Chapter 12: Security

IT Essentials v6.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 12 - Sections & Objectives

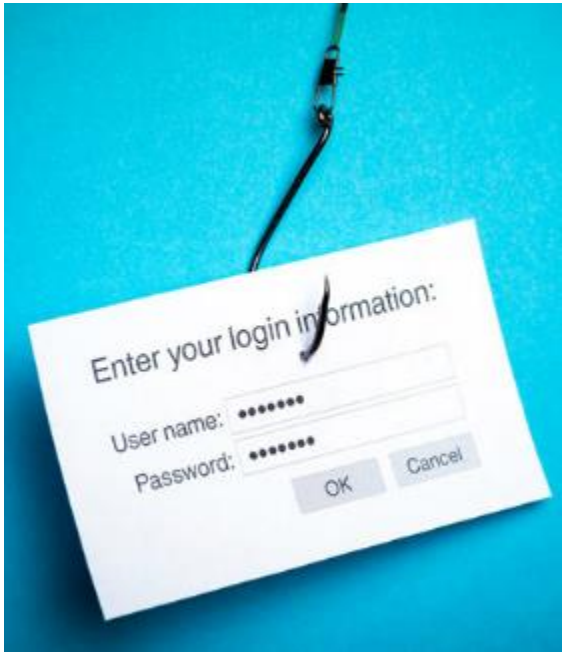
- 12.1 Security Threats
  - Explain security threats.
- 12.2 Security Procedures
  - Configure IT security.
- 12.3 Common Preventive Maintenance Techniques for Security
  - Manage IT security on an ongoing basis.
- 12.4 Basic Troubleshooting Process for Security
  - Explain how to troubleshoot basic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

12.1 Security Threats

Cisco | Networking Academy®
Mind Wide Open™

Types of Security Threats

- Malicious software (malware) is:
  - Usually installed without user knowledge
  - Capable of modifying the user's browser
  - Often collects user information
- Viruses, Trojans, and worms are examples of malware.
- Phishing is designed to trick a user into providing personal or financial information.
- Spam is unsolicited email that is often used for phishing attacks, or to deliver malware.
- Web browser tools, such as Java and Adobe Flash, can make computers more vulnerable to attacks.
- Zero-Day attacks attempt to exploit software vulnerabilities that are unknown or undisclosed by the software vendor.



Types of Security Threats

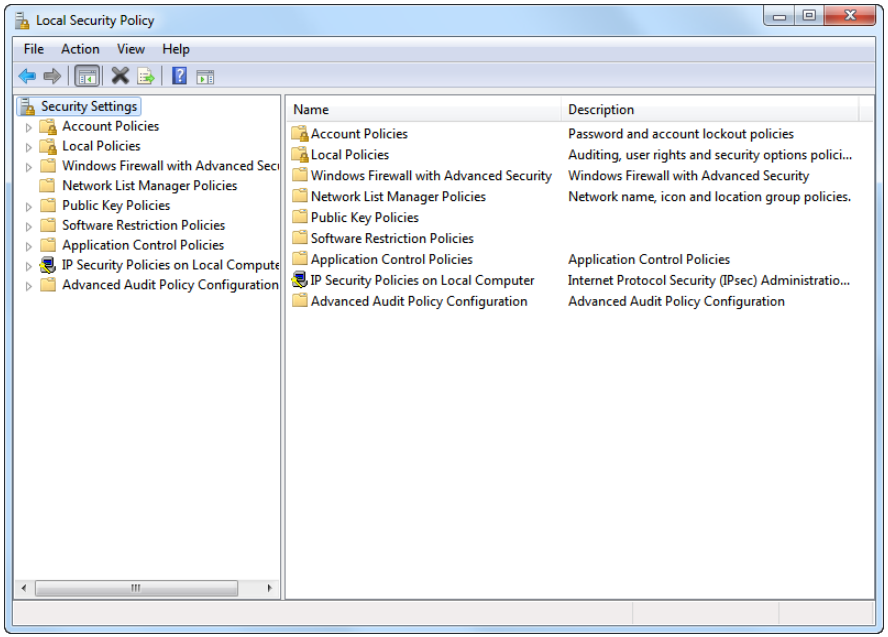
- TCP/IP is vulnerable to a variety of attacks including:
  - Denial of Service (DoS) attacks send an abnormally large amount of traffic. The goal is to completely overwhelm the device that is receiving this traffic so that it cannot respond to legitimate users.
  - Distribute DoS (DDoS) attacks use botnets located in different geographical places, making it difficult to trace the source.
  - A SYN flood attack randomly opens TCP ports at the source of the attack and ties up the network equipment or computer with a large amount of false SYN requests.
  - A spoofing attack is when a computer uses a forged IP or MAC address to impersonate a computer that is trusted on the network.
  - Man-in-the-middle (MitM) is an attacker intercepting communication between two computers.
  - Replay attacks are usually an extension of an MitM attacker, intercepting credentials and then posing as a legitimate source.
  - DNS Poisoning is an attempt to redirect traffic from legitimate websites to an imposter website.

