

15th Edition

Understanding Computers

Today and Tomorrow

Comprehensive

Chapter 9: Network and Internet Security



Deborah Morley
Charles S. Parker

Copyright 2015 Cengage Learning



Learning Objectives

1. Explain why computer users should be concerned about network and Internet security.
2. List several examples of unauthorized access and unauthorized use.
3. Explain several ways to protect against unauthorized access and unauthorized use, including access control systems, firewalls, and encryption.
4. Provide several examples of computer sabotage.
5. List how individuals and businesses can protect against computer sabotage.



Learning Objectives

6. Discuss online theft, identity theft, spoofing, phishing, and other types of dot cons.
7. Detail steps an individual can take to protect against online theft, identity theft, spoofing, phishing, and other types of dot cons.
8. Identify personal safety risks associated with Internet use.
9. List steps individuals can take to safeguard their personal safety when using the Internet.
10. Discuss the current state of network and Internet security legislation.



Overview

- This chapter covers:
 - Security concerns stemming from the use of computer networks and the Internet in our society
 - Safeguards and precautions that can be taken to reduce the risk of problems related to these security concerns
 - Personal safety issues related to the Internet
 - Legislation related to network and Internet security



Why Be Concerned About Network and Internet Security?

- Computer Crime (cybercrime)
 - Any illegal act involving a computer, including:
 - Theft of financial assets
 - Manipulating data for personal advantage
 - Act of sabotage (releasing a computer virus, shutting down a Web server)
 - Phishing and Internet scams
- All computer users should be aware of security concerns and the precautions that can be taken



Unauthorized Access and Unauthorized Use

- Unauthorized Access
 - Gaining access to a computer, network, file, or other resource without permission
- Unauthorized Use
 - Using a computer resource for unapproved activities
- Both can be committed by insiders and outsiders
- Codes of Conduct
 - Used to specify rules for behavior, typically by a business or school

Unauthorized Access and Unauthorized Use

- Hacking
 - Using a computer to break into another computer system
 - A serious threat for individuals, businesses, and the country (national security), i.e., cyberterrorism
 - Often performed via wireless networks today
 - Many wireless networks are left unsecured
- War Driving
 - Driving around an area to find a Wi-Fi network to access and use without authorization

FIGURE 9-2

Wi-Fi finders. Online mapping services and smartphone apps can show you the available Wi-Fi hotspots for a particular geographic area.



Courtesy of iWiire



Unauthorized Access and Unauthorized Use

- Wi-Fi Piggybacking
 - Accessing an unsecured Wi-Fi network from the hacker's current location without authorization
- Interception of Communications
 - Unsecured messages, files, logon information, etc., can be intercepted using software designed for that purpose
 - New trend: intercept credit and debit card information during the card verification process
 - Pocketsniffing software



Protecting Against Unauthorized Access and Unauthorized Use

- Access Control Systems
 - Used to control access to facilities, computer networks, company databases, and Web site accounts
 - Identification Systems
 - Verify that the person trying to access the facility or system is an authorized user
 - Authentication Systems
 - Determine if the person is who he or she claims to be



Protecting Against Unauthorized Access and Unauthorized Use

- Possessed Knowledge Access Systems
 - Use information that only the authorized user should know
 - Typically passwords
 - Passwords should be strong and changed frequently
 - Typically used in conjunction with usernames
 - Disadvantages
 - Passwords can be forgotten
 - If known, password can be used by someone who is not an authorized user



Protecting Against Unauthorized Access and Unauthorized Use

PASSWORD STRATEGIES

Make the password at least eight characters and include both uppercase and lowercase letters, as well as numbers and special symbols.

Choose passwords that are not in a dictionary—for instance, mix numbers and special characters with abbreviations or unusual words you will remember but that do not conform to a pattern a computer can readily figure out.

Do not use your name, your kids' or pets' names, your address, your birthdate, or any other public information as your password.

Determine a *passphrase* that you can remember and use corresponding letters and symbols (such as the first letter of each word) for your password. For instance, the passphrase "My son John is five years older than my daughter Abby" could be used to remember the corresponding strong password "Msji5yotMd@".

Develop a system using a basic password for all Web sites plus site-specific information (such as the first two letters of the site and a number you will remember) to create a different password for each site, but still ones you can easily remember. For instance, you can combine your dog's name with the site initials followed by a number that is significant to you to form a password such as "RoverAM27" for Amazon.com.

Do not keep a written copy of the password in your desk or taped to your monitor. If you need to write down your password, create a password-protected file on your computer that contains all your passwords or use a password manager program.

Use a different password for your highly sensitive activities (such as online banking or stock trading) than for other Web sites. If a hacker determines your password on a low-security site (which is easier to break into), he or she can use it on an account containing sensitive data if you use the same password on both accounts.

Change your passwords frequently—at least every 6 months.

FIGURE 9-4

Strategies for creating strong passwords.



Protecting Against Unauthorized Access and Unauthorized Use

- Cognitive Authentication Systems
 - Use information the individual knows or can easily remember (birthplace, pet names, etc.)
 - Used in many password recovery systems
- Two-Factor Authentication
 - Using two different methods to authenticate users
 - Typically possessed knowledge (password) with either
 - Biometric Feature – something you are
 - Possessed Object – something you have
 - Hard token – physical object used
 - Soft token – supplies a one-time password (OTP)

Protecting Against Unauthorized Access and Unauthorized Use



FIGURE 9-5

Facebook two-factor authentication. The first time you log on with a new device, you must supply the OTP sent to your mobile phone in addition to your conventional username/password combination.

Protecting Against Unauthorized Access and Unauthorized Use

- Possessed Object Access Systems
 - Use a physical object an individual has in his/her possession to identify that individual
 - Smart cards, magnetic cards
 - RFID-encoded badges, USB security keys or tokens



PHYSICAL ACCESS

The object (in this case a mobile phone containing an appropriate microSD card) is read by a reader to provide access to a facility.



LOGICAL ACCESS

The object (in this case a smart card employee badge) is read by a reader (this reader is integrated into the computer) to provide access to that computer system.

FIGURE 9-6

Possessed objects.
Can grant access to both facilities and computer resources (including computers, networks, and Web sites).



Protecting Against Unauthorized Access and Unauthorized Use

- Disadvantages
 - Can be lost or used by an unauthorized individual
- Biometric Access Systems
 - Identifies users by a particular unique biological characteristic
 - Fingerprint, hand, face, iris, voice, etc.
 - Data read by biometric reader must match what is stored in a database



Protecting Against Unauthorized Access and Unauthorized Use

- Often used to:
 - Control access to secure facilities
 - Log on to computers, punch in/out at work, law enforcement, etc.
- Advantages
 - Biometric access systems are very accurate
 - Cannot be lost or forgotten
- Disadvantages
 - Cannot be reset if compromised
 - Hardware and software are expensive

Protecting Against Unauthorized Access and Unauthorized Use



FINGERPRINT READERS

Typically used to protect access to work facilities or computers, to log on to secure Web sites, for law enforcement identification, and to pay for products or services.

