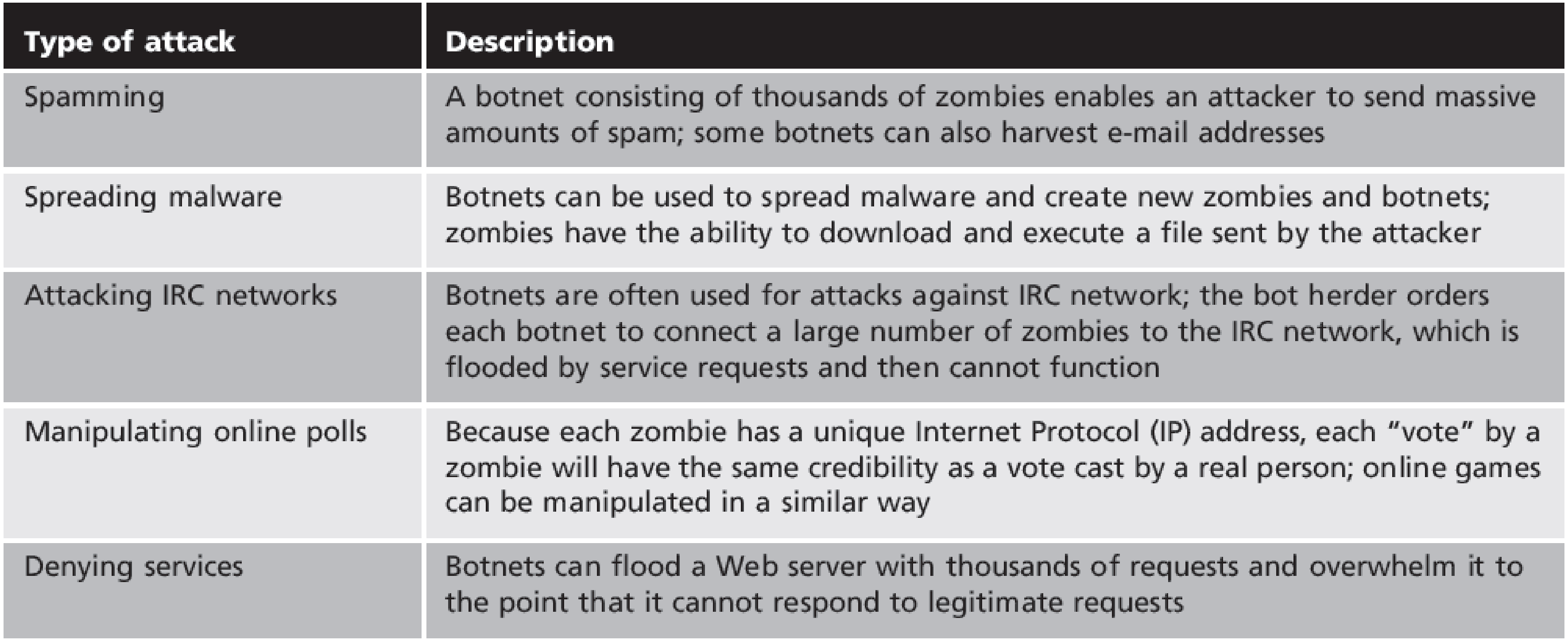
- Types of malware designed to profit attackers
  - Botnets
  - Spyware
  - Adware
  - Keyloggers

Malware That Profits (cont'd.)

- Botnets
  - Computer is infected with program that allows it to be remotely controlled by attacker
    - Often payload of Trojans, worms, and viruses
  - Infected computer called a zombie
  - Groups of zombie computers together called botnet
- Early botnet attackers used Internet Relay Chat to remotely control zombies
  - HTTP is often used today

Malware That Profits (cont'd.)

- Botnets' advantages for attackers
  - Operate in the background:
    - Often with no visible evidence of existence
  - Provide means for concealing actions of attacker
  - Can remain active for years
  - Large percentage of zombies are accessible at a given time
    - Due to growth of always-on Internet services



Type of attack	Description
Spamming	A botnet consisting of thousands of zombies enables an attacker to send massive amounts of spam; some botnets can also harvest e-mail addresses
Spreading malware	Botnets can be used to spread malware and create new zombies and botnets; zombies have the ability to download and execute a file sent by the attacker
Attacking IRC networks	Botnets are often used for attacks against IRC network; the bot herder orders each botnet to connect a large number of zombies to the IRC network, which is flooded by service requests and then cannot function
Manipulating online polls	Because each zombie has a unique Internet Protocol (IP) address, each "vote" by a zombie will have the same credibility as a vote cast by a real person; online games can be manipulated in a similar way
Denying services	Botnets can flood a Web server with thousands of requests and overwhelm it to the point that it cannot respond to legitimate requests

