Elk Technologies
https://elktech.org
Scott Stephenson

Chapter 13: Security

IT Essentials v7.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 13 - Sections & Objectives

- 13.1 Security Threats
  - Explain security threats.
    - Describe different types of malware.
    - Describe measures that protect against malicious software.
    - Describe different types of network attacks.
    - Describe different social engineering attacks.
- 13.2 Security Procedures
  - Explain security procedures.
    - Explain what a security policy is.
    - Explain physical security measures.
    - Describe measures that protect data.
    - Describe how to destroy data.

Chapter 13 - Sections & Objectives

- 13.3 Securing Windows Workstations
  - Configure basic security settings and policies for end devices.
    - Explain how to secure a workstation.
    - Configure security using the Windows Local Security Policy tool.
    - Manage Windows users and groups.
    - Configure security using the Windows firewall tool.
    - Configure a browser for secure access.
    - Configure security maintenance in Windows.
- 13.4 Wireless Security
  - Configure wireless security.
    - Configure wireless devices for secure communication.

Chapter 13 - Sections & Objectives

- 13.5 Basic Troubleshooting Process for Security
  - Explain how to troubleshoot basic security problems
    - Explain the six steps of the troubleshooting process for security.
    - Describe advanced problems and solutions for security.

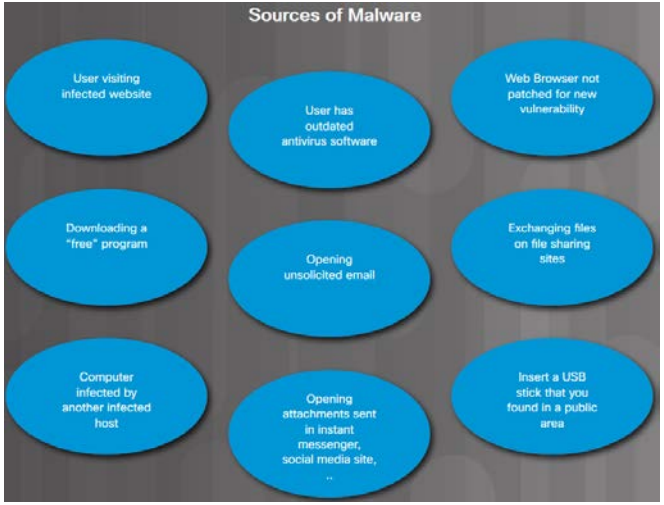
13.1 SECURITY THREATS

Adware, Spyware and Phishing

- **Malicious software (malware)** – 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.

Malware

- There are many types of threats created to disrupt computers and networks.
  - The greatest and most common threat for computers and the data contained on them is malware.
- Malware is typically installed on a computer without user knowledge. Once a host is infected, the malware could:
  - Change the computer configuration.
  - Delete files or corrupt hard drives.
  - Collect information stored on the computer without the user's consent.
  - Open extra windows on the computer or redirect the browser.



Viruses and Trojan Horses

- The first and most common type of computer malware is a **virus**.
  - Viruses require human action to propagate and infect other computers.
  - A virus hides by attaching itself to computer code, software, or documents on the computer. When opened, the virus executes and infects the computer.
- Cybercriminals also use Trojan horses to compromise hosts.
  - A **Trojan horse** is a program that looks useful but also carries malicious code.
  - It is named for its method of getting past computer defenses by pretending to be something useful.
  - Trojan horses are often provided with free online programs such as computer games.
  - Trojans can delete files, rename files, change permission, and give criminals access to your information.

Types of Malware

- **Adware** can display unsolicited advertising using pop-up web browser windows, new toolbars, or unexpectedly redirect a webpage to a different website.
- **Ransomware** typically denies a user access to their files by encrypting the files and then displaying a message demanding a ransom for the decryption key.
- **Rootkits** are difficult to detect and are used by cybercriminals to gain admin level access to a computer. Often, a direct attack on a system using a known vulnerability or password.
- **Spyware** is similar to adware but is used to gather information about the user and send it back to cybercriminals.
- **Worms** are self-replicating programs that propagate automatically without user action by exploiting vulnerabilities in software.

Anti-Malware Programs

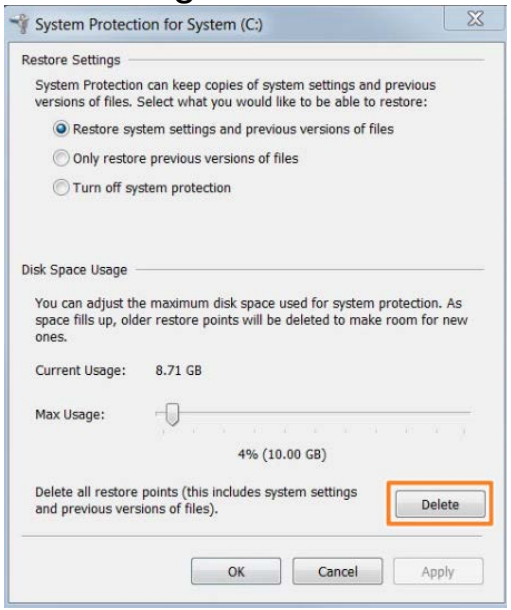
- It is important that you protect computers and mobile devices using reputable antivirus software.
- Today, antivirus programs are commonly referred to as anti-malware programs.
  - Anti-malware programs can detect and block worms, viruses, trojans, rootkits, ransomware, spyware, keyloggers, and adware programs.
  - Anti-malware programs continuously look for known patterns against a database of known malware signatures.
  - They can also use heuristic malware identification techniques which can detect specific behavior associated with some types of malware.

Signature File Updates

- New malware is always being developed; therefore, anti-malware software must be updated regularly. This process is often enabled by default.
- **Signature files** or **definitions** – an important part of how antivirus and antimalware software works. These files contain information (code patterns) about different viruses and malware, which is used by the software to detect, clean, and remove detected threats.
  - Always download the signature files from the manufacturer's website to make sure the update is authentic and not corrupted by malware.
  - To avoid creating too much traffic at a single website, some manufacturers distribute their signature files for download to multiple download sites. These download sites are called mirrors.
  - CAUTION: When downloading signature files from a mirror, ensure that the mirror site is a legitimate site. Always link to the mirror site from the manufacturer's website.

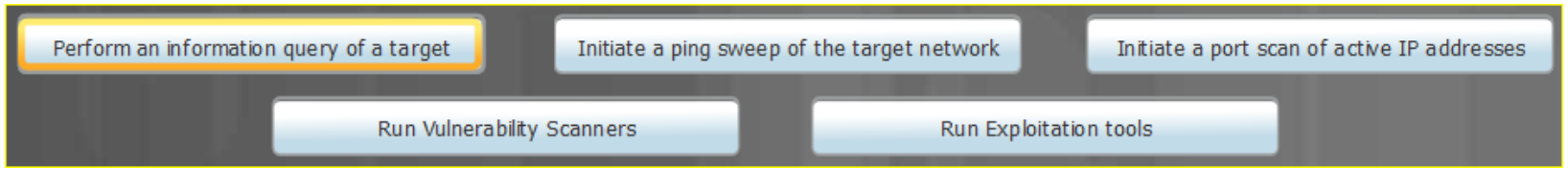
Remediating Infected Systems

- When a malware protection program detects that a computer is infected, it removes or quarantines the threat. However, the computer is most likely still at risk.
- Many antimalware programs can be set to run on system start before loading Windows.
- Removing malware may require that the computer be rebooted into Safe Mode.
- It may be necessary to contact a specialist to ensure that the computer has been completely cleaned. Otherwise, the computer may need to be reformatted, the operating system reinstalled, and your data recovered from the most recent backups.
- The OS system restore service may include infected files in a restore point. Therefore, after a computer has been cleaned of any malware, the system restore files should be deleted.



