Survey of Operating Systems 5th Edition Holcombe Solutions Manual

Survey of Operating Systems - Fifth Edition

Instructor Manual

Chapter 2

Computer Security Basics

Learning Outcomes

In this lesson you will provide students with an overview of security basics for computer users. At the end of the lesson students should be able to:

LO 2.1 Describe security threats and vulnerabilities to computers and users.

LO 2.2 Identify methods for protecting against security threats.

LO 2.3 Troubleshoot common security problems.

Estimated time for lesson: 3 to 4 hours

Preparing for Class

Technology moves fast, but nothing seems to change as fast as security threats and the technology developed in response to these evolving evils. At the time of this writing, all major software vendors even remotely affected by security threats were announcing plans for major updates to address threats, especially those in the form of viruses, spyware, and adware. There were also new concerns about threats accessing Bluetooth connections and vulnerabilities in the expanding area of the Internet of Things. Therefore, be prepared to bring the students up-to-date on both newly evolved threats (there seems to be no lack of creativity in that area) and newly evolved defenses against the threats.

Whenever possible, demonstrate new products—especially free products—that will aid them in their fight against such predation.

This chapter contains two Step-by-Step exercises and five Try This exercises. Review them before the start of class so that you are prepared for any additional information the students may need to complete them, depending on the computers and time available.

Prerequisites for Class

Ensure that the students are:

- Comfortable with basic computer skills (mouse and keyboard use).
- Able to access a running lab computer either individually or in small groups.
- Able to browse the Internet and capable of using a web browser.

Class Preparation Notes

Ensure that, if possible, all lab computers are returned to the default settings. If that is not possible, at least ensure that all lab systems are running the same version of Windows, or other selected OS, with the same components installed. If another person or department is responsible for the lab computers, make sure that you are personally familiar with any security measures implemented on the computers and whether OS components are used or third-party security is in effect. Test all the hands-on activities so that you will know beforehand if there is any conflict with the computers as configured.

Visit TestBankDeal.com to get complete for all chapters

Take time to review these activities beforehand so that you can gauge how much time you should devote to them, depending on the level of the students.

General Teaching Tips

Depending on the level of the students, this information on security threats can be intimidating. Therefore, as they move through the long list of threats, assure them that they will soon learn behaviors that will make them less vulnerable to threats, and they will learn about software that will protect them and/or remove the damage from other threats.

Key Terms

Teaching Tip:

We present many of these terms in a simplified form for the audience, with narrow definitions. You may choose to present broader definitions, depending on the level of the students.

administrator account type—A user account with permission to perform system-wide tasks.

adware—A form of spyware software that collects information about the user in order to display user-targeted advertisements.

authentication—Validation of a user account and password that occurs before the security components of an OS give a user access to the computer network.

authorization—The process of both authenticating a user and determining the permissions that the user has for a resource.

back door—A way to bypass security and gain access to a computer.

bitcoin—An online payment system.

black hat hacker—Someone with a great deal of computer programming skills who invades private computers and networks, exploring computer system weaknesses to take advantage of the system or systems, for illegal and possibly terroristic purposes.

bluesnarfing—The act of covertly obtaining information broadcast from wireless devices using the Bluetooth standard, a short-range wireless standard used for data exchange between computers and mobile devices.

botherder—A person who initiates and controls a botnet.

botnet—A group of networked computers that, usually unbeknown to their owners, have been infected with programs that forward information to other computers over the network. A bot, short for robot, is a program that acts as an agent for a user or master program, performing a variety of functions for good or evil.

browser hijacking—This occurs when malware alters a browser so that the home page points to a site other than the user's choice. This is often a site advertising some product, such adware removal software.

content filter—In an Internet browser, software that blocks content.

cookies—Very small text files an Internet browser saves on the local hard drive at the request of a web site. Cookies may contain user preferences for a specific site, information entered into a form at a web site (including personal information), browsing activity, and shopping selections made at a web site.

cybercriminal—A person who breaks laws using computer technology.

cybercrime—Illegal activity performed using computer technology.

cyberterrorist—Someone who uses a computer to cause destruction without regard to its effect on humanity.

cyberterrorism—The use of computers to cause destruction without regard to its effect on humanity.

data wiping—The permanent removal of data from a storage device.

digital certificate—A special file stored on a computer that may hold a secret key for decrypting data.

DMZ—Named for a wartime demilitarized zone, a network between the internal network and the Internet with a firewall on both sides. This is where an organization puts any servers that it wishes to have offer services over the Internet.

drive-by download—A program downloaded to a user's computer without consent. Often the simple act of browsing to a web site or opening an HTML email message may result in such a surreptitious download. A drive-by download may also occur when installing another application.

email spoofing—The act of forging an email address by modifying the sender’s address in the email message’s header (the information that accompanies a message but does not appear in the message).

Encrypting File System (EFS)—An NTFS file encryption feature introduced with Windows 2000 and NTFS5.

encryption—The transformation of data into a code that can only be decrypted through the use of a secret key or password.

exploit—A malware attack that takes advantage of some vulnerability in our computers or networks.

Family Safety—A feature of Windows 8 and newer that allows parents to protect their children from harm while surfing the Internet.

FileVault—A feature of Mac OS X that will encrypt all the files in the Home folder.

firewall—A hardware device or software that protects a network or computer by examining traffic and rejecting certain traffic based on a set of rules.

first-party cookie—A cookie that originates with the domain name of the URL to which you directly connect.

forged email address—An address that may appear but is in reality fake or forged.

fraud—The use of deceit and trickery to persuade someone to hand over money or other

valuables.

group account—A security account that may contain one or more individual accounts. Some security accounts databases may contain other groups.

guest account—A special account used when someone connects to a computer over a network, but is not a member of a security account recognized on that computer. That person connects as a guest (if the guest account is enabled) and will only have the permissions assigned to the guest account.

hacker—Someone with a great deal of computer programming skills who invades private computers and networks.

header—The information that accompanies a message but does not appear in the message.

honeypot—A server created as a decoy to draw malware attacks and gather information about attackers.

hotspot—A Wi-Fi network that connects to the Internet through a router.

identity theft—This occurs when someone collects personal information belonging to another person and uses that information to fraudulently make purchases, open new credit accounts, or even obtain new driver's licenses and other forms of identification in the victim's name.

keylogger—Another name for a keystroke logger.

keystroke logger —Software or a hardware device that monitors and records every keystroke entered at a computer.

malware—Malicious software. Any software security threat.

Parental Controls—A feature of Windows 7 that allows parents to protect their children from harm while surfing the Internet. Replaced by Family Safety.

password—A confidential string of characters that a user enters (along with a user name) in order to be authenticated.

password cracker—A program used to discover a password.

password manager—Software used to create strong passwords, storing credentials for many sites, and automatically filling in these credentials when needed.

permission—An action that may be performed on an object, such as a computer, file, or folder.

phishing—A fraudulent method of obtaining personal financial information through web page pop-ups, email, and even via letters mailed via the postal service.

pop-up—An ad that runs in a separate browser window that you must close before you can continue with your present task.

pop-up blocker—A program that works against pop-ups.

pop-up download—A program that is downloaded to a user's computer through the use of a pop-up page that appears while surfing the Web.

ransomware—Malware that threatens to do damage or lock the victim out of a computer

unless he or she pays a fee.

rootkit—Malware that hides itself from detection by anti-malware programs by concealing itself within the OS code or in any other program running on the computer.

scareware—Similar to a Trojan Horse (see below), an advertisement that appears to be something harmless and that offers to take some action, such as pretending to scan your computer for problems, but the results will be bogus. It offers to fix the problems it claims to find and asks for payment to support charities. Scareware threats state that you must donate or it will delete critical files.

secret key—A special code that can be used to decrypt encrypted data.

Secure HTTP (HTTPS)—An enhancement to the HTTP protocol that encrypts communications using the Secure Sockets Layer (SSL) security protocol.

Secure Sockets Layer (SSL)—A protocol used to encrypt messages.

security account—In a security accounts database, a security account is a listing of information about a user, group, or computer. A user or computer account is used for authentication; both user and group accounts are used for authorization with assigned permissions.

shoulder surfing—The act of reading information off a screen over the shoulder of the victim.

social engineering—The use of persuasion techniques to gain the confidence of individuals.

social media—Any service (Internet-based or other) that provides a place where people can interact in online communities, sharing information in various forms. Community members generate social-media content.

social networking—The use of social media.

social networking site—A website that provides space where members can communicate with one another and share details of their business or personal lives.

spam—Unsolicited email, (most often seeking financial gain for the sender). This includes email from a legitimate source selling a real service or product, but if you did not give them permission to send such information to you, it is considered spam.

spam filter—Software designed to combat spam by examining incoming email messages and filtering out those that have characteristics of span, including certain identified keywords.

spear phishing—A targeted phishing attack where the target is usually one that has a high probability of delivering a very valuable return.

spim—An acronym for "Spam over Instant Messaging;" the perpetrators are called spimmers.

spyware—A category of software that runs surreptitiously on a user's computer, gathers information without permission from the user, and then sends that information to the people or organizations that requested the information.

standard user account—An ordinary user without administrator status.

third-party cookie—A cookie that originates with a domain name beyond the one shown in your URL.

token—A physical device that can be used in authentication, either alone or together with a user name and password.

Trojan horse—A program that is installed and activated on a computer by appearing to be something harmless, which the user innocently installs. This is a common way that a virus or a worm can infect a computer.

user account—A security account that is assigned to a single person and contains, at minimum, a user name and password used to authenticate a user.

User Account Control (UAC)—Beginning in Windows Vista, a feature that prompts a user (even an administrator type account) when the user or any software attempts to perform a function requiring administrator permissions.

user right—In Windows, the privilege to perform a system wide function, such as access the computer from the network, log on locally, log onto a computer from the network, back up files, change the system time, or load and unload device drivers.

vector—A mode by which malware infects a computer.

virus—A program that is installed and activated on a computer without the knowledge or permission of the user. At the least the intent is mischief, but most often it intends to be genuinely damaging in one way or another.

war driving—The act of moving through a neighborhood in a vehicle or on foot, using either a laptop equipped with Wi-Fi wireless network capability or a simple Wi-Fi sensor available for a few dollars from many sources. War drivers seek to exploit open hotspots, areas where a Wi-Fi network connects to the Internet without the use of security to keep out intruders.

white hat hacker—Someone with a great deal of computer programming skills who invades private computers and networks, exploring computer system weaknesses for the purpose of making systems more secure.

worm—A self-replicating computer virus.

zero-day exploit—A software vulnerability unknown to the publisher of the targeted software. When someone devises a way to exploit that vulnerability (often with a virus), it is often very difficult to protect against such a threat.

zombie—An individual computer in a botnet, so-called because it mindlessly serves the person who originated the botnet.

Lecture Outline

I. LO 2.1 Threats to Computers and Users

Teaching Tip:

This section consists of several pages of information on threats to computers and users. Students will have heard of many of these concepts, but this may be the first time they are being formally presented to them. This text is broken up with three Try This activities that will encourage them to research the latest information on spam, phishing frauds, and identity theft. They can even take a phishing IQ test. Allow time for these activities because they will help the students assimilate all this information.

Discussion Point:

Try to avoid going into detail on actions to take to protect against these threats until you move on to the next major section on Defense Against Threats.

A. Introduction to Section

1. Risks of insecure computer or mobile devices.
    - i) Identity
    - ii) Work you created
    - iii) Employer's integrity
    - iv) Your job
    - v) Government regulations require organizations to protect certain personal information.
    - vi) Cybercrime is illegal activity using computer technology.

B. Malicious Tools and Methods

1. Vectors

Discussion Point:

To introduce vectors, ask the students if they have ever heard the term vector used outside of computer malware? They may have heard of vectors in reference to human viruses. Talk about the similarity between human viruses and malware.

i) Social networking

a) Using social media, such as a social networking site, to communicate with others.

b) Social networking is a vector for malware and social engineering because it's a rich source of personal information that many who use social networks seem willing to share.

ii) Email

Teaching Tip:

Take a moment to allow students to do the Try This! Activity titled More About Social Media.

iii) Malicious Code on Web sites

iv) Trojan horses: malware disguised as a harmless program.

v) Searching for unprotected computers

vi) Sneakernet—the oldest vector

vii) Back Doors

viii) Rootkits

ix) Pop-up Download – malware installed through a pop-up on a web page.

x) Drive-By Download – a program installed without consent; often by browsing to a website, opening an HTML email message, or during a program installation.

xi) War Driving

a) The act of moving through a neighborhood using either a laptop equipped with Wi-Fi wireless network capability, or a simple Wi-Fi sensor searching for open hotspots

b) War drivers may also leave a sign of an open hotspot by "war chalking"

c) Web sites and videos show how to war drive

xii) Bluesnarfing

a) War driving with Bluetooth signals

2. Password theft

i) Stealing passwords through websites

ii) Stealing passwords with password crackers

iii) Stealing passwords with keystroke loggers

3. Zero-Day Exploit

i) We use the noun form of exploit, but it is used as both a noun and verb. An exploit is something that takes advantage of an opportunity as well as the action of doing so. Not in itself a bad

thing. A malware attack is called an exploit because it takes advantage of a vulnerability in computers or networks.

ii) A zero-day exploit occurs when someone devises a way to exploit a previously unknown vulnerability.

