Unit 2

Cyber Frauds, DoS, Viruses

- **Cyber Stalking, Fraud, and Abuse**: Introduction, How Internet Fraud Works, Identity Theft, Cyber Stalking, Protecting Yourself Against Cyber Crime.
- **Denial of Service Attacks**: Introduction, DoS, Illustrating an Attack
- **Malware**: Introduction, Viruses, Trojan Horses, The Buffer-Overflow Attack. The Sassier Virus/Buffer Overflow, Spyware, Other Forms of Malware
- Detecting and Eliminating Viruses and Spyware

Internet Fraud

Internet fraud is a type of cybercrime fraud which makes use of the Internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance.

unsolicited communication sent in bulk

Illegally remove money from a bank account and/or transfer money to an account in a different bank

- **Common Types**
- **Spam**
- **Scam**
- **Spyware**
- **Phishing**
- **Identity Theft**
- **Internet Banking Fraud**

a fraudulent scheme that fools people into giving away their money for nothing

someone takes someone else's personal information without permission and then uses it for their own benefit

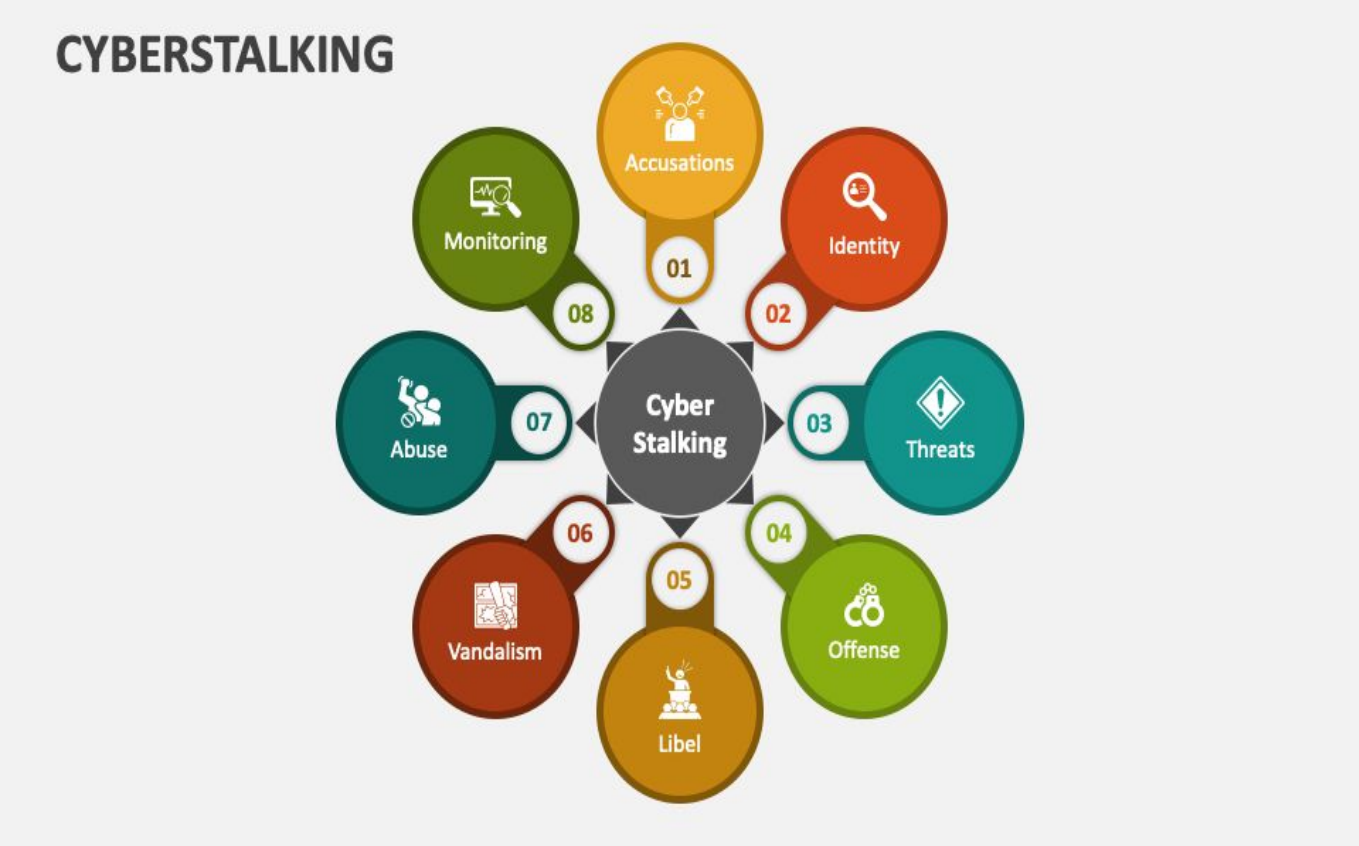
secretly installed on a computer and takes things from it without the permission or knowledge of the user.

sending fraudulent communications that appear to come from a reputable source

Cyber Stalking-

Cyberstalking is a type of cybercrime that uses the internet and technology to harass or stalk a person.