Networks Are Targets

- Attacker is looking for network information about a target using Google search, whois and other tools.
- Attacker initiates a ping sweep of the discovered target's public network address to determine which IP addresses are active.
- Attacker determines which services are available on the active port using Nmap, SuperScan and other tools.
- Attacker runs vulnerability scanner to discover the type of applications and OSs running on target host using Nipper, Secuna PSI and other tools.
- Attacker attempts to discover vulnerable services to exploit using Metasploit, Core Impact and other tools.



Types of TCP/IP Attacks

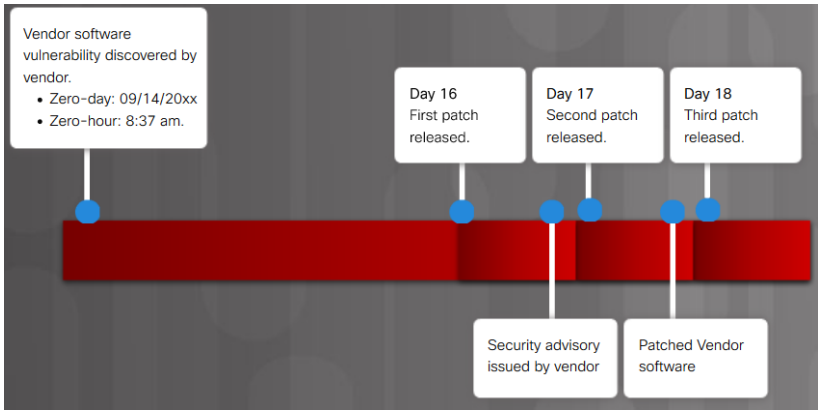
- TCP/IP suite controls communication on the Internet. Can be manipulated to prevents users from accessing normal services.
  - **Denial of Service (DoS)** – an attack where the attacker completely overwhelms a target device with false requests to create a denial of service for legitimate users.
  - **Distributed DoS (DDoS)** – an amplified DoS attack using many infected hosts called **zombies** to overwhelm a target.
  - **DNS Poisoning** – an attack where the attacker has successfully infected a host to accept false DNS records pointing to malicious servers.
  - **Man-in-the-Middle** – an attack where an attacker intercepts communication between two hosts.

Types of TCP/IP Attacks

- TCP/IP suite controls communication on the Internet. Can be manipulated to prevents users from accessing normal services.
  - **Replay** – a type of spoofing attack where the attacker captures an authenticated packet, alters it, and sends it to the original destination.
  - **Spoofing** – an attack where the attacker forges an IP address to gain access to resources.
  - **Syn Flood** – a type of DoS attack that exploits the TCP three-way handshake.
  - **Botnets** – a network of private computers (zombie network) infected with malicious software and controlled as a group without the owners' knowledge.

Zero-Day

- The following two terms are commonly used to describe when a threat is detected:
  - **Zero-day** – Sometimes also referred to as zero-day attacks, zero-day threat, or zero-day exploit. This is the day that an unknown vulnerability has been discovered by the vendor. The term is a reference to the amount of time that a vendor has had to address the vulnerability.
  - **Zero-hou**r – This is the moment when the exploit is discovered.
- The software can be exploited until a patch that addresses the vulnerability is made available.

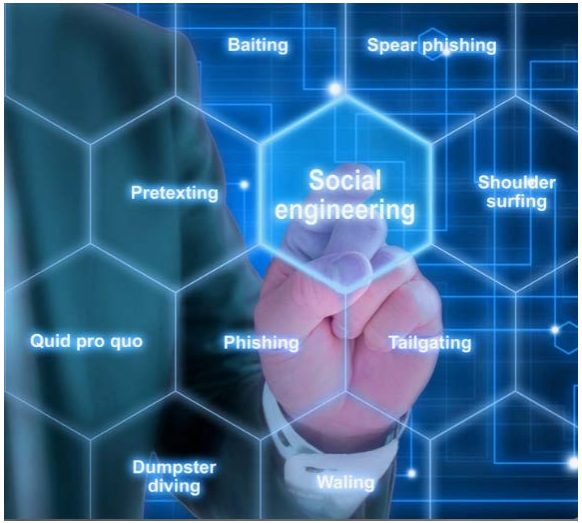


Protecting Against Network Attacks

- There is no single solution to protect against all TCP/IP or zero-day attacks.
- One solution is to use a defense-in-depth approach, also known as a layered approach, to security.
  - This requires a combination of networking devices and services working together in tandem.
- All network devices including the router and switches must be secured to prevent attackers from tampering with the devices.

Social Engineering

- Cybercriminals use **social engineering** techniques to deceive unsuspecting targets into revealing confidential information.
  - An access attack that attempts to manipulate individuals into performing actions or divulging confidential information.
  - Often rely on human nature and people's willingness to be helpful.
- Note: Social engineering is often used in conjunction with other network attacks.



Social Engineering Techniques

- **Pretexting** - An attacker pretends to need personal data in order to confirm the identity of the recipient.
- **Phishing** - An attacker sends fraudulent email disguised as being from a trusted source.
- **Spear Phishing** - An attacker creates a targeted phishing attack for a specific individual or organization.
- **Spam** – Unsolicited email which often contains harmful links, malware, or deceptive content.
- **Something for Something** – When an attacker requests personal information in exchange for something.
- **Baiting** - An attacker leaves a malware infected flash drive in a public location.
- **Impersonation** – An attacker pretends to be someone they are not.
- **Tailgating** – An attacker follows an authorized person into a secure area.
- **Shoulder surfing** - An attacker looks over someone's shoulder to steal information.
- **Dumpster Diving** - An attacker searches through trash for confidential information.

Protecting Against Social Engineering

- Protecting against social engineering attacks:
  - Never give your username or password credentials to anyone.
  - Never leave your credentials where they can easily be found.
  - Never open emails from untrusted sources.
  - Never release work related information on social media sites.
  - Never re-use work related passwords.
  - Always lock or sign out of your computer when unattended.
  - Always report suspicious individuals.
  - Always destroy confidential information according to the organization policy.

13.2 SECURITY PROCEDURES

What is a Security Policy

- A security policy is:
  - a set of security objectives that ensure the security of a network, the data, and the computers in an organization.
  - a constantly evolving document based on changes in technology, business, and employee requirements.
  - usually created by a committee with members consisting of management and IT staff.
- It is up to the IT staff to implement security policy specifications in the network.

Security Policy Identifies

- Which assets require protection?
- What are the possible threats?
- What to do in the event of a security breach?
- What training will be in place to educate the end users?

Security Policy

- Identification and Authentication Policies
- Password Policies
- Acceptable Use Policies
- Remote Access Policies
- Network Maintenance Policies
- Incident Handling Policies

Security Policy Category

- **Identification and Authentication Policies** – Outlines verification procedures and specifies authorized persons that can have access to network resources.
- **Password Policies** – Ensures passwords meet minimum requirements and are changed regularly.
- **Acceptable Use Policies** – Identifies network resources and usages that are acceptable to the organization and may include ramifications for policy violation.
- **Remote Access Policies** – Identifies how remote users access a network and what is accessible?
- **Network Maintenance Policies** – Specifies network device operating systems and end-user application update procedures.
- **Incident Handling Policies** – Describes how security incidents are handled.

Securing Devices and Data

- The goal of the security policy is to ensure a safe network environment and to protect assets.
- An organization's assets include their data, employees, and physical devices such as computers and network equipment.
- The security policy should identify hardware and equipment that can be used to prevent theft, vandalism, and data loss.