VEIN READERS

Beginning to replace hand geometry readers to control access to facilities (such as government offices, prisons, and military facilities) and to punch in and out of work.

FIGURE 9-7

Types of biometric access and identification systems.



FACE RECOGNITION SYSTEMS

Typically used to control access to highly secure areas, to identify individuals for law enforcement purposes, and to log on to devices or apps, as shown here.

IRIS RECOGNITION SYSTEMS

Typically used to control access to highly secure areas and by the military, such as to identify Afghan patients as shown here.



Protecting Against Unauthorized Access and Unauthorized Use

- Controlling Access to Wireless Networks
 - In general, Wi-Fi is less secure than wired networks
 - Security is usually off by default; wireless networks should be secured
 - Wireless network owners should:
 - Change the router's default password
 - Enable encryption (WPA2 is more secure than WPA)
 - Enable other security features as needed
 - Can hide network name (SSID)

Protecting Against Unauthorized Access and Unauthorized Use



FIGURE 9-8
Accessing a Wi-Fi network. To access a secure network, the appropriate passphrase must be supplied.

How It Works Box

Securing a Wireless Home Router

- Use router's configuration screen
- Be sure to change the access password
- Enter the SSID name, select the security mode, and type a secure passphrase
- Can use MAC filtering

Use the router's IP address to display the router's configuration screen.

Use this tab to enable MAC address filtering.

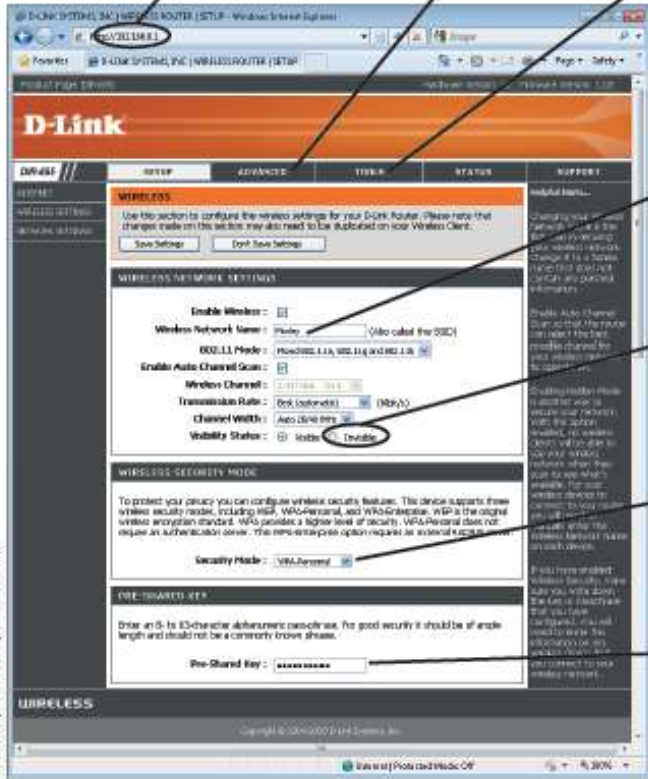
Use this tab to change the administrator password used to access this configuration screen.

Type your desired SSID here.

Disable SSID broadcast here.

Select the desired security mode here.

Type your desired network key here.



The screenshot shows the D-Link router's configuration page in a web browser. The browser address bar shows the IP address 192.168.1.1. The page has a navigation menu with tabs: BASIC, WIRELESS, ADVANCED, TOOL, and STATUS. The WIRELESS tab is selected. The page contains several sections: WIRELESS NETWORK SETTINGS, WIRELESS SECURITY MODE, and WIRELESS SETUP. Annotations with arrows point to various fields: the IP address in the browser bar, the WIRELESS tab, the 'Enable Wireless' checkbox, the 'Wireless Network Name' field (containing 'Pinky'), the 'Broadcast SSID' checkbox (unchecked), the 'Security Mode' dropdown (set to 'WPA Personal'), and the 'Pre-Shared Key' field (containing '1234567890').

Courtesy D-Link Systems, Inc.

Configuring a home router.



Protecting Against Unauthorized Access and Unauthorized Use

- Firewalls
 - A collection of hardware and/or software intended to protect a computer or computer network from unauthorized access
 - Typically two-way, so they check all incoming (from the Internet) and outgoing (to the Internet) traffic
 - Important for home computers that have a direct Internet connection, as well as for businesses
 - Work by closing down external communications ports

Protecting Against Unauthorized Access and Unauthorized Use

FIGURE 9-9
A personal firewall.





Protecting Against Unauthorized Access and Unauthorized Use

- Intrusion Prevention System (IPS) Software
 - Monitors traffic to try and detect possible attacks
 - If an attack is discovered, IPS software can immediately block it
- Encryption
 - Method of scrambling contents of e-mail or files to make them unreadable if intercepted
 - Secure Web pages use encryption
 - SSL and EV SSL



Protecting Against Unauthorized Access and Unauthorized Use

- Private Key Encryption (symmetric key encryption)
 - Uses a single key
 - Most often used to encrypt files on a computer
 - If used to send files to others, the recipient and sender must agree on the private key to be used
- Public Key Encryption (asymmetric key encryption)
 - Uses two keys (a private key and a public key) to encrypt and decrypt documents
 - Public key can be given to anyone
 - Key pairs are obtained through a Certificate Authority

