Chapter 12: Security

IT Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 12 - Sections & Objectives

- 12.1 Security Threats
  - Explain security threats.
- 12.2 Security Procedures
  - Configure IT security.
- 12.3 Common Preventive Maintenance Techniques for Security
  - Manage IT security on an ongoing basis.
- 12.4 Basic Troubleshooting Process for Security
  - Explain how to troubleshoot basic security problems.
- 12.5 Chapter Summary

12.1 Security Threats

Cisco | Networking Academy®
Mind Wide Open™

The Importance of Security

- Private information, company secrets, financial data, computer equipment, and items of national security are placed at risk if proper security procedures are not followed.
- A technician's primary responsibilities include data and network security.

Security Threats

Potential threats to computer security:

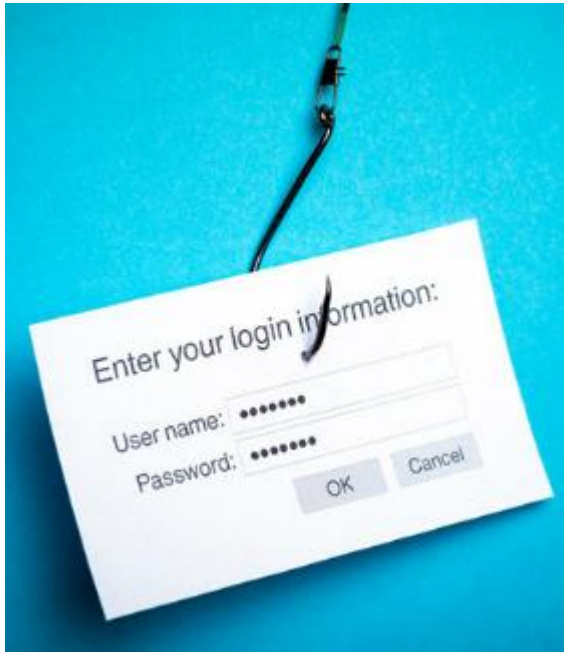
- Internal threats
  - Employees can cause a malicious threat or an accidental threat.
- External threats
  - Outside users can attack in an unstructured or structured way.

Types of attacks to computer security:

- Physical
  - Theft, damage, or destruction to computer equipment.
- Data
  - Removal, corruption, denial of access, unauthorized access, or theft of information.

Types of Security Threats

- Malicious software (malware) is:
  - Usually installed without user knowledge
  - Capable of modifying the user's browser
  - Often collects user information
- **Signatures** is the name given to the programming-code patterns of viruses and other malware.



Adware, Spyware and Phishing

- **Malicious software (malware)** is any software designed to damage or to disrupt a system:
- **Adware** - software program that displays advertising on your computer, often displayed in a pop-up window.
- **Spyware** - distributed without user intervention or knowledge, monitors activity on the computer.
- **Phishing** - uses email that appears to be from a legitimate sender and asks the email recipient to visit a website to enter confidential information such as password or username.
- Zero-Day attacks attempt to exploit software vulnerabilities that are unknown or undisclosed by the software vendor.

Viruses, Worms, Trojans, and Rootkits

- **Virus** is a software code that is deliberately created by an attacker. Viruses may collect sensitive information or may alter or destroy information.
- A **worm** is a self-replicating program that travels to new computers without any intervention or knowledge of the user. At a minimum, worms consume bandwidth in a network.
- A **Trojan** is malicious software that is disguised as a legitimate program. It is named for its method of getting past computer defenses by pretending to be something useful.
- **Anti-virus** software is designed to detect, disable, and remove viruses, worms, and Trojan horses before they infect a computer.
- A **Rootkit** is a malicious program that gains full access to a computer system. Often, a direct attack on a system using a known vulnerability or password.

Web Security

Tools that make web pages powerful can make computers vulnerable:

- **Active X** - Controls interactivity on web pages.
- **Java** - Allows applets to run within a browser.
- **Java Script** - Interacts with HTML source code to allow interactive web sites.
- **Adobe Flash** - used to create interactive media (animation, video and games) for the web.
- **Microsoft Silverlight** -used to create rich, interactive media for the web, similar to flash.

Most browsers have settings to help prevent these attacks, for example:

- **ActiveX filtering**
- **Pop-up Blockers**
- **SmartScreen Filter** (Internet Explorer)

InPrivate Browsing

- **InPrivate browsing** prevents the web browser from storing the following information:
  - Usernames
  - Passwords
  - Cookies
  - Browsing history
  - Temporary Internet files
  - Form data
- The browser stores temporary files and cookies but the information is deleted when InPrivate session is ended.
- To start InPrivate Browsing in Windows 7:
  - Right-Click **Internet Explorer > Start InPrivate Browsing**

Spam

- **Spam** is unsolicited email that can be used to send harmful links or deceptive content.
- **Popups** are windows that automatically open and are designed to capture your attention and lead you to advertising sites.

Use anti-virus software, options in e-mail software, popup blockers, and common indications of spam to combat these.

TCP/IP Attacks

- TCP/IP suite controls communication on the Internet. Can be manipulated to prevents users from accessing normal services.
  - **Denial of Service (DoS)** - sending enough requests to overload a resource or even stopping its operation. Prevents the target server from being able to handle additional requests
  - **Distributed DoS (DDoS)** - an attack launched from many computers, called zombies or botnets.
  - **SYN Flood** - randomly opens TCP ports at the source of the attack and ties up the computer with a large amount of false SYN requests.
  - **Spoofing** - uses a forged IP or MAC address to impersonate a trusted computer.
  - **Man-in-the-Middle** - intercepting communications between computers to steal information transiting through the network.
  - **Replay** - data transmissions are intercepted and recorded by an attacker, then replayed to gain access.
  - **DNS Poisoning** - changing DNS records to point to imposter servers. Involves the misdirection of a user from a legitimate web site to a fake web site.