Cyberstalkers take advantage of the anonymity afforded by the internet to stalk or harass their victims, sometimes without being caught, punished or even detected.



Direct and indirect cyberstalking

Direct- Perpetrators may directly email their victims or flood their inboxes with emails. Or they may harass them through IM, voicemail, texting or other forms of electronic communications.

Indirect- perpetrators may damage the victim's device. They may do this by infecting it with ransomware to lock their files and then forcing them to pay a ransom for unlocking them. Or they may install a virus or keystroke logger that monitors the victim's digital behavior and/or steals data from the device.

Cyberstalking Examples-

- Posting offensive, suggestive, or rude comments online
- Sending threatening, lewd, or offensive emails or messages to the victim
- Joining the same groups and forums as the victim
- Releasing the victim's confidential information online
- Tracking all online movements of the victim through tracking devices
- Excessively tagging the victim in irrelevant posts
- Creating fake profiles on social media to follow the victim
- Posting or distributing real or fake photos of the victim
- Excessively sending explicit photos of themselves to the victim
- Making fake posts intended to shame the victim
- Using hacking tools to get into the victim's laptop or smartphone camera and secretly record them
- Continuing harassment even after being asked to stop

Types of cyberstalking

1. **Catfishing**

The creation of fake profiles or copying of existing ones on social media to approach victims.

2. **Monitoring check-ins on social media**

Keeping an eye on the activities of a victim on social media to accurately gauge their behavior pattern.

3. **Spying via Google Maps and Google Street View**

Using Street View to spy on a victim and find their location from posts or photos on social media.

4. **Hijacking webcam**

Webcams can be hijacked by introducing malware-infected files into the victim's computer.

5. **Installing stalkerware**

Stalkerware tracks the location, enables access to texts and browsing history, makes audio recordings, etc., without the victim's knowledge.

6. **Tracking location with geotags**

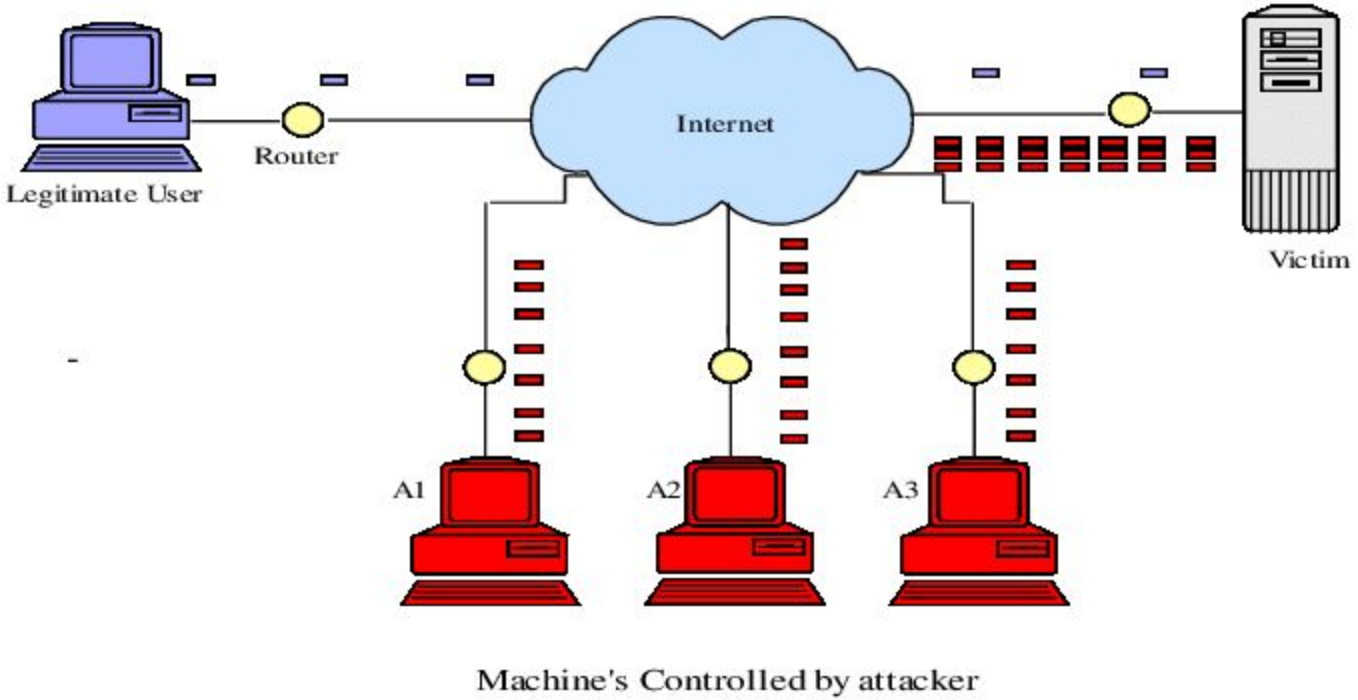
Digital pictures mostly have geotagged with the time and location of the picture if it is in the metadata format, which makes it easier for stalkers to access that information by using special apps.