Protecting Against Unauthorized Access and Unauthorized Use

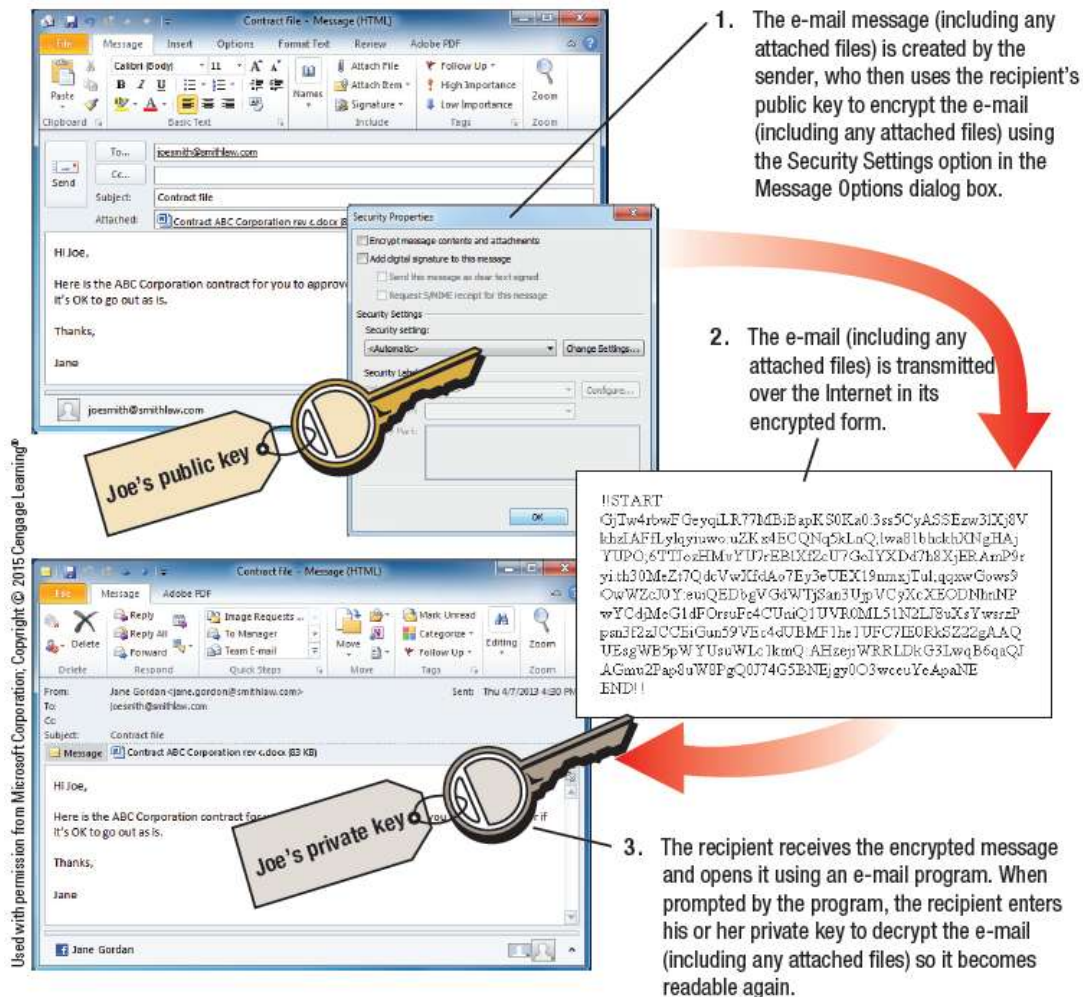


FIGURE 9-11

Using public key encryption to secure an e-mail message.



Protecting Against Unauthorized Access and Unauthorized Use

- Web-based encrypted e-mail (HushMail) is available
- Various strengths of encryption available
 - Stronger is more difficult to crack
 - Strong = 128-bit (16-character keys)
 - Military = 2,048-bit (256-character keys)



Protecting Against Unauthorized Access and Unauthorized Use

- Virtual Private Networks (VPNs)
 - A private secure path over the Internet
 - Allows authorized users to securely access a private network via the Internet
 - Much less expensive than a private secure network
 - Can provide a secure environment over a large geographical area
 - Typically used by businesses to remotely access corporate networks via the Internet
 - Personal VPNs can be used by individuals to surf safely at a wireless hotspot



Protecting Against Unauthorized Access and Unauthorized Use

- Additional Public Hotspot Precautions
 - Individuals should take additional precautions when using public hotspots in addition to using security software, secure Web pages, VPNs, and file encryption

PUBLIC HOTSPOT PRECAUTIONS

Turn off automatic connections and pay attention to the list of available hotspots to make sure you connect to a legitimate access point (not an evil twin).

Use a personal firewall to control the traffic going to and coming from your device and temporarily use it to block all incoming connections.

Use a virtual private network (VPN) to secure all activity between your device and the Internet.

Only enter passwords, credit card numbers, and other data on secure Web pages using a VPN.

If you're not using a VPN, encrypt all sensitive files before transferring or e-mailing them.

If you're not using a VPN, avoid online shopping, banking, and other sensitive transactions.

Turn off file sharing so others can't access the files on your hard drive.

Turn off Bluetooth and Wi-Fi when you are not using them.

Disable *ad hoc* capabilities to prevent another device from connecting to your device directly without using an access point.

Use antivirus software and make sure your operating system and browser are up to date.

FIGURE 9-12

Sensible precautions for public Wi-Fi hotspot users.



Protecting Against Unauthorized Access and Unauthorized Use

- Sensible Employee Precautions
 - Screen potential new hires carefully
 - Watch for disgruntled employees and ex-employees
 - Ask business partners to review their security
 - Develop policies and controls
 - Use software to manage devices and prevent data leaks
 - Data leakage prevention systems
 - Outbound-content monitoring systems
 - Mobile device management (MDM) - BYOD

Protecting Against Unauthorized Access and Unauthorized Use

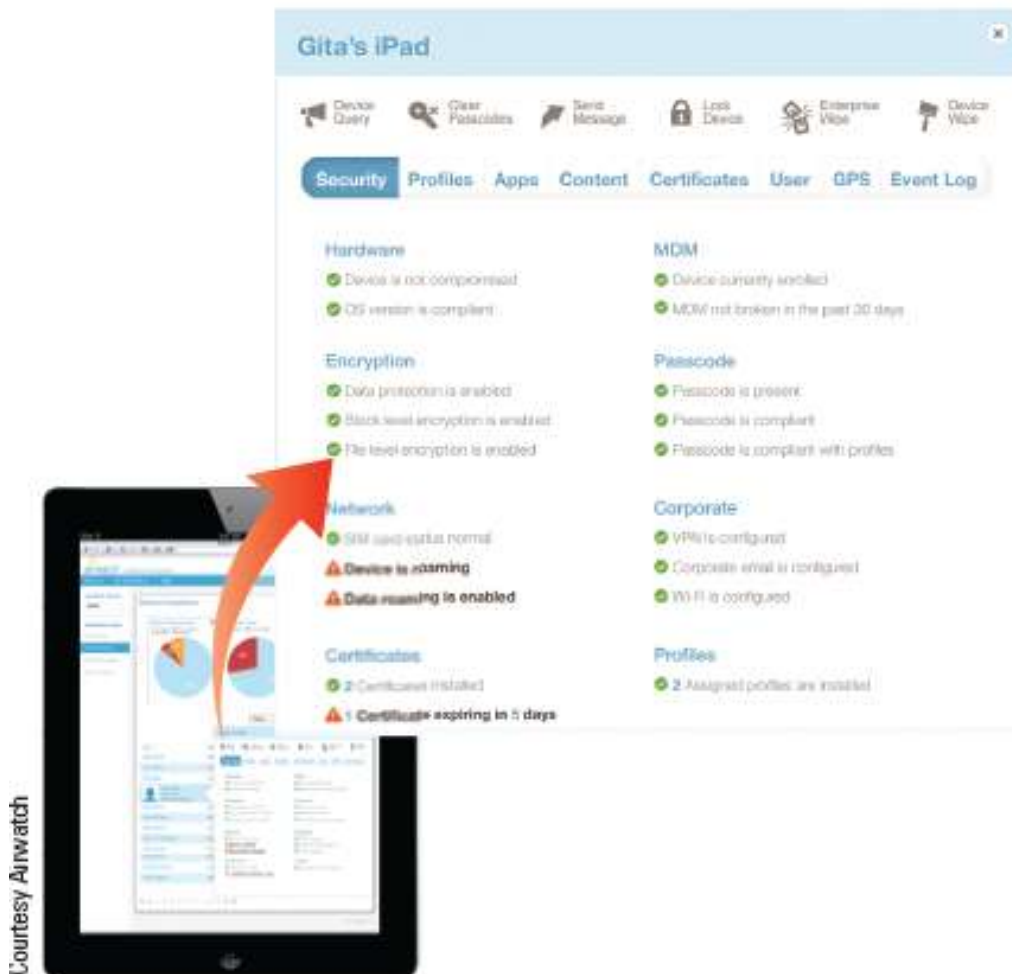


FIGURE 9-13
Mobile device management (MDM) software. Secures and manages the mobile devices used in an organization.