Social Engineering

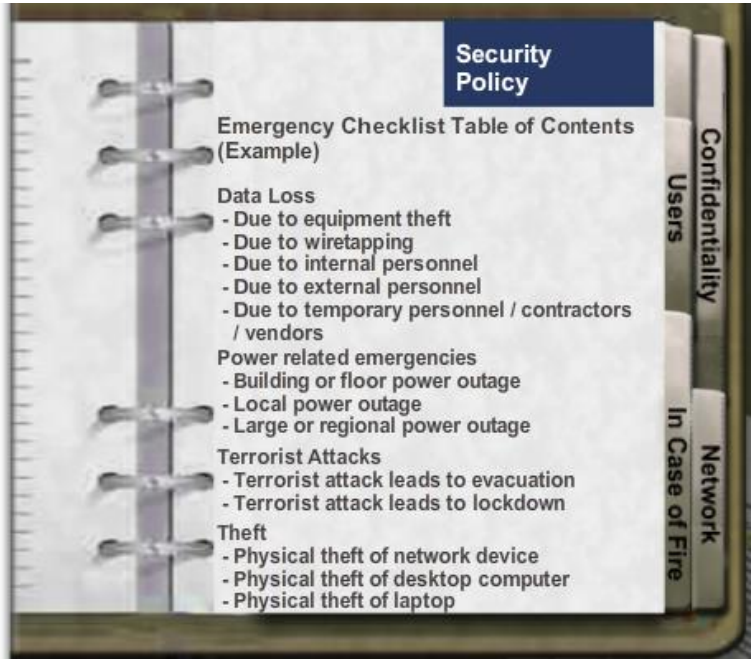
- A social engineer is a person who is able to gain access to equipment or a network by tricking people into providing the necessary access information.
- To protect against social engineering:
  - Never give out a password.
  - Always ask for the ID of the unknown person.
  - Restrict access of visitors.
  - Register and escort all visitors.
  - Never post your password.
  - Lock your computer when you leave your desk.
  - Do not let anyone follow you through a door that requires an access card.
  - Ensure that each use of an access card allows access to only one user at the time

12.2 Security Procedures

Cisco | Networking Academy®
Mind Wide Open™

Security Policy

- A security policy should describe how a company addresses security issues
- Questions to answer in writing a local security policy:
  - What assets require protection?
  - What should be done in the event of a security breach?
  - What training will be in place to educate the end users?
  - What are the possible threats to the assets of the organization?



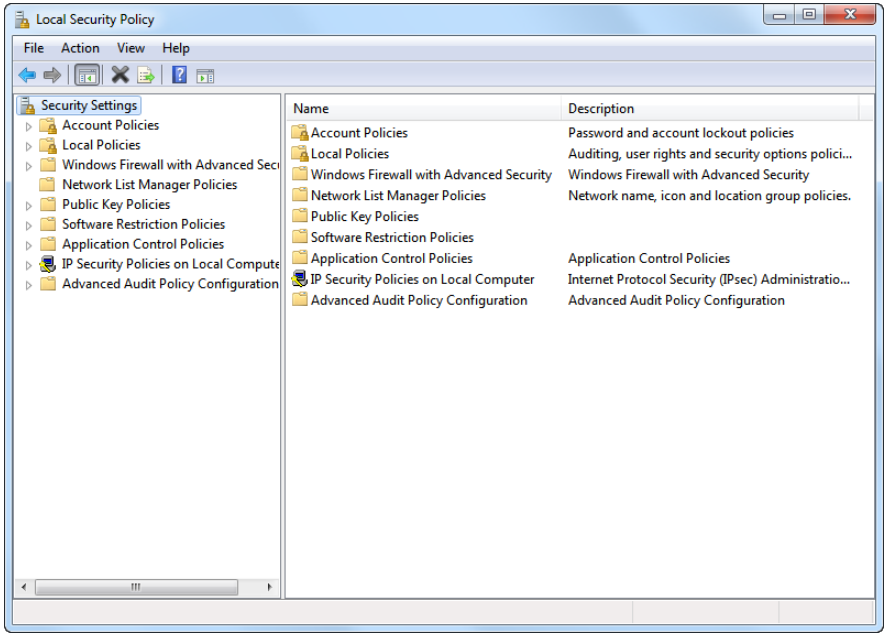
Security Policy Requirements

A security policy should address these key areas:

- Process for handling network security incidents
- Process to audit existing network security
- General security framework for implementing network security
- Behaviors that are allowed
- Behaviors that are prohibited
- What to log and how to store the logs: Event Viewer, system log files, or security log files
- Network access to resources through account permissions
- Authentication technologies to access data: usernames, passwords, biometrics, and smart cards

