COURSE TECHNOLOGY
CENGAGE Learning

A+ Guide to Managing and Maintaining Your PC, 7e

Chapter 19
Security Essentials

Objectives

- Learn why it is important to comply with established security policies
- Learn ways to authenticate and classify users so that you can control who has access to your resources and what users can do with them
- Learn about additional methods you can use to protect resources
- Learn how to monitor and maintain the security measures you have implemented

Comply With Security Policies

- Factors influencing implementation
  - Free to decide, legal requirements, value added
- Security standards
  - International Organization for Standardization
  - National Institute of Standards and Technology
  - Health Insurance Portability and Accountability Act
- Security goals
  - Protect resources
  - Avoid interference with system functions

Comply With Security Policies (cont'd.)

- Security plan implementation
  - Plan-Do-Study-Act (PDSA)

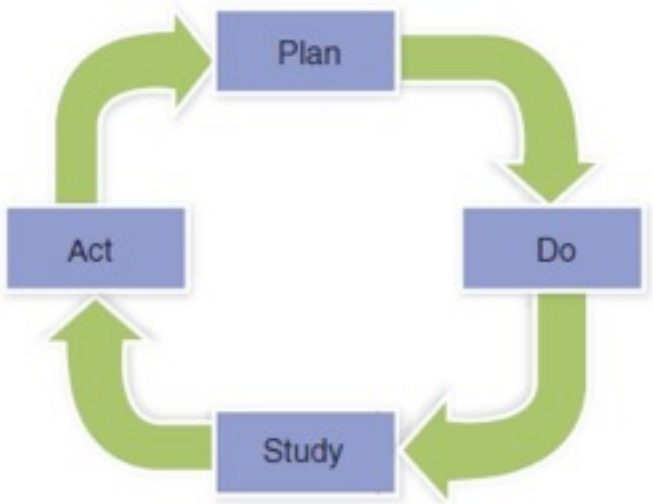

Figure 19-2 A four-step plan to develop a system for an organization. Courtesy: Course Technology/Cengage Learning

Controlling Access to Secured Resources

- Controlling access in Windows
  - Authentication
    - Proves that an individual is who he says he is
  - Authorization
    - Determines what an individual can do in the system after authentication
  - Physical security in place is also required

Authenticate Users

- Local computer and network users
  - BIOS settings control computer access
  - Local user account login to Windows
- Large networks
  - Domain controllers manage network authentication
- Most common authentication method
  - Password
- Other methods
  - Biometric data
  - smart cards

Authenticate Users (cont'd.)

- Authenticate users in Windows
  - Control access with account password
    - Provides ability to change password at any time
  - Control log on methods
    - User clicks name and enters password from Welcome screen (malware can intercept)
    - User presses Ctrl+Alt+Del to get to logon window (more secure method)

Authenticate Users (cont'd.)

- Updating Windows Vista to use Ctrl+Alt+Del logon
  - Enter netplwiz in Start Search box, press Enter
  - Respond to UAC box: User Accounts box appears
    - Click Advanced tab, check Require users to press Ctrl+Alt+Delete, click Apply and close box

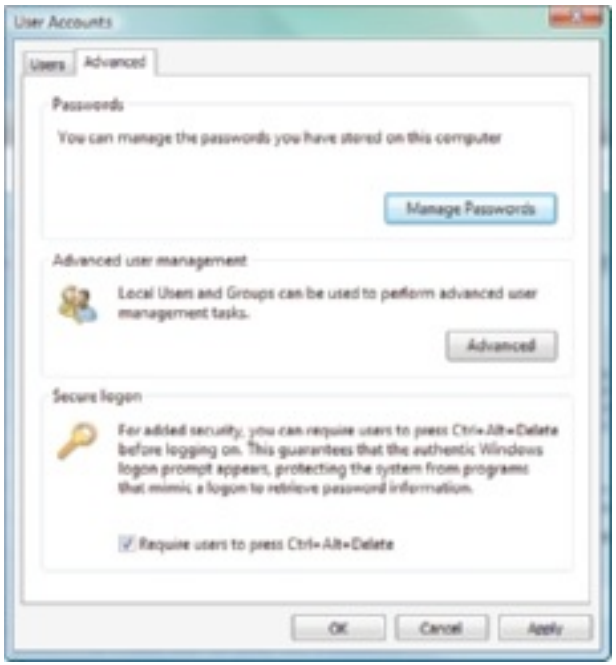

Figure 19-4 Change the way users log onto Vista. Courtesy: Course Technology/Cengage Learning

Authenticate Users (cont'd.)

- Updating Windows XP to use Ctrl+Alt+Del logon
  - Open Control Panel, open User Accounts applet
  - Click Change the way users log on or off
    - User Accounts window opens
    - Make appropriate changes

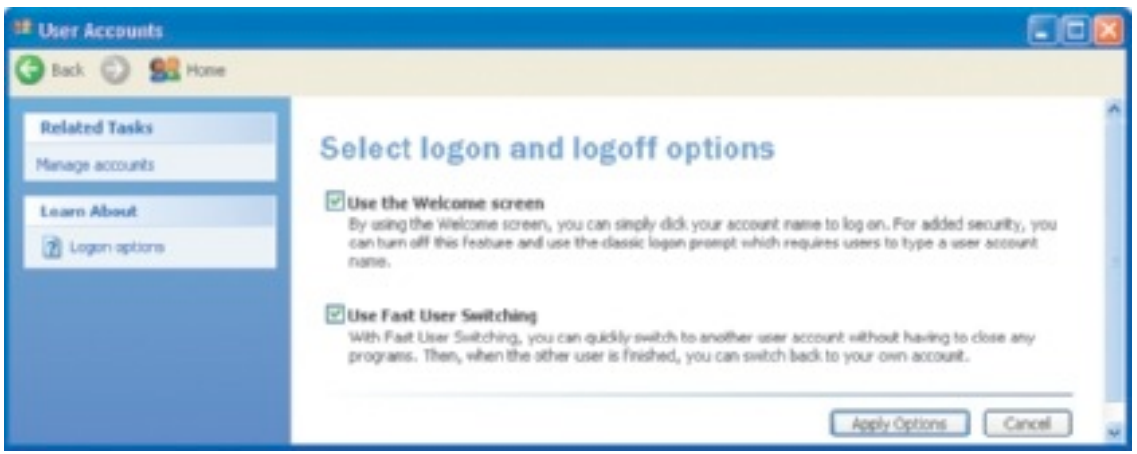

Figure 19-5 Options to change the way Windows XP users log on or off. Courtesy: Course Technology/Cengage Learning

