NASSCOM® FOUNDATION

Directorate General of Training

Powered by Microsoft

Secure Computer and the Network

Secure computers & the network

Recall Secure a Computer

- Use a firewall
- Keep all software up to date
- Use antivirus software and keep it current
- Make sure your passwords are well-chosen and protected
- Browse the web safely
- Stay away from pirated material
- & prevent and remove malware
- Don't use USBs or other external devices unless you own them
- Protect your personal information online & Protect yourself from scams
- Windows Security
- Microsoft Defender Offline

Describe Information Security and its Basic Principles

Use a firewall

- Firewall: A firewall is a series of rules that control incoming and outgoing network traffic.
- Windows has a firewall already built in and automatically turned on.

Keep all software up to date

- Make sure to turn on automatic updates in Windows Update to keep Windows, Microsoft Office, and other Microsoft applications up to date.
- Turn on automatic updates for non-Microsoft software as well, especially browsers, Adobe Acrobat Reader, and other apps you regularly use.

Use antivirus software and keep it current

- Only install these programs from a known and trusted source.
- Keep virus definitions, engines and software up-to-date to ensure your programs remains effective.

Make sure your passwords are well-chosen and protected

- Using passwords that feature letters, symbols, numbers and some uppercase letters will make the password stronger.
- A password manager can help you to maintain strong unique passwords for all of your accounts.
- These programs can generate strong passwords for you, enter credentials automatically, and remind you to update your passwords periodically.

Browse the web safely

- Avoid visiting sites that offer potentially illicit content. Many of these sites install malware on the fly or offer downloads that contain malware.
- Use a modern browser like Microsoft Edge, which can help block malicious websites and prevent

malicious code from running on your computer.

Stay away from pirated material & prevent and remove malware

Stay away from pirated material

- Avoid streaming or downloading movies, music, books, or applications that do not come from trusted sources. They may contain malware.

Prevent and remove malware

- One important step toward greater workplace security is to protect your computer against malware.

Don't use USBs or other external devices unless you own them

To avoid infection by malware and viruses, ensure that all external devices either belong to you or come from a reliable source.

Protect your personal information online & Protect yourself from scams

Protect your personal information online

- Your privacy on the internet depends on your ability to control both the amount of personal information that you provide and who has access to that information.

Protect yourself from scams

- When you read email, use social media, or browse the web, you should be wary of scams that try to steal your personal information (also known as identity theft), your money, or both. Many of these scams are known as "phishing scams" because they "fish" for your information.

Windows Security

- Windows Security (or Windows Defender Security Center in Windows 8 or early versions of Windows 10) is built in to Windows and provides real-time malware detection, prevention, and removal with cloud-delivered protection. It is intended for home, small business, and enterprise customers.

Microsoft Defender Offline

- Microsoft Defender Offline runs outside of Windows to remove rootkits and other threats that hide from the Windows operating system. This tool uses a small, separate operating environment, where evasive threats are unable to hide from antimalware scanners.

- With Windows 10 and 11, Microsoft Defender Offline is built in to the operating system and can run from Windows Security. It is provided as a separate download for previous versions of Windows.

Working of network security

How does a network security work

- Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls.
- Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.
- Network security also helps you protect proprietary information from attack. Ultimately it protects your reputation.

Network Security Types

Firewalls: Not every user should have access to your network. To keep out potential attackers, need to recognize each user and each device. Then can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This is called network access control(NAC)

Email security: Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and

controls outbound messages to prevent the loss of sensitive data.

Anti-virus and anti-malware software: Any software you use to run your business needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.

Network segmentation: Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

Access control: Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).

Application security: Any software you use to run your business needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, that attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.

Behavioral analytics: To detect abnormal network behavior, you must know what normal behavior looks like. Behavioral analytics tools automatically discern activities that deviate from the norm. Your security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.

Data loss prevention: Organizations must make sure that their staff does not send sensitive information outside the network. Data loss prevention, or DLP, technologies can stop people from uploading, forwarding, or even printing critical information in an unsafe manner.

Intrusion prevention systems: An intrusion prevention system (IPS) scans network traffic to actively block attacks. Cisco Next-Generation IPS (NGIPS) appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinfection.

Mobile device security: Cybercriminals are increasingly targeting mobile devices and apps. Within the next 3 years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, you need to control which devices can access your network. You will also need to configure their connections to keep network traffic private.

Security information and event management: SIEM products pull together the information that your security staff needs to identify and respond to threats. These products come in various forms, including physical and virtual appliances and server software.

VPN: A virtual private network encrypts the connection from an endpoint to a network, often over the Internet.