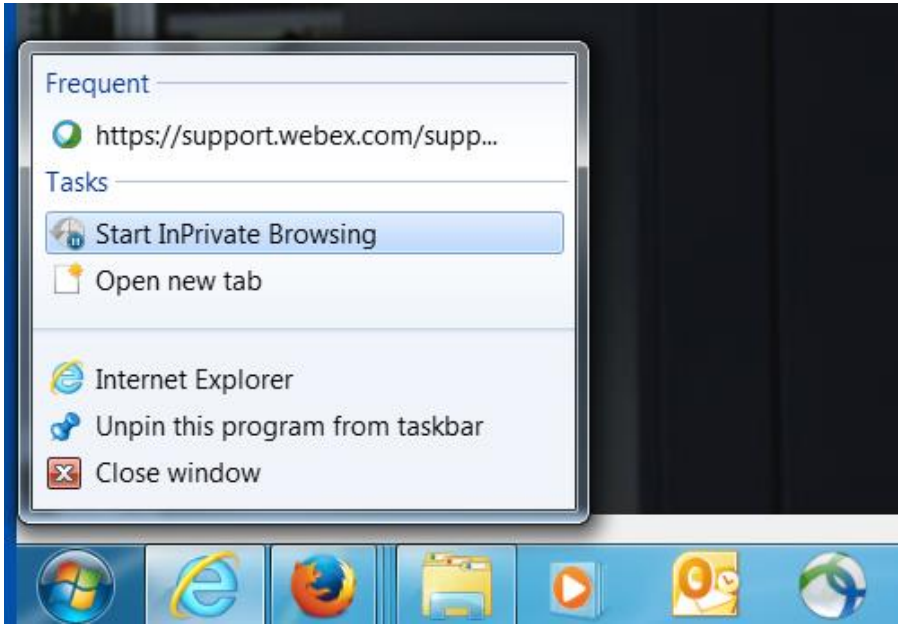
Windows Local Security Policy

- A security policy is a set of security objectives that ensure the security of a network, the data, and the computer systems in an organization.
- You can use the Windows Local Security Policy tool to implement a security policy on computers that are not part of an Active Directory domain.
- Password Policy can be configured to meet a variety of requirements including password history, max age, min age, min length, and complexity.
- Audit Policy can be enabled to record all logon events.
- You can then export the Local Security Policy to make it easier to update another computer with the same security policy.



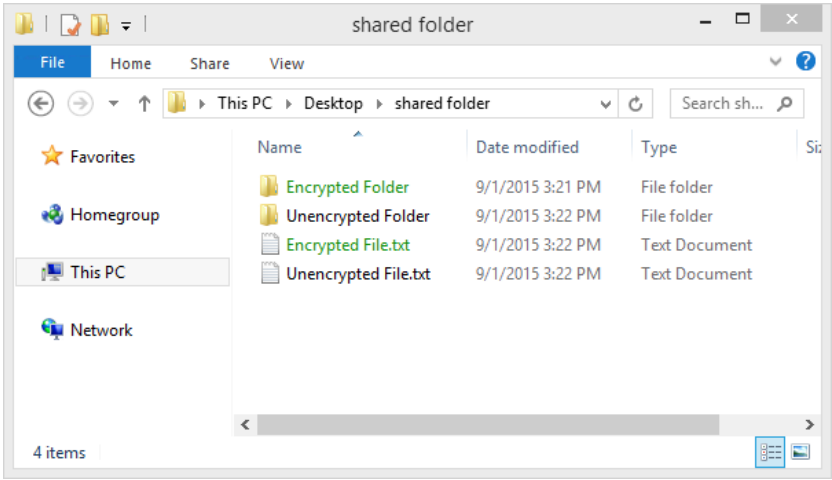
Securing Web Access

- Browsers include various tools that can be exploited by attackers.
- Most browsers have features that can be enabled to increase web security.
- For example, Internet Explorer security can be enhanced by enabling:
  - ActiveX Filtering
  - Pop-up Blocker
  - SmartScreen Filter
  - InPrivate Browsing



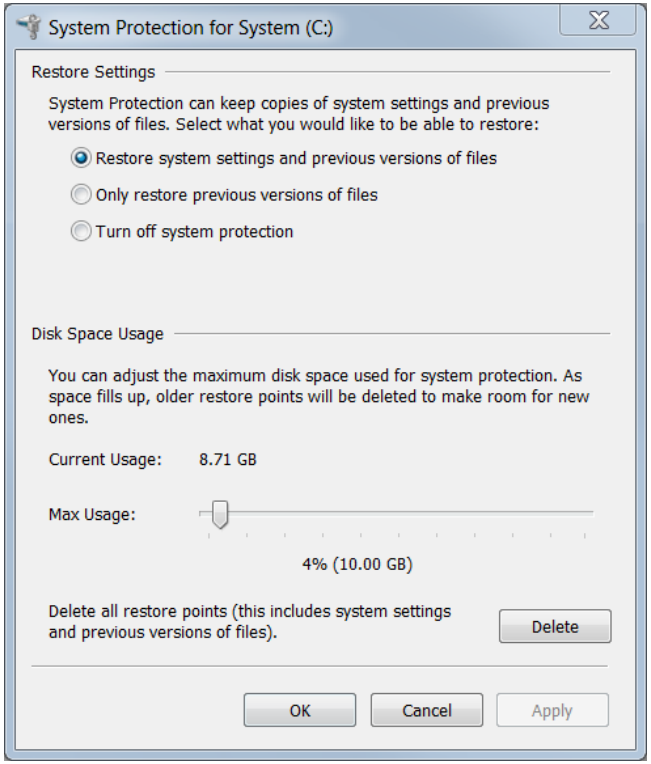
Protecting Data

- Protecting data on computers includes a variety of techniques including:
  - Software, such as Windows Firewall, that filters traffic between the computer and other computers to which it is connected
  - Biometric, smart card, and key fob security to help prevent unauthorized physical access to the computer.
  - Backing up data in case of theft, loss, or damage with programs like Windows 7 Backup and Restore, or Windows 8.1 File History tools.
  - File and folder permissions and encryption can be used to prevent unauthorized users from viewing or modifying data.
  - An entire hard drive can be encrypted using Windows BitLocker.
  - Hard drives that need to be disposed of should be data wiped either with a software tool or a degaussing device.
  - When data is wiped, the hard drive can be either recycled or destroyed.