Authenticate Users (cont'd.)

- Forgotten password
  - Administrator can reset password
  - Vista Business/Ultimate or XP Professional
    - Use Computer Management console
  - All versions of Vista or XP
    - Use a Control Panel applet
  - Password reset issue
    - Operating system locks user out from encrypted e-mail or files and stored Internet passwords
    - Solution: password reset disk

Authenticate Users (cont'd.)

- Creating a password reset disk
  - Open the User Accounts window in Control Panel
    - Vista: click Create a password reset disk
    - XP: click Prevent a forgotten password

Figure 19-8 Create a password reset disk
Courtesy: Course Technology/Cengage Learning

Authenticate Users (cont'd.)

- Authenticate users with BIOS settings
  - Power-on passwords
    - Supervisor password and a user password
    - Assigned in BIOS setup and kept in CMOS RAM
    - Prevents unauthorized access to computer and/or to BIOS setup utility
    - Use security screen to set passwords
      - Under boot menu or security menu options
    - Requested by the system when powering up

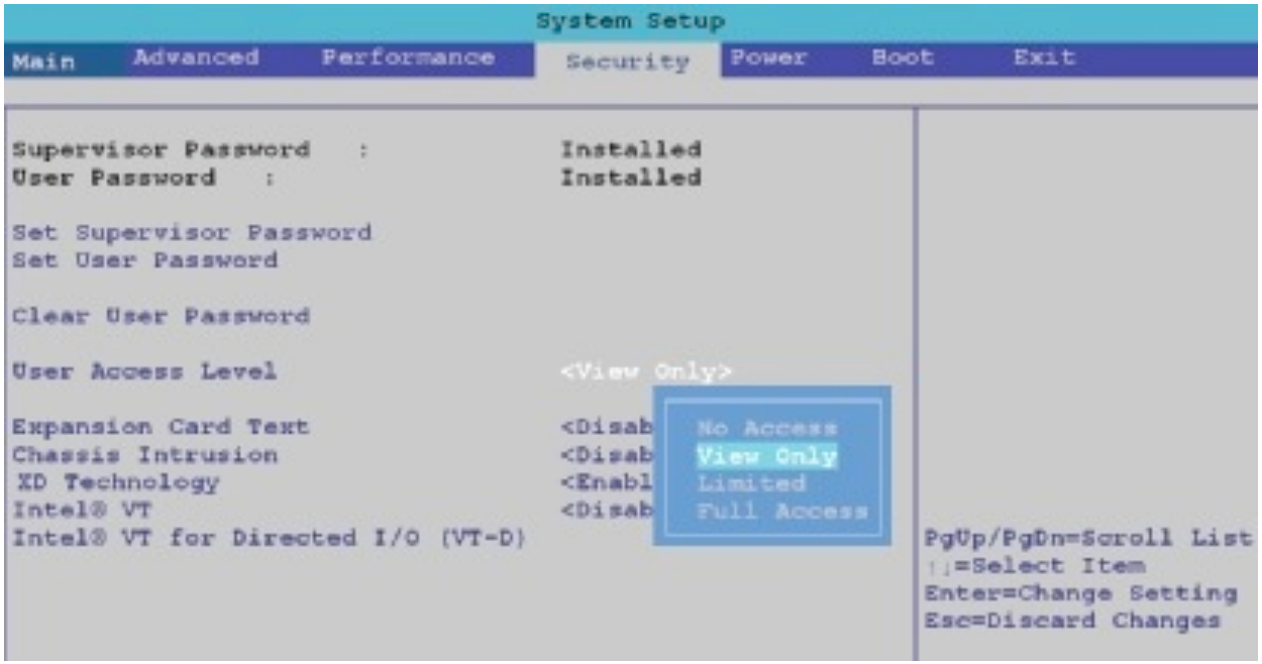

Figure 19-9 Set supervisor and user passwords in BIOS setup to lock down a computer. Courtesy: Course Technology/Cengage Learning