Inside the Industry Box

Securing BYOD

- BYOD = Bring Your Own Device
- Some businesses use BYOD as a cost-saving measure
- Individuals want to carry their devices with them and use for both work and personal use
- Security is a disadvantage
 - Businesses need to ensure company networks and data are not adversely affected
 - MDM software can help
 - Containerization can separate work and personal data and apps





Quick Quiz

1. Which of the following is an example of possessed knowledge?
 - a. Password
 - b. Smart card
 - c. Fingerprint
2. True or False: With public key encryption, a single key is used to both encrypt and decrypt the file.
3. A(n) _____ controls access to a computer from the Internet and protects programs installed on a computer from accessing the Internet without authorization from the user.

Answers:

1) a; 2) False; 3) firewall



Computer Sabotage

- Computer Sabotage
 - Acts of malicious destruction to a computer or computer resource
 - Launching a computer virus
 - Denial of Service (DoS) attack
- Botnet
 - A group of bots (computers controlled by a hacker) that are controlled by one individual and work together in a coordinated fashion
 - Used by botherders (criminals) to send spam, launch Internet attacks, and spread malware



Computer Sabotage

- Malware
 - Any type of malicious software
 - Written to perform destructive acts (damaging programs, deleting files, erasing drives, etc.)
 - Logic bomb
 - Time bomb
 - Writing malware is considered unethical; distributing is illegal



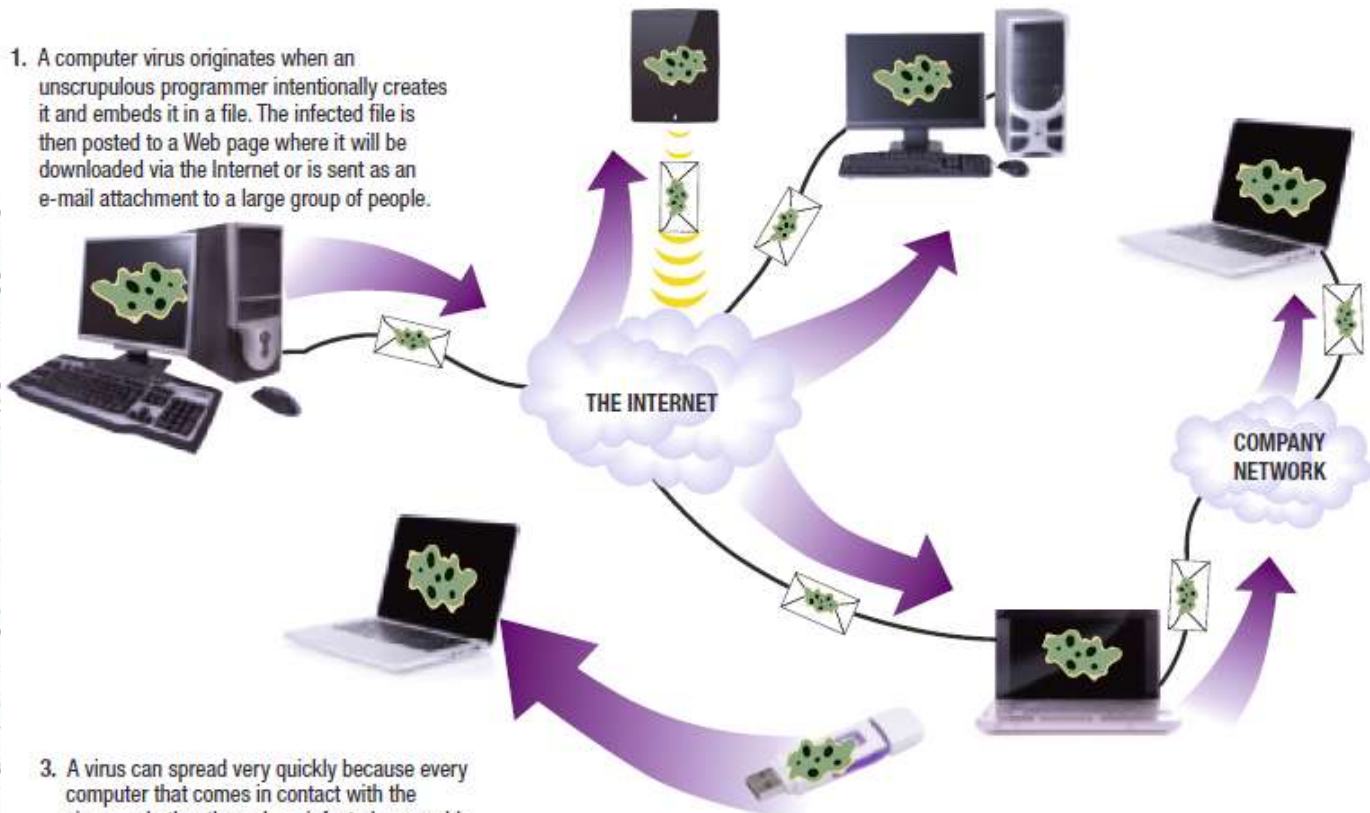
Computer Sabotage

- Computer Viruses
 - A software program installed without the user's knowledge and designed to alter the way a computer operates or to cause harm to the computer system
 - Often embedded in downloaded programs and e-mail messages (games, videos, music files)
- Computer Worm
 - Malicious program designed to spread rapidly by sending copies of itself to other computers via a network
 - Typically sent as an e-mail attachment

Computer Sabotage

1. A computer virus originates when an unscrupulous programmer intentionally creates it and embeds it in a file. The infected file is then posted to a Web page where it will be downloaded via the Internet or is sent as an e-mail attachment to a large group of people.

© 300dpi/Shutterstock.com; © Mr. Aesthetis/Shutterstock.com; © K. MF/Shutterstock.com; © FIMM/Shutterstock.com; Courtesy Kingston Technology Company, Inc.; © Evgeny Karandev/Shutterstock.com; Copyright © 2015 Cengage Learning®



3. A virus can spread very quickly because every computer that comes in contact with the virus—whether through an infected removable storage medium, infected downloaded file, or infected e-mail attachment—becomes infected, unless virus-protection software is used to prevent it.