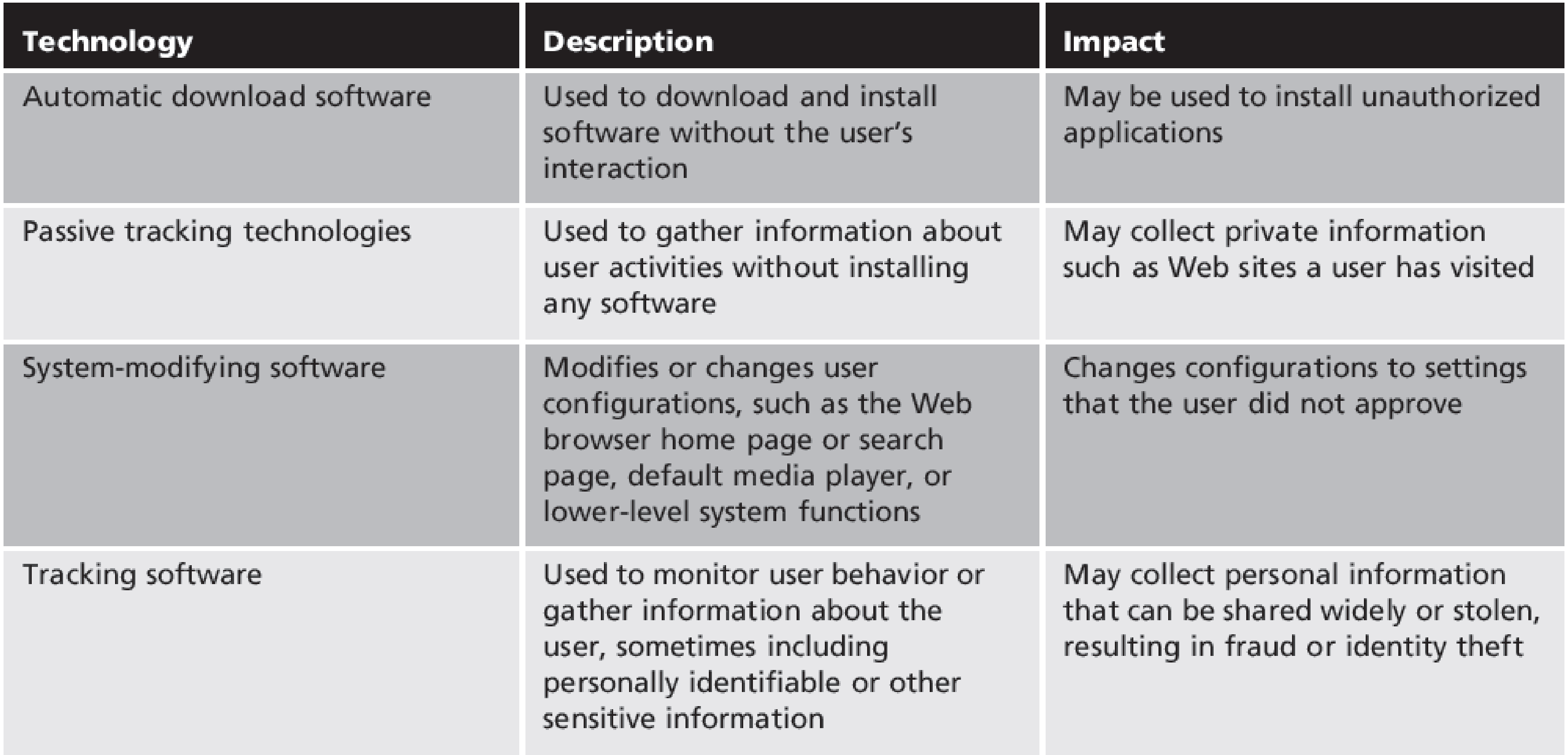
Table 2-3 Uses of botnets

Malware That Profits (cont'd.)

- Spyware
  - Software that gathers information without user consent
  - Usually used for:
    - Advertising
    - Collecting personal information
    - Changing computer configurations

Malware That Profits (cont'd.)