Physical Security

- Physical security is as important as data security.
  - For example, if a computer is taken from an organization, the data is also stolen or worse, lost.
- Physical security involves securing:
  - Access to an organization's premise
  - Access to restricted areas
  - The computing and network infrastructure

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

Security Policy Category

- **Conventional lock** – Unlocked by entering the required key into the door handle mechanism.
- **Deadbolt lock** – Unlocked by entering the required key into a lock separate from the door handle mechanism.
- **Electronic lock** – Unlocked by entering a secret combination code or PIN into the keypad.
- **Token-based lock** – Unlocked by swiping a secure card or by using a near proximity reader to detect a smart card or wireless key fob.
- **Biometric lock** – Unlocked by using a biometric scanner such as a thumbprint reader.
- **Multifactor lock** – A lock that uses a combination of the above mechanisms.

Mantraps

- In high-security environments, **mantraps** are often used to limit access to restricted areas and to prevent tailgating.
  - A mantrap is a small room with two doors, one of which must be closed before the other can be opened.
  - Typically, a person enters the mantrap by unlocking one door. Once inside the mantrap, the first door closes and then the user must unlock the second door to enter the restricted area.
- Using security guards that checks IDs can also prevent tailgating.

Securing Computers and Network Hardware

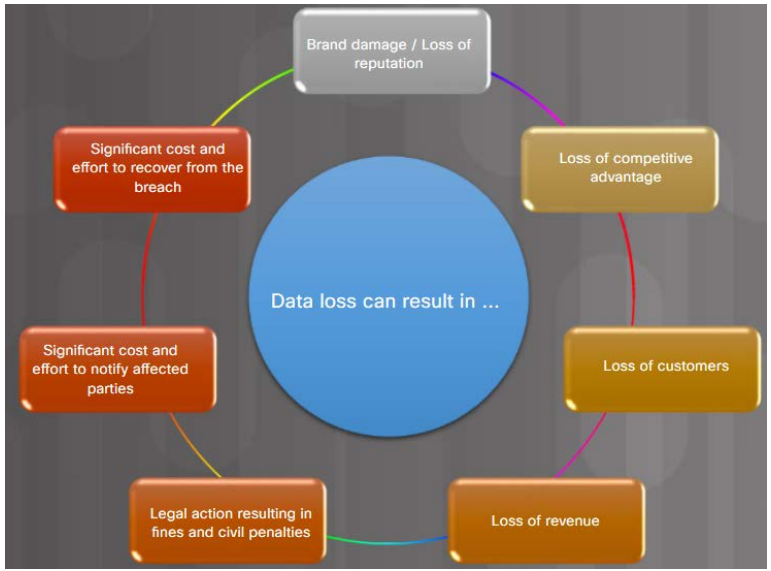
- Organizations must protect their computing and network infrastructure.
  - This includes cabling, telecommunication equipment, and network devices.
- There are several methods of physically protecting computer and networking equipment.
- Network equipment should only be installed in secured areas. As well, all cabling should be enclosed within conduits or routed inside walls to prevent unauthorized access or tampering.

Securing Computers and Network Hardware

- Factors that determine the most effective equipment to use to secure equipment and data include:
  - How the equipment is used
  - Where the computer equipment is located
  - What type of user access to data is required
- For example:
  - A computer in a busy public place requires additional protection from theft and vandalism.
  - In a busy call center, a server may need to be secured in a locked equipment room.
  - While using a laptop in a public place, a security dongle and key fob ensure that the computer locks if the user and laptop are separated.

Data – Your Greatest Asset

- Data is likely to be an organization's most valuable assets. Organizational data may include research and development, sales, financial, human resource, employee, and customer data.
- Data can be lost or damaged in circumstances such as theft, equipment failure, or a disaster.
- Data loss or exfiltration are terms used to describe when data is lost, stolen, or leaked to the public.
- Data can be protected from data loss using data backups, file/folder encryption and permissions.

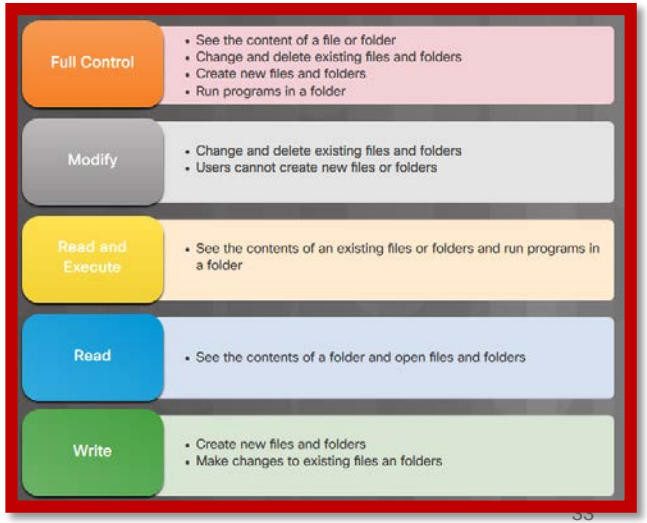


Data Backups

- Backing up data is one of the most effective ways of protecting against data loss.
  - A data backup stores a copy of the information on a computer to removable backup media
  - Data backups should be performed on a regular basis as identified in the security policy.
  - Data backups are usually stored offsite to protect the backup media if anything happens to the main facility.
- Windows hosts have a backup and restore utility.
- macOS hosts have a **Time Machine** utility to perform backup and restore functions.

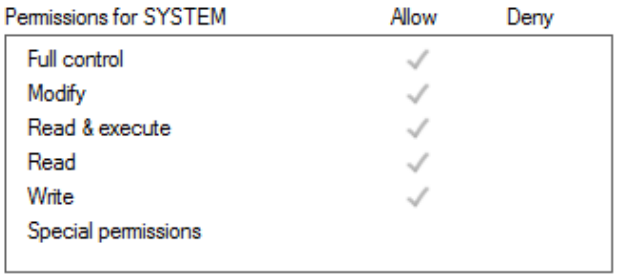
File and Folder Permissions

- 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.



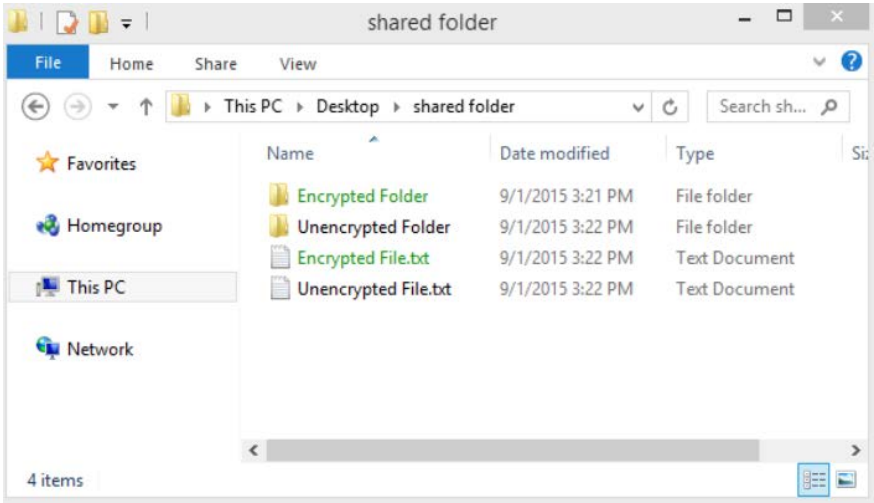
File and Folder Permissions

- 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.