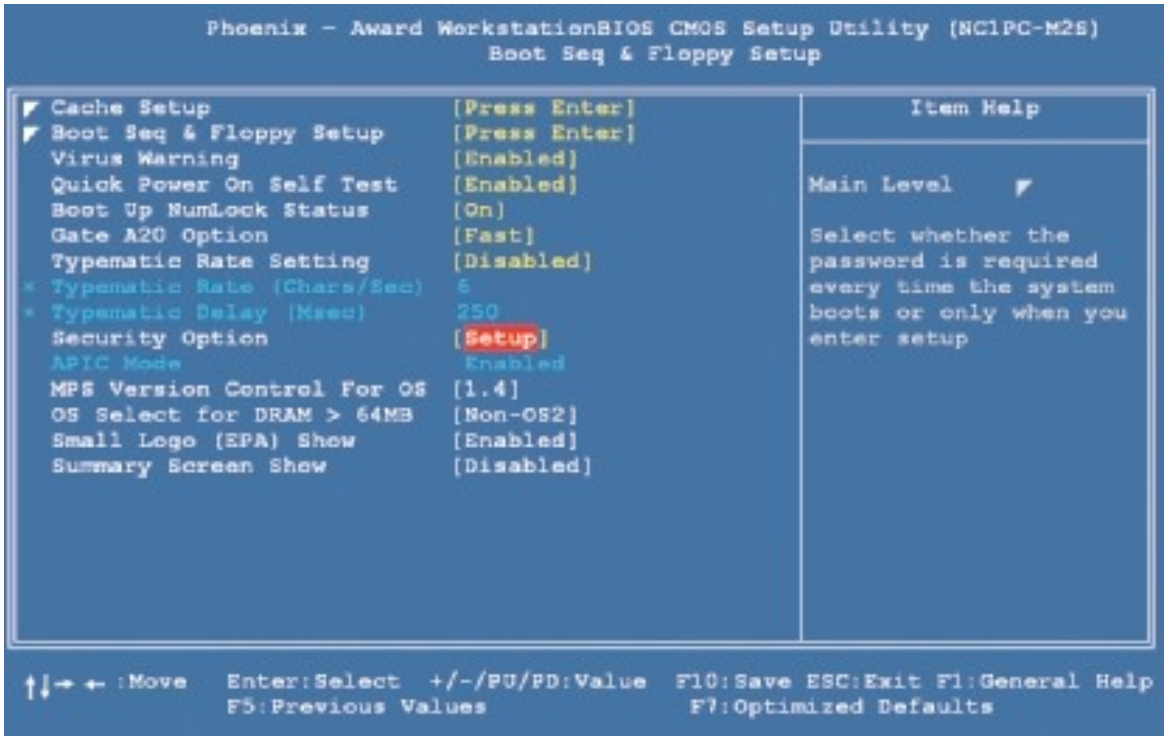

Figure 19-10 Change the way a user password functions to protect the computer. Courtesy: Course Technology/Cengage Learning

Authenticate Users (cont'd.)

- Authenticate users with BIOS settings (cont'd.)
  - Drive lock password
    - Notebook option
    - Set in BIOS setup and written on the hard drive
    - Advantage over a power-on password or Windows password:
      - If hard drive is removed and installed in another notebook, hard drive data remains protected
    - Requested by system when powering up

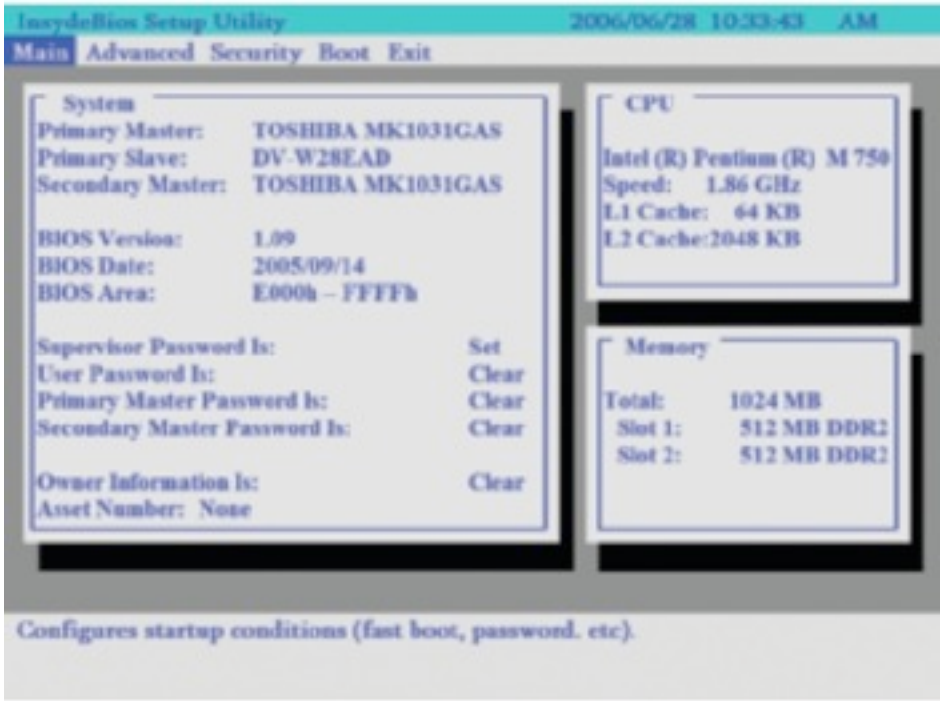

Figure 19-11 BIOS setup main menu shows support for four power-on passwords. Courtesy: Course Technology/Cengage Learning

Authenticate Users (cont'd.)

- Authenticate users for larger networks
  - User accounts and passwords sent over the network when authenticating the user must be encrypted
  - Encryption protocols
    - CHAP (Challenge Handshake Authentication Protocol)
    - Kerberos: Windows Vista/XP default

Authenticate Users (cont'd.)

- Smart Cards
  - Small device containing authentication information
    - Keyed into a logon window by a user
    - Read by a smart card reader
  - Used in two-factor authentication
    - Acts as a token
  - Variations of smart cards
    - Key fob
    - Credit card like smart cards with embedded microchip
    - Smart cards with magnetic stripes
    - Smart card plugging directly into a USB port

Figure 19-13 A smart card such as this SecurID key fob is used to authenticate a user gaining access to a secured network
Courtesy of RSA Security

Figure 19-14 A smart card with a magnetic strip can be used inside or outside a computer network
Courtesy of IDenticard Systems

Figure 19-15 This smart card reader by Athena Smartcard Solutions (*www.athena-scs.com*) uses a USB connection
Courtesy of Athena Smartcard Solutions Ltd.