- Spyware's negative effects
  - Slows computer performance
  - Causes system instability
  - May install new browser menus or toolbars
  - May place new shortcuts
  - May hijack home page
  - Causes increased pop-ups



Technology	Description	Impact
Automatic download software	Used to download and install software without the user's interaction	May be used to install unauthorized applications
Passive tracking technologies	Used to gather information about user activities without installing any software	May collect private information such as Web sites a user has visited
System-modifying software	Modifies or changes user configurations, such as the Web browser home page or search page, default media player, or lower-level system functions	Changes configurations to settings that the user did not approve
Tracking software	Used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information	May collect personal information that can be shared widely or stolen, resulting in fraud or identity theft

Table 2-4 Technologies used by spyware

Malware That Profits (cont’d.)

- Adware
  - Program that delivers advertising content:
    - In manner unexpected and unwanted by the user
  - Typically displays advertising banners and pop-up ads
  - May open new browser windows randomly
  - Can also perform tracking of online activities

Malware That Profits (cont'd.)

- Downsides of adware for users
  - May display objectionable content
  - Frequent pop-up ads cause lost productivity
  - Pop-up ads slow computer or cause crashes
  - Unwanted ads can be a nuisance

Malware That Profits (cont’d.)

- Keyloggers
  - Program that captures user’s keystrokes
  - Information later retrieved by attacker
  - Attacker searches for useful information
    - Passwords
    - Credit card numbers
    - Personal information

Malware That Profits (cont'd.)

- Keyloggers (cont'd.)
  - Can be a small hardware device
    - Inserted between computer keyboard and connector
    - Unlikely to be detected
    - Attacker physically removes device to collect information

Malware That Profits (cont'd.)