12.2 Security Procedures

Cisco | Networking Academy®
Mind Wide Open™

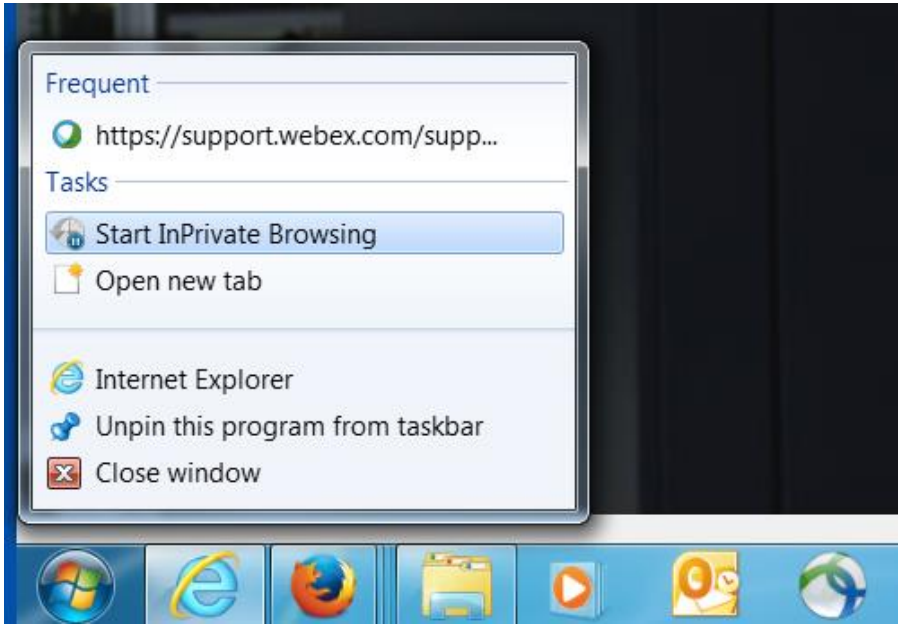
Windows Local Security Policy

- 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.