CYBERSTALKING

How to Prevent Cyberstalking

DoS Attacks

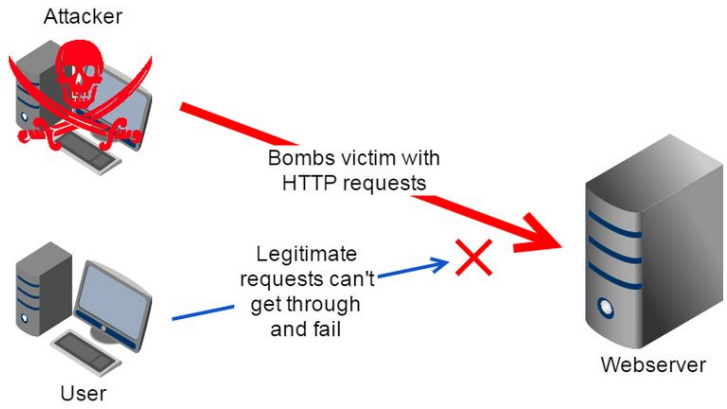
A security threat that occurs when an attacker makes it impossible for legitimate users to access computer systems, network, services or other information technology (IT) resources



For example, if a bank website can handle 10 people a second by clicking the Login button, an attacker only has to send 10 fake requests per second to make it so no legitimate users can log in.

How Do DoS Attacks Work?

- Flooding a network with useless activity so that genuine traffic cannot get through. The TCP/IP SYN and Smurf attacks are two common examples.
- Remotely overloading a system's CPU so that valid requests cannot be processed.
- Changing permissions or breaking authorization logic to prevent users from logging into a system. One common example involves triggering a rapid series of false login attempts that lockout accounts from being able to log in.
- Deleting or interfering with specific critical applications or services to prevent their normal operation (even if the system and network overall are functional).



Signs of a DoS attack

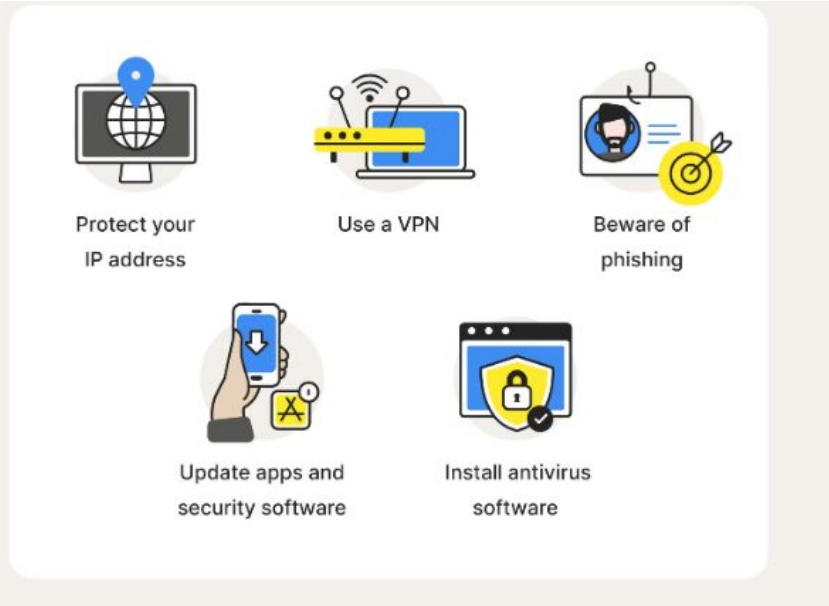
Degradation in network performance
Especially when attempting to open files stored on the network or when accessing websites.

Specific website unavailable
A particular site does not open or cannot be found.