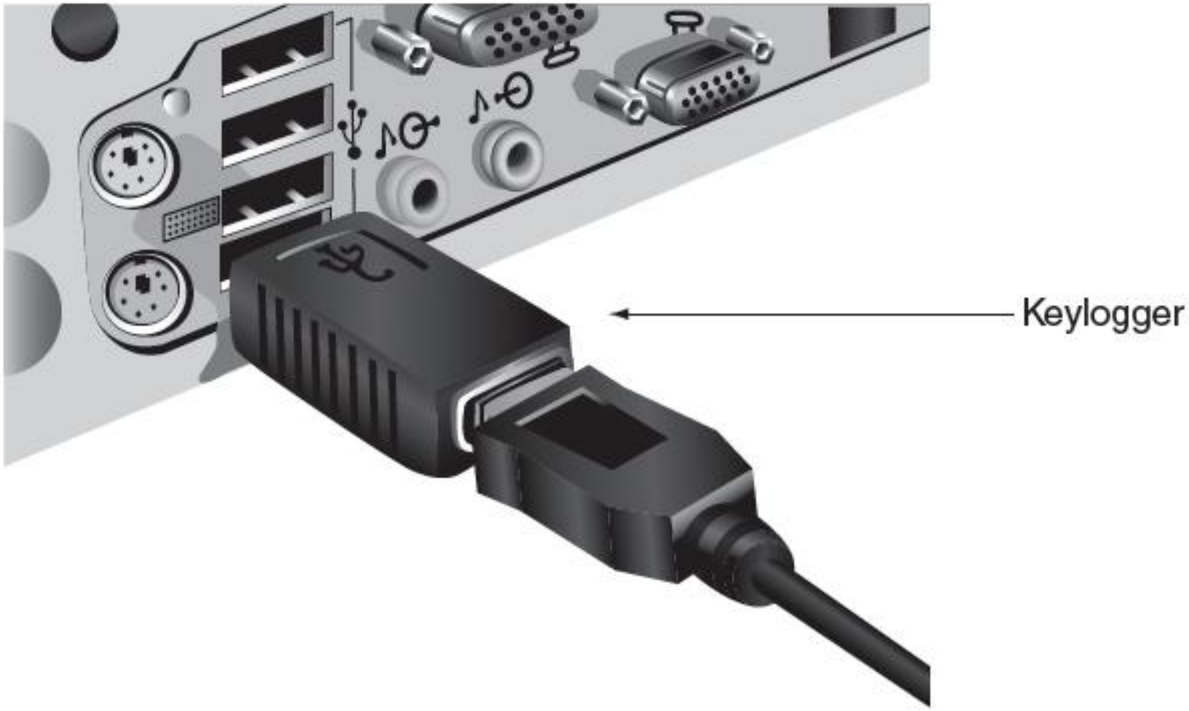
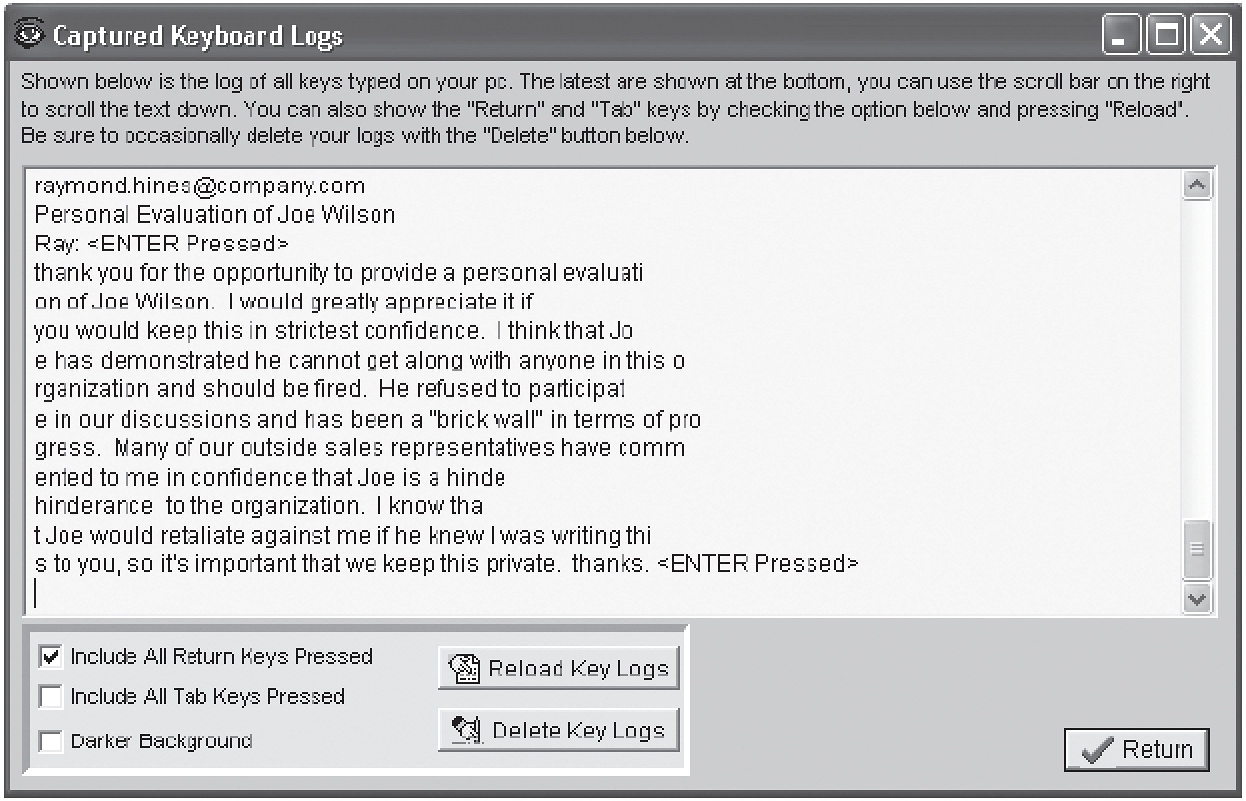


Figure 2-6 Hardware keylogger

r

Malware That Profits (cont'd.)



Shown below is the log of all keys typed on your pc. The latest are shown at the bottom, you can use the scroll bar on the right to scroll the text down. You can also show the "Return" and "Tab" keys by checking the option below and pressing "Reload". Be sure to occasionally delete your logs with the "Delete" button below.

```
raymond.hines@company.com
Personal Evaluation of Joe Wilson
Ray: <ENTER Pressed>
thank you for the opportunity to provide a personal evaluati
on of Joe Wilson.  I would greatly appreciate it if
you would keep this in strictest confidence.  I think that Jo
e has demonstrated he cannot get along with anyone in this o
rganization and should be fired.  He refused to participat
e in our discussions and has been a "brick wall" in terms of pro
gress.  Many of our outside sales representatives have comm
ented to me in confidence that Joe is a hinde
hinderance  to the organization.  I know tha
t Joe would retaliate against me if he knew I was writing thi
s to you, so it's important that we keep this private.  thanks. <ENTER Pressed>
```

☑ Include All Return Keys Pressed

□ Include All Tab Keys Pressed

□ Darker Background

Figure 2-7 Information captured by a software keylogger

© Cengage Learning 2012

Social Engineering Attacks

- Directly gathering information from individuals
  - Relies on trusting nature of individuals
- Psychological approaches
  - Goal: persuade the victim to provide information or take action
  - Flattery or flirtation
  - Conformity
  - Friendliness

Social Engineering Attacks (cont’d.)