4. Viruses

   i) A program installed and activated without the knowledge or permission of the user

   ii) Mischief or damaging results

5. Worms

   i) A virus that self-replicates

   ii) Travel between computers via many vectors

   iii) Netsky and MyDoom worms generated disabling amounts of network traffic

   iv) Nimda inserted its code into other executable files on the local drive of each machine

6. Botnets and Zombies

   i) Botnet is a group of network computers

   ii) Infected with programs that forward information to other computers

   iii) Bot (short for robot) program acts as an agent

   iv) Can be used for good or evil

   v) Zombie is a computer working mindlessly as part of the botnet

   vi) Botherder is someone who initiates and controls a botnet

7. Spyware

   i) Gathers information and sends it to the people who requested it

   ii) Tracks surfing or buying patterns for marketing

   iii) Used for industrial espionage

iv) Law enforcement uses spyware to track sexual predators or other criminals

v) Governments use spyware to investigate terrorism

8. Adware

i) A form of spyware that collects information about the user in order to display advertisements targeted to the user, either in the form of inline banners or pop-ups

ii) Pop-ups run in a separate browser window that you must close before continuing

iii) Clicking to accept an offer presented in an inline banner or pop-up may trigger a pop-up download installing a virus or worm

9. Browser Hijacking

i) When your home page points to a site you didn't select

ii) Remedy by changing default home page in options unless the browser was modified so that options are not available

10. Spam and Spim

i) Spam

a) Unsolicited email

b) May be from legitimate sources selling real services or products

c) May involve a scam.

d) Perpetrators of spam are called spammers

Teaching Tip:

Take a moment to allow students to do the Try This! Activity titled Research Spam Statistics.

Discussion Point:

When a new Domain Naming System top-level domain (TLD) becomes available the authors have seen a flood of new spam originating from newly-created domains. For instance, the ninja and work TLDs are fairly new additions. Not everyone who acquired a second-level domain within one of these TLDs is a spammer, but there are enough new spams generated from these domains that we have blocked each entire TLD with our spam filters.

We have yet another experience with this scenario from a different point of view. In 2001 a

new generic TLD (.biz) became available and the authors decided to register a domain name in this TLD. At that time, Jane managed mail and file-and-print servers in small businesses. She was surprised to receive an advisory recommending blocking all incoming mail from .biz sources. This didn't last long, and the authors only recall one of their own emails that was rejected. That was remedied by a conversation with the email administrator at the recipient's company, Read the Wikipedia article on .biz to learn other interesting facts, like what "biz" means in Turkish (It's a good thing.)

ii) Spim

a) An acronym for Spam over Instant Messaging

b) Bots (or spimbots) collect instant messaging screen names

c) Typical spim message contains links to product web sites

d) Perpetrators are called spimmers

11. Social Engineering

Discussion Point:

When introducing this section, bring up some real world examples you may have experienced or learned about, and then ask if students have ever received a message they thought suspicious or that they discovered was not from the source it appeared to be from?

Teaching Tip:

Have the students do Step-by-Step 2.01, "Take a Phishing IQ Test!" This will take them a while to perform but it leads to a very rich discussion session on the subtleties that phishers use to fool victims.

i) Uses persuasion techniques to gain the confidence of individuals.

ii) Fraud: The use of deceit and trickery to obtain money or other valuables.

a) One form of fraud, ransomware, is malware that threatens to do damage or lock out a user who doesn't pay them. Some ransomware claims to have proof that the victim committed an illegal act and threatens to report this to the authorities unless paid a ransom.

b) Online payment system, such as bitcoin, used for ransomware payments.

iii) Phishing: Fraudulent method of obtaining personal financial information through using pop-ups or email appearing to be from legitimate organizations.

iv) Hoaxes

a) Take many forms

b) Example: an email message claiming to be from Microsoft and including a link to a web site for downloading a fix. Microsoft never sends out updates through email

v) Enticements to Open Attachments that may install malware on your computer

12. Identify Theft

i) Personal information stolen in order to commit fraud

ii) Obtaining a social security number and other key personal information is all that is needed to steal someone's identity

Teaching Tip:

Take a moment to allow students to do the Try This! Activity titled Learn More About Identity Theft.

13. Exposure to Inappropriate or Distasteful Content

14. Invasion of Privacy

15. Misuse of Cookies

    i) Cookies may contain:

        a) User preferences from visiting a specific site

        b) Information you may have entered into a form at the Web site, including personal information

        c) Browsing activity

        d) Shopping selections on a web site

    ii) Cookies can be a convenience to a user

    iii) Most good web sites describe how they use cookies and what they use them for in a privacy statement.

    iv) First-party cookies originate with the domain name of the URL to which you connect.

    v) Third-party cookies originate with a domain name beyond the one shown in your URL. Source can be an ad embedded in a Web page.

16. Computer Hardware Theft

    i) Physical security best protection.

    ii) Mobile devices more vulnerable to theft.

C. Accidents, Mistakes, and Disasters

1. Accidents, mistakes, and disasters happen.

2. Prepare with frequent backups.

D. Keeping Track of New Threats

1. Federal Trade Commission (FTC) Bureau of Consumer Protection (www.ftc.gov/bcp)

E. The People behind the Threats (Cybercriminals)

1. Organized Crime

2. Cyberterrorists
3. Hackers / white hat hacker / crackers
4. Script Kiddies
5. Click Kiddies
6. Packet Monkeys

II. LO 2.2 Defense Against Threats

A. Education

1. Computer symptoms to watch for:
    i) Strange screen messages
    ii) Sudden computer slowdown
    iii) Missing data
    iv) Inability to access the hard drive
2. Non-computer activities of concern:
    i) Charges on credit accounts that you are sure you or your family did not make
    ii) Calls from creditors about overdue payments on accounts you never opened
    iii) A turndown when applying for new credit, for reasons you know are not true
    iv) A credit bureau report of existing credit accounts you never opened

B. Security Policies

1. Define data sensitivity and data security practices
2. Exist in both document form and software form
    i) Administrators configure computer security to enforce written policy
    ii) Password policy should require strong passwords and state the complexity requirements that are enforced on computers

C. Firewalls

1. Network-based Firewalls
    i) Firewall Technology
        a) IP packet filter
        b) Proxy service
        c) Encrypted authentication
        d) Virtual private network (VPN)

Teaching Tip:

Inform the students that the professionals who work with dedicated firewalls for large organizations must be highly-trained and are usually well-compensated for a job that carries a great deal of responsibility.

1. Personal Firewalls
    i) Come with most OSs
    ii) Come with third-party security software

Discussion Point:

The margin Note on page 57 mentions honey pot, *a decoy server used to attract malicious attackers. Consider discussing the use of such methods to catch criminals of all sort. For instance, sexual predators are lured by law enforcement officers posing as potential victims.*

D. Security Software

1. Antispam Software
    i) Spam filter
        a) On email clients.
        b) On central mail servers.
        c) Internet-based.
2. Antivirus Software
    i) Examine contents of storage and RAM.
    ii) Require frequent updating
3. Pop-Up Blockers
    i) In free and commercial security programs
    ii) Feature of browsers
    iii) Configure to exclude or include (as exceptions) sites
4. Privacy Protection and Cookies
    i) Privacy settings include several features
    ii) Individual settings for first-part and third-party cookies
5. Parental Controls and Family safety
    i) Feature of browsers
    ii) Set specific controls for a child's user account
6. Content Filtering
    i) Blocks or allows certain sites
    ii) May be part of a multifunction package
    iii) May be included in browser
    iv) Services on Internet give ratings to web sites
    v) Configure filter to allow or disallow unrated sites

vi) Content Advisor in Internet Explorer

7. Software Updates

i) Keep software updated with security patches

ii) Older versions of Windows may not be supported by updates

Teaching Tip:

Allow time for students to do the Try This! Activity titled View the Windows Update History.

E. Authentication and Authorization

1. Authentication

    i) Verification of who you are.

    ii) One-factor authentication based on something you know, such as user name and password

    iii) Two-factor authentication based on something you know plus something you have (a token)

        a) ATM cash card is a token.

    iv) Three-factor authentication may add biometric data such as a retinal scan, voiceprint, or fingerprint.

2. Authorization

    i) Determines the level of access to a computer or a resource

    ii) Includes both authentication, plus verification of access level (permissions and/or rights)

    iii) Permission describes an action that can be performed on an object

    iv) User right is a system-wide action a user or group may perform

F. Passwords

1. A password is a string of characters entered for authentication
2. Don’t take passwords for granted
3. Do not use the same password everywhere
4. Basic defense against invasion of privacy/identify theft
5. Use long and complex passwords
6. Do not use common words
7. Use a password manager to create strong passwords and store all your credentials for all devices.

G. Security Account Basics

1. Security account: An account that can be assigned permission to take action on an object (such as a file, folder, or printer) or the right to take some action on an entire system, such as install device drivers into an

operating system on a computer. Or simply to log on to a computer or web site.

i) User Accounts

a) Assigned to a single person—can be created by administrator user

b) Contains (at minimum)

1) User name

2) Password

ii) Built-in User Accounts

a) Administrator (Windows)

b) Root (Mac OS X and Linux)

c) Guest

iii) Standard versus Administrator Accounts

a) Standard user account (previously limited account in Windows XP)

b) Administrator account type

Teaching Tip:

Point out that they can view the Windows Administrator account in the Local Users and Groups node of Computer Management. Show students that the Administrator account is disabled by opening the Administrator Properties in Local Users and Groups. Then (only if your computer does not belong to a Windows Domain) restart the computer in Safe Mode and sign in with the Administrator account.

iv) Group Accounts

a) Security account that contains one or more individual accounts

b) May contain other groups

c) Some built-in (Windows Administrators, Users, Guests)

d) Some software will create a special group account for use by the software

Teaching Tip:

This last point may be confusing. Point out that at one time, many programs ran with "System" privileges, which are all-powerful. Therefore, this practice was a huge security hole. Now, software that requires a special account to run will have an individual account with lesser privileges than those given to System.

e) Administrators can create others

v) Computer Accounts

a) Computers may have security accounts

b) Windows computers join an Active Directory Domain where an account is created for the computer

Discussion Point:

Tell students that if their school or work has a Windows Active Directory domain, Windows computers log on to the domain when they start up each day. Ask if they can think of why this would be true. See if they understand that this guarantees that the computers are not "rogue" computers. Of course, each user must also log on.

2. User Account Control (UAC)

Discussion Point:

Ensure that students understand the reason for UAC. The text explains the scenario, but students may miss the significance of the protection UAC gives you.

i) Began in Windows Vista

ii) Prompts a user (even an administrator type account) when the user or any software attempts to perform a function requiring administrator permissions

iii) Two scenarios

a) A user logged on with an administrator type account only has privileges of a standard account until the user (or malware) attempts to do something privileged

1) UAC dims the desktop and displays the Consent Prompt

2) User must respond in order to continue.

b) User logged on as a standard type account

1) UAC dims the desktop and displays the Credentials Prompt

2) User must enter both a username and password of an administrator type account.

iv) UAC-type function in Mac OS X

a) Certain dialog boxes have a lock symbol

1) If the lock is turned on, only “safe” actions can be completed

2) Unlocking a dialog box requires credentials; then you will see advanced settings

H. Best Practices When Assigning Permissions

1. Principle of least privilege

i) Assign permissions that allow each user only the level of access required to complete assigned tasks

ii) Do not give users more access than necessary

I. Best Practices with User Names and Passwords

1. You are at risk if you answer "yes" to any of the following:

i) Do you have too many passwords to remember?

ii) Do you use the same password everywhere?

iii) Do you have your password written on sticky notes or your desk calendar?

iv) Have you used the same password for more than a few months?

v) Reusing the same user name also puts user at risk

2. Protect Your User Name and Password

i) If you use the same user name and password at your bank as you do at a web site where you took what seemed like a harmless personality test, you may have put your bank account and your other financial assets at risk

ii) The web site might have been created to surreptitiously gather just such personal information, or it may have an innocent mission but simply employ weak security practices

3. Create Strong Passwords

i) A strong password is one that meets certain criteria, which change over time as hackers create more techniques and tools for discovering passwords

ii) Microsoft defines a strong password as one that contains at least eight characters, includes a combination of letters, numbers, and other symbols (+, -, **$**, and so on), and is easy for you to remember but difficult for others to guess. (This may have changed, especially the recommendation on number of characters.)

iii) Always use strong passwords for the following types of accounts:

a) Banks, investments, credit cards, and online payment providers

b) Email

c) Work-related accounts

d) Online auction sites and retailers

e) Sites where you have provided personal information

4. Avoid Creating Unnecessary Online Accounts

i) When a web site requests that you "join," question the benefits of joining

ii) Question why a web site needs information about you

5. Never Reuse Passwords

i) Every account should have a unique name (not always possible when an using email address as an account name).

ii) Every account should have a unique password.

6. Don't Provide More Information than Necessary

i) Avoid creating accounts with web sites that request your social security number and other personal and financial information

ii) Avoid having your credit card numbers and bank account information stored on a web site

iii) Although it's not easy to do online, in person you can ask the following questions:

a) Why do you need it?

b) How will you protect it?

c) How will you use it?

d) What happens if I don't give it to you?

Discussion Point:

Ask how many students do online banking or purchase items online. Ask if they know to look for the HTTPS protocol in the address box of the browser?

J. Encryption

1. The transformation of data into a code that you can decrypt only with a secret key or password
2. Secret key is a special code used to decrypt encrypted data
3. You can encrypt data before sending it over a network
    i) Most online methods use digital certificate:
    ii) A secret key in the form of a file stored on a computer
4. You can encrypt stored data files
5. Encrypting Network Traffic
    i) Secure HTTP (HTTPS) encrypts communications using Secure Sockets Layer (SSL) security protocol
6. Windows Encrypting File System
    i) Windows NTFS file system includes Encrypting File System (EFS) for encrypting files
7. Encrypting with Window BitLocker
    i) Windows BitLocker Drive Encryption a feature of some editions of Windows
    ii) BitLocker to Go encrypts external hard drives and flash drives.
8. Encrypting with OS X FileVault

K. Data Wiping

1. Remove data from old computers before disposing of them
2. Data wiping is the permanent removal of data from storage
    i) Reformat of hard drive does not truly remove data
    ii) Data wiping software writes over data many times to completely erase it
    iii) Can wipe data on any rewritable storage device
    iv) On newer hard drives wiping programs use built-in Secure Erase

L. Physical Security

1. Limit access to building or room
2. Laptops and other mobile devices are more vulnerable

M. Security for Mobile Computing

i) Be extra wary of the danger of theft

ii) Encrypt sensitive and confidential data

III. LO 2.3 Troubleshooting Common Security Problems

A. Troubleshooting Log-on Problems

1. Caps lock key turned on
2. Too many log-on attempts

i) Account locked out

ii) Must wait for the lockout duration to expire or have administrator unlock.