Figure 19-16 This eToken by Aladdin can contain digital certificates so that a user can do business over a VPN
Courtesy of Aladdin

Authenticate Users (cont'd.)

- Using biometric data
  - Validates the person's physical body
    - Iris, facial features, fingerprint
  - Disadvantage
    - Danger of false negatives or false positives
    - Must decide input data fault tolerance limit

Authenticate Users (cont'd.)

- Create strong passwords
  - Not easy to guess by humans and computer programs
  - Criteria
    - Use eight or more characters
    - Use a passphrase if possible
    - Combine uppercase and lowercase letters, numbers, symbols
    - Use at least one symbol: second through sixth positions
    - Do not use consecutive letters or numbers, adjacent keyboard keys, your logon name, words in any language
    - Do not use same password for more than one system

Figure 19-18 Microsoft password checker window
Courtesy: Course Technology/Cengage Learning

Classify Users and Data

- Computer user classification is determined by the rights needed to perform jobs
  - Windows rights or privileges
    - Assigned to user account created
  - Vista user accounts
    - Administrator account, standard account, and guest account
  - Windows XP accounts
    - Administrator account, guest account, limited account, power user account, and backup operator

Classify Users and Data (cont'd.)

- Computer user classification (cont'd.)
  - Vista Business/Ultimate editions or XP Professional
    - Use Computer Management console to change groups
    - Rights (privileges)
      - Tasks an account allowed to do in the system
      - Rights assigned to an account
    - Permissions
      - User accounts or groups allowed to access data
      - Permissions assigned to data
      - Manage data permissions by creating new user groups

Classify Users and Data (cont'd.)

- Data classification
  - Permissions assigned to folders and files
  - Data classification as applied to security
    - Put data into categories
    - Decide category security
  - Guidelines
    - Must follow security policies
    - Data folder must have an owner
    - Base on organization security needs
    - Document access to protect data integrity
    - Protect backup data as well

Classify Users and Data (cont'd.)

- Data classification in Windows
  - Individual user private data
    - Vista: C:\Users folder
    - XP: C:\Documents and Settings folder
  - Vista shared folders and files
    - C:\Users\Public folder
  - Folder created on a drive
    - Assign share permissions to that folder/subfolders/files
    - Allow all users access or only certain users/user groups
    - Assign permissions according to who can view/change contents

Classify Users and Data (cont'd.)

- Data classification in Windows (cont'd.)
  - Folder can be hidden
  - Folder/file can be encrypted
    - Digital certificate required for access
  - Passwords can be required to access shared resources
  - Computer can be locked down
    - No files or folders shared on the network

Sharing Files and Folders

- Windows Vista: steps to share a file or folder
  - Windows Explorer: right-click folder/file to share, select Share
    - Click the down arrow
    - List of users of this computer displays
    - Allow everyone to access by selecting Everyone
    - Click Add
      - Assigns Reader permission level
    - Allow users right to make changes
      - Click down arrow, select Co-owner
      - Click Share, respond to the UAC box, click Done

Sharing Files and Folders (cont'd.)

- Windows XP: steps to share a file or folder
  - In Windows Explorer, right-click a folder
    - Select Sharing and Security from the shortcut menu
    - Properties box opens with Sharing tab active
    - Click If you understand the security risks but want to share files without running the wizard, click here
    - Enable File Sharing dialog box appears
    - Select Just share the folder and click OK
    - Sharing tab on Properties box now has the Share this folder on the network, check box available

Sharing Files and Folders (cont'd.)

- Troubleshooting problems: Vista
  - Open Network and Sharing Center and verify:
    - File sharing turned on
    - Public folder sharing turned on if necessary
    - Password protected sharing turned on if necessary
    - Printer sharing turned on if necessary
  - In the Network and Sharing Center:
    - Click Manage network connections
      - Right-click the network connection icon, select Properties, respond to the UAC box
      - Verify that File and Printer Sharing for Microsoft Networks checked

Sharing Files and Folders (cont'd.)

- Troubleshooting problems: XP
  - Open the Network Connections window, right-click the connection icon, select Properties
    - Local Area Connection Properties dialog box opens
    - Verify Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks both checked
    - Click Install to install them if necessary

Quick Quiz #1

Quick Quiz #1

- 1. _____ proves that an individual is who they say they are and is accomplished by a variety of techniques, including a username, password, personal identification number (PIN), smart card, or biometric data.

Quick Quiz #1

- 1. _____ proves that an individual is who they say they are and is accomplished by a variety of techniques, including a username, password, personal identification number (PIN), smart card, or biometric data.
- Answer: Authentication

Quick Quiz #1

- 1. _____ proves that an individual is who they say they are and is accomplished by a variety of techniques, including a username, password, personal identification number (PIN), smart card, or biometric data.
- Answer: Authentication
- 2. _____ determines what an individual can do in the system after he or she is authenticated.

Quick Quiz #1

- 1. _____ proves that an individual is who they say they are and is accomplished by a variety of techniques, including a username, password, personal identification number (PIN), smart card, or biometric data.
- Answer: Authentication
- 2. _____ determines what an individual can do in the system after he or she is authenticated.
- Answer: Authorization

Quick Quiz #1

- 1. _____ proves that an individual is who they say they are and is accomplished by a variety of techniques, including a username, password, personal identification number (PIN), smart card, or biometric data.
- Answer: Authentication
- 2. _____ determines what an individual can do in the system after he or she is authenticated.
- Answer: Authorization
- 3. _____ (also called privileges) refer to the tasks an account is allowed to do in the system.