Inability to access any website
All websites are inaccessible on the network.

High volume of email spam
A higher than usual volume of spam email.

How to prevent DoS Attacks



Malicious Software

Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.

Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware.

Malware has actually been a threat to individuals and organizations since the early 1970s when the Creeper virus first appeared

A wide variety of malware types exist:-

1. Computer Viruses
2. Worms
3. Trojan Horses
4. Ransom ware
5. Java scripts and Java applets
6. Spyware, etc.

Virus

- A computer virus is a computer program that, when executed, replicates itself by modifying other computer programs
- It can attach itself to other healthy programs.
- It is difficult to trace a virus after it has spread across a network.
- Viruses can be spread through email and text message attachments, Internet file downloads, and social media scam links.
- Computer viruses cause billions of dollars' worth of economic damage each year.
- If a virus has entered in the system then there might be frequent pop-up windows, Frequent crashes, Unusually slow computer performance, Unknown programs that start up when you turn on your computer, Unusual activities like password changes.
- Examples of virus:- Melissa, I Love You.

Worms

- A computer worm is a type of malware that spreads copies of itself from computer to computer without any human interaction.
- Computer worms could arrive as attachments in spam emails or instant messages (IMs).
- When computer is infected with worms then it starts to take up free space of your hard drive, programs might crash, your files may be replaced or deleted.
- A worm is however different from a virus. A worm does not modify a program like a virus.
- Examples of worms:- Code Red, Nimda

Trojan Horse

- A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software.
- The term "Trojan" derives from the ancient Greek story about the deceptive Trojan horse which led to the fall of the city of Troy.
- A Trojan must be executed by its victim to do its work.
- Trojan horses contain programs that corrupt the data or damage the files, corrupt software applications.
- Trojan horse does not replicate themselves like viruses.
- If your computer is breached by Trojan malware then, computer will start frequent crashing, redirected to unfamiliar websites when browsing online, increase in pop-ups.

Java Scripts, Java applets and ActiveX Controls

Java Scripts

- JavaScript is a dynamic computer programming language, most commonly used as a part of web pages, whose implementations allow client-side script to interact with the user and make dynamic pages.
- JavaScript is widely used in Netscape, Internet Explorer, and other web browsers.
- JavaScript also allows website creators to run any code they want when a user visits their website.
- Cyber criminals frequently manipulate the code on countless websites to make it perform malicious functions. If we're browsing a malfunctioned website, the attackers can easily get access to our device.

Java Applets and ActiveX Controls

- Applets (Java programs), and ActiveX controls are used with Microsoft technology, generally used to provide added functionality such as sound and animation which are inserted in Web page.
- Anyone who uses the Internet will eventually access websites that contain mobile code.
- If these programs are designed with a malicious intention, then it can be disastrous for the client machine.
- Java's design and security measures are better designed and inherently safer than ActiveX, which provides very few restrictions on the developer.

Common malicious mobile code

- Browser scripts
- ActiveX controls
- Java applets

Hacking

- Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data.
- Hackers are the one who are responsible for hacking and are increasingly growing in sophistication, using stealthy attack methods designed to go completely unnoticed by cyber security software and IT teams.
- Hacking is not always done for malicious purposes, nowadays most references to hacking as unlawful activity by cybercriminals motivated by financial gain, protest, spying, and even just for the "fun" of the challenge.
- Nowadays, hacking has become a multibillion-dollar industry with extremely sophisticated and successful techniques
- There are various ways hackers invade our privacy by packet sniffing, email hacking, password cracking.

Packet Sniffing

- The act of capturing data packet across the computer network is called packet sniffing.
- It is mostly used by *crackers and hackers* to collect information illegally about network. It is also used by *ISPs, advertisers and governments*.
- Packet sniffing attacks normally go undetected.
- Ethereal and Zx Sniffer are some freeware packet sniffers.
- Telnet, FTP, SMTP are some services that are commonly sniffed.

Password Cracking

- Password cracking is the process of guessing the correct password to an account in an unauthorized way.
- Password cracking can be done for several reasons, but the most malicious reason is in order to gain unauthorized access to a computer without the computer owner's awareness.
- One of the most common types of password attacks is a dictionary attack.
- The password is generally stored in the system in an encrypted form. Password cracker is an application that tries to obtain a password

Email Hacking

- Email hacking is the unauthorized access to, or manipulation of an account or email correspondence.
- Fraudster get our email by tricking us into clicking on a link in an SMS or email.
- Once they access your account, they read all your correspondence, have access to all your contacts and send emails from your account.
- Hackers use packet replay to retransmit message packets over a network. Packet replay may cause serious security threats to programs that require authentication sequences.