Teaching Tip:

Please point out that they will probably only encounter the problem of being locked out after too many wrong passwords if they are logging on to a network. Setting the account lock out and other password policy settings is an advanced task, not usually applied to a computer unless it is logging on to a network server, as in the case of a desktop computer that is a member of a Windows Active Directory domain.

B. Using the Administrator Account in Troubleshooting

1. The local built-in Administrator account in Windows is disabled by default and does not have a password.
2. If a computer is not a member of a Windows Active Directory domain when starting in Safe Mode, you can log on with an Administrator account and attempt to troubleshoot.

Teaching Tip:

Please point out that they can view the Windows Administrator account in the Local Users and Groups node of Computer Management.

C. Troubleshooting a Suspected Malware Attack

1. Run a scan of all drives and memory
2. If no malware is found, try a reputable online scanner, such as Housecall by Trend Micro

Step-by-Step 2.02—Perform an Online Virus Scan on a PC or Mac.

Extra Project One

After completing Lab Project 2.3 take the job titles you discovered through your research of a security certification and look online for a salary survey that includes one or more of the job titles. Then report on the job titles and salaries you find.

Project Solution

It will depend on the certification and job title.

One example: Security+ is a certification that people have who hold the following job titles and salaries:

Job Title	**Annual salary range**
Information Technology Specialist	$44,636-66,711
Security Engineer, Information Systems	$59,212-83,868
Systems Administrator	$45,612 – 63,770
System Administrator, Computer/Network	$42,180 – 63,141
Senior Systems Administrator	$65,396 – 80,539

A high-end example: Certified Information Systems Security Professional (CISSP) can lead to the following job titles and median salary ranges:

Job Title	**Annual salary range**
Security Engineer, Information Systems	$75,171 – 102,417
Security Consultant, (Computing/Networking/Information Technology)	$74,075 – 107,213
Security Manager, IT	$83,030 – 112,344
Senior Network Engineer	$79,145 – 110,859
Information Technology (IT) Director	$85,519 – 129,590

Discussion Point:

Point out that the salary surveys often show several job titles with a range of salary. Just because a job title is associated with a certification does not mean that the certification is all that is required for the job. Many security-related jobs require on-the-job experience and additional certifications. Someone aiming for one of the higher-paid job titles related to security may need to start at a lower level, such as systems administrator (with qualifications for that role) before acquiring the experience to apply for the desired job.

Extra Project Two

In the spring of 2015 the FBI reported that a hacker had taken control of a United Airlines airliner while he was a passenger on that plane. The FBI detained him and confiscated all his equipment. He later reported in an interview that he had not actually taken control of the plane. Research this or another similarly incident relating to hacking of transportation or utilities and discuss the outcomes and any known precautions taken by the transportation company or utility involved.

Project Solution

The solution will depend on the incident chosen. At this writing the incident described above is still evolving.

Assessment Quiz

This extra quiz, not included in the text book, will test the knowledge students have gained during the lesson.

Questions

1. Logging on with something you know (username and password) plus something you have (fingerprint) is known as _____ authentication.
2. A/an _____ is one that originates from a domain name beyond the one shown in the URL for the current web page, and it may be used by an ad embedded in a Web page to track your Web surfing habits.
3. The term "brute force" is used to describe one category of _____.
4. While browsing the Internet, Celine answered survey questions that appeared in a pop-up window and inadvertently became the recipient of a/an _____.
5. Harry's smartphone became the target of _____ via a wireless technology he normally uses for his headphones. Using this method, a stranger acquired Harry's address book.
6. No matter how you connect to the Internet, it is important for you to turn on and configure a/an _____ on that computer.
7. If your child has a standard account on a Windows computer, you can use _____ to set specific restrictions on Internet browsing, providing you have a password-protected administrator account.

8. A user and a group are examples of types of _____,
9. A very frustrated user complains that he has correctly entered his password several times, but was rejected each time. Experience has shown that leaving the _____ turned on is a frequent cause of failure to log on.
10. The oldest malware vector is called _____because malware moves from computer-to-computer by being carried by a person with a flash drive or other portable storage device.

Answers

1. Logging on with something you know (username and password) plus something you have (fingerprint) is known as *two-factor* authentication.
2. A *third-party cookie* is one that originates from a domain name beyond the one shown in in the URL for the current Web page, and it may be to track your Web surfing habits.
3. The term "brute force" is used to describe one category of *password cracker*.
4. While browsing the Internet, Celine answered survey questions that appeared in a pop-up window and inadvertently became the recipient of a *pop-up download*.
5. Harry's smartphone became the target of *Bluesnarfing* via a wireless technology he normally uses for his headphones. Using this method, a stranger acquired Harry's address book.
6. No matter how you connect to the Internet, it is important for you to turn on and configure a *personal firewall* on that computer.
7. If your child has a standard account on a Windows computer, you can use *Parental Controls* to set specific restrictions on Internet browsing, providing you have a password-protected administrator account.
8. A user and a group are examples of types of *security accounts*,
9. A very frustrated user complains that he has correctly entered his password several times, but was rejected each time. Experience has shown that leaving the *Caps Lock key* turned on is a frequent cause of failure to log on.
10. The oldest malware vector is called *sneakernet* because malware moves from computer-to-computer by being carried by a person with a flash drive or other portable storage device.

Chapter 2 Textbook Solutions

Answers to Key Terms Quiz

1. permission
2. cookies
3. spam
4. identity theft
5. user right
6. authorization
7. encryption
8. authentication
9. content filter
10. rootkit

Answers to Multiple-Choice Quiz

1. Correct answer: B. Written security policies define rules and practices for protecting and managing sensitive information.

   A is not correct because firewalls are devices or software that protect a network or individual computer from suspicious traffic.

   C is incorrect because security software is software that protects against many types of attacks.

   D is incorrect because software designed to work with a Web browser performs content filtering to either block certain sites or to only allow certain sites.

   E is incorrect because an antivirus is software that examines the contents of a storage device or RAM looking for hidden viruses and files that may act as hosts for virus code.

2. Correct answer: B. A pop-up displays uninvited in a separate window when you are browsing the Web and can provide a vector for malware infections.

   A is not correct because an inline banner runs within the context of the current page, taking

up space, but it does not have a separate window.

C is incorrect because spam is unsolicited e-mail, not something that loads in a separate window while you are browsing the Web.

D is incorrect because adware is a form of spyware, not a separate window that displays when you are browsing.

E is incorrect because a back door is a vector by which someone can gain access to a computer, not a separate window that displays while you are browsing.

3. Correct answer: D. UAC, or user account control, is a feature introduced in Windows Vista by which a logged-on user has only the privileges of a standard account, even if that user is logged on as an administrator, and must confirm the operation or (if logged on as a standard user) provide the password of an administrator to perform most administrative tasks.

   A is not correct because account lockout threshold is a feature that locks someone out after a specified number of failed log-on attempts.

   B is incorrect because EFS, or encrypting file system, is a feature in NTFS that encrypts files saved to a folder which has encryption enabled.

   C is incorrect because lockout policy is a Windows security policy with settings for the number of failed attempts that will trigger a lockout (account lockout threshold) and then the length of time such a lockout will last (account lockout duration).

   E is incorrect because account lockout duration is the period of time during which an account is locked out before the security system will accept another log-on attempt.

4. Correct answer: D. Spim is unsolicited e-mail received via instant messaging.

   A is not correct because spam refers to unsolicited e-mail received via conventional e-mail.

   B is incorrect because spyware is software that runs surreptitiously on a user's computer, gathers information without the user's permission, and then sends that information to the people or organizations that requested the information.

   C is incorrect because a zombie is a computer in a botnet.

   E is incorrect because a bot is a program that acts as an agent for a user or master program, performing a variety of functions.

5. Correct answer: C. The symptoms describe browser hijacking in which the browser points to a site advertising something.

A is not correct because spyware does not have the set of symptoms described in the question.

B is incorrect because a worm is a self-replicating malware, not something that would have the set of symptoms described in the question.

D is incorrect because a keystroke logger quietly collects keystrokes, it does not hijack your browser.

E is incorrect because a Trojan horse is malware disguised as a benign program, not specifically something that hijacks your browser.

6. Correct answer: C. Worm is malware that installs on a computer without the knowledge or permission of the user, and which replicates itself on the computer or throughout a network

   A is not correct because, while a virus is a program that installs on a computer without the knowledge or permission of the user, the term virus alone does not indicate the ability to replicate itself.

   B is incorrect because utility is not the term used for the type of program described in the question. Many useful programs are included in the utility category.

   D is incorrect because scam is not the term used for the type of program described in the question.

   E is incorrect because spim is not the term used for the type of program described in the question.

7. Correct answer: B. A Trojan horse is a virus hidden inside a seemingly harmless program.

   A is not correct because the term worm describes self-replicating malware, but does not describe malware that is disguised as a harmless program.

   C is incorrect because antivirus is something that fights viruses, not a type of virus.

   D is incorrect because optimizer is not the term used for a virus.

   E is incorrect because a cookie is not a virus, but a file used by a browser to keep track of browsing activity, and it is often a benefit rather than a threat.

8. Correct answer: E. A pop-up blocker inhibits the annoying windows that open when you are browsing the Web.

   A is not correct because a content filter is used to block or allow entire websites based on their known content.

B is incorrect because a firewall is a device or software that examines network traffic, rejecting that which looks dangerous to the network or computer the firewall is protecting.

C is incorrect because an antivirus is a program that protects against virus infections, detects existing virus infections, and removes identified viruses.

D is incorrect because a spam filter examines incoming e-mail messages and filters out those that have characteristics of spam, including certain identified key words.

9. Correct answer: D. Virus infection will cause symptoms such as strange screen messages, sudden computer slowdown, missing data, and inability to access the hard drive.

   A is not correct because war riding does not cause the symptoms described in the question.

   B is incorrect because spam is not associated with the symptoms described in the question.

   C is incorrect because encryption does not cause the symptoms described in the question.

   E is incorrect because fraud is not associated with the symptoms described in the question.

10. Correct answer: B. Firewall is a device that sits between a private network and the Internet (or other network) and examines all traffic in and out of the network it is protecting, blocking any traffic it recognizes as a potential threat.

    A is not correct because a router does not perform the functions listed in the question.

    C is incorrect because a bridge does not perform the functions listed in the questions.

    D is incorrect because a worm is a type of virus, not a device.

    E is incorrect because a keystroke logger is a threat, not a device that offers protection, as described in the question.

11. Correct answer: B. Account lockout threshold is the setting that would cause a message stating that you have been locked out to appear after you have made multiple log-on attempts, exceeding the number of the account lockout threshold.

    A is not correct because a password length setting would not cause the behavior described in the question.

    C is incorrect because account lockout duration controls how long you are locked out after exceeding the account lockout threshold.

    D is incorrect because the maximum password age setting does not come into play in the scenario described in the question.

E is incorrect because complexity requirements do not come into play in the scenario described in the question.

12. Correct answer: A. A rootkit hides itself from detection by concealing itself within the OS code and giving someone administrative access to a computer.
    B is not correct because a pop-up download is a program that downloads to a user's computer through a pop-up page.
    C is incorrect because a drive-by download is a program downloaded to a user's computer without consent when the user takes some action, such as browsing to a website or opening an HTML e-mail message.
    D is incorrect because a worm is malware that replicates itself on the computer or throughout a network.
    E is incorrect because a hoax is a deception, not a type of malware.

13. Correct answer: D. Social engineering is the term used to describe the use of persuasion to gain the confidence of individuals.
    A is not correct because, while a hoax is an example of social engineering in action, it is not the term used to generally describe this type of behavior.
    B is incorrect because fraud is not the term that described the use of persuasion to gain the confidence of individuals, although fraud may be committed through using social engineering.
    C is incorrect because phishing is simply an example of social engineering in action.
    E is incorrect because, while social engineering may employ enticement, that is just part of the scope of social engineering.

14. Correct answer: B. A brute force password cracker simply tries a huge number of permutations of possible passwords.
    A is not correct because a keystroke logger is a hardware device or software that captures all the keystrokes entered at a computer.
    C is incorrect because statistical analysis would be part of a more sophisticated method for stealing passwords.
    D is incorrect because mathematical analysis would be part of a more sophisticated method for stealing passwords.

E is incorrect because phishing is a type of social engineering. While it might be used to obtain someone's password, it does not use the method described in the question.

15. Correct answer: C. IP packet filter is a firewall technology that inspects each packet that enters or leaves the protected network, applying a set of security rules defined by a network administrator; packets that fail are not allowed to cross into the destination network.
    A is not correct because proxy service, while a technology associated with firewalls, does not filter packets, but watches for application-specific traffic and, acting as a stand-in (a proxy) for internal computers, it intercepts outbound connection requests to external servers and directs incoming traffic to the correct internal computer.
    B is incorrect because a VPN is a virtual tunnel created between two endpoints over a network or internetwork. This is achieved by encapsulating the packets.
    D is incorrect because encrypted authentication is the encryption of credentials (user name and password) before they travel over a network.
    E is incorrect because a DMZ is a construct of a network, using two firewalls to protect, first the Internet network, and second a separate portion of that network containing servers to which outside (Internet) users must connect to access services.