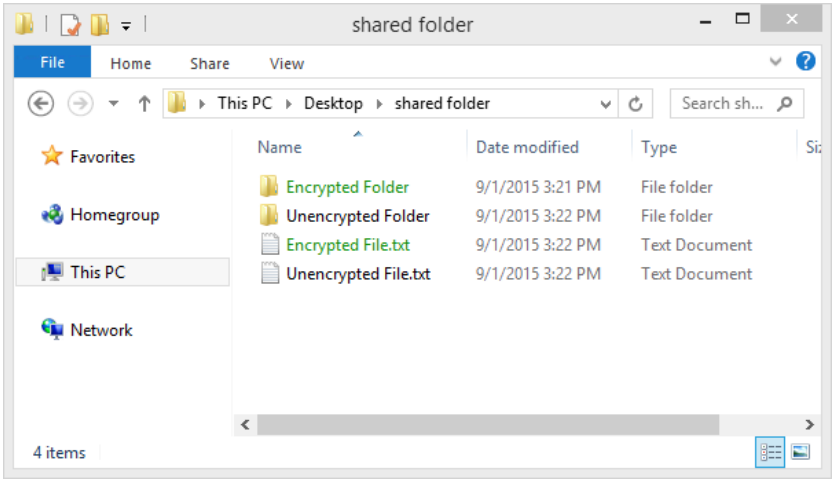
Securing Web Access

- 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



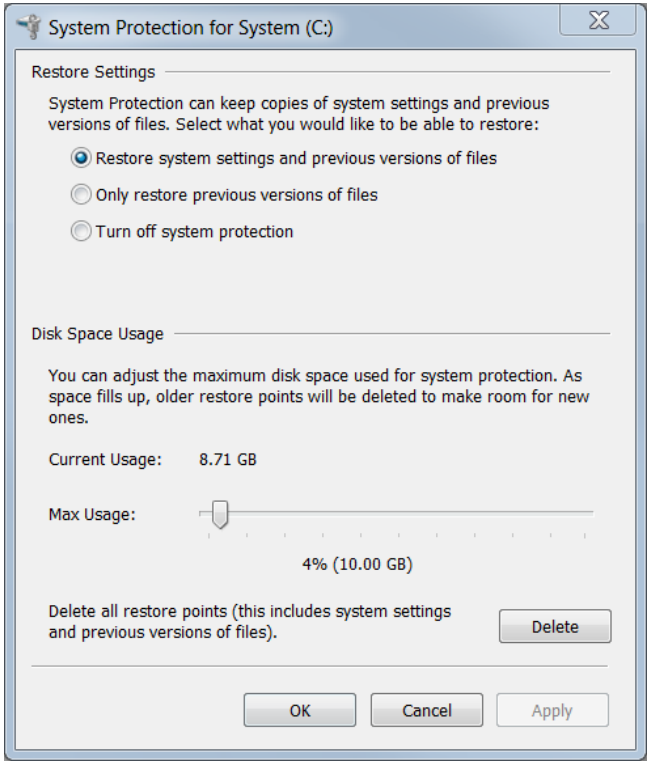
Protecting Data

- 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.



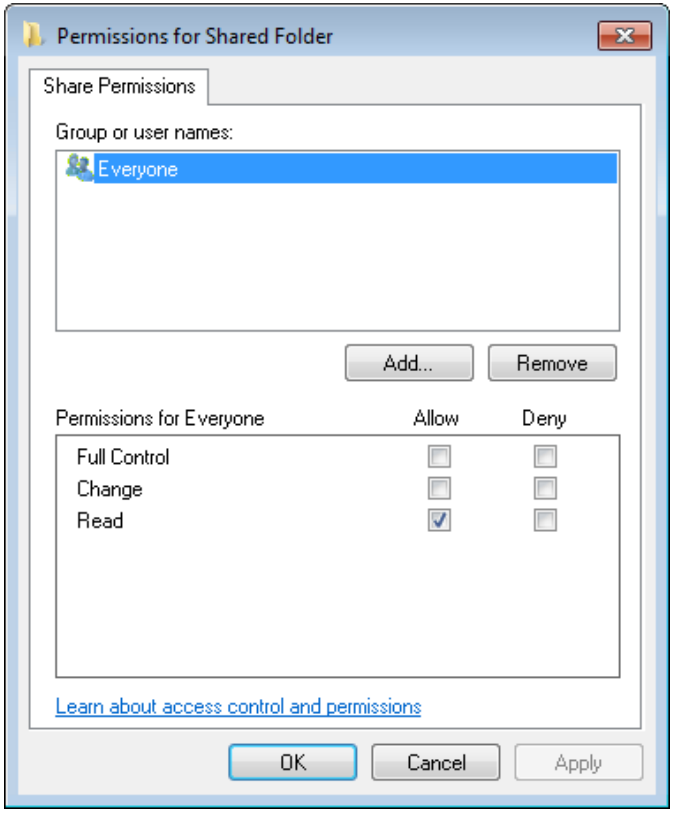
Protection Against Malicious Software

- 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.