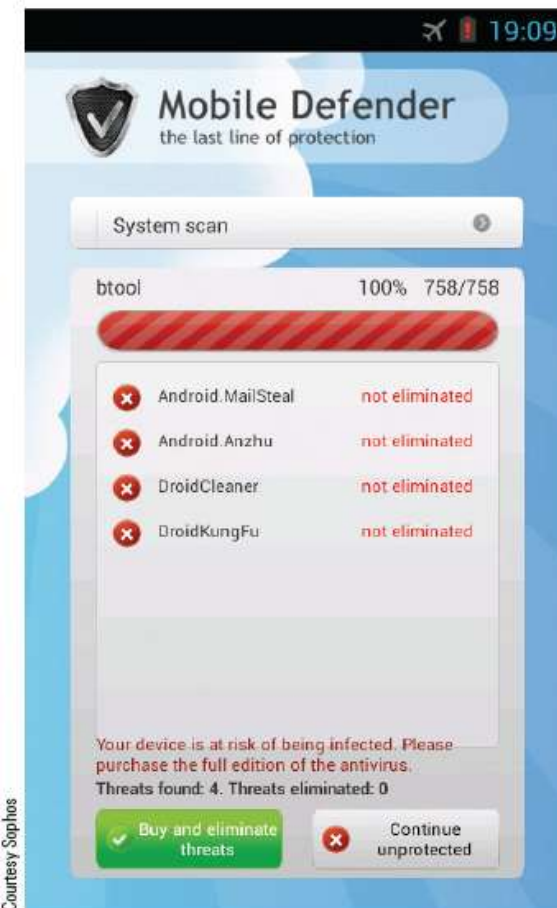
2. When the infected file is opened on a computer, the virus copies itself to that computer's hard drive and the computer becomes infected. The virus may then e-mail itself to people in the newly infected computer's e-mail address book or copy itself to any removable storage medium inserted into that computer.

FIGURE 9-14
How a computer virus or other type of malicious software might spread.

Computer Sabotage

- Trojan Horse
 - Malicious program that masquerades as something else
 - Usually appears to be a game or utility program
 - Cannot replicate themselves; must be downloaded and installed
 - Rogue antivirus programs (scareware) are common today
 - Ransomware

FIGURE 9-15
Rogue anti-malware apps. These programs try to trick victims into purchasing subscriptions to remove nonexistent malware supposedly installed on their devices.





Computer Sabotage

- Mobile Malware
 - Can infect smartphones, media tablets, printers, etc.
 - Smartphones with Bluetooth are particularly vulnerable to attack
 - Mobile threats are expected to continue to increase
- Denial of Service (DoS) Attacks
 - Act of sabotage that attempts to flood a network server or Web server with so much activity that it is unable to function
 - Distributed DoS Attacks target popular Web sites and use multiple computers

Computer Sabotage

1. Hacker's computer sends several simultaneous requests; each request asks to establish a connection to the server but supplies false return information. In a distributed DoS attack, multiple computers send multiple requests at one time.

Hello? I'd like some info...

2. The server tries to respond to each request but can't locate the computer because false return information was provided. The server waits for a short period of time before closing the connection, which ties up the server and keeps others from connecting.

I can't find you, I'll wait and try again...

3. The hacker's computer continues to send new requests so, as a connection is closed by the server, a new request is waiting. This cycle continues, which ties up the server indefinitely.

Hello? I'd like some info...

Hello? I'd like some info...

I'm busy, I can't help you right now.

LEGITIMATE COMPUTER

4. The server becomes so overwhelmed that legitimate requests cannot get through and, eventually, the server usually crashes.

WEB SERVER

FIGURE 9-16

How a denial of service (DoS) attack might work.

© tamiz/Shutterstock.com



HACKER'S COMPUTER

© K. Miry/Shutterstock.com



© tamiz/Shutterstock.com





Computer Sabotage

- Data, Program, or Web Site Alteration
 - Sabotage occurs when a hacker breaches a computer system in order to delete/change data or modify programs
 - Student changing grades
 - Employee performing vengeful acts, such as deleting or changing corporate data
 - Data on Web sites can also be altered
 - Hacking into and changing social networking account contents (Facebook pages, Twitter tweets, etc.)
 - Altering legitimate site to perform malware attacks



Protecting Against Computer Sabotage

- Security Software
 - Typically a suite of programs used to protect your computer against a variety of threats
 - Antivirus Software
 - Used to detect and eliminate computer viruses and other types of malware
 - Should be set up to run continuously to check incoming e-mail messages, instant messages, Web page content, and downloaded files
 - Quarantines any suspicious content as it arrives
 - Should be set to perform regular system scans



Protecting Against Computer Sabotage

- Keep your security software up to date as new malware is introduced all the time
- ISPs and Web mail providers today also offer some malware protection to their subscribers
- Other Security Precautions
 - Control access to computers and networks
 - Intrusion protection systems can help businesses detect and protect against denial of service (DoS) attacks