- Attacker will ask for only small amounts of information
  - Often from several different victims
- Request needs to be believable
- Attacker “pushes the envelope” to get information:
  - Before victim suspects anything
- Attacker may smile and ask for help

Social Engineering Attacks

- True example of social engineering attack
  - One attacker called human resources office
    - Asked for and got names of key employees
  - Small group of attackers approached door to building
    - Pretended to have lost key code
    - Let in by friendly employee
    - Entered another secured area in the same way
  - Group had learned CFO was out of town
    - Because of his voicemail greeting message

Social Engineering Attacks

- True example of social engineering attack (cont'd.)
  - Group entered CFO's office
  - Gathered information from unprotected computer
  - Dug through trash to retrieve useful documents
  - One member called help desk from CFO's office
    - Pretended to be CFO
    - Asked for password urgently
    - Help desk gave password
  - Group left building with complete network access

Social Engineering Attacks (cont'd.)

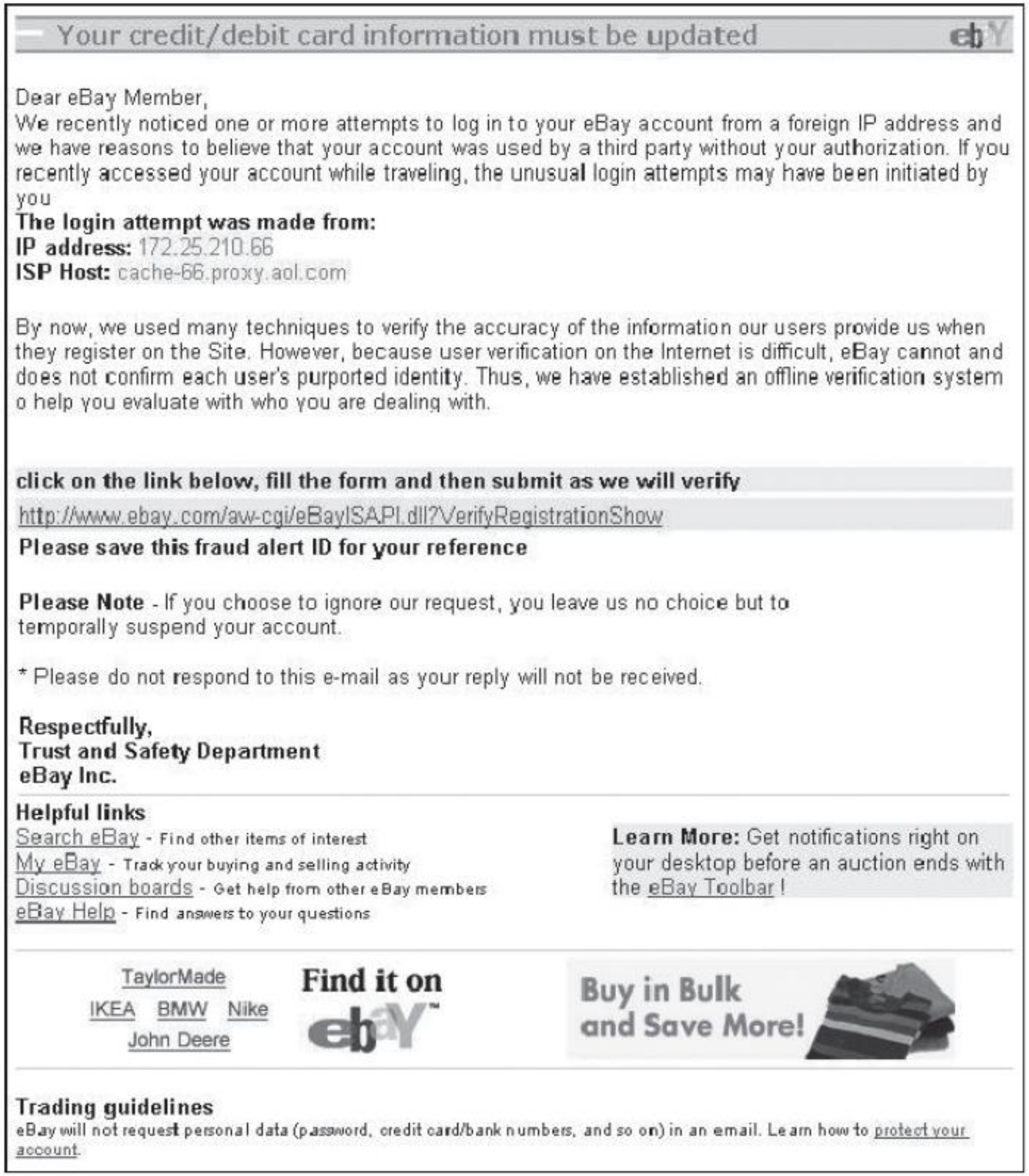
- Impersonation
  - Attacker pretends to be someone else
    - Help desk support technician
    - Repairperson
    - Trusted third party
    - Individuals in roles of authority

Social Engineering Attacks (cont'd.)