Answers to Essay Quiz

Answers will vary.

1. With automatic login anyone who turns on your computer is authenticated using the same credentials you have and has access to everything to which you normally have access. No login dialog box appears requiring someone to enter the credentials. It is done for you. For this reason, you should never enable automatic login on a computer at school or work. You should also consider disabling this on home computers, so that users will be required to login with credentials. You should also require strong passwords.

2. The statement "User Account Control limits the damage that someone can do who accesses your computer when automatic login is enabled" is partially true, as long as the automatic login is using a standard account. In that case, the user will need to provide administrator credentials before performing administrator-level tasks. If the automatic login is using an administrator account, the user will only need to confirm any administrative actions.

However, the real damage lies in the access this person has to all your data. UAC does not protect your data when the user is logged on with your credentials, which is the case with automatic login.

3. You should disable the Guest account because it allows anyone without a user account to access your computer. The amount of damage a user logged in with the guest account can do is somewhat limited: a guest account cannot see anyone else's files and cannot make changes to the system.

4. The use of cookies can be an invasion of privacy because the user may not know they are saved and retrieved, and they may include personal information innocently provided by the user while at a web page. Cookies are saved on the local computer by the browser at the request of a website. First party cookies originate at a web page visited by the user, while third-party cookies originate at another web site (a third party) that places them on the first-party website.

5. A permission is the level of access to a single object (file, folder, or printer) assigned to a user or group. A user right is a system wide action (log on locally, install device drivers) assigned to a user or group.

Solution to Lab Project 2.1

Answers will vary.

1. According to a report released by Javelin Strategy and Research (www.javelinstrategy.com/news/1387/92/1), in February 2013, there were more than 12 million identity fraud victims in the United State in 2012, an increase of more than one million over the previous year, with losses to the victims of over $21 billion. This shows an upward trend since 2010.

   An article published at Security Affairs (securityaffairs.co) in March of 2015 cited a study by Javelin Strategy and Research that estimated that identity fraud cost U.S. consumers $16 billion in 2014, which was less than in 2013. Javelin estimated that 12.7 million U.S. consumers were the victims of identity theft in 2014, down from an estimated 13.1 million U.S. victims in 2013.

   The Javelin estimate is less than that of the Bureau of Justice Statics. In a press release

published in September 2015, the Bureau of Justice Statics (www.bjs.gov) stated that in 2014 17.6 million U.S. residents experienced identity theft.

2. Example A: While this example is a bit dated, it shows how one population (in this case, Asian immigrants) is targeted. In September 2010 arrests were made of members of a large identity theft and fraud ring. They obtained and sold identity documents, which they used to commit credit card, tax, and bank fraud. They obtained the Social Security cards of Asian immigrants who worked in the American territories decades ago but returned to their native countries. They then sold these to individuals who used them fraudulently.
   Example B: In this more recent example (August, 2013) thieves replicated the codes scanned from legitimate credit cards and re-encoded onto other credit cards for fraudulent use. The article, titled *ID-Theft Ring May Have "Thousands of Victims"* appeared on the website for NBC in Southern California (http://www.nbclosangeles.com/news/local/ID-Theft-Ring-Bust-Nets-7-Arrests-219470431.html).

3. Share and discuss your findings with others in your class. For instance, if a student reported on a ring that targeted a certain population, as in Example A, he might observe that this is a different spin on the identity theft we all fear—theft of our personal identities that keeps us from functioning. This type is less likely to be reported because the victims may no longer use their American credentials in their native countries and not notice the theft of their identities.

Solution to Lab Project 2.2

Answers will vary as sites that post this information update it frequently.

In December 2015 Symantec's security intelligence team published a list of predications of cyber threats for 2016.

More malware will target Apple devices running Mac OS X or iOS. While the number of threats against apple operating systems is lower compared to those targeting Windows OSs, they have increased. Users of Apple products should be just as diligent as those using Windows products and enable all possible security protections available to them.

Not exactly an example of a threat, but the increase in the use of biometrics is leading to a reduction in the use of passwords for authentication.

IoT devices present security vulnerabilities. A Gartner report titled *Agenda Overview for the Internet of Things* predicts, "by 2020 close to 30 billion connected things will be in use across a

wide range of industries…" Consumers need to question the security of devices used in their homes and cars.

They predicted an increase in attacks on infrastructure by both terrorists and criminals.

Ransomware will increase. Infected computers normally require drastic means to remove the malware—usually repartitioning and reformatting the system and reinstalling the OS.

More malware will target mobile devices. Users should enable encryption for all data communications.

Solution to Lab Project 2.3

Answers will vary depending on the student's research at a point in time.

Following is a partial list of security degrees and certifications offered in the United States:

Degree or Certification	**Source**	**Description**
Undergraduate Certificate in Cybersecurity	American Public University	Online certificate program
Bachelor of Science in Cybersecurity	American Public University	Online degree program
Master of Science in Cybersecurity Studies	American Public University	Online degree program
Graduate Certificate in Cybersecurity, Law, and Policy	Drexel University	Online graduate certificate program
CompTIA Security+	CompTIA	Entry-level security certification. Single exam.
Certified Ethical Hacker (CEH)	International Council of Electronic Commerce Consultants (EC-Council)	Five-day CEH course. Self-study candidates must pay an additional fee and submit Exam Eligibility Application prior to exam. Single exam.
GIAC Security Essentials (GSEC)	SANS GIAC	Entry-level security certification. Single exam.
Certified Information Systems Security Professional (CISSP)	International Information Systems Security Certification Consortium $(ISC)^2$ "ISC-squared"	Certification for experienced security professional (minimum of 5 years' appropriate experience).
Certified Information Security Manager (CISM)	Information Systems Audit and Control Association (ISACA)	Advanced certification.

The following are two security certifications: Security+ by CompTIA and Certified Information Systems Security Professional (CISSP) by International Information Systems Security Certification Consortium, Inc. (ISC).[2]

Security+

The CompTIA Security+ certification is a vendor-neutral certification of competency in system security, network infrastructure, access control, and organizational security. A candidate should have the CompTIA Network+ certification and two years of technical networking experience, with an emphasis on security. This certification is recommended to IT professionals who need to prove that they are current on these security areas. The domains in the 2011 version of the exam are:

- Network Security
- Compliance and Operational Security
- Threats and Vulnerabilities
- Application, Data, and Host Security
- Access Control and Identity Management
- Cryptography

Certified Information Systems Security Professional (CISSP)

Certified Information Systems Security Professional (CISSP) is a vendor-neutral certification. The certifying organization is International Information Systems Security Certification Consortium, Inc. (ISC)^2. Someone taking this exam should have at least five years' experience in information systems security. The target audience for this exam is a mid- to senior-level manager seeking a position such as CISO (chief information security officer), CSO (chief security officer), or senior security engineer. The exam domains include the following:

- Access Control
- Application Development Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security Governance and Risk Management
- Legal, Regulations, Investigations, and Compliance

- Operating Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security

Chapter 2

Computer Security Basics

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Learning Outcomes

- Describe security threats and vulnerabilities to computers and users
- Identify methods for protecting against security threats
- Troubleshoot common security problems

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Threats to Computers and Users

LO 2.1

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Introduction

Risks

- Identity
- Users' data
- Employer's integrity
- Job loss
- Violation of government regulations
- Cybercrime

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Malware
  - Short for “malicious software”
  - Large and growing list of threats
  - Malware development an industry

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Vectors
  - Social networking
  - Email
  - Malicious code on websites
  - Trojan horses

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Social Networking Is a Possible Vector

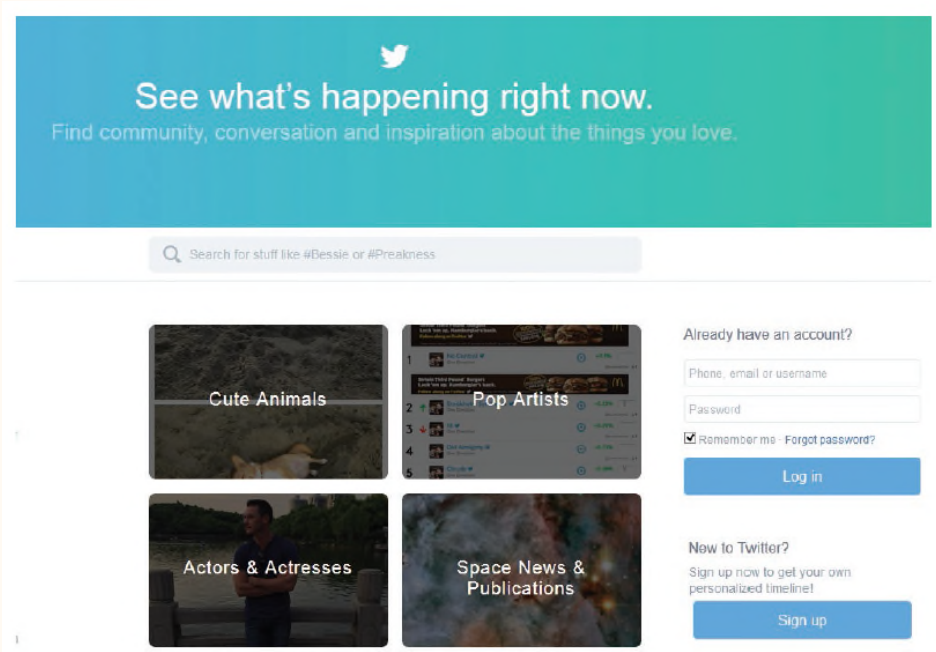


FIGURE 2–1 The Twitter home page.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Vectors (continued)
  - Searching for unprotected computers
  - Sneakernet—the oldest vector
  - Back doors
  - Rootkits

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Vectors (continued)
  - Pop-up downloads
  - Drive-by downloads
  - War driving
  - Bluesnarfing

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

War Driving Is a Vector

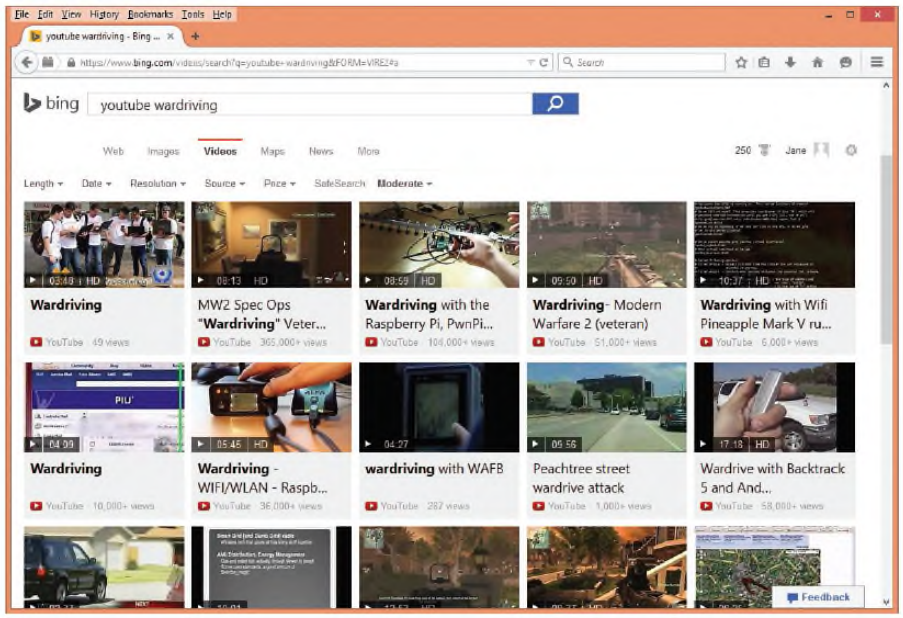


FIGURE 2–2 Online videos show examples of war driving.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods: Password Theft

- Stealing passwords through websites
- Stealing passwords with password crackers
- Stealing passwords with keystroke loggers

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods: Zero-Day Exploits

- Exploit is a malware attack
- Zero-day exploit
  - Uses a vulnerability unknown to publisher
  - Difficult to prevent

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods: Viruses

- Installed and activated without user knowledge
- Wide range of symptoms

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods: Worms

- Virus that replicates itself
- Network-aware
  - Examples
    - Netsky
    - MyDoom
    - Nimda

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods: Botnets and Zombies

- Botnet
- Zombie
- Botherder

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods: Spyware

- Gathers information
- Sends information to requestor
  - Marketing
  - Industrial espionage
  - Law enforcement
  - Terrorism

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods: Adware

- A type of spyware
- Sends information to requester
  - Marketing
  - Industrial espionage
  - Law enforcement
  - Terrorism

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods: Browser Hijacking

- Changes to unrequested Web page
- May be persistent
- Change home page in Internet Options

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods: Spam and Spim

- Spam – unsolicited email
- Spim – unsolicited instant message

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods: Social Engineering

- Use of persuasion to gain confidence
- Used for good and bad
- Seeking confidential information

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Social Engineering
  - Fraud
    - Identity theft
    - Ransomware

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Social Engineering (continued)
  - Phishing
    - Fake Message is “bait” to receive information
    - Spear phishing is targeted
    - Forged email address for email spoofing

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Social engineering (continued)
  - Hoaxes
    - Deceptions
    - Fake message from friend in trouble

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Social Engineering (continued)
  - Enticements to open attachments
    - May appeal to base human characteristics
    - May appeal to sympathy and compassion
    - Opening attachment infects computer

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Social Engineering (continued)
  - Identity Theft
    - Stolen personal information used fraudulently
    - Existed before computers
    - Expanded by consumer computer use
    - Information at www.idtheft.gov