Typically, a remote-access VPN uses IPsec or Secure Sockets Layer to authenticate the communication between device and network.

Web security: A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

Wireless security: Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network.

Benefits of network security:

- A well-designed network security solution reduces overhead expenses and safeguards organizations from costly losses that occur from a data breach or other security incident.
- Ensuring legitimate access to systems, applications and data enables business operations and delivery of services and products to customers.

A Robust Network Security will protect against:

- Virus
- Worms
- Trojan
- Spyware
- Adware
- Ransomware

Recall Setting up Network Security

Setting up Network Security

- Unauthorized access to your private data, eavesdropping and stealing are very common due to your wireless connection not being secure enough.
- This could become a huge loss if personal or business information gets into the wrong hands.
- Setting up a secure network helps you to secure your network and data.

Following steps are required to set up a network:

Step 1: Locate and Open Up Your Router Settings Page

Step 2: Create a Password for Your Router

Step 3: Change the Name of Your Network's SSID

Step 4: Enable Network Encryption

Step 5: Filter Out Your Mac Addresses

Step 6: Reduce Your Wireless Signal's Range

Step 7: Upgrade your Firmware

Step 8: Connect to Your Secure Wireless Network

Step 9: Install a Firewall

Setting up a network

Step 1: Locate and Open Up Your Router Settings Page: To locate your router's settings page, it is said that you can type "192.168.1.1" into your web browser, the same area you would type the web address you want to visit. When you are prompted to, type in your user name and password. If this doesn't work, you can reference your router's user manual for directions.

Step 2: Create a Password for Your Router:

Once logging on to your router, create a password to begin making your network more secure. Others will not have access to your network now and only you can maintain and make changes to the settings.

To change the password, access the settings and you should have no problem locating password information there. It should be noted that, as with any password, you should make this unique, and difficult to crack.

When a password is effectively typed into a device, it is not visible and becomes a bunch of dots or asterisks, so the people with whom you decide to share it with will not tell someone else.

Preferably, the password should be 20 characters long and made up of a mix of characters, randomly boggled together.

Step 3: Change the Name of Your Network's SSID:

Upon purchase and set-up of your router, the SSID(Service Set Identifier) of your router is pre-set as something very basic, which is usually a product name drop. Changing this name will help you out.

This setting and the process to change the name can be located within the wireless settings when you go to access your router's settings home page.

Once you change this name, you will always be reassured that you are joining the correct network in the sea of all the other random ones. Steer clear of utilizing any personal information in the SSID name. It should be unique and random.

Step 4: Enable Network Encryption:

Network encryption is a security process that utilizes crypto services at the network transfer layer which is just above the data link level but still below the application level. For those that are less tech-savvy, this means that data moving over communications networks is protected. To prevent and/or stop other computers and users from using your internet connection and possibly tapping into your files, encrypting your network is essential.

To get started allowing encryption on your home or work network, head over to the wireless security settings on your router's settings and/or configuration page and open them up. This page should then allow you to be able to choose which security process you want to select. Enter the password to sign on to the network.

Step 5: Filter Out Your Mac Addresses

The MAC address is the media access control address that is used to communicate with a network segment.

Adding every MAC address on all your devices to your wireless router's options will make it so that only your devices are able to form a connection to your safe network.

MAC addresses are deeply coded so only one device will be allowed on the network if that is how you establish your settings.

It should be noted that one can mimic a MAC address, but it is a little more challenging with these extra precautions.

To enable and allow MAC address "filtering", you will input all addresses you trust to connect to the network (think all devices you use to connect to the internet).

Find these device's "MAC addresses," and then go ahead and add them to the list that you can locate in the settings.

Step 6: Reduce Your Wireless Signal's Range

For a small house or an apartment, there is no need for a high range. This is overshooting predictions and can lead to someone farther away trying to tap into your network. To decrease the range of the signal, try altering the router mode to 802.11g or use a completely separate wireless channel.

Reducing the direction of the signals can be done by placing the router inside a drawer, inside a cardboard box or by wrapping some tape around the router antennas.

Step 7: Upgrade your Firmware: It is important to make sure that your router has the most up to date firmware on occasion. You can locate the most up to date firmware for your router using the router's dashboard with the 192.168 trick discussed earlier.

Step 8: Connect to Your Secure Wireless Network

After you have sorted through these motions listed and successfully enabled the numerous security options, it is pertinent to input your new options into all of your devices. This will ensure that they will all be able to connect to the wifi network without error.

You can even elect to have your computer connect on its own to this particular network without you having to provide any credentials.