Quick Quiz #1

- 1. _____ proves that an individual is who they say they are and is accomplished by a variety of techniques, including a username, password, personal identification number (PIN), smart card, or biometric data.
- Answer: Authentication
- 2. _____ determines what an individual can do in the system after he or she is authenticated.
- Answer: Authorization
- 3. _____ (also called privileges) refer to the tasks an account is allowed to do in the system.
- Answer: Rights

Quick Quiz #1

- 1. _____ proves that an individual is who they say they are and is accomplished by a variety of techniques, including a username, password, personal identification number (PIN), smart card, or biometric data.
- Answer: Authentication
- 2. _____ determines what an individual can do in the system after he or she is authenticated.
- Answer: Authorization
- 3. _____ (also called privileges) refer to the tasks an account is allowed to do in the system.
- Answer: Rights
- 4. _____ refer to which user accounts or groups are allowed to access data.

Quick Quiz #1

- 1. _____ proves that an individual is who they say they are and is accomplished by a variety of techniques, including a username, password, personal identification number (PIN), smart card, or biometric data.
- Answer: Authentication
- 2. _____ determines what an individual can do in the system after he or she is authenticated.
- Answer: Authorization
- 3. _____ (also called privileges) refer to the tasks an account is allowed to do in the system.
- Answer: Rights
- 4. _____ refer to which user accounts or groups are allowed to access data.
- Answer: Permissions

Quick Quiz #1

- 1. _____ proves that an individual is who they say they are and is accomplished by a variety of techniques, including a username, password, personal identification number (PIN), smart card, or biometric data.
- Answer: Authentication
- 2. _____ determines what an individual can do in the system after he or she is authenticated.
- Answer: Authorization
- 3. _____ (also called privileges) refer to the tasks an account is allowed to do in the system.
- Answer: Rights
- 4. _____ refer to which user accounts or groups are allowed to access data.
- Answer: Permissions
- 5. _____, as it applies to security, involves putting data into categories and then deciding how secure each category must be.

Quick Quiz #1

- 1. _____ proves that an individual is who they say they are and is accomplished by a variety of techniques, including a username, password, personal identification number (PIN), smart card, or biometric data.
- Answer: Authentication
- 2. _____ determines what an individual can do in the system after he or she is authenticated.
- Answer: Authorization
- 3. _____ (also called privileges) refer to the tasks an account is allowed to do in the system.
- Answer: Rights
- 4. _____ refer to which user accounts or groups are allowed to access data.
- Answer: Permissions
- 5. _____, as it applies to security, involves putting data into categories and then deciding how secure each category must be.
- Answer: Data classification

Quick Quiz #1

- 1. _____ proves that an individual is who they say they are and is accomplished by a variety of techniques, including a username, password, personal identification number (PIN), smart card, or biometric data.
- Answer: Authentication
- 2. _____ determines what an individual can do in the system after he or she is authenticated.
- Answer: Authorization
- 3. _____ (also called privileges) refer to the tasks an account is allowed to do in the system.
- Answer: Rights
- 4. _____ refer to which user accounts or groups are allowed to access data.
- Answer: Permissions
- 5. _____, as it applies to security, involves putting data into categories and then deciding how secure each category must be.
- Answer: Data classification

Sharing Files and Folders (cont'd.)

- Steps to set up a network drive
  - Host computer
    - Share the folder or entire volume to which you want others to have access
  - Remote computer
    - Connect to the network, access Windows Explorer, click the Tools menu and select Map Network Drive
  - Select a drive letter from the drop-down list
    - Click Browse button, locate shared folder or drive
    - Click OK to close the Browse For Folder dialog box, and click Finish to map the drive

Additional Methods to Protect Resources

- Securing data and other computer resources
  - A never-ending task
- More ways to secure a computer or small network
  - Hardware security devices
  - Encryption techniques
  - BIOS security features
  - Locking a workstation
  - Protecting against malicious software
  - Educating users

Security Devices to Protect Data and Computers

- Suggestions:
  - Keep really private data under lock and key
  - Lock down the computer case
  - Use lock and chain to physically tie computer to a desk or other permanent fixture
  - Use a theft-prevention plate

Security Devices to Protect Data and Computers (cont'd.)

- Notebook computers susceptible to thieves (Dell)
  - 12,000 laptops stolen each year from U.S. airports
  - 65 percent of business travelers have not secured the corporate hard drive data
  - 42 percent don't back up corporate hard drive data
- Common sense rules to help protect a notebook
  - Use one or more Windows techniques in this chapter to protect the data on your laptop hard drive

Security Devices to Protect Data and Computers (cont'd.)

- Common sense rules to help protect a notebook
  - Use one or more Windows techniques to protect the data on your laptop hard drive
  - When traveling, always know where your notebook is
  - Never leave a notebook in an unlocked car
  - Consider using laptop tracking software
  - When at work, lock your notebook in a secure place or use a notebook cable lock to secure it to your desk

Encryption Techniques

- Encryption puts data into code
  - Must be translated before accessed
- Encryption techniques
  - Encrypt folders and files in Windows
    - Windows Encrypted File System (EFS)
  - Encrypt an entire hard drive
    - BitLocker Encryption: Windows Vista Ultimate/ Enterprise editions
  - Encrypt wireless networks

Encryption Techniques (cont'd.)