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Identity Theft

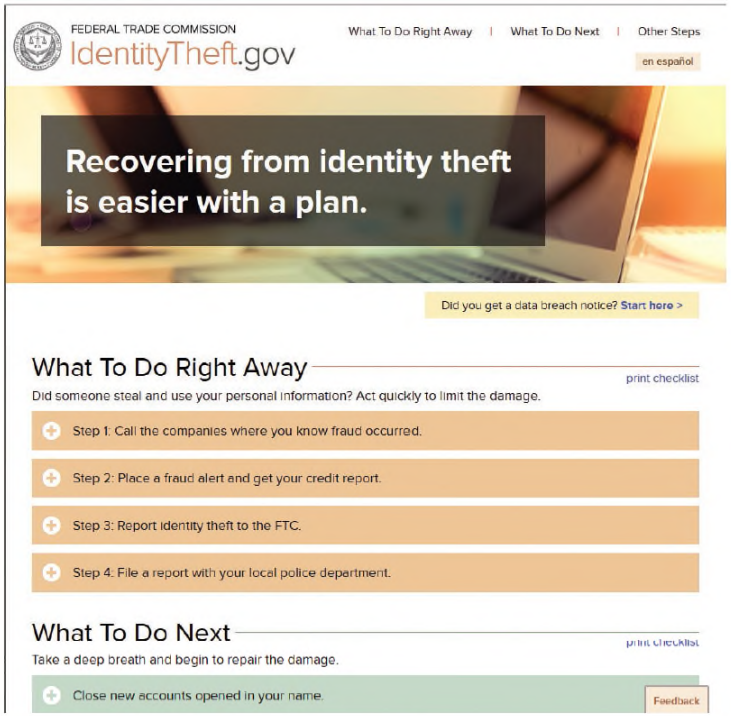


FIGURE 2–3 The FTC Identity Theft Web page.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Exposure to Inappropriate or Distasteful Content
  - Individual judgement for adults
  - Harmful to young children

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Invasion of Privacy
  - Personal financial information
  - Health information
  - Physical security
  - Shoulder surfing

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Misuse of Cookies
  - Provide convenience to user
  - Contain browsing and shopping information
  - First-party cookie
  - Third-party cookie

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Malicious Tools and Methods

- Computer Hardware Theft
  - Mobile devices targeted
  - Information more valuable than hardware

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Accidents, Mistakes, and Disasters

- Accidental erasure of data
- Fires, earthquakes, weather-induced disasters
- Protect data with backups

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Keeping Track of New Threats

- Federal Trade Commission (FTC)
- Bureau of Consumer Protection (www.ftc.gov/bcp/)

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Keeping Track of New Threats

FIGURE 2–4 The FTC Bureau of Consumer Protection website.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

The People Behind the Threats

- Cybercriminals
- Organized Crime
- Cyberterrorists
- Hackers
- Crackers
- Script Kiddies
- Click Kiddies
- Packet Monkeys

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Defense Against Threats

LO 2.2

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Education

Signs to look for

- Strange screen messages
- Sudden computer slowdown
- Missing data
- Inability to access the hard drive

Symptoms of identity theft

- Unknown charges on credit accounts
- Accounts opened without your knowledge
- Unexplained credit rejections
- Credit report shows strange accounts

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Education

- Reliable Sources of Security News
  - ZDNet Zero Day Weekly
  - www.schneier.com
  - A healthy dose of paranoia

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Policies

- Describe how to protect and manage data
- Define data sensitivity and security classifications
- List security practices
- Specify who can assess each class of data
- Security policy document and implementation

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Windows Local Security Policy

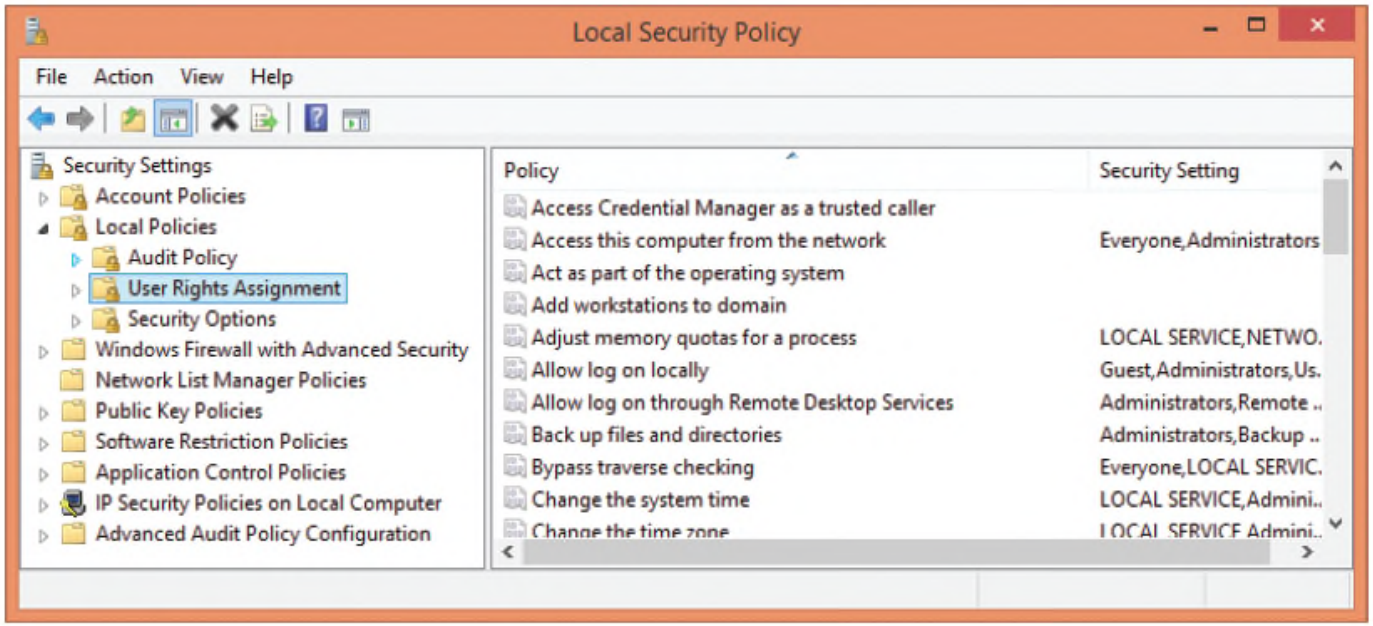


FIGURE 2–5 The Windows Local Security Policy console.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Firewalls

- Software or hardware devices
- Examine network traffic
- Allow/disallow entry based on rules
- Network-based firewall protects a network
- Personal firewall protects a computer

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Table 2-1 Firewall Technologies

Technology	Description
IP packet filter	Inspects each packet entering or leaving the network. Applies security rules. Will not allow failed packets through firewall.
Proxy service	Watches for application-specific traffic. Web proxy examines Web browser traffic. Intercepts outbound connection request and directs incoming traffic to correct computer. May block specific domains or addresses.
Encrypted authentication	External users authenticate before getting access.
Virtual private network (VPN)	Not true firewall technology. A virtual tunnel between two endpoints over one or more networks.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Network-Based Firewalls

- Hardware between networks
- Examines all traffic
- Blocks recognized threats
- Sophisticated firewalls require trained technicians
- Simple firewalls for homes or small offices

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Firewalls for Home or Small Business

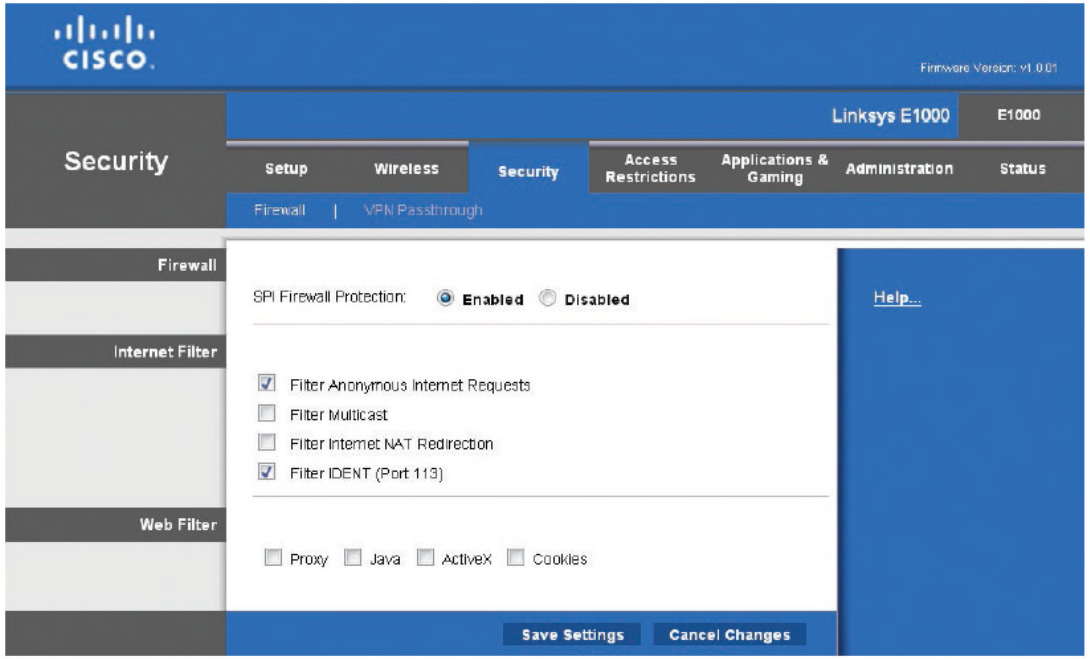


FIGURE 2–6 The Security page from a Cisco Wireless Router's configuration utility.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

A Private Network behind a Firewall

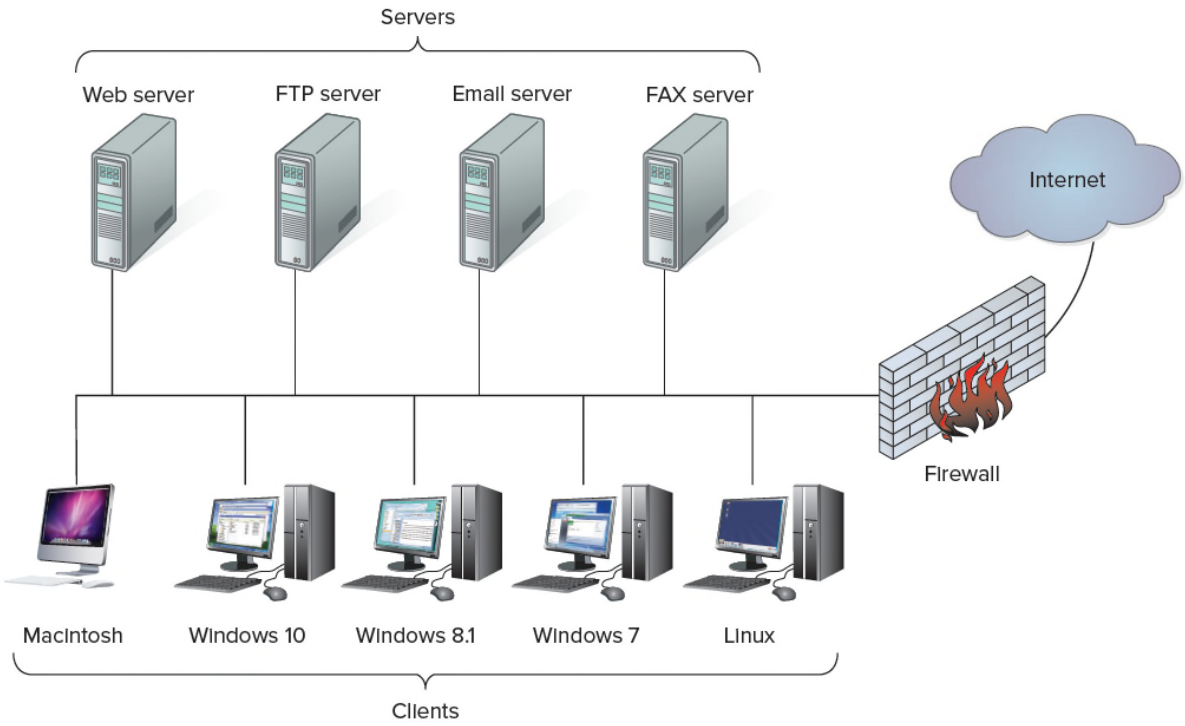


FIGURE 2–7 A private network protected by a firewall.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Personal Firewalls

- Protects against attacks within private network
- Included with Windows, OS X, and Linux

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Windows Firewall

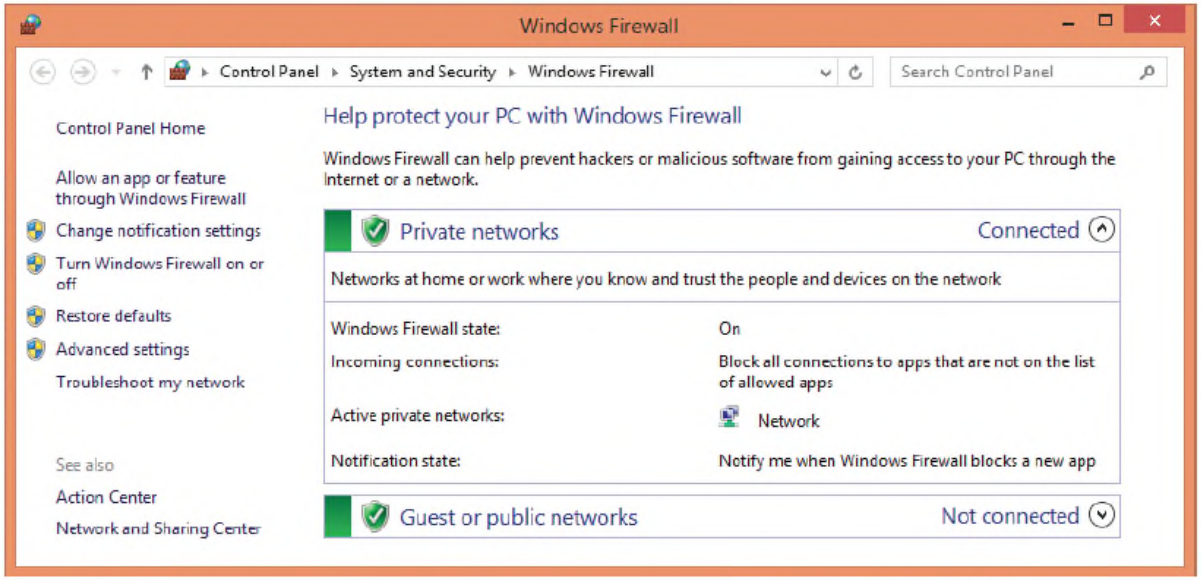


FIGURE 2–8 The Windows Firewall Control Panel.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Windows Firewall with Advanced Security