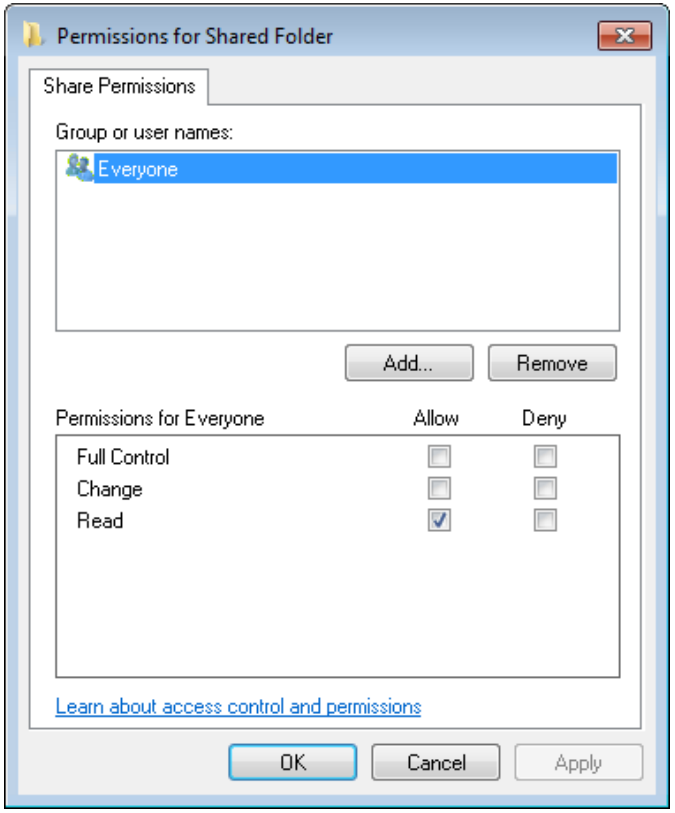
Protection Against Malicious Software

- Antimalware programs, such as those offered by McAffee, Symantec, and Kaspersky, include antivirus protection, adware protection, phishing protection, and spyware protection.
- Always retrieve the signature files from the manufacturer's website to make sure the update is authentic and not corrupted by viruses.
- If a computer becomes infected, follow these steps:
  1. Remove the infected computer from the network.
  2. Follow the incident response policy, which may inlcude:
     - Notify IT personnel
     - Save log file to removable media
     - Turn off computer
     - Home users should update all antimalware programs.
  3. Boot the computer with a scan disk. This may include booting in Safe Mode.
  4. After the computer is clean, delete system restore files to protect against reinfection.



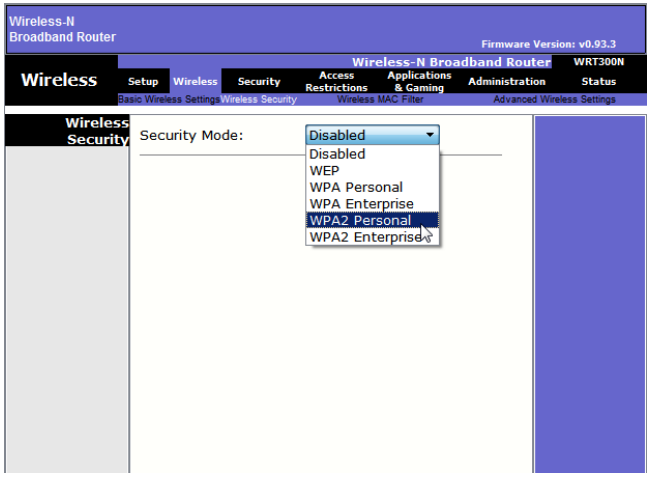
Security Techniques

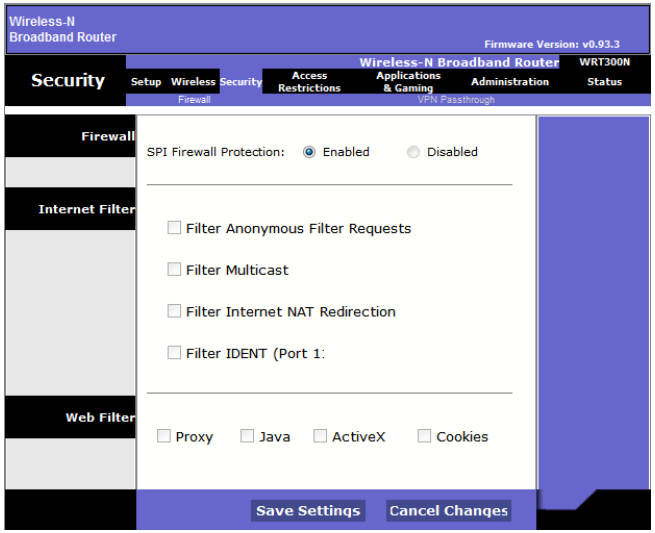
- All Windows computers on a network must be part of either a domain or a workgroup.
- Before computers can share resources, they must share the same domain name or workgroup name.
- Mapping a local drive is a useful way to access a single file, specific folders, or an entire drive between different operating systems over a network.
- Determine which resources will be shared over the network and the type of permissions users will have to the resources.
  - Read - user can view data in files and run programs
  - Change - user can add files and subfolders, change the data in files, and delete subfolders and files
  - Full Control - user can change permissions of files and folders



Security Techniques

- Common security techniques include:
  - Encrypted communications between two computers should occur over an encrypted channel, such as those provided by virtual private networks (VPNs).
  - The service set identifier (SSID) broadcasting on wireless networks (WLANs) can be disabled, although this does not provide sufficient security.
  - Secure WLANs with the strongest security mode, which is currently WPA2.
  - Universal Plug and Play (UPnP), which enables devices to add themselves to the network, should be disabled. UPnP is not secure.
  - Be sure the firmware is up-to-date with the latest security patches.
  - Install and configure a firewall. Most wireless routers today include a stateful packet inspection firewall.
  - If you want others to be able to access a computer, server, or gaming console across untrusted or public networks, use port forwarding and isolate the computer in a demilitarized zone (DMZ).