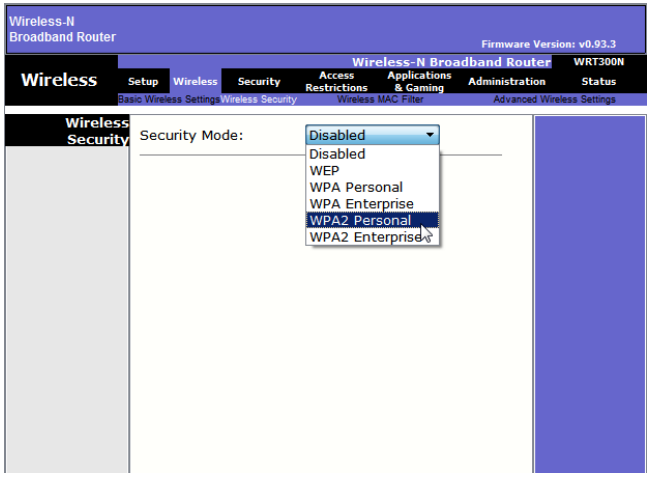
Security Techniques

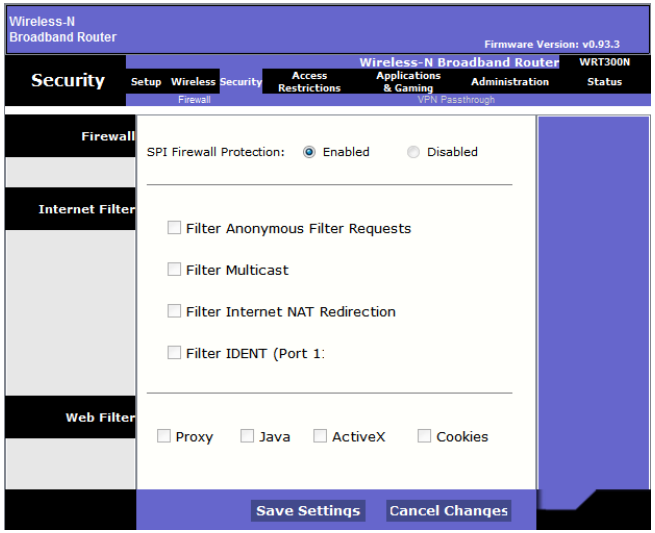
- All Windows computers on a network must be part of either a domain or a workgroup.
- Before computers can share resources, they must share the same domain name or workgroup name.
- Mapping a local drive is a useful way to access a single file, specific folders, or an entire drive between different 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

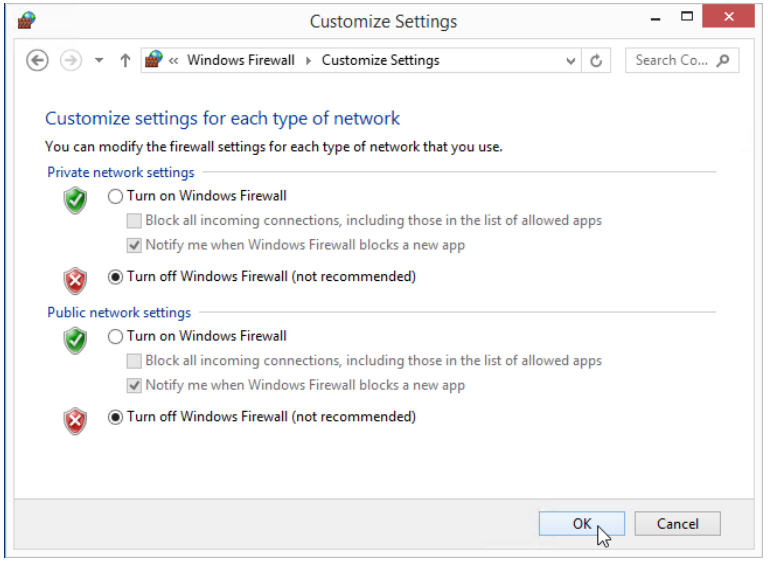
- Common techniques for protecting physical equipment include:
  - Store network equipment in a locked wiring closet
  - Consider setting a BIOS or UEFI password
  - Disable AutoRun and AutoPlay
  - Implement multifactor authentication which includes:
    - Something you know (e.g. password)
    - Something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

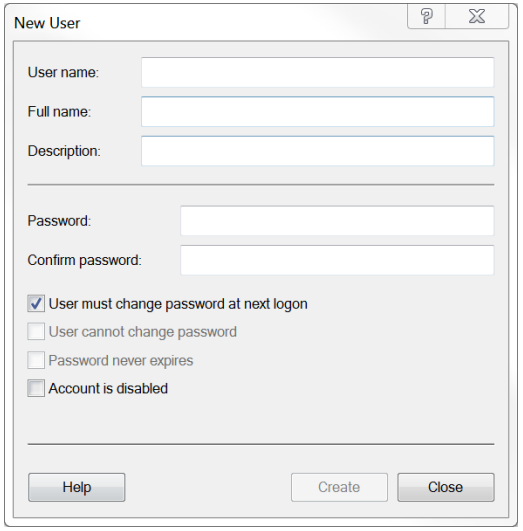
12.3 Common Preventive Maintenance Techniques for Security

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™

Applying the Troubleshooting Process to Security

- Identify the Problem
  - The first step in the troubleshooting process.
  - A list of open and closed-ended questions is useful.
- Establish a Theory of Probable Cause
  - Based on the answers received, establish a theory probable cause.
  - A list of common problems can be useful.
- Test the Theory to Determine Cause
  - Test your theories to determine the cause of the problem.
  - A list of quick procedures to common problems can help.
- Establish a Plan of Action to Resolve the Problem and Implement the Solution
  - A plan of action is needed to solve the problem and implement a permanent solution.

Applying the Troubleshooting Process to Security

- Verify Full System Functionality and, If Applicable, Implement Preventive Measures
  - It is important to perform a full re-scan of the computer.
  - If applicable, implement preventive measures to avoid future problem recurrences, such as enabling automatic updates.
- Document Findings, Actions and Outcomes
  - Findings, actions, and notes should be documented.
  - This log can be helpful for future reference.

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™

Chapter Summary

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 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.