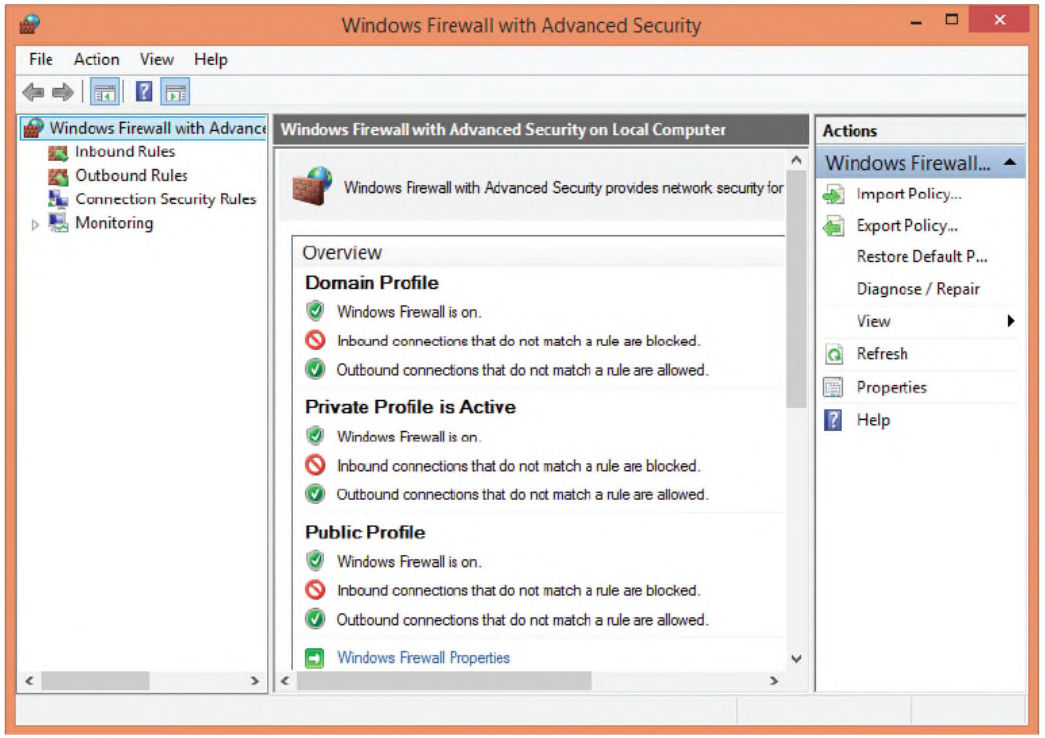


FIGURE 2–9 Windows Firewall with Advanced Security console.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Software

- Antispam Software
- Antivirus Software
- Pop-Up Blockers
- Privacy Protection and Cookies
- Parental Controls and Family Safety
- Content Filtering
- Software Updates

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Software

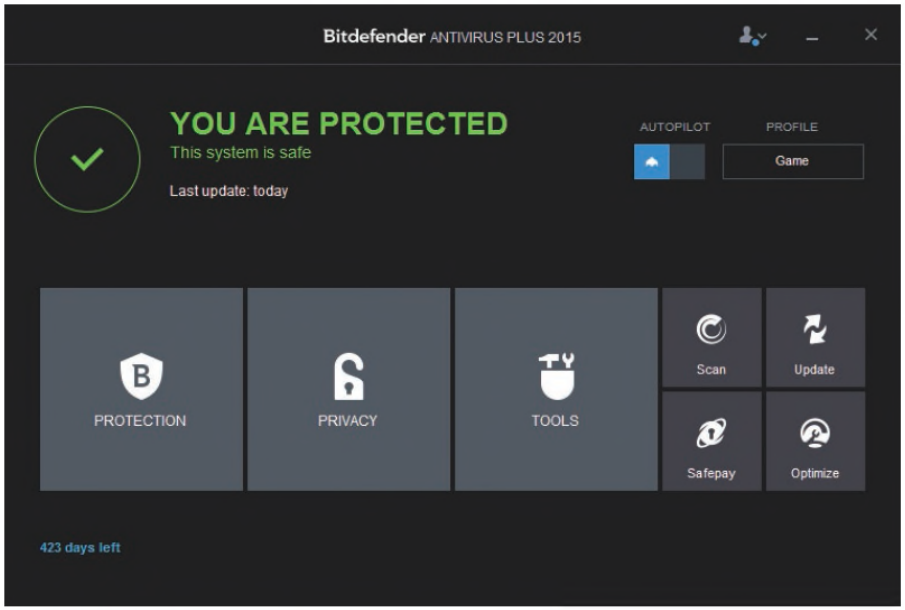


FIGURE 2–10 Security software with many bundled components.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Software

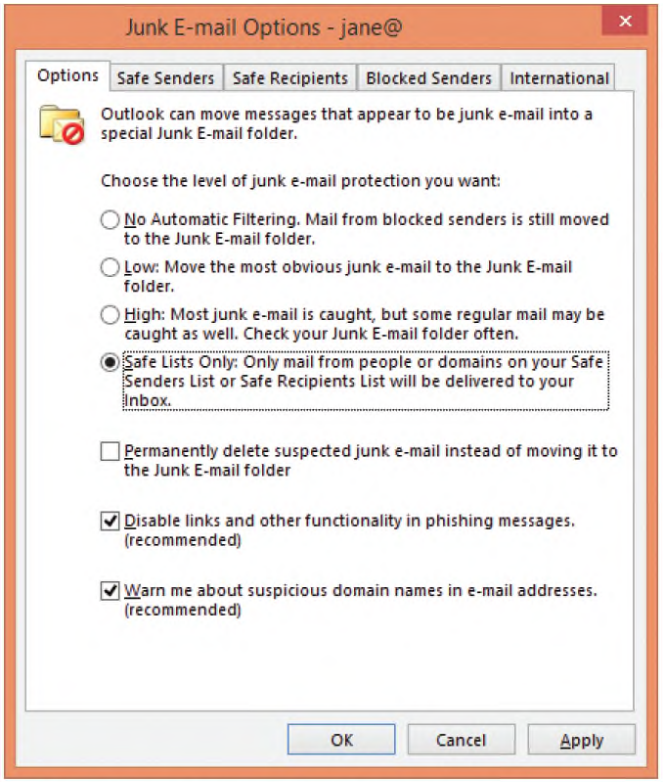


FIGURE 2–11 The Outlook Junk Email Options page.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Software

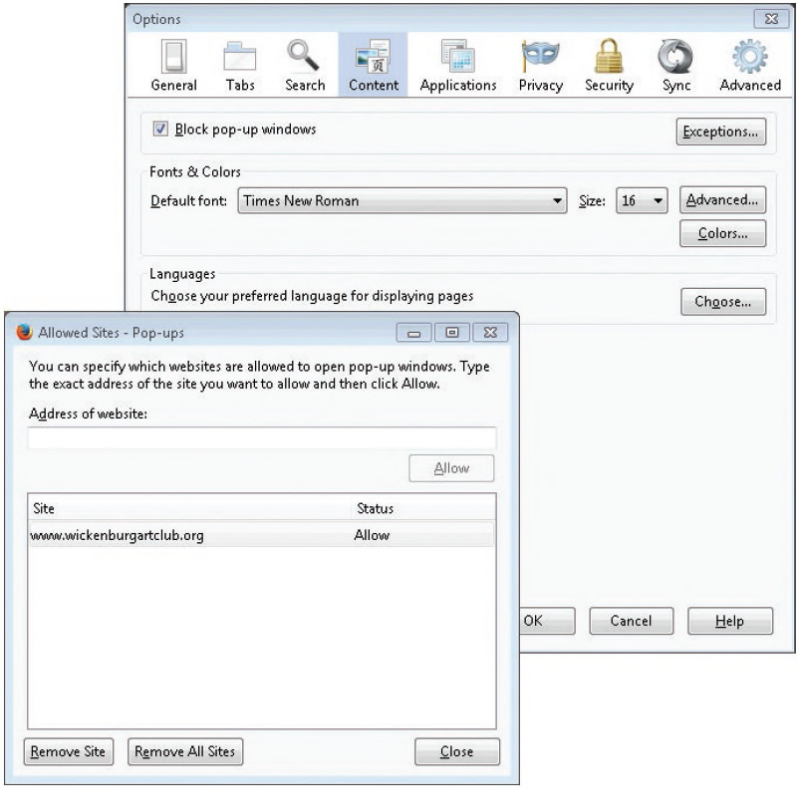


FIGURE 2–12 The Firefox Pop-Up Blocker Exceptions page.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Software

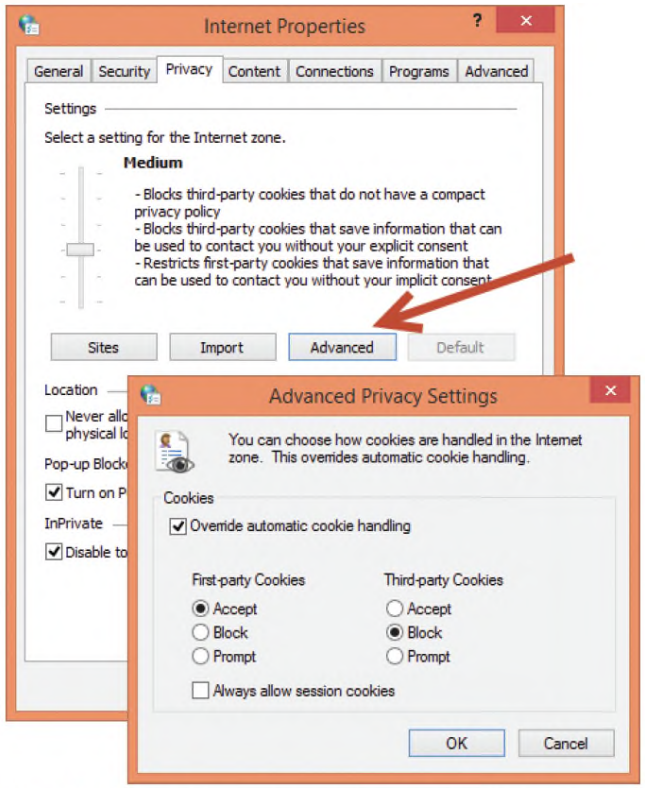


FIGURE 2–13 Use the Advanced Privacy Settings in Internet Options to control the use of cookies.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Software

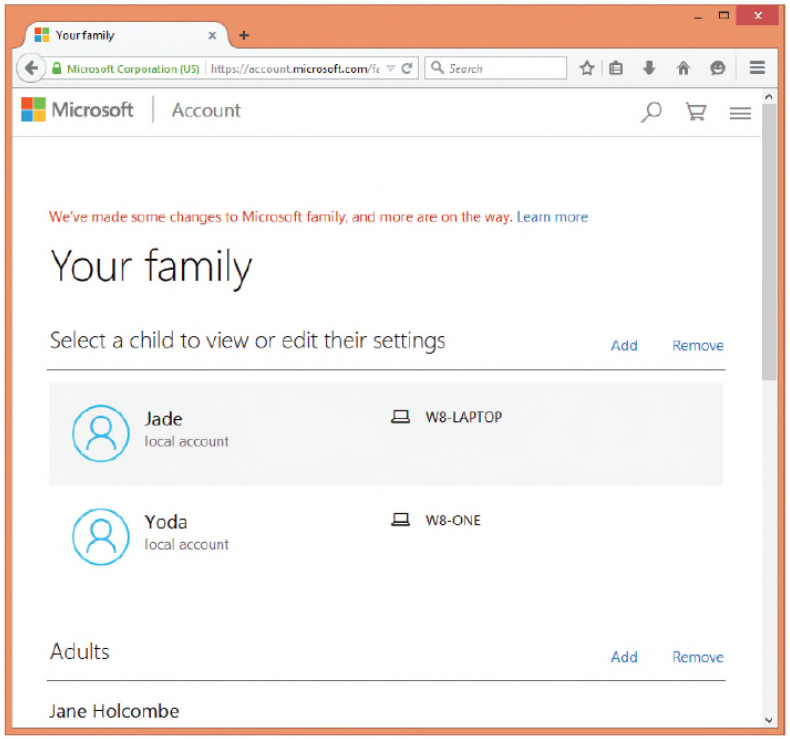


FIGURE 2–14 The Family Safety website.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Software