Protecting Against Computer Sabotage

SECURITY SOFTWARE

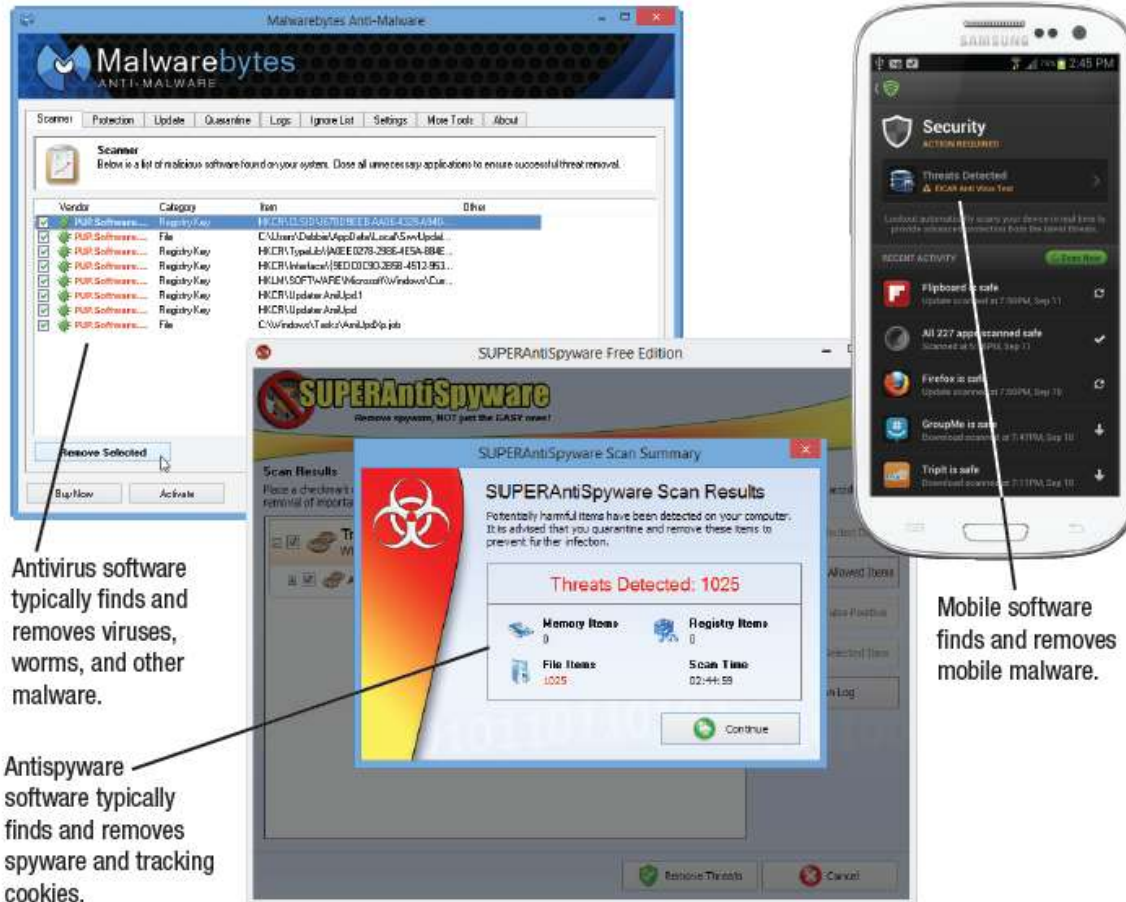


FIGURE 9-17

Security software.

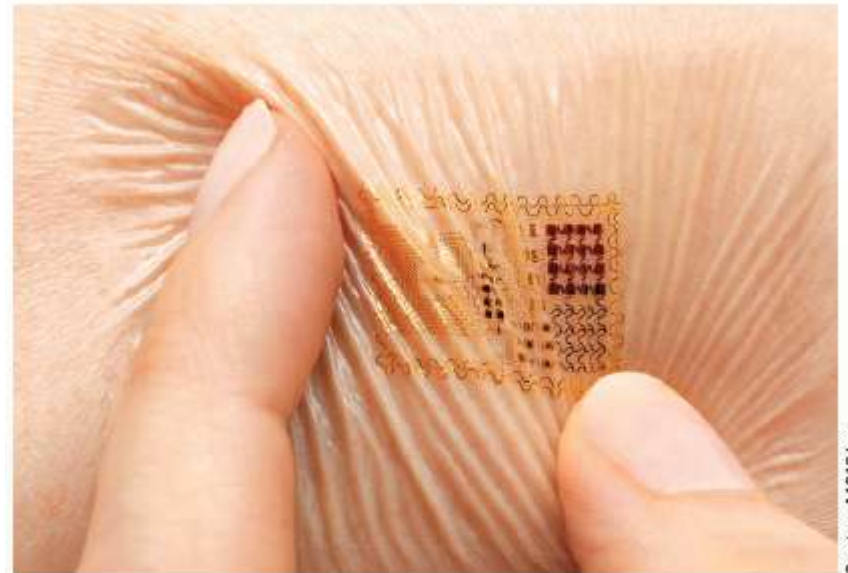
Different security programs will typically find different types of malware.



Trend Box

Beyond Fingerprint Readers—Digital Tattoos and More

- Facial gestures can be used to unlock a phone by smiling or winking at it
 - Some include Liveness Check
- Future alternatives for logging individuals on to devices or secure Web sites
 - Digital tattoos are stamped onto skin
 - Authentication pills are swallowed



Courtesy MC10 Inc.



Quick Quiz

1. Which of the following is used to control your computer by someone else?
 - a. Worm
 - b. Trojan horse
 - c. Botnet
2. True or False: Computer viruses can only be spread via the Internet.
3. A(n) _____ is a type of malware that masquerades as something else.

Answers:

1) c; 2) False; 3) Trojan horse



Online Theft, Online Fraud, and Other Dot Cons

- Dot Con
 - A fraud or scam carried out through the Internet
 - The Internet Crime Complaint Center received and processed more than 24,000 complaints per month in 2012
- Data or Information Theft
 - Theft of data or information located on or being sent from a computer
 - Can occur in several ways
 - Stealing an actual computer or mobile device
 - A hacker gaining unauthorized access



Online Theft, Online Fraud, and Other Dot Cons

- Identify Theft
 - Using someone else's identity to purchase goods or services, obtain new credit cards or bank loans, or illegally masquerade as that individual
 - Information obtained via documents, stolen information, spyware, etc.
 - Expensive and time consuming to recover from
 - Millions of Americans have their identity stolen each year

Online Theft, Online Fraud, and Other Dot Cons



1. The thief obtains information about an individual from discarded mail, employee records, credit card transactions, Web server files, or some other method.
2. The thief makes purchases, opens new credit card accounts, and more in the victim's name. Often, the thief changes the address on the account to delay discovery.
3. The victim usually finds out by being denied credit or by being contacted about overdue bills generated by the thief. Clearing one's name after identity theft is time consuming and can be very difficult and frustrating for the victim.

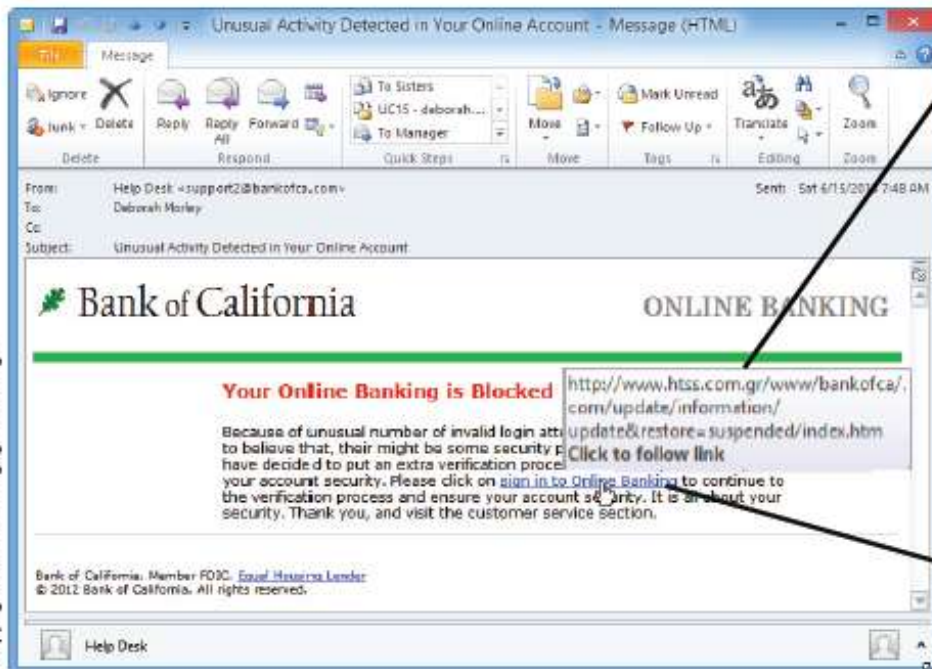
FIGURE 9-19
How identity theft works.



Online Theft, Online Fraud, and Other Dot Cons

- Phishing
 - Use of spoofed e-mail messages to gain credit card numbers and other personal data
- Spear Phishing
 - A personalized phishing scheme targeted to specific individuals
- Social Media Hacks
 - The act of accessing someone else's social media account to make changes to the content or to perform an activity as that individual

Online Theft, Online Fraud, and Other Dot Cons



The link is for non-secure Web page and does not use the bank's domain.