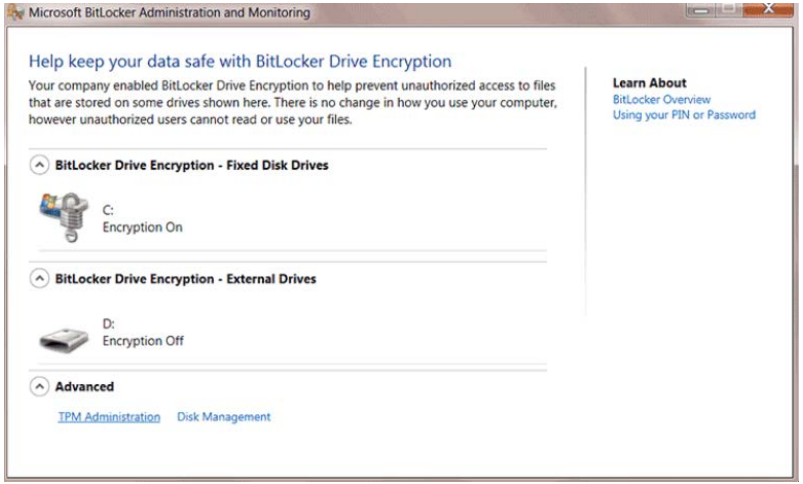
File and Folder Encryption

- Encryption is often used to protect data.
  - Encryption is where data is transformed using a complicated algorithm to make it unreadable.
  - A special key must be used to return the unreadable information back into readable data.
- **Encrypting File System (EFS)** is a Windows feature that can encrypt data.
  - EFS is directly linked to a specific user account.
    - Only the user that encrypted the data will be able to access it after it has been encrypted.



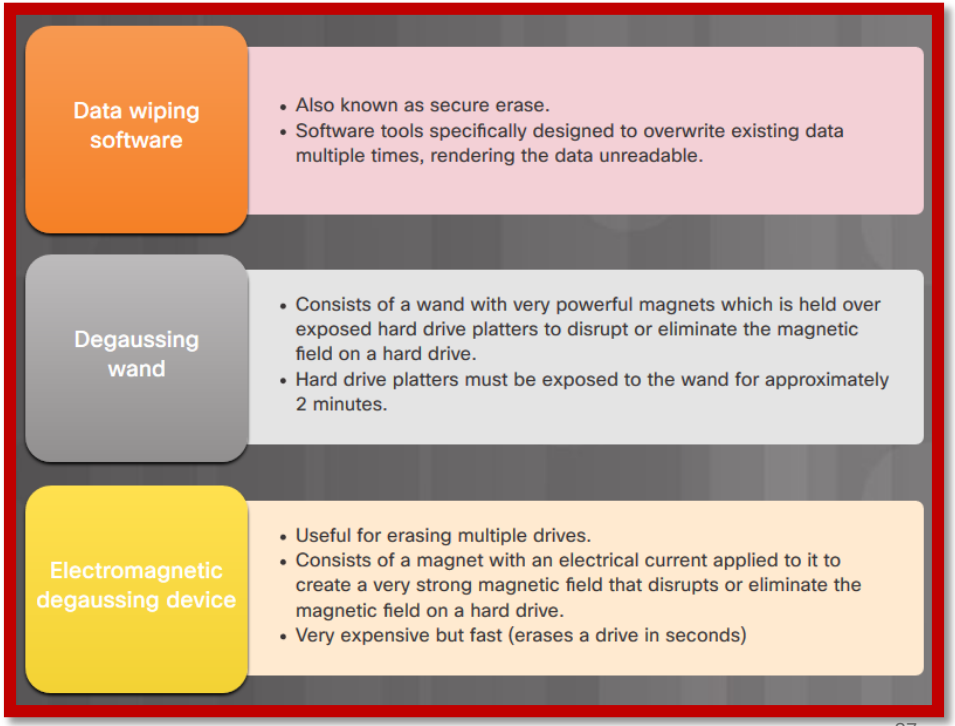
Windows BitLocker and BitLocker to Go

- You can encrypt an entire hard drive using a feature called **BitLocker**.
- To use BitLocker:
  - At least two volumes must be present on a hard disk.
  - The **Trusted Platform Module (TPM)** must be enabled in BIOS.
    - The TPM is a specialized chip installed on the motherboard that stores encryption keys, digital certificates, and passwords.
- BitLocker encryption can also be used with removable drives by using **BitLocker To Go**.
  - BitLocker To Go does not use a TPM chip, but still provides encryption and requires a password.



Data Wiping Magnetic Media

- Protecting data also includes removing files from storage devices when they are no longer needed.
- Simply deleting files or reformatting the drive may not be enough to ensure your privacy.
- Software tools can be used to recover folders, files, and even entire partitions.
  - For this reason, storage media should be fully erased using one or more of the methods listed in the figure.



Data Wiping Other Media

- SSDs are comprised of flash memory instead of magnetic platters.
  - Common techniques used for erasing data such as degaussing are not effective with flash memory.
  - Perform a secure erase to fully ensure that data cannot be recovered from an SSD and hybrid SSD.
- Other storage media and documents (e.g., optical disks, eMMC, USB sticks) must also be destroyed.
  - Use a shredding machine or incinerator that is designed to destroy documents and each type of media.
- When thinking about what devices must be wiped or destroyed, remember that devices besides computers and mobile devices store data.
  - Printers and multifunction devices may also contain a hard drive that caches printed or scanned documents. This caching feature can be turned off in some instances, or the device needs to be wiped on a regular basis.

Hard Drive Recycling and Destruction

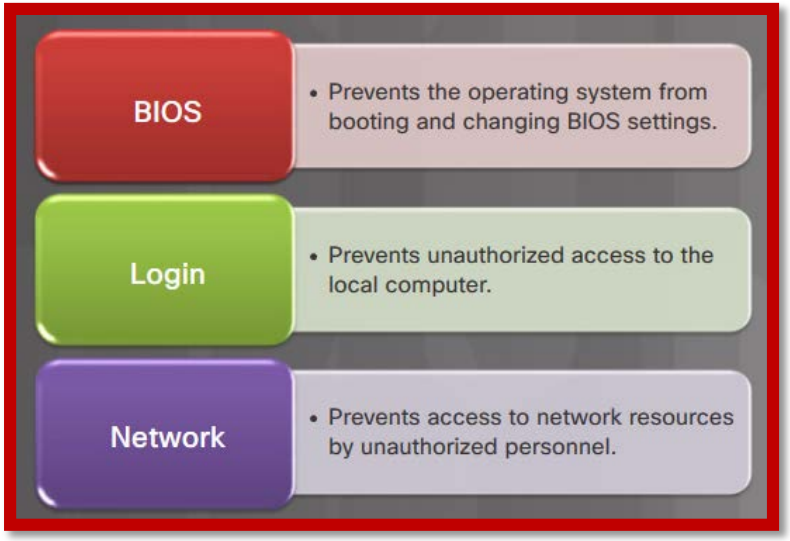
- When a storage media is no longer needed, the media can either be:
  - **Destroyed** - Destroying the hard drive fully ensures that data cannot be recovered from a hard drive.
  - **Recycled** - Hard drives that have been wiped can be reused in other computers. The drive can be reformatted, and a new operating system installed.

Low-level Format	• The surface of the disk is marked with sector markers identifying tracks where the data will be physically stored on the disk. • Most often performed at the factory after the hard drive is assembled.
Standard Format	• Also called high-level formatting. • Process creates a boot sector and a file system. • A standard format can only be performed after a low-level format has been completed.

13.3 SECURING WINDOWS WORKSTATIONS

Securing a Computer

- Computers and workstations should be secured from theft.
  - Lock your workstation when you are not present to prevent unauthorized users from stealing or accessing local computer and network resources.
  - If you must leave a computer in an open public area, cable locks should be used to deter theft.
  - Use a privacy screen to protect the information displayed on your screen from prying eyes.



Securing a Computer

- Access to your computer must also be protected.
- There are three levels of password protection that can be used on a computer:
  - **BIOS** – Prevents the operating system from booting and changing BIOS setting.
  - **Login** – Prevents unauthorized access to the local computer.
  - **Network** – Prevents access to network resources by unauthorized personnel.