- Encryption techniques (cont'd.)
  - Encryption used by a VPN
  - Use Embedded encryption in devices
  - Other secured connections used for data transmissions
    - Public Key Encryption uses public and private keys
    - Pretty Good Privacy (PGP) by PGP Corporation

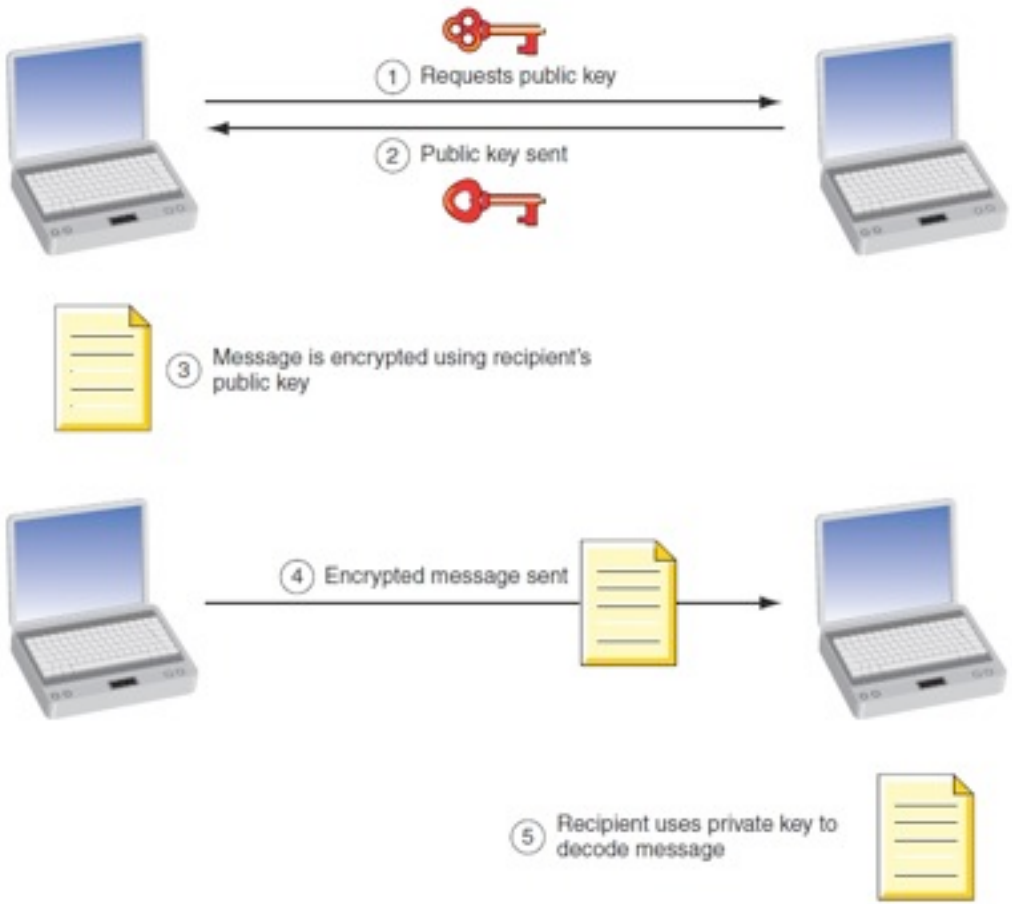

Figure 19-30 Public key encryption uses two keys: the recipient's public key to encrypt the message and her private key to decrypt it. Courtesy: Course Technology/Cengage Learning

Use Bios Features to Protect the System

- Motherboards BIOS features designed to secure the system
  - Power-on passwords
  - Drive lock password protection
  - Trusted Platform Module (TPM) chip
  - Intrusion detection
  - Boot sector protection for the hard drive

Lock a Workstation

- Techniques
  - Press the Windows key and L
  - Press Ctrl-Alt-Del, user clicks “Lock this computer”
    - Use Group Policy to make passwords required

Figure 19-31 Results of pressing Crtl-Alt-Del when a user is already logged on. Courtesy: Course Technology/Cengage Learning

Protect Against Malicious Software

- Malicious software (malware, computer infestation)
  - Any unwanted program that means harm
  - Transmitted to a computer without user's knowledge
- Grayware
  - Any annoying and unwanted program
    - Might or might not mean harm

Protect Against Malicious Software (cont'd.)

- Virus program
  - Replicates by attaching itself to other programs
- Adware
  - Produces unwanted pop-up ads

Figure 19-32 This pop-up window is luring the user to take the bait
Courtesy: Course Technology/Cengage Learning

Protect Against Malicious Software (cont'd.)

- Spyware software
  - Installs itself on a computer
  - Spies on user and collects personal information
- Keylogger
  - Tracks all keystrokes
- Worm program
  - Copies itself throughout a network or the Internet without a host program

Protect Against Malicious Software (cont'd.)

- Browser hijacker (home page hijacker)
  - Changes a home page and other browser settings

Figure 19-33 Internet Explorer with toolbars installed and home page changed. Courtesy: Course Technology/Cengage Learning

Protect Against Malicious Software (cont'd.)

- Spam
  - Junk e-mail user does not want, did not ask for, and gets in the user's way
- Virus hoax (e-mail hoax)
  - E-mail tempting user to forward it to everyone in address book
    - Clogs up e-mail systems
    - May delete critical Windows system file
- Phishing
  - Type of identity theft
    - Sender scams user into responding with personal data

Protect Against Malicious Software (cont'd.)

- Scam e-mail
  - Used by scam artists to lure user into scam scheme
- Logic bomb
  - Dormant code added to software
  - Triggered at a predetermined time or predetermined event
- Trojan horse
  - Does not need a host program to work
    - Substitutes itself for a legitimate program
  - May install a backdoor