Protecting Physical Equipment

- Common techniques for protecting physical equipment include:
  - Store network equipment in a locked wiring closet
  - Consider setting a BIOS or UEFI password
  - Disable AutoRun and AutoPlay
  - Implement multifactor authentication which includes:
    - Something you know (e.g. password)
    - Something you have (e.g. key fob)
    - Something you are (e.g. fingerprint)
  - Lock down all equipment with security cable
  - Use card keys, video surveillance, and/or security guards if the cost is warranted. (e.g. data centers)

Hard Drive Disposal and Recycling

- Erase all hard drives, then use a third-party data wiping tool to fully erase all data.
- Degaussing disrupts or eliminates the magnetic field on a hard drive that allow for the storage of data. A degaussing tool is very expensive and not practical for most users.
- The only way to fully ensure that data cannot be recovered from a hard drive is to carefully shatter the platters with a hammer and safely dispose of the pieces.
- To destroy software media (floppy disks and CDs), use a shredding machine designed for shredding these materials.
- **Hard Drive Recycling** - Hard drives that do not contain sensitive data can be reformatted and used in other computers.

Usernames and Passwords

- Username and Password policies:
  - Change the default username for accounts such as administrator or guest.
  - Network admin defines a naming convention for usernames.
  - Three levels of password protection are recommended:
    - BIOS
    - Login
    - Network

Password Requirements

Guidelines for creating strong passwords:

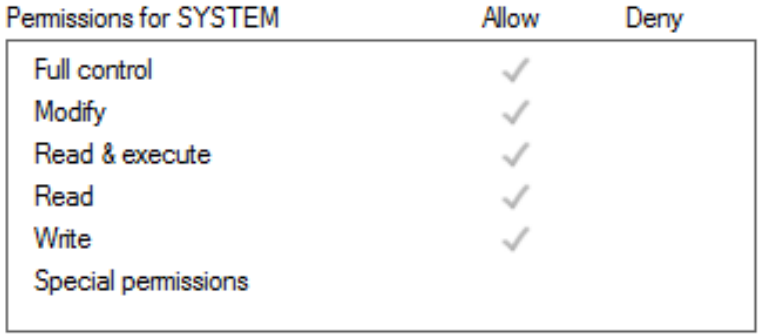
- **Length** - Use at least eight characters.
- **Complexity** - Include letters, numbers, symbols, and punctuation. Use a variety of keys on the keyboard, not just common letters and characters.
- **Variation** - Change passwords often. Set a reminder to change the passwords you have for email, banking, and credit card websites on the average of every three to four months.
- **Variety** - Use a different password for each site or computer that you use.

File and Folder Permissions

- Permission levels are configured to limit individual or group user access to specific data.
- **NTFS** – File system that uses journals which are special areas where file changes are recorded before changes are made.
  - Can log access by user, date, and time
  - Has encryption capability
- **FAT 32** – no encryption or journaling
- **Principle of Least Privilege** – only allow users access to the resources they need.
- **Restricting User Permissions** – If an individual or a group is denied permissions to a network share, this denial overrides any other permissions given.

File and Folder Permissions

- Permission level:
  - **Full Control –** Permits reading, writing, changing, and deleting of files, folders, and subfolders
  - **Modify –** Permits reading and writing of files and subfolders; allows deletion of the folder or file
  - **Read & Execute –** Permits viewing and listing of files and subfolders as well as executing of files; inherited by files and folders
  - **Read –** Permits viewing and listing of files and subfolders
  - **Write –** Permits adding of files and subfolders. It is the minimum level of Windows security required to allow a local user to restore backed up files.



Protecting Data

- The value of physical equipment is often far less than the value of the data it contains. To protect data, there are several methods of security protection that can be implemented.
  - Software Firewall
  - Smartcard Security
  - Biometric Security
  - Data backups
  - Data encryption

Data Encryption

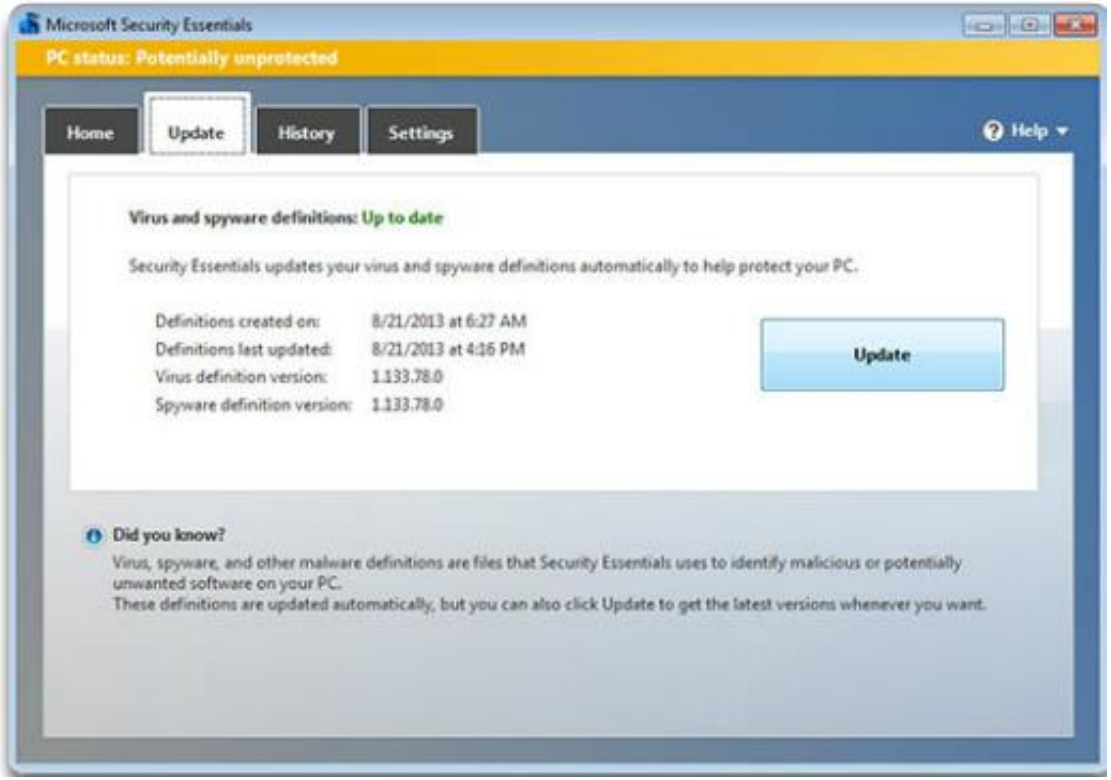
- **Encryption** - data is transformed using a complicated algorithm to make it unreadable.
- **Encrypting File System (EFS)** is a Windows feature that can encrypt data.
- **BitLocker** can encrypt the entire hard drive volume included in Windows 7 and Windows Vista Ultimate and Enterprise editions.
- **Trusted Platform Module (TPM)** is a specialized chip installed on the motherboard to be used for hardware and software authentication.
  - TPM stores information specific to the host system, such as encryption keys, digital certificates, and passwords.