- Phishing
  - Sending an email claiming to be from legitimate source
    - May contain legitimate logos and wording
  - Tries to trick user into giving private information
- Variations of phishing
  - Pharming
    - Automatically redirects user to fraudulent Web site

Social Engineering Attacks (cont'd.)

- Variations of phishing (cont'd.)
  - Spear phishing
    - Email messages target specific users
  - Whaling
    - Going after the "big fish"
    - Targeting wealthy individuals
  - Vishing (voice phishing)
    - Attacker calls victim with recorded "bank" message with callback number
    - Victim calls attacker's number and enters private information



Your credit/debit card information must be updated

Dear eBay Member,
We recently noticed one or more attempts to log in to your eBay account from a foreign IP address and we have reasons to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you

The login attempt was made from:
IP address: 172.25.210.66
ISP Host: cache-66.proxy.aol.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site. However, because user verification on the Internet is difficult, eBay cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system o help you evaluate with who you are dealing with.

click on the link below, fill the form and then submit as we will verify

http://www.ebay.com/aw-cgi/eBayISAPI.dll?VerifyRegistrationShow

Please save this fraud alert ID for your reference

Please Note - If you choose to ignore our request, you leave us no choice but to temporally suspend your account.

* Please do not respond to this e-mail as your reply will not be received.

Respectfully,
Trust and Safety Department
eBay Inc.

Helpful links
Search eBay - Find other items of interest
My eBay - Track your buying and selling activity
Discussion boards - Get help from other eBay members
eBay Help - Find answers to your questions

Learn More: Get notifications right on your desktop before an auction ends with the eBay Toolbar !

Trading guidelines
eBay will not request personal data (password, credit card/bank numbers, and so on) in an email. Learn how to protect your account.

Figure 2-8 Phishing message

© Cengage Learning 2012

Social Engineering Attacks (cont'd.)

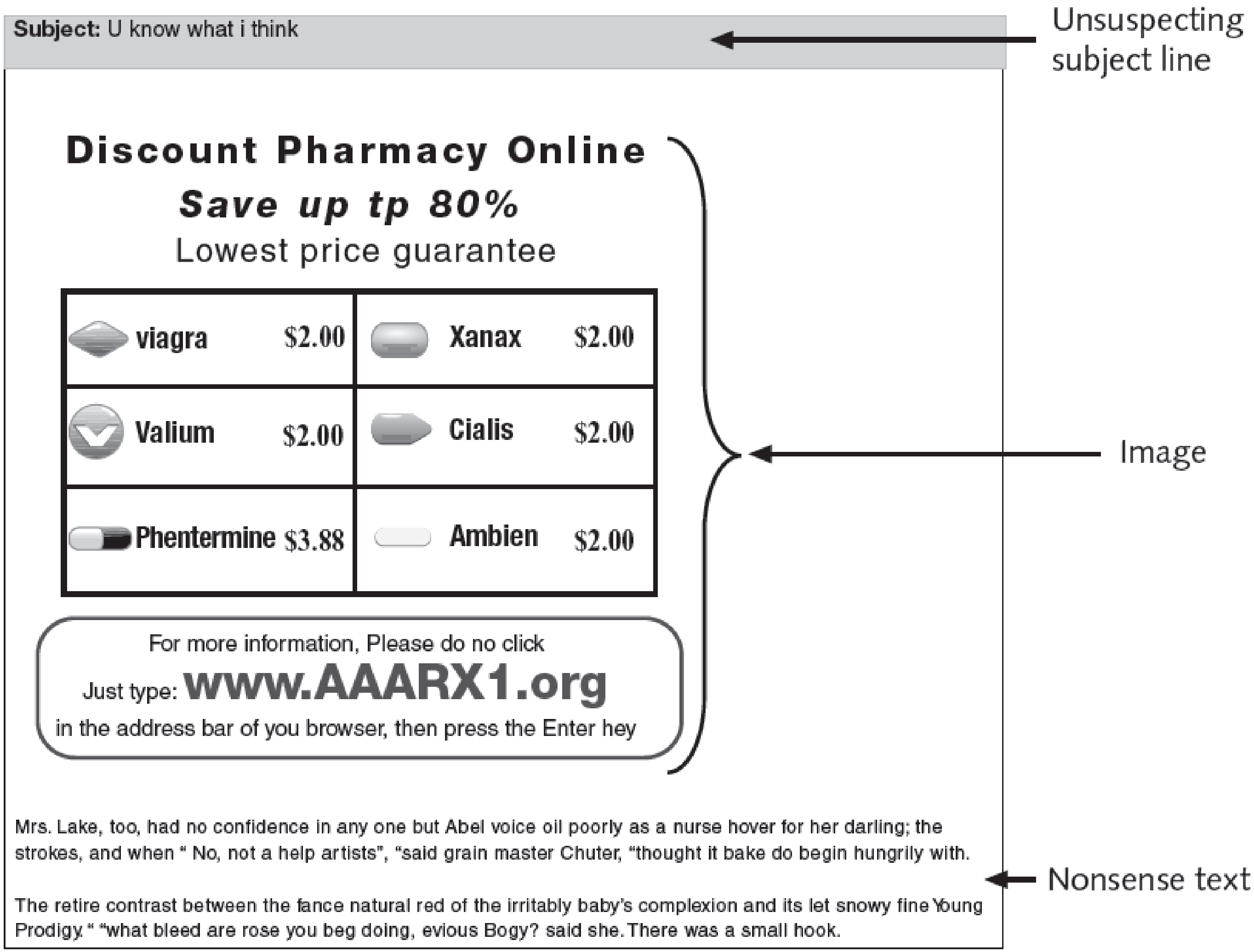
- Ways to recognize phishing messages
  - Deceptive Web links
    - @ sign in middle of address
  - Variations of legitimate addresses
  - Presence of vendor logos that look legitimate
  - Fake sender's address
  - Urgent request