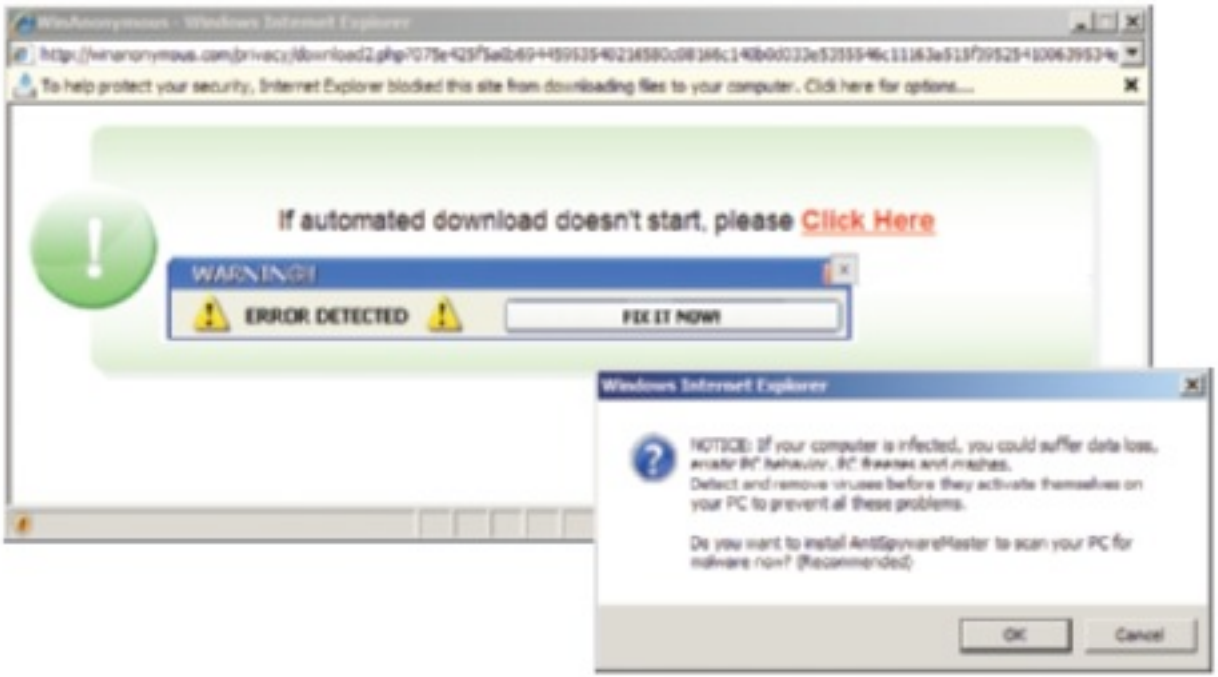

Figure 19-34 Clicking an action button on a pop-up window might invite a Trojan into your system. Courtesy: Course Technology/Cengage Learning

Protect Against Malicious Software (cont'd.)

- Ways a virus attacks and hides:
  - Boot sector virus
  - File virus
  - Multipartite virus
  - Macro virus
  - Script virus
  - Rootkit

Protect Against Malicious Software (cont'd.)

- Best practices:
  - Always use a software firewall
  - Use antivirus (AV) software
  - Use the Vista UAC box
  - Limit use of administrator accounts
  - Set Internet Explorer for optimum security
  - Use alternate client software
  - Keep good backups

Educate Users

- Social engineering
  - Practice of tricking people
    - Give out private information
    - Allow unsafe programs into the network or computer
- Important security measures for users
  - Never give out passwords to anyone
  - Do not store passwords on a computer
  - Do not use same password on more than one system

Educate Users (cont'd.)

- Important security measures for users (cont'd.)
  - Lock down workstation when leaving the desk
    - Press the Windows key and L (the quickest method)
    - Press Ctrl-Alt-Del and choose Lock this computer from the menu
    - For Vista, click Start and the lock icon
    - For Vista, put the system into a sleep state
    - Power down system when leaving for the day
  - Beware of social engineering techniques

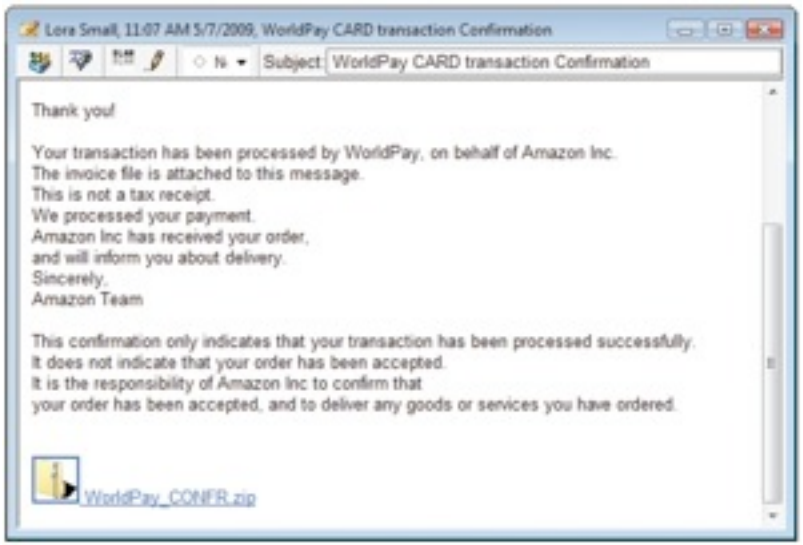

Figure 19-39 This phishing technique using an e-mail message with an attached file is an example of social engineering. Courtesy: Course Technology/Cengage Learning

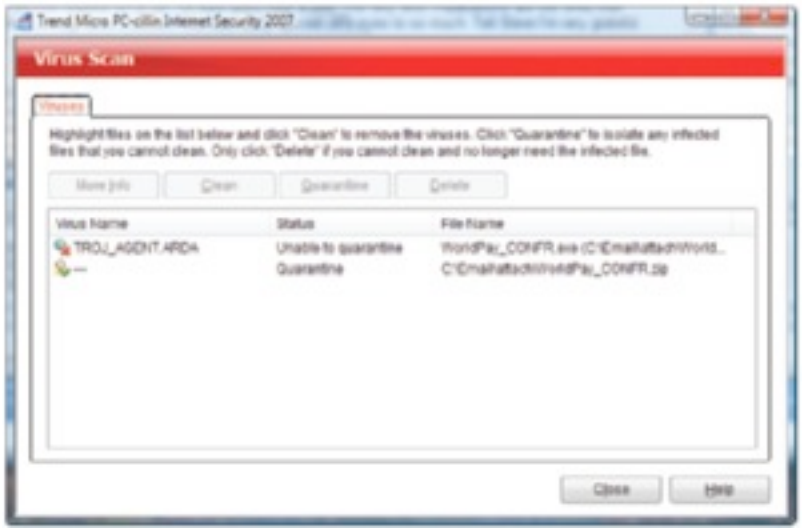

Figure 19-40 Antivirus software that scanned the attachment reports a Trojan Courtesy: Course Technology/Cengage Learning

Educate Users (cont'd.)