Malware Software Protection Programs

- **Malware** is malicious software that is installed on a computer without the knowledge or permission of the user.
- It may take several different anti-malware programs and multiple scans to completely remove all malicious software.
- Anti-malware available for these purpose are: Anti-virus, anti-spyware, anti-adware, and phishing programs.

Signature File Updates

- New viruses are always being developed, therefore security software must be continually updated.



Common Communication Encryption Types

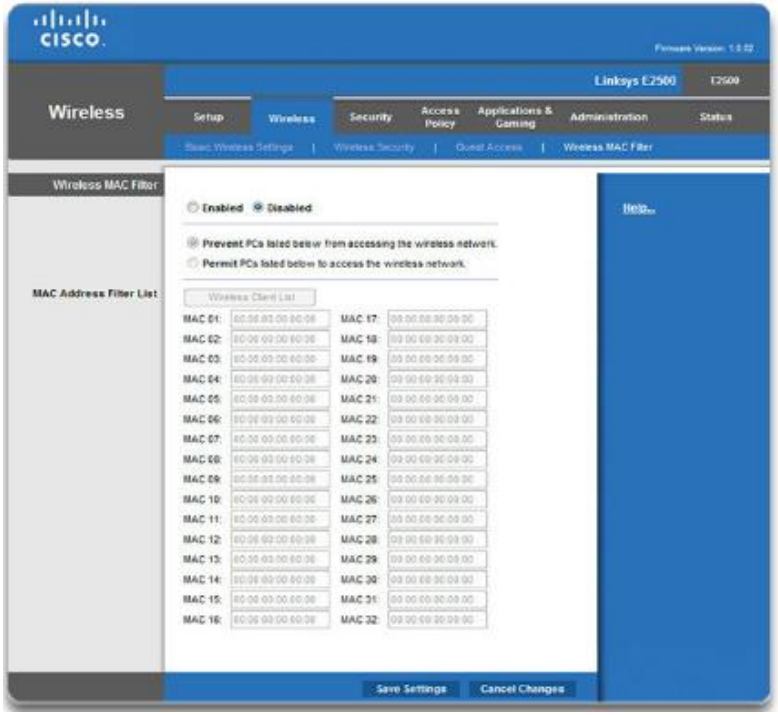
- **Hash Encoding** uses a mathematical function to create a numeric value that is unique to the data.
- **Symmetric Encryption** requires both sides of an encrypted conversation to use an encryption key to encode and decode the data.
- **Asymmetric Encryption** requires two keys, a private key and a public key.

Service Set Identifiers

- The **Service Set Identifier** (SSID) is the name of the wireless network. A wireless router or access point broadcasts the SSID by default so that wireless devices can detect the wireless network.
- To disable SSID broadcasting, use the following path, as shown in the figure:
  - **Wireless > Basic Wireless Settings >** select **Disabled** for SSID Broadcast **> Save Settings > Continue**
- Disabling the SSID broadcast provides very little security. If the SSID broadcast is disabled, each computer user that wants to connect to the wireless network must enter the SSID manually. When a computer is searching for a wireless network, it will broadcast the SSID.

Mac Address Filtering

- **MAC address filtering** is a technique used to deploy device-level security on a wireless LAN.



Wireless Security Modes

- **Wired Equivalent Privacy (WEP)** – The first generation security standard for wireless. Attackers quickly discovered that WEP encryption was easy to break.
- **Wi-Fi Protected Access (WPA)** An improved version of WEP, uses much stronger encryption.
- **Wi-Fi Protected Access 2 (WPA2)** WPA2 supports robust encryption, providing government-grade security. This is the most effective way of securing wireless traffic.

Wireless Access

- **Wireless Antennae**
  - Avoid transmitting signals outside of the network area by installing an antenna with a pattern that serves your network users.
- **Network Device Access**
  - On first connection to the network device, change the default username and password.
- **Wi-Fi Protected Setup (WPS)**
  - The user connects to the wireless router using the factory-set PIN that is either printed on a sticker or shown on a display.
  - Software has been developed that can intercept traffic and recover the WPS PIN and the pre-shared encryption key. Disable WPS on the wireless router if possible.