Social Engineering Attacks (cont'd.)

- Spam
  - Unsolicited e-mail
  - Primary vehicles for distribution of malware
  - Sending spam is a lucrative business
- Spim: targets instant messaging users
- Image spam
  - Uses graphical images of text
  - Circumvents text-based filters
  - Often contains nonsense text

Social Engineering Attacks (cont'd.)

- Spammer techniques
  - GIF layering
    - Image spam divided into multiple images
    - Layers make up one complete legible message
  - Word splitting
    - Horizontally separating words
    - Can still be read by human eye
  - Geometric variance
    - Uses speckling and different colors so no two emails appear to be the same



Subject: U know what i think

Discount Pharmacy Online

Save up tp 80%

Lowest price guarantee

viagra	$2.00	Xanax	$2.00
Valium	$2.00	Cialis	$2.00
Phentermine	$3.88	Ambien	$2.00

For more information, Please do no click

Just type: **www.AAARX1.org**

in the address bar of you browser, then press the Enter hey

Mrs. Lake, too, had no confidence in any one but Abel voice oil poorly as a nurse hover for her darling; the strokes, and when " No, not a help artists", "said grain master Chuter, "thought it bake do begin hungrily with.

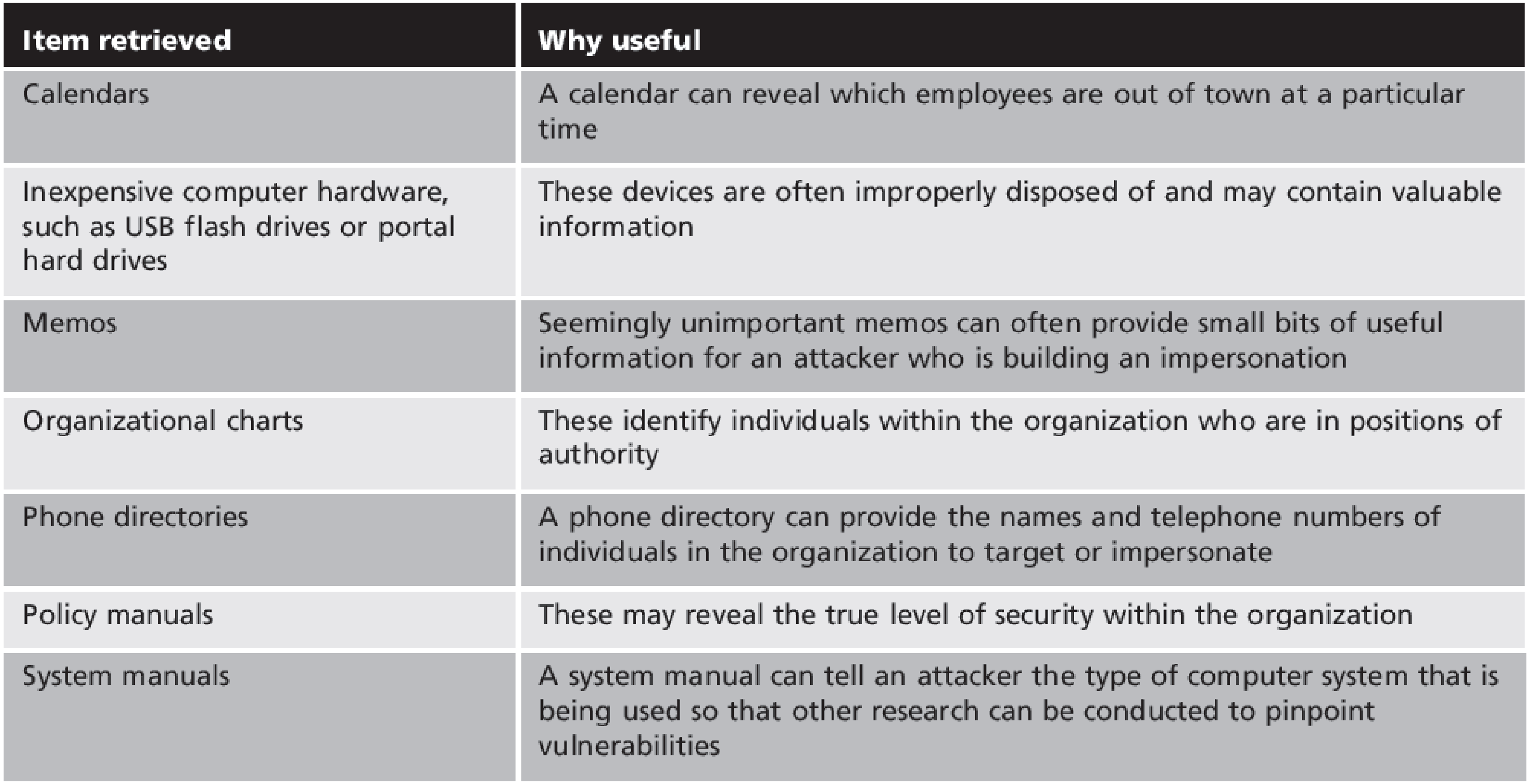
The retire contrast between the fance natural red of the irritably baby's complexion and its let snowy fine Young Prodigy. " "what bleed are rose you beg doing, evious Bogy? said she. There was a small hook.

Figure 2-10 Image spam

© Cengage Learning 2012

Social Engineering Attacks (cont'd.)

- Hoaxes
  - False warning or claim
  - May be first step in an attack
- Physical procedures
  - Dumpster diving
    - Digging through trash to find useful information
  - Tailgating
    - Following behind an authorized individual through an access door



Item retrieved	Why useful
Calendars	A calendar can reveal which employees are out of town at a particular time
Inexpensive computer hardware, such as USB flash drives or portal hard drives	These devices are often improperly disposed of and may contain valuable information
Memos	Seemingly unimportant memos can often provide small bits of useful information for an attacker who is building an impersonation
Organizational charts	These identify individuals within the organization who are in positions of authority
Phone directories	A phone directory can provide the names and telephone numbers of individuals in the organization to target or impersonate
Policy manuals	These may reveal the true level of security within the organization
System manuals	A system manual can tell an attacker the type of computer system that is being used so that other research can be conducted to pinpoint vulnerabilities

Table 2-5 Dumpster diving items and their usefulness

Social Engineering Attacks (cont'd.)

- Methods of tailgating
  - Tailgater calls "please hold the door"
  - Waits outside door and enters when authorized employee leaves
  - Employee conspires with unauthorized person to walk together through open door
- Shoulder surfing
  - Casually observing user entering keypad code

Summary

- Malware is software that enters a computer system without the owner’s knowledge or consent
- Malware that spreads include computer viruses and worms
- Malware that conceals include Trojans, rootkits, logic bombs, and backdoors
- Malware with a profit motive includes botnets, spyware, adware, and keyloggers

Summary (cont'd.)

- Social engineering is a means of gathering information for an attack from individuals
- Types of social engineering approaches include phishing, impersonation, dumpster diving, and tailgating