Step 9: Install a Firewall

Installing a firewall can assist you in defending your network against any external threats.

A firewall will block any malicious traffic from setting foot into your secure network and will notify you when any potentially dangerous activity begins to occur.

When it is appropriately configured and set up, it can also act as a barrier for any internal threats, preventing any of your files from leaving your computer.

Describe How Directory Services Work

what are directory services?

- Directory services are software systems that store, organize and provide access to directory information in order to unify network resources.
- It maps the network names of network resources to network addresses and define a naming structure for networks.
- Directory services identify every resource such as email address, peripheral devices and computers on the network, and make these resources accessible to users and applications.

Why are directory services important?

- Directory services are the authoritative identity provider (IdP) for all of an organization's IT infrastructure.
- It becomes the source of truth for authentication and authorization throughout your digital workspace.

what to consider while selecting a directory?

- User provisioning and deprovisioning
- Authentication to both on-prem and web-based applications
- Securing network access over wired and wireless networks

Choosing the best directory services

When choosing the best directory services, we we'll be comparing two directory services that often function as the primary identity provider in an enterprise.

Active Directory

Microsoft® Active Directory® (AD) is the most well-known on-prem directory service.

It stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

JumpCloud Directory-as-a-Service

JumpCloud's DaaS is the first cloud-based directory with the ability to authenticate, authorize, and manage users, devices, and applications. The service acts as a single-user store for an organization or can extend existing AD/LDAP user stores to the cloud.

Describe How Access Control Helps in Reducing Threats

Access Controls

- Access control helps in preventing your data from unauthorized individuals or groups.
- Access controls are the tools, policies, models, and mechanisms that enable you to grant or restrict access to your organization's digital or physical resources.
- By restricting access to sensitive systems or data, you're authorized to give permission to do any of the following:
- Access
- Read
- Modify
- Communicate
- Delete or otherwise destroy

Technical Control Systems

Limiting which IP addresses (or ranges of IP addresses) can access your network through your firewall

Administrative Control Systems

Limiting which of your employees or groups of employees can make changes to specific files

Physical Control Systems

Limiting employees from accessing specific areas of the office premise is an example for physical control system

Benefits of having an access control system:

Following are some of the benefits of having an access control system:

1. Increase ease of access for employees
2. Get rid of traditional keys
3. Save money and energy
4. Keep track of who comes and goes
5. Protect against unwanted visitors

6. Give employees the freedom to work when they need to
7. Prevent against data breaches
8. Create a safe work environment
9. Reduce theft and accidents
10. Provide access to multiple buildings and locations
11. Comply with industry regulations or security standards

Security Audits Help in Reducing Threats

Security Audits

- A security audits involves a comprehensive analysis and review of the IT infrastructure of your business. It detects vulnerabilities and threats, displaying weak links, and high-risk practices.
- Cybersecurity audits ensure a 360-degree in-depth audit of your organization's security postures.

Cyber security audit detects vulnerabilities, risks, and threats that organizations face and the influence of such risks causing across the following areas:

Data Security – involves a review of network access control, encryption use, data security at rest, and transmissions

Operational Security – involves a review of security policies, procedures, and controls

Network Security – involves a review of network & security controls, SOC, anti-virus configurations, security monitoring capabilities, etc.

System Security – This review covers hardening processes, patching processes, privileged account management, role-based access, etc.

Physical Security – involves a review that covers disk encryption, role-based access controls, biometric data, multifactor authentication, etc.

Working of Cyber Security

A detailed cybersecurity audit will do the following:

- Evaluate overall data security
- Determine whether your software and hardware work the way they should
- Demonstrate compliance with legal and industry regulations
- Discover unknown vulnerabilities
- Uncover inefficiencies in your software or hardware
- Determine the adequacy of existing policies and training
- Gauge employee compliance or threats

Recap:

- A firewall is a series of rules that control incoming and outgoing network traffic.
- Using passwords that feature letters, symbols, numbers and some uppercase letters will make the password stronger.
- Your privacy on the internet depends on your ability to control both the amount of personal information that you provide and who has access to that information.
- Windows Security is built in to Windows and provides real-time malware detection, prevention, and removal with cloud-delivered protection.
- Microsoft Defender Offline runs outside of Windows to remove rootkits and other threats that hide from the Windows operating system.
- Network security combines multiple layers of defenses at the edge and in the network.
- Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.
- Setting up a secure network helps you to secure your network and data.
- Directory services are software systems that store, organize and provide access to directory information in order to unify network resources.
- Access controls are the tools, policies, models, and mechanisms that enable you to grant or restrict access to your organization's digital or physical resources.