This e-mail looks legitimate, but the link goes to a spoofed Web page.

FIGURE 9-20
Phishing. Phishing schemes typically use legitimate-looking e-mails to trick users into providing private information.



Online Theft, Online Fraud, and Other Dot Cons

- Pharming
 - The use of spoofed domain names to obtain personal information
 - DNS servers are hacked to route requests for legitimate Web pages to spoofed Web pages (DNS poisoning)
- Drive-by Pharming
 - Hacker changes the victims designated DNS server to the pharmer's DNS server



Online Theft, Online Fraud, and Other Dot Cons

- Online Auction Fraud
 - Occurs when an item purchased through an online auction is never delivered or the item is not as specified
 - Illegal, but as with other types of online fraud, prosecution is difficult
- Other Internet Scams
 - Loan and pyramid scams
 - Work-at-home cons
 - Nigerian letter fraud scheme
 - Pornographic sites
 - Fake job site postings



Protecting Against Online Theft, Online Fraud, and Other Dot Cons

- Protecting Against Data and Information Theft
 - Businesses should use good security measures
 - Individuals should not give out personal information (Social Security number, mother's maiden name, etc.) unless absolutely necessary
- Protecting Against Identity Theft, Phishing, and Pharming
 - Shred documents containing sensitive data, credit card offers, etc.
 - Order a full credit history on yourself a few times a year to check for accounts listed in your name
 - Don't place sensitive outgoing mail in your mailbox



Protecting Against Online Theft, Online Fraud, and Other Dot Cons

- Watch bills and credit report to detect identity theft early
- Never click a link in an e-mail message to go to a secure Web site—always type the URL in the browser instead
- Antiphishing Tools
 - Antiphishing tools built into Web browsers can help warn you of potential phishing sites
 - Some secure sites use additional layers of security to protect against identity thieves
 - Some banks and other financial institutions add an additional step in their logon process



Protecting Against Online Theft, Online Fraud, and Other Dot Cons

A PHISHING E-MAIL OFTEN . . .

Tries to scare you into responding by sounding urgent, including a warning that your account will be cancelled if you do not respond, or telling you that you have been a victim of fraud.

Asks you to provide personal information, such as your bank account number, an account password, credit card number, PIN number, mother's maiden name, or Social Security number.

Contains links that do not go where the link text says it will go (point to a hyperlink in the e-mail message to view the URL for that link to see the actual domain being used—a phisher would have to use a URL like `microsoft.phisher.com`, not `microsoft.com`).

Uses legitimate logos from the company the phisher is posing as.

Appears to come from a known organization, but one you may not have an association with.

Appears to be text or text and images but is actually a single image; it has been created that way to avoid being caught in a spam filter (a program that sorts e-mail based on legitimate e-mail and suspected spam) because spam filters cannot read text that is part of an image in an e-mail message.

Contains spelling or grammatical errors.

FIGURE 9-22

Tips for identifying phishing e-mail messages.



Protecting Against Online Theft, Online Fraud, and Other Dot Cons

TIPS FOR AVOIDING IDENTITY THEFT

Protect your Social Security number—give it out only when necessary.

Be careful with your physical mail and trash—shred all documents containing sensitive data.

Secure your computer—update your operating system and use up-to-date security (antivirus, antispyware, firewall, etc.) software.

Be cautious—never click on a link in an e-mail message or respond to a too-good-to-be-true offer.

Use strong passwords for your computer and online accounts.

Verify sources before sharing sensitive information—never respond to e-mail or phone requests for sensitive information.

Be vigilant while on the go—safeguard your wallet, smartphone, and portable computer.

Watch your bills and monitor your credit reports—react immediately if you suspect fraudulent activity.

Use security software or browser features that warn you if you try to view a known phishing site.

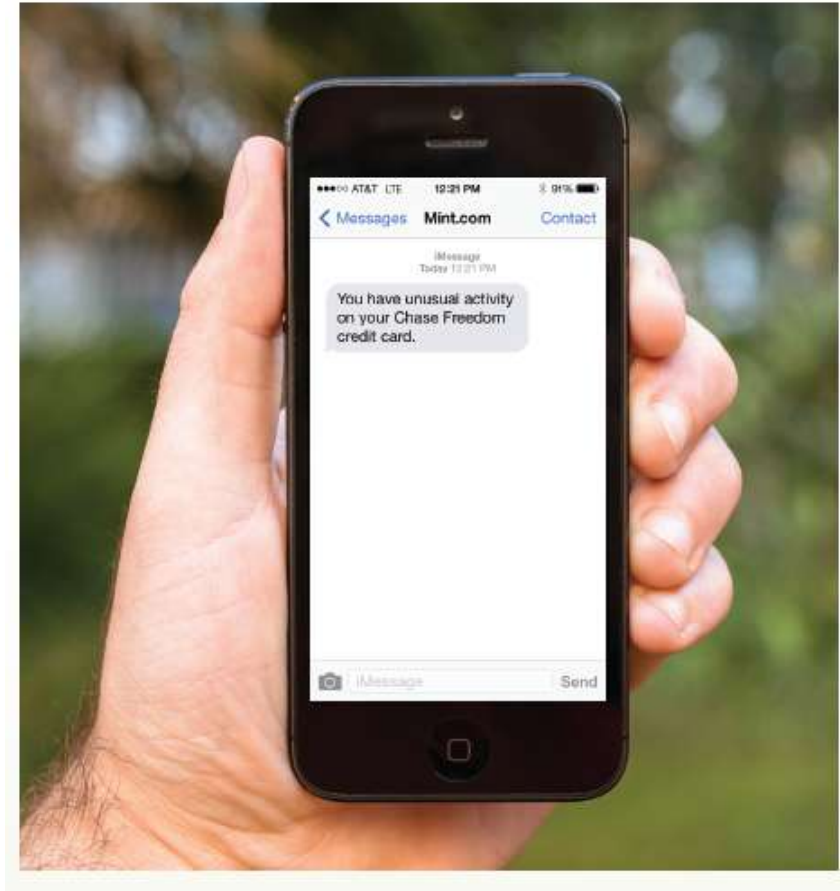
FIGURE 9-23

Tips to reduce your risk of identity theft.