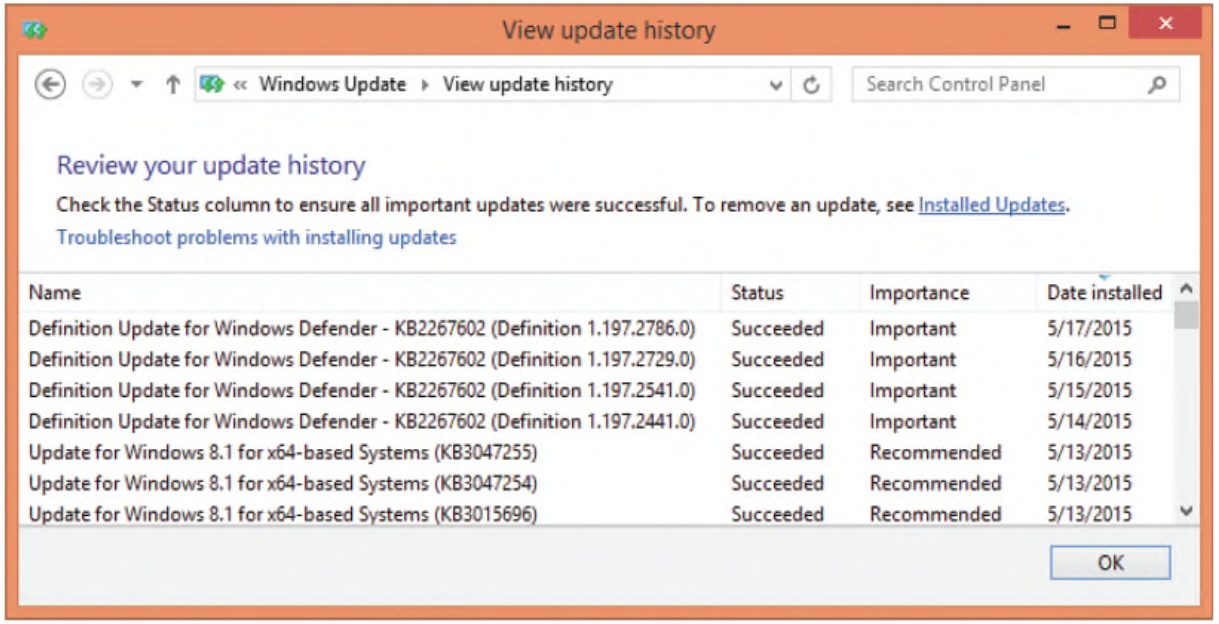


FIGURE 2–15 Windows Update maintains a list of updates.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Authentication and Authorization

Authentication

- Verifies identity
- One-factor: something you know
- Two-factor:
  - Something you know (password)
  - Plus something you have (token)
- Three-factor:
  - Plus biometrics

Authorization

- Give level of access to resource
- Authentication plus access verification
- Permission is level of access to resource
- User right is a system-wide action

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Passwords

- Authenticate with identifier plus password
- Use unique password for each service
- Central to secure authentication
- Create strong passwords
- Password manager creates and stores passwords

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Account Basics

- Security account can be assigned permission to take actions
- May identify a single entity: person or computer
- May identify a group of entities

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Account Basics

- User Accounts
  - Each assigned to a single person
  - Contains user name and password
  - May contain additional information
    - User's full name
    - Description
    - Email address, department, phone number, etc.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Account Basics

- Built-In User Accounts
  - Super user
    - Windows Administrator (disabled by default)
    - OS X and Linux root
  - Guest account
    - Least privileged
    - Disabled in Windows
    - No password needed

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Account Basics

- Standard User Account
  - Windows Standard User Account for ordinary user
  - Windows child account = Standard account with restrictions
  - Can change password and other personal settings
  - Cannot do systemwide administrative tasks

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Account Basics

- Administrator Account Type
  - Can perform systemwide tasks
  - First account created in Windows is administrator type
  - That account can create both types of accounts

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Accounts

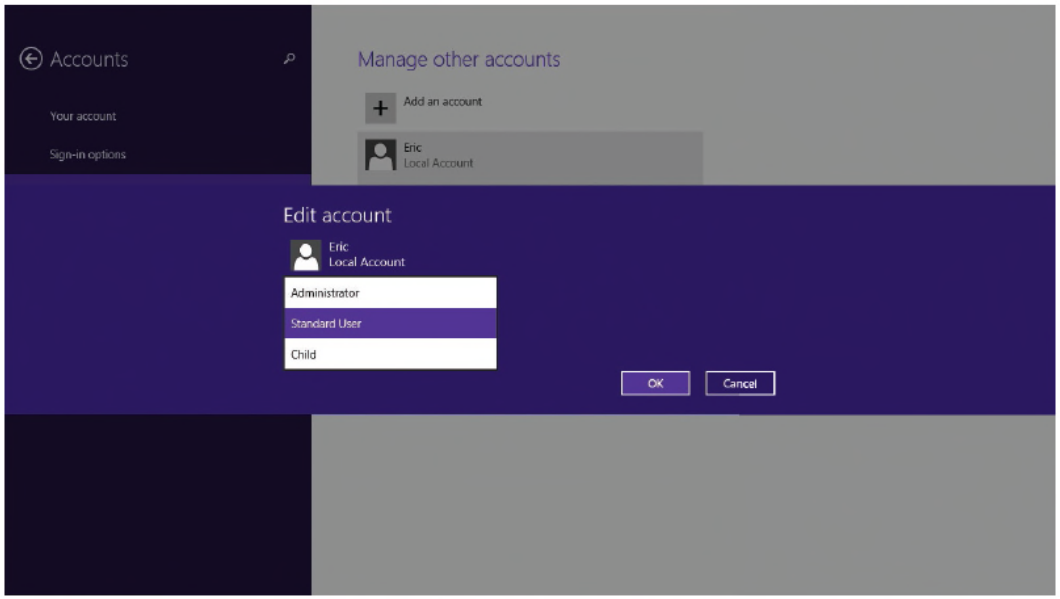


FIGURE 2–16 An administrator account can create accounts, assigning a type to each account.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Account Basics

- Group Accounts
  - Contains user accounts
  - May contain other groups
  - Windows Groups
    - Administrators
    - Users
    - Guests
    - Others created when services and apps install

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Account Basics

- Windows Groups
  - Administrators
  - Users
  - Guests
  - Others created when services and apps install

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Accounts

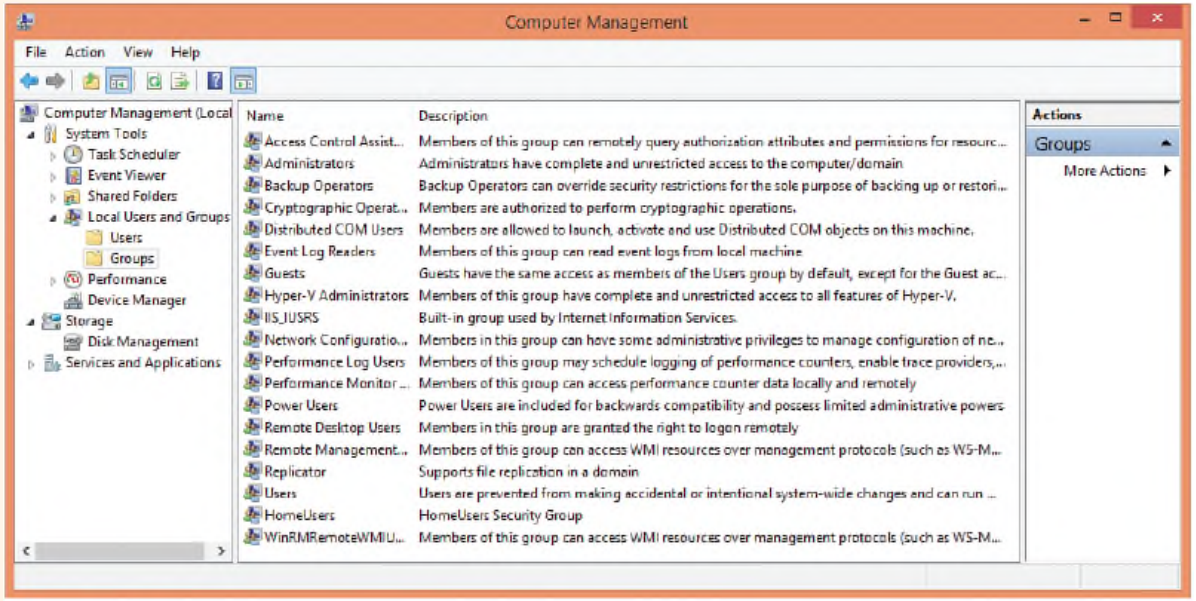


FIGURE 2–17 The Local Users and Groups node in Computer Management showing all groups on the local computer.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Account Basics

- Computer Accounts
  - Within security database on network server
  - Computers in Windows Active Directory Domain

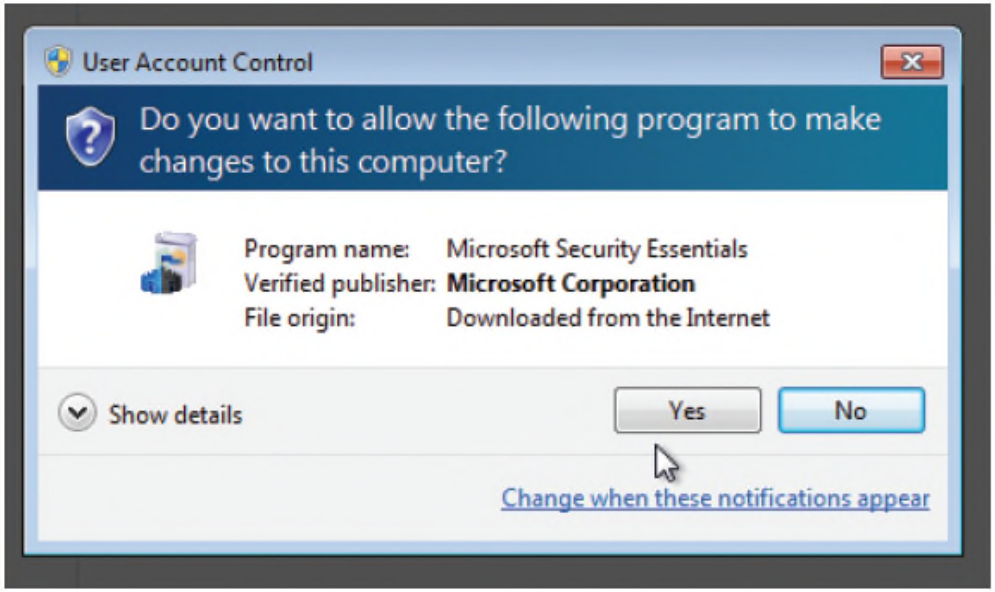
© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Account Basics

- User Account Control
  - Prevents unauthorized changes to Windows
  - Administrative user responds to Consent Prompt
  - Standard user responds to Credentials Prompt

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

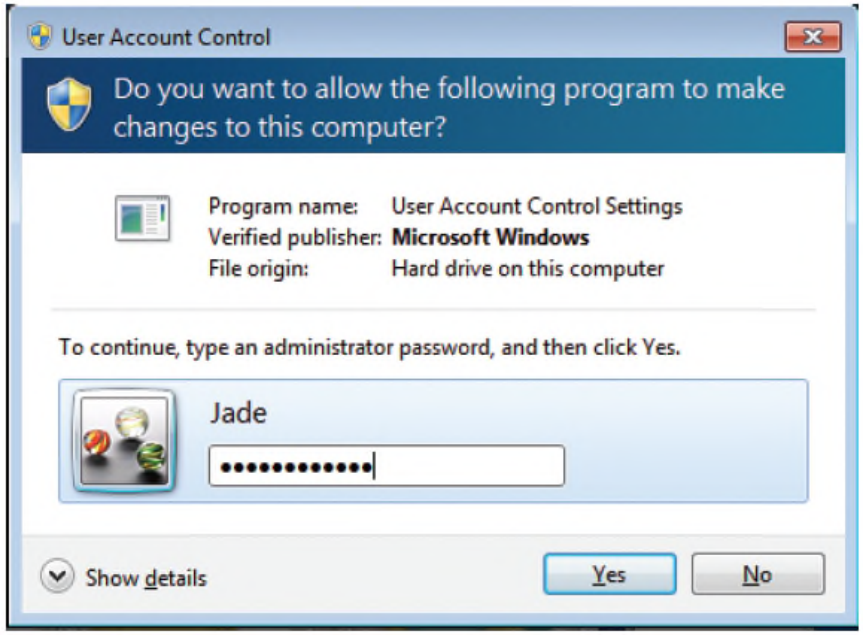
Security Accounts



The Windows 7 User Account Control Consent Prompt.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Accounts



The Windows 7 User Account Control Credentials Prompt.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Account Basics

- OS X "User Account Control"
  - Subtle
  - Dialog boxes for advanced settings locked
  - Unlock with username and password