- Important security measures for users (cont'd.)
  - Exercise good judgment when using the Internet
    - Scan e-mail attachments before opening
    - Do not click links inside e-mail messages
    - Check for a hoax before forwarding e-mail message
    - Always check out a Web site before downloading anything from it
    - Verify website before providing private information
    - Never trust an e-mail message asking to verify private data on a Web site for business

Perform Routine Security Maintenance

- Steps:
  - Change administrator password
  - Verify Windows Automatic Updates
    - Turned on and working
  - Verify antivirus software
    - Installed and current
  - Verify Windows Firewall turned on
    - Verify port security
  - For only one computer user with administrative privileges verify Windows settings

Quick Quiz #2

Quick Quiz #2

- 1. True or False: A passphrase is made of several words with spaces allowed.

Quick Quiz #2

- 1. True or False: A passphrase is made of several words with spaces allowed.
- Answer: True

Quick Quiz #2

- 1. True or False: A passphrase is made of several words with spaces allowed.
- Answer: True
- 2. _____ puts data into code that must be translated before it can be accessed.

Quick Quiz #2

- 1. True or False: A passphrase is made of several words with spaces allowed.
- Answer: True
- 2. _____ puts data into code that must be translated before it can be accessed.
- Answer: Encryption

Quick Quiz #2

- 1. True or False: A passphrase is made of several words with spaces allowed.
- Answer: True
- 2. _____ puts data into code that must be translated before it can be accessed.
- Answer: Encryption
- 3. _____ engineering is the practice of tricking people into giving out private information or allowing unsafe programs into the network or computer.

Quick Quiz #2

- 1. True or False: A passphrase is made of several words with spaces allowed.
- Answer: True
- 2. _____ puts data into code that must be translated before it can be accessed.
- Answer: Encryption
- 3. _____ engineering is the practice of tricking people into giving out private information or allowing unsafe programs into the network or computer.
- Answer: Social

Quick Quiz #2

- 1. True or False: A passphrase is made of several words with spaces allowed.
- Answer: True
- 2. _____ puts data into code that must be translated before it can be accessed.
- Answer: Encryption
- 3. _____ engineering is the practice of tricking people into giving out private information or allowing unsafe programs into the network or computer.
- Answer: Social
- 4. _____ is a type of identity theft where the sender of an e-mail message scams you into responding with personal data about yourself.

Quick Quiz #2

- 1. True or False: A passphrase is made of several words with spaces allowed.
- Answer: True
- 2. _____ puts data into code that must be translated before it can be accessed.
- Answer: Encryption
- 3. _____ engineering is the practice of tricking people into giving out private information or allowing unsafe programs into the network or computer.
- Answer: Social
- 4. _____ is a type of identity theft where the sender of an e-mail message scams you into responding with personal data about yourself.
- Answer: Phishing

Quick Quiz #2

- 1. True or False: A passphrase is made of several words with spaces allowed.
- Answer: True
- 2. _____ puts data into code that must be translated before it can be accessed.
- Answer: Encryption
- 3. _____ engineering is the practice of tricking people into giving out private information or allowing unsafe programs into the network or computer.
- Answer: Social
- 4. _____ is a type of identity theft where the sender of an e-mail message scams you into responding with personal data about yourself.
- Answer: Phishing
- 5. A(n) _____ hoax is e-mail that does damage by tempting you to forward it to everyone in your e-mail address book with the intent of clogging up e-mail systems or to delete a critical Windows system file by convincing you the file is malicious.

Quick Quiz #2

- 1. True or False: A passphrase is made of several words with spaces allowed.
- Answer: True
- 2. _____ puts data into code that must be translated before it can be accessed.
- Answer: Encryption
- 3. _____ engineering is the practice of tricking people into giving out private information or allowing unsafe programs into the network or computer.
- Answer: Social
- 4. _____ is a type of identity theft where the sender of an e-mail message scams you into responding with personal data about yourself.
- Answer: Phishing
- 5. A(n) _____ hoax is e-mail that does damage by tempting you to forward it to everyone in your e-mail address book with the intent of clogging up e-mail systems or to delete a critical Windows system file by convincing you the file is malicious.
- Answer: virus or e-mail

Perform Routine Security Maintenance (cont'd.)

- Steps (cont'd.)
  - Visually inspect equipment
  - Check Event Viewer
  - Verify user data backups
    - Complete and current backups exist
    - Automatically create restore points
  - Destroy all data on discarded media with a zero-fill utility
  - Document monthly maintenance noting anything unusual
  - File incident reports

Summary

- To secure a computer and its resources:
  - Comply with security policies
  - Goal of security is to protect resources and avoid interference with system functions
  - Control access using authentication and authorization
    - Authenticate users with passwords, smart cards, biometric data
      - Use strong passwords
  - Classify users and data
    - Rights and permissions

Summary (cont'd.)

- Share files and data
  - Drive mapping
- Other protection mechanisms
  - Encryption Techniques
  - BIOS passwords
  - Lock a workstation
- Protect against malware
- Educate users
  - Social engineering