Securing BIOS

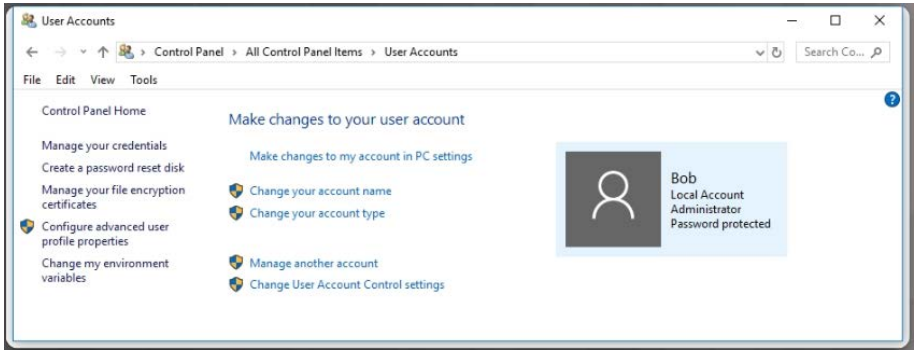
- A Windows, Linux, or Mac login password can be bypassed.
- Setting a BIOS or UEFI password prevents someone from altering the configured setting and may also prevent someone from booting the computer.
- All users, regardless of user account, share BIOS passwords.
- UEFI passwords can be set on a per-user basis, however, an authentication server is required.

Securing Windows Login

- The most common type of password protection is the computer login.
- Depending on your computer system, Windows 10 may also support other sign-in options. Specifically, Windows 10 supports the following sign-in options:
  - **Windows Hello** – Feature that enables Windows to use facial recognition or use your fingerprint to access Windows.
  - **PIN** – Enter a pre-configured PIN number to access Windows.
  - **Picture password** - You choose a picture and gestures to use with the picture to create a unique password.
  - **Dynamic lock** – Feature makes Windows lock when a pre-paired device such as a cell phone goes out of range of the PC.

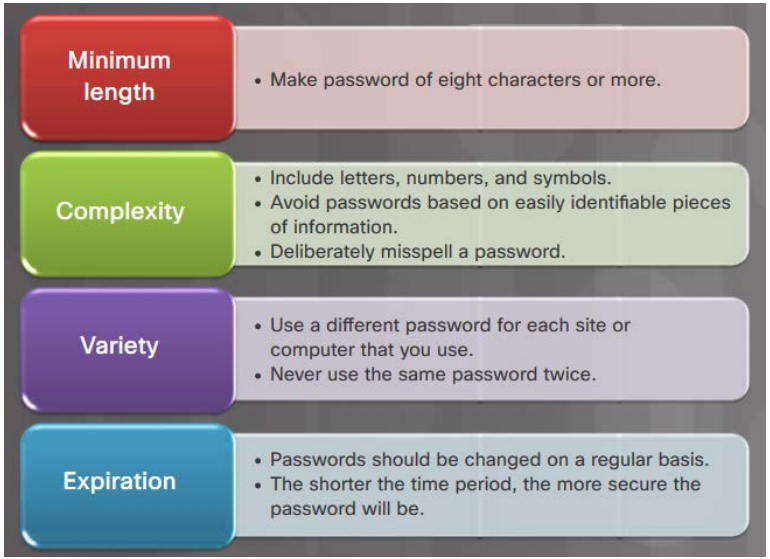
Local Password Management

- Password management for stand-alone Windows computers can be set locally using the Windows **User Accounts** tool.
  - To create, remove, or modify a password in Windows, use Control Panel > User Accounts
- It is also important to make sure that computers are secure when users are away.
  - A security policy should contain a rule about requiring a computer to lock when the screensaver starts.
  - In all versions of Windows, use Control Panel > Personalization > Screen Saver
    - Choose a screen saver and a wait time, and then select the On resume, display logon screen option.



Usernames and Passwords

- Password guidelines are an important component of a security policy.
- Usernames, like passwords, are an important piece of information and should not be revealed.
- Passwords help prevent theft of data and malicious acts.
- Any user that must log on to a computer or connect to a network resource should be required to have a password.
- Passwords also help to confirm that the logging of events is valid by ensuring that the user is the correct person.



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.
  - **Variety** – Use a different password for each site or computer that you use.
  - **Expiration** – 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. Shorter time period are more secure.

The Windows Local Security Policy

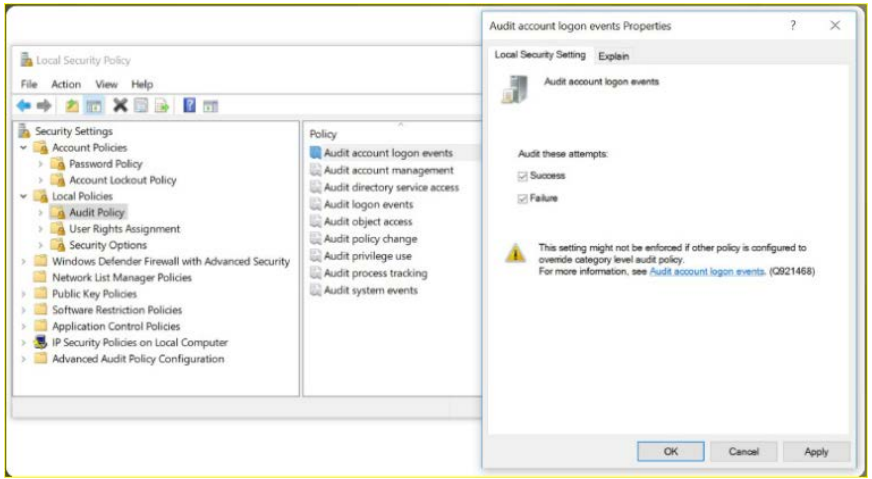
- In most networks that use Windows computers, Active Directory is configured with Domains on a Windows Server.
  - Windows computers are members of a domain.
  - The administrator configures a Domain Security Policy that applies to all computers that join.
  - Account policies are automatically set when a user logs in to Windows.
- For stand-alone computers that are not part of an Active Directory domain, the Windows Local Security Policy can be used to enforce security settings.
  - To access Local Security Policy in Windows 7 and Vista, use Start > Control Panel > Administrative Tools > Local Security Policy.
  - In Windows 8, 8.1, and Windows 10, use Search > **secpol.msc** and then click secpol.
- Note: In all versions of Windows, you can use the Run command secpol.msc to open the Local Security Policy tool.

Account Policies Security Settings

- The security policy will identify the password policies required.
- The Windows local security policy can be used to implement the password policies.
  - Use **Account Policies** > **Password Policy** to enforce password requirements
  - Use **Account Policies** > **Account Lockout Policy** to prevent brute-force attacks
    - This Account Lockout Policy would also protect against a dictionary attack. This is a type of brute-force attack that attempts every word in a dictionary hoping to gain access.

Local Policies Security Settings

- The Local Policy in the Local Security Policy is used to configure audit policies, user rights policies, and security policies.
  - It can also be used to log successful and unsuccessful login attempts.
- Use the Local Policies > Audit Policy to enable auditing.



Exporting the Local Security Policy

- An administrator may need to implement an extensive local policy for user rights and security options. This policy most likely would need to be replicated on each system.
- To help simplify this process, the **Local Security Policy** can be exported and copied to other Windows hosts.
- The steps to replicate a Local Security Policy on other computers are:
  1. Use the Action > Export List… feature to export the policy of a secure host.
  2. Save the policy with a name, such as workstation.inf. to external media.
  3. Then import the Local Security Policy file to other stand-alone computers.

Maintaining Accounts

- **Terminating Employee Access** – When an employee leaves an organization, immediately disable the account, or change login credentials.
- **Guest Access** – Special guest account for temps and guests with additional privileges can be created and disabled as required.
- **Track Login Times** – Allow employee login only during specified hours of the day, and block logins the rest of the day.
- **Log Failed Login Attempts** – Configure a specified number of times a user can attempt to login.
- **Idle Timeout and Screen Lock** – Configure an idle timer to automatically log the user out. User must log back in to unlock the screen.