Technology and You Box

Online Financial Alerts

- Can get e-mail or text alerts for account activity
- Can help identify unauthorized activity quickly
- Online money management aggregator services can be used to view the status of multiple accounts (credit cards, bank accounts, etc.)
 - Can set up alerts



© frankreporter/Stockphoto; Courtesy Mint.com



Protecting Against Online Theft, Online Fraud, and Other Dot Cons

- Digital Certificate
 - Group of electronic data that can be used to verify the identity of a person or organization
 - Obtained from Certificate Authorities
 - Typically contains identity information about the person or organization, an expiration date, and a pair of keys to be used with encryption and digital signatures
 - Are also used with secure Web sites to guarantee that the site is secure and actually belongs to the stated individual or organization
 - Can be SSL or EV SSL



Protecting Against Online Theft, Online Fraud, and Other Dot Cons

- Digital signatures
 - Unique digital codes that can be attached to an e-mail message or document
 - Can be used to verify the identity of the sender
 - Can be used to guarantee the message or file has not been changed since it was signed
 - Uses public key encryption
 - Document is signed with the sender's private key
 - The key and the document create a unique digital signature
 - Signature is verified using the sender's public key

Protecting Against Online Theft, Online Fraud, and Other Dot Cons

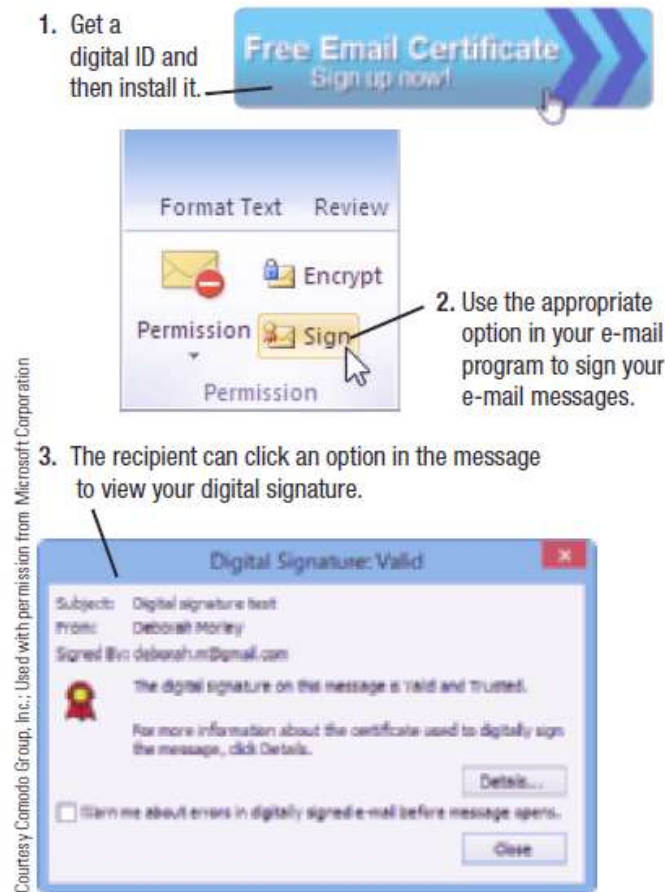


FIGURE 9-26
Digitally signing an e-mail message in Microsoft Outlook.



Protecting Against Online Theft, Online Fraud, and Other Dot Cons

- Protecting Against Online Auction Fraud and Other Internet Scams
 - Use common sense
 - Check online auction seller's feedback before bidding
 - Pay for online purchases via a credit card so transactions can be disputed if needed
 - Use an online payment system
 - Take advantage of buyer protection
 - Use an escrow service for high-priced items

Personal Safety Issues

- Cyberbullying
 - Children or teenagers bullying other children or teenagers via the Internet
 - E-mails
 - Social networking sites
 - Blogs
 - Common today--estimated to affect 50% of all US teenagers



FIGURE 9-27
An anti-cyberbullying Web banner.



Personal Safety Issues

- Cyberstalking
 - Repeated threats or harassing behavior between adults carried out via e-mail or another Internet communication method
 - Although there are no specific federal laws against cyberstalking, all states have made it illegal
- Online Pornography
 - Attempts to ban this type of material from the Internet have not been successful
 - Online pornography involving minors is illegal



Protecting Against Cyberbullying, Cyberstalking, and Other Personal Safety Concerns

- Safety Tips for Adults
 - Be cautious and discreet online
 - Use gender-neutral, nonprovocative identifying names
 - Do not reveal personal information
 - Can request your personal information be removed from online dire
- Safety Tips for Children and Teens
 - Monitor children’s computer and smart phone activities
 - Caution older children about sending compromising photos; sexting can result in child pornography charges being filed against teens

Network and Internet Security Legislation

DATE LAW AND DESCRIPTION

2004	Identity Theft Penalty Enhancement Act Adds extra years to prison sentences for criminals who use identity theft (including the use of stolen credit card numbers) to commit other crimes.
2003	CAN-SPAM Act Implements regulations for unsolicited e-mail messages.
2003	Fair and Accurate Credit Transactions Act (FACTA) Amends the Fair Credit Reporting Act (FCRA) to require that the three nationwide consumer reporting agencies (Equifax, Experian, and TransUnion) provide consumers, upon request, a free copy of their credit report once every 12 months.
2003	PROTECT Act Includes provisions to prohibit virtual child pornography.
2003	Health Insurance Portability and Accountability Act (HIPAA) Includes a Security Rule that sets minimum security standards to protect health information stored electronically.
2002	Homeland Security Act Includes provisions to combat cyberterrorism, including protecting ISPs against lawsuits from customers for revealing private information to law enforcement agencies.
2002	Sarbanes-Oxley Act Requires archiving a variety of electronic records and protecting the integrity of corporate financial data.
2001	USA PATRIOT Act Grants federal authorities expanded surveillance and intelligence-gathering powers, such as broadening the ability of federal agents to obtain the real identity of Internet users, intercept e-mail and other types of Internet communications, follow online activity of suspects, expand their wiretapping authority, and more.
1998	Identity Theft and Assumption Deterrence Act of 1998 Makes it a federal crime to knowingly use someone else's means of identification, such as name, Social Security number, or credit card, to commit any unlawful activity.
1997	No Electronic Theft (NET) Act Expands computer piracy laws to include online distribution of copyrighted materials.
1996	National Information Infrastructure Protection Act Amends the Computer Fraud and Abuse Act of 1984 to punish information theft crossing state lines and to crack down on network trespassing.
1984	Computer Fraud and Abuse Act of 1984 Makes it a crime to break into computers owned by the federal government. This act has been regularly amended over the years as technology has changed.

FIGURE 9-28

Computer network and Internet security legislation.



Quick Quiz

1. Sending an e-mail that looks like it came from someone else in order to obtain information for fraudulent purposes is called _____.
 - a. hacking
 - b. online auction fraud
 - c. phishing
2. True or False: Cyberstalkers often find their victims online.
3. Using someone else's identity to purchase goods or services or perform other transactions is called _____.

Answers:

1) c; 2) True; 3) identity theft



Summary

- Why Be Concerned About Network and Internet Security?
- Unauthorized Access and Unauthorized Use
- Protecting Against Unauthorized Access and Unauthorized Use
- Computer Sabotage
- Protecting Against Computer Sabotage
- Online Theft, Online Fraud, and Other Dot Cons
- Protecting Against Online Theft, Online Fraud, and Other Dot Cons
- Personal Safety Issues



Summary

- Protecting Against Cyberbullying, Cyberstalking, and Other Personal Safety Concerns
- Network and Internet Security Legislation