Online Access and Computer Security

Online Access

- **Online access means exploring or browsing or searching anything** from any location and on any web-enabled device.

Network security is the process of physical and software Preventative measures to **protect** the networking infrastructure **from**

unauthorized access,
malfunction,
destruction,
misuse,
modification,
or improper disclosure,

thereby creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment.

Threats to Computer Security

- **Threats** – are basically a violation of security . Attackers execute these threats.
- **Common threats are:**
  - **Viruses**-worms,Trojans
  - **Spyware**
  - **Adware**
  - **Spamming**
  - **Phishing**
  - **Sweeping**
  - **Denial of Service(DOS) Attack**

MALWARES

MALWARE

- It is code or software that is specifically designed to damage, disrupt, steal, or "bad" or illegitimate action on data or hosts, or networks.
- Malware infects the computer.
- It is unwanted software that someone else wants to run our computer/system.

Computer Viruses

- These are malicious codes/programs that cause damage to data and files on a system
- All computer viruses are manmade.
- Viruses can attack any part of computer's software such as operating system, boot block, files, application program etc.
- It spreads from one computer to another, leaving infections as it travels.
- Almost all viruses are attached to an executable file
- It requires the spreading of an infected host file.

Ways to prevent from computer virus –

- Open emails carefully even coming from friends.
- Do not open emails from unknown senders.

- Install Anti-virus Software and keep it up to Date
- Scan System Regularly
- Browse Safely
- Download Files Carefully
- Do not use disks/software from unknown sources.

- WORMS and TROJANS or TROJAN HORSES

  are

  two similar programs also cause virus like effects

Worms

- Worms are self replicating program which eats up the entire disk space or memory
- It keeps on creating its copies its copies until all the disk space or memory is filled.
- Worms are standalone software and do not require a host program or human help to propagate.

Ways to prevent from computer worms

- Since software vulnerabilities are major infection vectors for computer worms, be sure that computer’s operating system and applications are up to date with the latest versions.

- Install these updates as soon as they’re available because updates often include patches for security flaws.

- Phishing is another popular way for hackers to spread worms Always be extra cautious when opening unsolicited emails, especially those from unknown senders that contain attachments or dubious links.

- Be sure to invest in a strong internet security software solution that can help block computer worms.

Question: What is Worm ? How is it removed ?

Answer:
A worm is a self-replicating computer program. It uses a network to send copies of itself to other computers on the network and it may do so without any user intervention.
Most of the common anti-virus (anti-worm) remove worm.

Question : Differentiate between WORM and VIRUS in Computer terminology.

Answer:
VIRUS directly effects the system by corrupting the useful data. A computer virus attaches itself to a program or file enabling it to spread from one computer to another.

A worm is similar to a virus by design and is considered to be sub class of a virus. Worm spread from computer to computer, but unlike a virus, it has the capability to travel without any human action.

TROJANS or TROJAN HORSES

- Trojans neither replicate nor copy itself , but cause damage or compromises the security of the computer.
- Trojans are used to capture logins and passwords(keylogger).
- Trojans mainly spread through user interaction such as opening an email attachment or downloading and running a file from the Internet.

Ways to prevent from Trojan Horse

- Never download or install software from a source you don’t trust completely

- Never open an attachment or run a program sent in an email from someone you don’t know.

- Keep all software on your computer up to date with the latest patches

- Make sure a Trojan antivirus is installed and running on computer

Question: What is Trojan Horse ?

Answer:

A Trojan Horse is a code hidden in a program, that looks safe but has hidden side effects typically causing loss or theft of data, and possible system harm.

Damage caused by Malwares (Viruses,Worms and Trojans)

- Slow down the computer
- Invade through email program
- Eating up all the disk space
- Damage or delete files

SPYWARE

Purpose:-

- These software are used to track the user activities , behavior , identity (credit/debit card info, ID ,phone no) and report to the central authority.
- These can be used for legal or illegal purpose

Threat:-

- Alter PC settings
- Slow down the PC
- Compromise your data

Ways to prevent from SPYWARE

- Use dropdown boxes.

- User should be alert and look for clues when using their computer.