Managing Users Account Tools and User Account Tasks

User Account Control (UAC)	• Control Panel > User Accounts > Manage another account • Use this to add, remove, or change attributes of individual users. • When logged in as an administrator, use the UAC to configure settings to prevent malicious code from gaining administrative privileges.
Local Users and Groups Manager	• Control Panel > Administrative Tools > Computer Management > Local Users and Groups • Can be used to create, configure, and manage users and groups rights and permissions that are stored locally on a computer.

Local Users and Groups Manager

- The Local Users and Groups tool can limit the ability of users and groups to perform certain actions by assigning rights and permissions
- To configure all of the users and groups on a computer using the Local Users and Groups Manager tools, type lusrmgr.msc in the Search box, or Run Line utility.
  - The Local Users and Groups > Users window displays current user accounts on the computer.
- Double-clicking a user or right-clicking and choosing Properties opens the user properties window:
    - change the user options defined when the user was created
    - lock an account
    - assign a user to a group
    - control which folders the user has access to.
    - To add a user, click the Action menu and select New User.
    - Here you can assign a username, full name, description, and account options.

Managing Groups

- Users can be assigned to groups for easier management.
- The Local Users and Groups Manager tool is used to manage local groups on a Windows computer.
  - Use Control Panel > Administrative Tools > Computer Management > Local Users and Groups to open the Local Users and Groups Manager.
  - From the Local Users and Groups window, double-click Groups to list all of the local groups on the computer.
- Double click a group to view its properties.
- To create a new group, click the Action > New Group to open the New Group window
  - Here you can create new groups and assign users to them.

Active Directory Users and Computers

- While local accounts are stored in the in the Local Security Accounts database of a local machine, domain accounts are stored in the Active Directory on a Windows Server Domain Controller (DC).
- Only domain administrators are allowed to create domain accounts on the Domain Controller.
  - Domain accounts are accessible from any computer joined to the domain.
- The Active Directory is a database of all computers, users, and services in an Active Directory domain.
  - The Active Directory Users and Computers console on Windows server is used to manage Active Directory users, groups, and Organizational Units (OUs).
    - Organizational units provide a way to subdivide a domain into smaller administrative units.
- Creating a new group account in active directory is similar to creating a new user.
  - Open Active directory Users and Computers and select the container that will house the group, click Action, click New and then click Group and fill in the group details and click OK.

Firewalls

- A firewall protects computers and networks by preventing undesirable traffic from entering internal networks.
- A firewall can allow outside users-controlled access to specific services.
- Firewall services can be provided as follows:
  - **Host-based firewall** – Using software such as Windows Defender Firewall.
  - **Small office home office (SOHO)** – Network-based solution using a home or small office wireless router.
  - **Small to medium-sized organization** - Network-based solution using a dedicated device such as a **Cisco Adaptive Security Appliance (ASA)** or enabled on a **Cisco Integrated Services Router (ISR)**.
  - The focus of this section is on the host-based firewall solution using Windows Firewall.

Software Firewalls

- A software firewall is a program that provides firewall services on a computer to allow or deny traffic to the computer.
  - A software firewall applies a set of rules to data transmissions through inspection and filtering of data packets.
- Windows Firewall is an example of a software firewall that helps prevent cybercriminals and malware from gaining access to your computer.
  - It is installed by default when the Windows OS is installed.
    - Note: In Windows 10 the Windows Firewall was renamed to Windows Defender Firewall. In this section, Windows Firewall includes Windows Defender Firewall.
- Windows Firewall settings are configured using the Windows Firewall window.
  - To change Windows Firewall settings, you must have administrator privileges to open the Windows Firewall window.
  - To open the Windows Firewall window, use Control Panel > Windows Firewall.

Windows Firewall

- Windows Firewall has a standard set of inbound and outbound rules that are enabled depending on the location of the connected network.
  - Firewall rules can be enabled for a private network, a guest or public network, or a corporate domain network.
- From the Windows Firewall window, you can enable or disable Windows Firewall, change notification settings, allow apps through the firewall, configure advanced settings, or restore firewall defaults.
- If you wish to use a different software firewall, you will need to disable Windows Firewall.
- Note: Using more than one firewall or antivirus may cause adverse effects and leave your computer vulnerable.

Configuring Exceptions in Windows Firewall

- You can allow or deny access to specific programs or ports from the Windows Firewall window.
- To configure exceptions and allow or block applications or ports, click on **Allow an app or feature through the Windows Firewall** to open the allowed apps window and be able to:
  - Add an allowed program or port
  - Change an allowed program or port
  - Remove an allowed program or port

Windows Firewall with Advanced Security

- Another Windows tool that is available to provide even greater access control with Windows Firewall policies is the Windows Firewall with Advanced Security.
  - It is called Windows Defender Firewall with Advanced Security in Windows 10.
- To open it, from the Windows Firewall window, click on Advanced settings to open it.
  - Note: Alternatively, enter **wf.msc** in the search box and press enter.
- Windows Defender Firewall with Advanced Security provides these features:
  - **Inbound and Outbound Rules** – Configure inbound rules that are applied to incoming internet traffic and outbound rules which are applied to traffic leaving your computer.
  - **Connection Security Rules** – Secures traffic between two computers and requires that both computers have the same rules defined and enabled.
  - **Monitoring** – Displays the firewall inbound or outbound active rules or any active connection security rules.

Hardware Firewalls

- A hardware firewall passes two different types of traffic into your network:
  - Responses to traffic that originates from inside your network
  - Traffic destined for a port that you have intentionally left open
- There are several types of hardware firewall configurations:
  - **Packet filter** - Packets cannot pass through the firewall, unless they match the established rule set configured in the firewall. Traffic can be filtered based on different attributes, such as source IP address, source port or destination IP address or port. Traffic can also be filtered based on destination services or protocols such as WWW or FTP.
  - **Stateful Packet Inspection (SPI)** - This is a firewall that keeps track of the state of network connections traveling through the firewall. Packets that are not part of a known connection are dropped.

Hardware Firewalls

- There are several types of hardware firewall configurations:
  - **Application layer** - All packets traveling to or from an application are intercepted. All unwanted outside traffic is prevented from reaching protected devices.
  - **Proxy** - This is a firewall installed on a proxy server that inspects all traffic and allows or denies packets based on configured rules. A proxy server is a server that is a relay between a client and a destination server on the Internet.
  - A **Demilitarized Zone (DMZ)** is a subnetwork that provides services to an untrusted network. An email, web, or FTP server is often placed into the DMZ so that the traffic using the server does not come inside the local network. This protects the internal network from attacks by this traffic but does not protect the servers in the DMZ in any way.

Web Security

- Web browsers are not only used for web browsing, they are also now used to run other applications including Microsoft 365, Google docs, interface for remote access SSL users, and more.
- To help support these additional features, browsers use plug-ins to support other content.
  - However, some of these plug-ins may also introduce security problems.
- Browsers are targets and should be secured.