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security Accounts

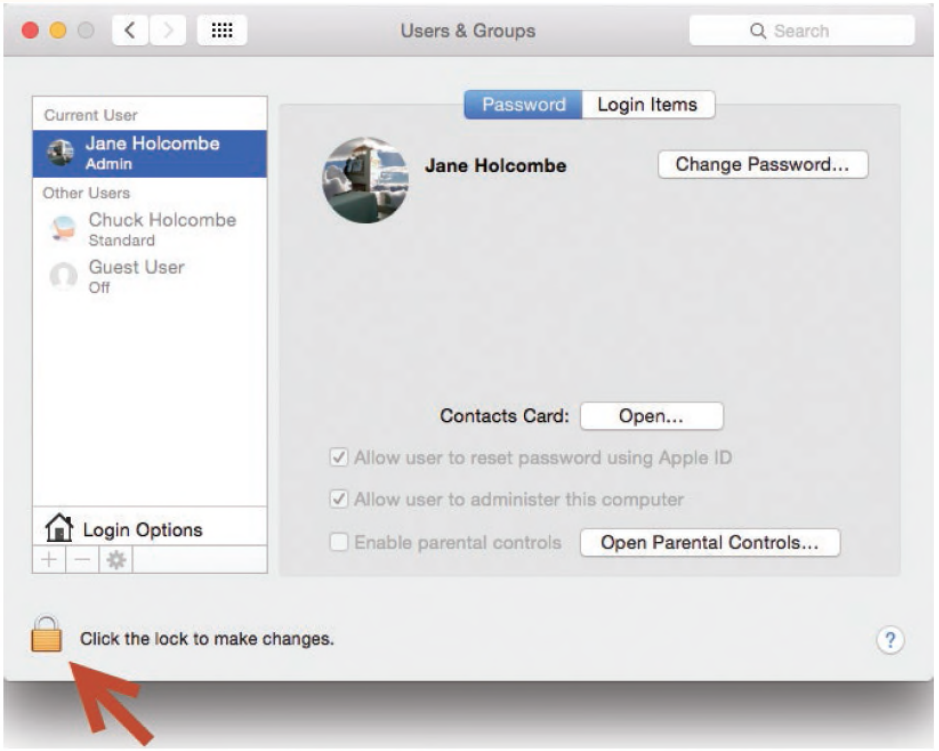


FIGURE 2–18 Unlock a dialog box in OS X to access advanced settings.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Best Practices When Assigning Permissions

- Rule of least privilege
  - Apply to each user or group
  - Do not give more access than required

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Best Practices with User Names and Passwords

- Examine your habits
  - Too many passwords to remember
  - Using same password for multiple services
  - Password written in plain site
  - Keeping same password for many months

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Best Practices with User Names and Passwords

- Protect your user name and password
- Create strong passwords
- Avoid creating unnecessary online accounts
- Never reuse passwords
- Don’t provide more information than necessary

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Encryption

- Transformation of data into cypher text
- Secret key used to decipher
- Digital certificate file may contain secret key

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Encryption

- Encrypting network traffic
  - Secure HTTP (HTTPS)
  - Secure Sockets Layer (SSL)

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Encryption

- Windows Encrypting File System
  - Requires NTFS
  - Encrypts selected files and folders

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Windows Encrypting File System

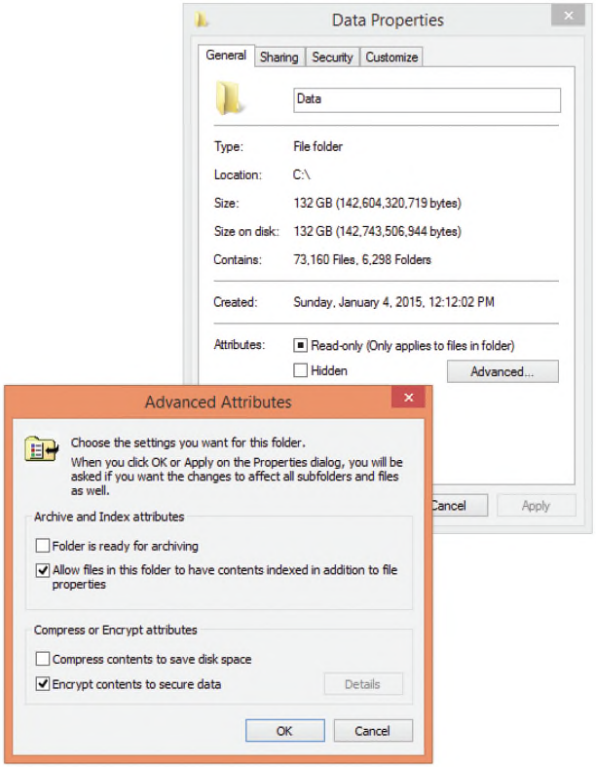


FIGURE 2–19 Turn NTFS encryption on or off using the Properties of a folder.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Encryption

- Encrypting with Windows BitLocker Drive Encryption
  - Encrypts an entire drive
  - Feature of Windows 7 Ultimate and Enterprise
  - Feature of Windows 8.x Pro and Enterprise editions
  - Feature of Windows 10 Pro and Enterprise editions

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Encryption

- Encrypting with OS X FileVault
  - Encrypts an entire drive
  - Encrypt using Security & Privacy in System Preferences

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

OS X FileVault

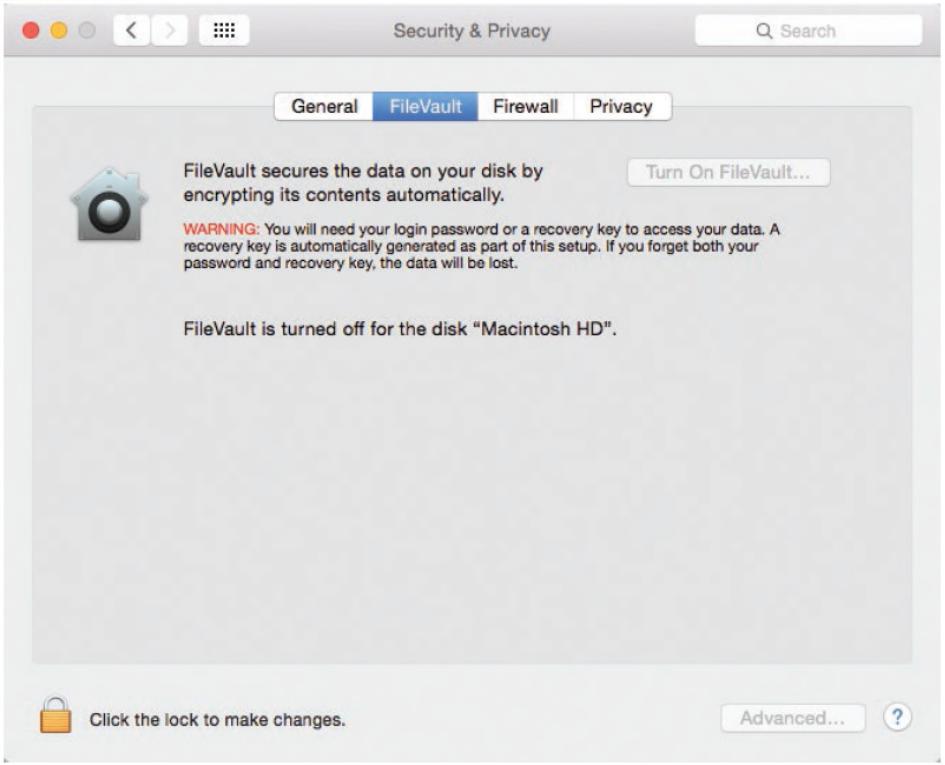


FIGURE 2–20 Configuring FileVault in OS X.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Data Wiping

- Beyond simple delete
- Reformat does not wipe data
- Data wiping software overwrites
  - Apply to entire volume or portions
  - Possible on any rewritable media
  - Secure Erase is government-approved standard

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Physical Security

- Limit access to building or rooms
- Defined in organization's security policy
- Modes of limiting physical access
  - Guarded entrance
  - Confirmation of credentials
  - Key card access

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Security for Mobile Computer

- Be extra wary of the danger of theft
- Encrypt sensitive and confidential data

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Troubleshooting Common Security Problems

LO 2.3

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Troubleshooting Log-On Problems

- Caps Lock key turned on
- Too Many Log-On Attempts
  - Account policy *account lockout threshold*
  - Account lockout duration

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Error Messages

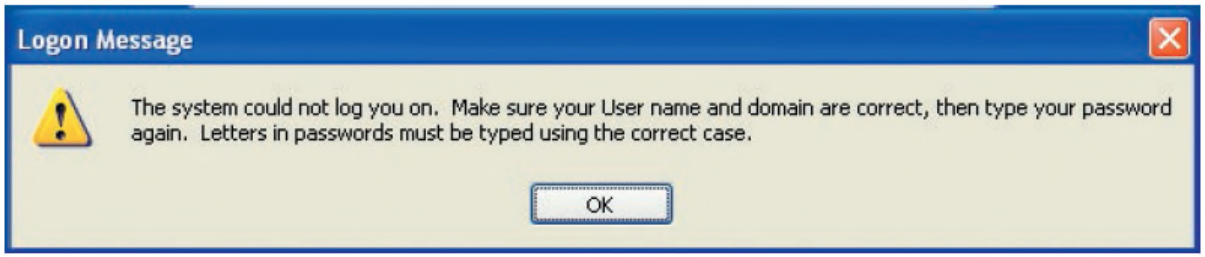


FIGURE 2–21 Log-on error message.

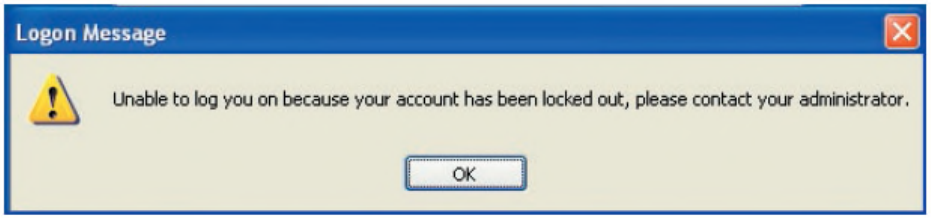


FIGURE 2–22 Log-on lockout message.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Windows Account Lockout Policy

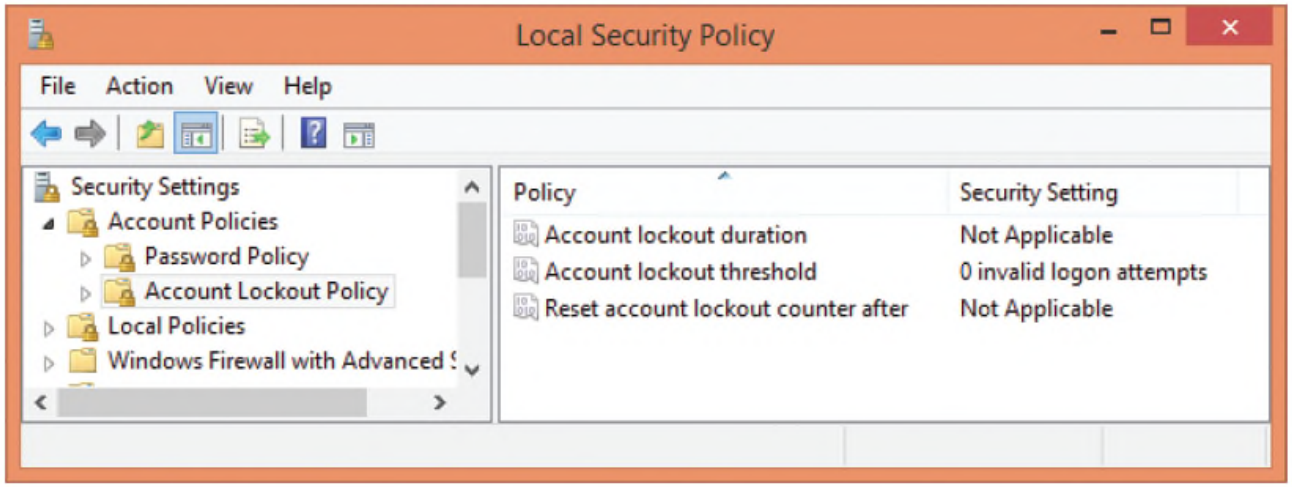


FIGURE 2–23 The Windows Account Lockout policy, where an administrator can set values for lockout duration, threshold, and a period of time after which the counter resets.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Using the Administrator Account in Troubleshooting

- Administrator account disabled by default
- Safe Mode enables Administrator
  - Only on non-member computer of Active Directory domain
  - Log on and troubleshoot
  - Only necessary if user account not administrator type

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Windows Administrator Account

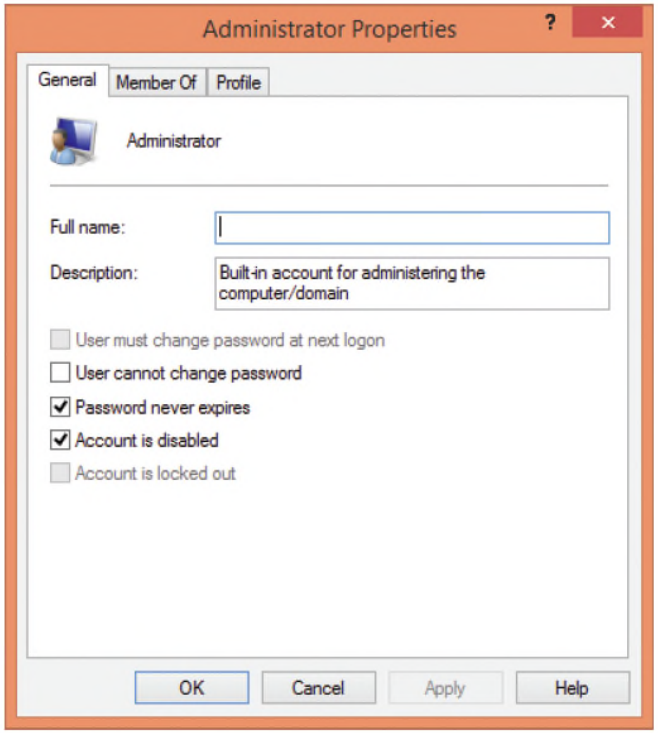


FIGURE 2–24 The Properties dialog box for the Administrator account shows it is disabled by default.

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Troubleshooting a Suspected Malware Attack

- Scan drives and memory with antivirus program
- Use online virus scanner

© 2017 by McGraw-Hill Education. This proprietary material solely for authorized instructor use. Not authorized for sale or distribution in any manner. This document may not be copied, scanned, duplicated, forwarded, distributed, or posted on a website, in whole or part.

Visit TestBankDeal.com to get complete for all chapters