Firewalls

Hardware Firewall	Software Firewall
Dedicated hardware component	Available as third-party software, cost varies
Initial cost for hardware and software updates can be expensive	Free version included with Windows operating system
Multiple computers can be protected	Typically protects only the computer on which it is installed
No impact on computer performance	Uses the CPU, potential impact on computer performance

Port Forwarding and Port Triggering

- **Port forwarding** is a rule-based method of directing traffic between devices on separate networks:
  - Used when specific ports must be opened so that certain programs and applications can communicate with devices on different networks.
  - Router determines if the traffic should be forwarded to a certain device based on the port number found with the traffic. For example HTTP – Port 80.
- **Port triggering** allows the router to temporarily forward data through inbound ports to a specific device.
  - For example, a video game might use 6508 to open port 27000 to connect inbound traffic from other players.

Physical Equipment Protection Methods

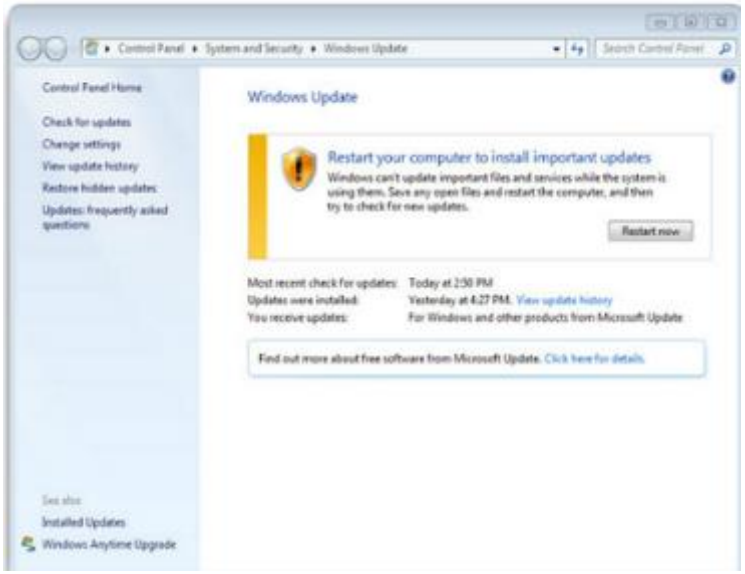
- Physical security is as important as data security. Network infrastructure can be protected by:
  - Secured telecommunications rooms, equipment cabinets, and cages
  - Implement biometric authentication
  - Cable locks and security screws for hardware devices
  - Wireless detection for unauthorized access points
  - Hardware firewalls
  - Network management system that detects changes in wiring and patch panels
- **Two- factor Authentication** - secured using overlapping protection techniques to prevent unauthorized access to sensitive data.
  - An example of two-factor authentication is using a password and a smart card to protect an asset.

Security Hardware

- There are several methods of physically protecting computer equipment:
  - Use cable locks with equipment.
  - Keep telecommunication rooms locked.
  - Fit equipment with security screws.
  - Use security cages around equipment.
  - Label and install sensors, such as Radio Frequency Identification (RFID) tags, on equipment.
  - Install physical alarms triggered by motion-detection sensors.
  - Use webcams with motion-detection and surveillance software.
- For access to facilities, there are several means of protection:
  - Card keys that store user data, including level of access
  - Biometric sensors that identify physical characteristics of the user, such as fingerprints or retinas
  - Posted security guard
  - Sensors, such as RFID tags, to monitor equipment

Service Packs and Security Patches

- Regular security updates are essential to combat new viruses or worms.
- A technician should understand how and when to install patches and updates.
- **Patches** are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack



- A **Service Pack** is a combination of patches and updates.
- Windows automatically downloads and installs updates by default or can be controlled locally;
  - **Start > All Programs > Windows Update > Change settings**

Data Backup

- Windows backups can be done manually or scheduled to takes place automatically.
- To start the Windows 7 Backup Files wizard for the first time, use the following path:
  - **Start> All Programs > Maintenance >Backup and Restore >Set up backup**
- Administrator and Backup Operators are the two Windows default groups that are allowed to back up and restore all files, folders, and subfolders regardless of what permissions are assigned to those files and folders.

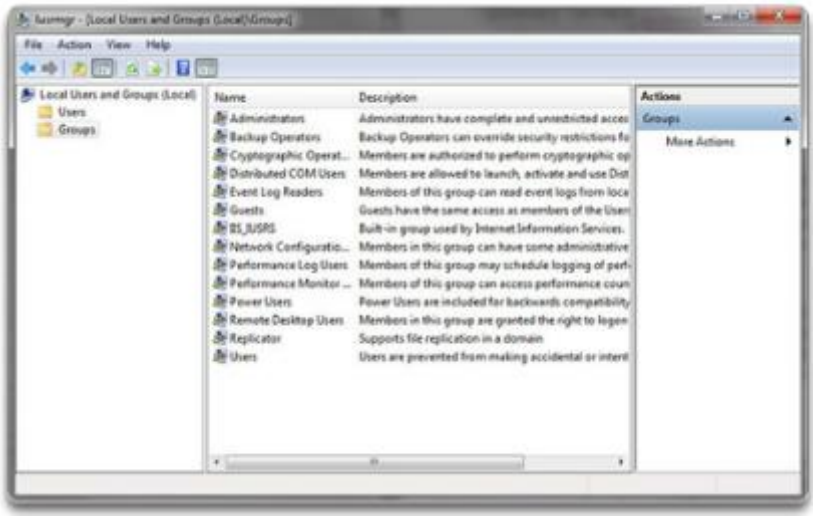
Type of Backup	Description
Full or Normal	This backup type copies all selected files and marks each file as having been backed up.
Incremental	This backup type backs up only files that have been created or changed since the last full or incremental backup. Restoring files requires that you have the last full backup set and all incremental backup sets.
Differential	This backup type copies only files that have been created or changed since the last full backup. Restoring files requires that you have the last full and one differential backup.
Daily	This backup type copies all selected files that have been modified the day that the daily backup has been performed.
Copy	This backup type copies all selected files but does not mark them as having been backed up.