Web Security

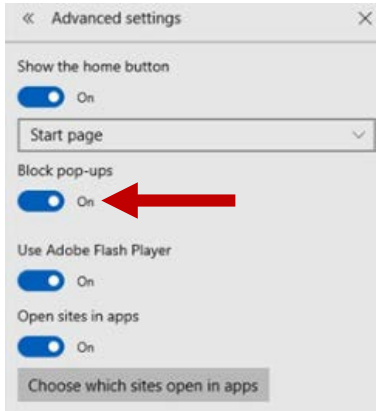
- Tools that make web pages powerful can make computers vulnerable:
  - **Active X** – Controls interactivity on web pages.
  - **Java** – Allows applets to run within a browser.
  - **Java Script** – Interacts with HTML source code to allow interactive web sites.
  - **Adobe Flash** – used to create 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

- Web browsers retain information about the web pages that you visit, the searches that you perform, and other identifiable information including usernames, passwords, and more.
- The information retained by web browsers can be recovered and exploited to steal your identity, your money, or change your passwords on important accounts.
- To improve security when using a public computer, always:
  - **Clear your browsing history** – All web browser have a way to clear their browsing history, cookies, files, and more.
  - **Use the InPrivate mode** – Using an InPrivate browser temporarily stores files and cookies and deletes them when the InPrivate session has ended.
- For Internet Explorer 11, use Tools > InPrivate Browsing
  - Note: As an alternative press Ctrl+Shift+P to open an InPrivate window.

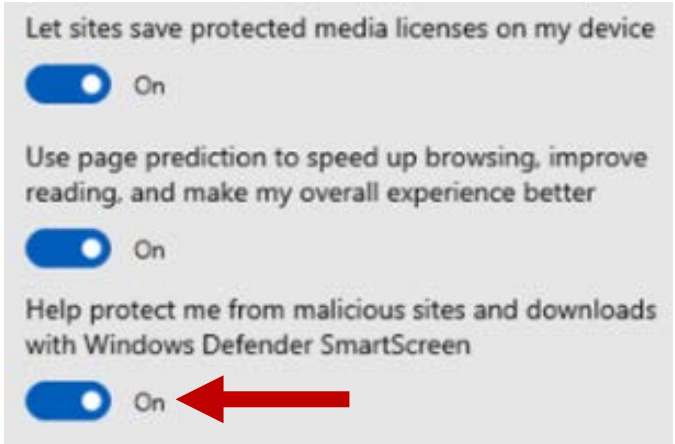
Pop-up Blocker

- Pop-ups are initiated while browsing, such as a link on a page that opens a pop-up to deliver additional information or a close-up of a picture.
- Some pop-ups are initiated by a website or advertiser and are often unwanted or annoying.
- Most web browsers offer the ability to block pop-up windows.
  - This enables a user to limit or block most of the pop-ups that occur while browsing the web.
  - To enable the Internet Explorer 11 Pop-up Blocker feature, use Tools > Pop-up Blocker > Turn on Pop-up Blocker.
  - To enable the MS Edge Pop-up blocker feature:
    - Click on More actions three dotted icon (...) on the right-hand side of MS Edge.
    - Select Settings.
    - Under the Advanced settings label select View advanced settings.
    - Ensure the block pop-ups slider is On.



SmartScreen Filter

- To use SmartScreen Filter:
  1. Click on More actions three dotted icon (...) on the top right-hand side of MS Edge.
  2. Select Settings.
  3. Under the Advanced settings label select View advanced settings.
  4. Scroll to the bottom of this list to the Help protect me from malicious sites and downloads with Windows Defender SmartScreen and ensure the slider is On.



ActiveX Filtering

- Some web browsers may require you to install an ActiveX control.
  - ActiveX controls can be used for malicious reasons.
- When ActiveX filtering is enabled, you can choose which websites are allowed to run ActiveX controls.
  - Sites that are not approved cannot run these controls, and the browser does not show notifications for you to install or enable them.
- To enable ActiveX filtering in Internet Explorer 11, use Tools > ActiveX Filtering.
- To view a website that contains ActiveX content when ActiveX filtering is enabled, click the blue ActiveX Filtering icon in the address bar, and click Turn off ActiveX Filtering.
  - After viewing the content, you can turn ActiveX filtering for the website back on by following the same steps.

Restrictive Settings

- Devices often come with security features that are not enabled or the security features use default settings.
  - Default permissive settings may leave devices exposed to attackers.
- Many devices now ship with restrictive settings and must be configured to enable access.
- It is your responsibility to secure devices and configure restrictive settings whenever possible.

Disable Auto-Play

- Older Windows hosts used AutoRun to simplify the user experience.
  - When new media (e.g., flash drive, CD, or DVD drive) is inserted into the computer, AutoRun would automatically look for a file named autorun.inf and execute it.
  - Malicious users used this feature to infect hosts.
- Newer Windows hosts now use AutoPlay.
- AutoPlay provides additional controls and can prompt the user to choose an action based on the content of the new media.
  - Use the Control Panel > AutoPlay window, to open the AutoPlay window and configure the actions associated with specific media.
- The most secure solution is to turn off AutoPlay.

Operating System Service Packs and Security Patches

- Infections can cause unexpected performance (system files renamed, file permissions changed, users locked out).
- **Patches** are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack.
  - Manufacturers can combine patches and upgrades into a comprehensive update application called a **service pack**.
- It is critical to apply security patches and OS updates whenever possible.
- Windows routinely checks the Windows Update website for high-priority updates that can help protect a computer from the latest security threats.
  - Depending on the setting you choose, Windows automatically downloads and installs any high-priority updates that your computer needs or notifies you as these updates become available.
- Note: Missing a prior update can cause later updates to fail.

13.4 CONFIGURE WIRELESS SECURITY

Common Communication Encryption Types

- Communication between two computers may require secure communication.
- There are two major requirements:
  - The first requirement is that received information has not been altered by someone who has intercepted the message.
  - The second is that anyone who can intercept the message is unable to read it.
- The following technologies accomplish these requirements:
  - Hash encoding
  - Symmetric encryption
  - Asymmetric encryption

Common Communication Encryption Types

- **Hash encoding**, or **hashing**, ensures the integrity of the message.
  - This means that the message is not corrupt, nor has it been tampered with during transmission.
  - Hashing uses a mathematical function to create a numeric value, called a message digest that is unique to the data
  - The most popular hashing algorithm is **Secure Hash Algorithm (SHA)**, which is replacing the older **Message Digest 5 (MD5)** algorithm.

Common Communication Encryption Types

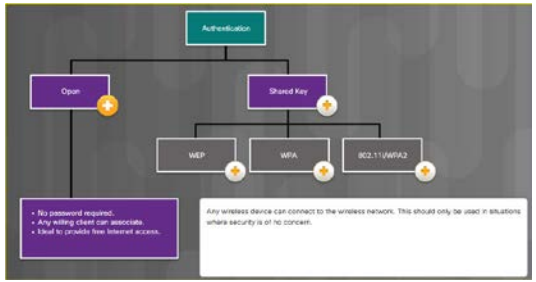
- **Symmetric** encryption ensures the confidentiality of the message.
  - If an encrypted message is intercepted, it cannot be understood. It can only be decrypted (i.e., read) using the password (i.e., key) that it was encrypted with.
  - Symmetric encryption requires both sides of an encrypted conversation to use an identical encryption key to encode and decode the data.
  - Advanced Encryption Standard (AES) and the older Triple Data Encryption Algorithm (3DES) are examples of symmetric encryption.
- **Asymmetric** encryption also ensures confidentiality of the message.
  - It requires two keys, a **private key** and a **public key**.
  - The public key can be widely distributed, including emailing in plain text or posting on the web.
  - The private key is kept by an individual and must not be disclosed to any other party.
  - RSA is the most popular example of asymmetric encryption.

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 devices can detect the wireless network.
- If the SSID broadcast setting has been disabled on a wireless router or access point, users must manually enter the SSID on wireless clients to connect to the wireless network.
  - Disabling the SSID broadcast provides very little security:
    - Someone who knows the SSID of the wireless network can manually enter it.
    - A wireless network will also broadcast the SSID during a computer scan.
    - A SSID can also be intercepted in transit.