ADWARE

Purpose:-

- These programs deliver unwanted ads
- Adware consume network bandwidth
- Adware is a useful program to earn something online.

Threat:-

- Tracks information like spyware
- Slow down the PC
- Displays many adveritisements

SPAMMING- is any kind of unwanted, unsolicited digital communication that gets sent out in bulk through email

Purpose:-

- It refers to the receiving bulk mail from identified or unidentified sources.
- In malicious form- the attacker keeps on sending mail until mail server runs out of disk space
- In non-malicious form- bulk advertising mail is sent to many accounts

Threat:-

- Reduces system performance
- Waste time
- It can lead to worse things—fraudulent calls or messages

Ways to prevent from spam

- Never give out or post your email address publicly
- Think before to click
- Do not reply to spam messages
- Download spam filtering tools (SpamTitan,**Mailwasher**,ZEROSPA etc) and use anti-virus

Question :

What is a spam mail ?

Answer:

Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately.

Phishing

Purpose:-

- Phishing is a cyber attack that uses disguised email as a weapon.
- The goal is to trick the email recipient into believing that the message is something they want or need — recipient fills/send sensitive information like account no, username ,password etc. then attacker use these.

How to prevent phishing

- Always check the spelling of the URLs before click
- Watch out for URL redirects, that sent to a different website with identical design
- If receive an email from that seems suspicious, contact that source with a new email, rather than just hitting reply
- Don't post personal data, like your birthday, vacation plans, or your address or phone number, publicly on social media
- When in doubt , do not click

Pharming

Purpose:-

- It is actually a code installed on the hard drive of a user’s computer or on actual web server
- Pharming code redirects user to a bogus/fake website without user knowing

How to prevent Pharming

- Use filters to authenticate websites.

- User should be alert and look for pharming clues which indicate being directed to a bogus site.

Cookies

Purpose:-

- Cookies are small text file created on client computers .
- These are automatically generated by the web site server .
- These cookies can contain information about the user.
- Cookies are harmless.

Cookies

Question : Explain the importance of Cookies.

Answer:

When the user browses a website, the web server sends a text file to the web browser. This small text file is a cookie. They are usually used to track the pages that we visit so that information can be customized for us for that visit.

Question : What kind of data gets stored in cookies and how is it useful ?

Answer:

When a Website with cookie capabilities is visited, its server sends certain information about the browser, which is stored in the hard drive as a text file. It is as way for the server to remember things about the visited sites.

Firewall

- It is a system that is designed to prevent unauthorized access from entering a private network.
- It creates a safety barrier between a private network and the public internet.
- It is especially important to large organizations

Question : Define firewall.

Answer:

A system designed to prevent unauthorized access to or from a private network is called firewall. It can be implemented in both hardware and software or combination of both.

Firewall rules can be based on

- IP addresses
- Domain Name (i.e.website name)
- Protocols
- Programs
- Ports
- Keywords

Firewall Types

1. Network Based firewall- (a) Combination of hardware and software

(b) protects an entire network

2. Host based firewall- (a) software firewall that is installed on a computer

(b) protects that computer only

(c) A lot of antivirus programs come with a host based firewall

Firewall can be (1) stand-alone firewall (hardware firewall),

(2) router have a built-in firewall (hardware firewall),

(3) cloud firewall (software firewall) this is testing

Digital signatures

- These are useful for authenticating the identity of creator or producers of digital information

Digital Certificates

- These can verify the identity of a message sender.
- It is a way of authenticating the creator's identity online.

Anti Virus Software

- These software are designed to detect and block attacks from malwares.
- These software when loaded, resides in memory and checks every operation if it is malicious or not.
- If it finds any suspicious activity, it blocks that operation and saves our computer.

Authentication

- It is the process of determining whether someone is a legal user or not.
- It is the process of identifying an individual, usually based on a username and password
- It is the primary step for file protection from unauthorized users.

Authorization

- Asking the user a legal login-id performs authorization. If the user is able to provide a legal login-id, he /she is considered an authorized user.

What is the need of secure passwords?

- It also helps the network manager trace unusual activity to a specific user.
- A good password should include an upper case and lower case letters , numbers and special characters.
- A good combination of these makes a strong password and difficult to crack it.
- Strong password keeps our system secure.