Configuring Firewall Types

- A **Firewall** selectively denies traffic to a computer or network segment.
- **Restrictive security policy** - A firewall that opens only the required ports. Any packet not explicitly permitted is denied.
- Configuring the Windows 7 or Windows Vista firewall can be completed in two ways:
  - **Automatically** - The user is prompted to **Keep Blocking**, **Unblock**, or **Ask Me Later** for unsolicited requests.
  - **Manage Security Settings** – the user adds the program or ports that are required for the applications in use on the network.

Maintaining Accounts

- Group employees by job requirements to give access to files by setting up group permissions.
- When an employee leaves an organization, access to the network should be terminated immediately.
- Guests can be given access through a Guest account.
- To configure all of the users and groups on a computer, type **lusrmgr.msc** in the Search box, or Run Line utility.



Best Practices

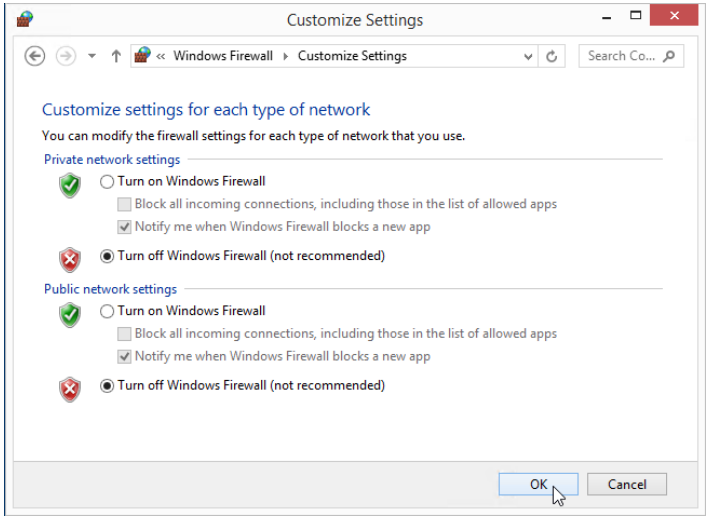
- Best practices for managing user accounts:
  - Limit the number of failed login attempts.
  - Restrict the time of day that users can log into a computer.
  - **User Account Idle Timeout** – logs a user out of a computer after a specified amount of time.

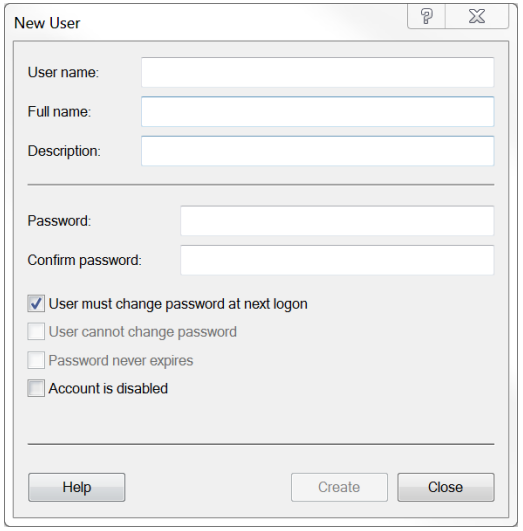
12.3 Common Preventive Maintenance Techniques for Security

Cisco | Networking Academy®
Mind Wide Open™

Security Maintenance

- Maintaining security includes the following:
  - Keep operating systems up-to-date with security patches and service packs.
  - Back up data regularly.
  - Install, enable, and configure a software firewall, such as Windows Firewall.
  - Manage users including removing terminated employees, assigning temporary guest accounts, configuring login times, monitoring failed login attempts, and enforcing idle timeouts and screen locks.
  - In Windows, use the User Account Control or Local Users and Groups Manager to manage users.





12.4 Basic Troubleshooting Process for Security

Cisco | Networking Academy®
Mind Wide Open™

Troubleshooting Process

Step 1 Identify the problem

Step 2 Establish a theory of probable causes

Step 3 Test the Theory to Determine cause

Step 4 Establish a Plan of Action to Resolve the Problem and Implement the Solution

Step 5 Verify Full System Functionality and Implement Preventative Measures

Step 6 Document Findings, Actions, and Outcomes

Common Problems and Solutions for Security

- Security problems can be attributed to hardware, software, or connectivity issues
- Common security problems include:
  - A user receiving thousands of junk emails daily
  - A rogue wireless access point is discovered on the network.
  - User flash drives are infecting computers.
  - Windows update fails.
  - System files have been renamed.

12.5 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Conclusion

This chapter introduced the operation of computer networks. The following concepts from this chapter are important to remember:

- Malicious software (malware) is usually installed without user knowledge; capable of modifying the user's browser; and often collects user information.
- DDoS attacks use botnets located in different geographical places, making it difficult to trace.
- A security policy is a set of security objectives that ensure the security of a network, the data, and the computer systems in an organization.
- Most browsers have features that can be enabled to increase web security.
- Protecting data on computers includes a variety of techniques including firewalls, backing up data, and file/folder permissions.
- Antimalware programs, such as those offered by Malwarebytes, McAffee, Symantec, and Kaspersky, include antivirus protection, adware protection, phishing protection, and spyware protection.
- All Windows computers on a network must be part of either a domain or a workgroup.
- Common security techniques include VPNs, secure WLANs, disable UPnP, updated firmware, firewalls, and a DMZ.
- Store network equipment in a locked wiring closet.
- Maintaining security includes updating operating systems, backing up data regularly, managing firewall configurations, and managing users.
- A security policy should require a systematic preventive maintenance and troubleshooting methodology.


Cisco | Networking Academy®
Mind Wide Open™


CISCO