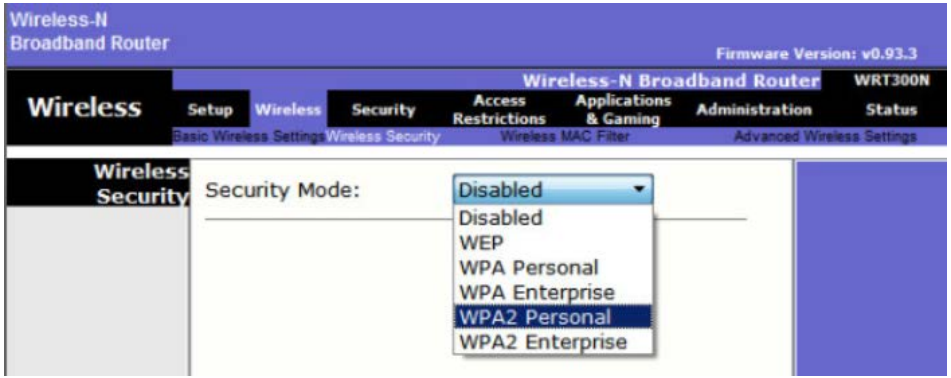
Authentication Methods

- A Shared Key provides mechanisms to authenticate and decrypt data between a wireless client and AP of wireless router.
- **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.
  - IEEE 802.11i/WPA2 is the current industry standard for securing WLANs.
  - Both use the **Advanced Encryption Standard (AES)**.



Wireless Security Modes

- Use a wireless encryption system to encode the information being sent to prevent unwanted capture and use of data.
- Most wireless access points support several different security modes.
- Always implement the strongest security mode possible which is (WPA2).
- WPA2 Personal is for home and SOHO use.
- WPA2 Enterprise is for businesses implementing Radius or TACACS+ servers.



Wireless Security Modes

- Many routers offer **Wi-Fi Protected Setup (WPS)**.
  - Both the router and the wireless device will have a button that, when both are pressed, automatically configures Wi-Fi Security between the devices.
  - A software solution using a PIN is also common.
  - It is important to know that WPS is not entirely secure. It is vulnerable to brute-force attack.
  - WPS should be turned Off as a security best practice.

Wireless Best Practices

- To secure your wireless router you should:
  - Change the default passwords.
  - Change the default SSID.
  - Disable the SSID.
  - Enable wireless authentication and encryption.
  - Change the default IP address.
  - Limit the number of devices allows.
  - Enable Mac Address Filtering.

Firmware Updates

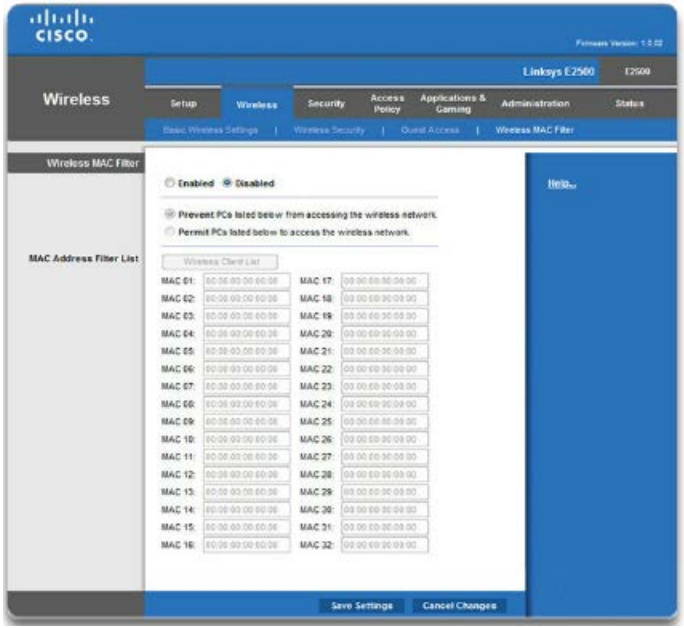
- Most wireless routers offer upgradable firmware.
  - Firmware releases may contain fixes for common problems reported by customers as well as security vulnerabilities.
- It is important to periodically check the manufacturer's website for updated firmware.
- It is common to use a GUI to upload the firmware to the wireless router.

Firewalls

- A hardware firewall inspects data packets from the network before they reach devices on the inside network.
  - The firewall can be configured to block individual ports, a range of ports, or specific application traffic.
- Most wireless routers also include an integrated hardware firewall.
- They can be configured to allow two different types of traffic into your network:
  - Responses to traffic that originates from inside your network
  - Traffic destined for a port that you have intentionally left open

Mac Address Filtering

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



Port Forwarding and Port Triggering

- Hardware firewalls can be used to block ports to prevent unauthorized access in and out of a LAN.
- However, there are situations when specific ports must be opened so that certain programs and applications can communicate with devices on different networks.
- **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.

Universal Plug and Play

- **Universal Plug and Play (UPnP)** is a protocol that enables devices to dynamically forward traffic through network ports without the need for user intervention or configuration.
- Port forwarding is often used for:
  - Streaming media
  - Hosting games
  - Providing services from home and small business computers to the internet.

13.5 BASIC TROUBLESHOOTING PROCESS FOR SECURITY

The 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

Step 1 – Identify the Problem

Open-ended questions	• When did the problem start? • What problems are you experiencing? • What websites have you visited recently? • What security software is installed on your computer? • Who else has used your computer recently?
Closed-ended questions	• Is your security software up to date? • Have you scanned your computer recently for viruses? • Did you open any attachments from a suspicious email? • Have you changed your password recently? • Have you shared your password?

Step 2 – Establish a Theory of Probable Cause

Common causes of security problems	• Virus • Trojan Horse • Worm • Spyware • Adware • Grayware or Malware • Phishing scheme • Password compromised • Unprotected equipment rooms • Unsecured work environment

Step 3 – Test the Theory to Determine Cause

Common steps to determine cause	• Disconnect from the network. • Update antivirus and spyware signatures. • Scan computer with protection software. • Check computer for the latest OS patches and updates. • Reboot the computer or network device. • Login as an administrative to change a user's password. • Secure equipment rooms. • Secure work environment. • Enforce security policy.

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

If no solution is achieved in the previous step, further research is needed to implement the solution.	• Helpdesk repair logs • Other technicians • Manufacturer FAQ websites • Technical websites • News groups • Computer manuals • Device manuals • Online forums • Internet search

Limiting login times is a good way to keep users from accessing computer after hours.

Step 5 – Verify Full System Functionality and if Applicable Implement Preventative Measures

Verify solution and full system functionality for laptops	• Re-scan computer to ensure no viruses remain. • Re-scan computer to ensure no spyware remains. • Check the security software logs to ensure no problems remain. • Check computer for the latest OS patches and updates. • Test network and Internet connectivity. • Ensure all applications are working. • Verify access to authorized resources such as shared printers and databases. • Make sure entries are secured. • Ensure security policy is enforced.

Step 6 – Document Findings, Actions, and Outcomes

Document your findings, actions, and outcomes	• Discuss the solution implemented with the customer. • Have the customer verify problem has been solved. • Provide the customer with all paperwork. • Document the steps taken to solve the problem in the work order and technician's journal. • Document any components used in the repair. • Document the time spent to solve the problem.

Identify Common Problems and Solutions

- Security problems can be attributed to several reasons. You will resolve some types of security problems more often than others.

A security alert is displayed.

Probable Causes	Possible Solutions
The windows firewall is disabled.	Enable the Windows Firewall.
Virus definitions are out-of-date.	Update virus definitions
Malware has been detected.	Scan for malware.

13.6 CHAPTER SUMMARY

Chapter 13: Security

- Explain common security threats and how to prevent and recover from threats.
- Identify the purpose and use of security procedures in protecting physical equipment and data.
- Secure Windows workstations within the BIOS, Operating System, and firewall.
- Configure wireless security settings on a small office / home office router.
- Troubleshoot common problems for security

Elk Technologies
https://elktech.org
SCOTT STEPHENSON