Explain various types of cybersecurity threats

- Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems.
- Common categories of cyber threats include malware, social engineering, man in the middle (MitM) attacks, denial of service (DoS), and injection attacks

Malware attack :

- Malware is an abbreviation of "malicious software", which includes viruses, worms, trojans, spyware, and ransomware, and is the most common type of cyberattack.
- **Trojan virus** — tricks a user into thinking it is a harmless file. A Trojan can launch an attack on a system and can establish a backdoor, which attackers can use.
- **Ransomware** — prevents access to the data of the victim and threatens to delete or publish it unless a ransom is paid. Learn more in our guide to ransomware prevention.
- **Wiper malware** — intends to destroy data or systems, by overwriting targeted files or destroying an entire file system. Wipers are usually intended to send a political message, or hide hacker activities after data exfiltration.
- **Worms** — this malware is designed to exploit backdoors and vulnerabilities to gain unauthorized access to operating systems. After installation, the worm can perform various attacks, including Distributed Denial of Service (DDoS).
- **Spyware** — this malware enables malicious actors to gain unauthorized access to data, including sensitive information like payment details and credentials. Spyware can affect mobile phones, desktop applications, and desktop browsers.
- **Fileless malware** — this type of malware does not require installing software on the operating system. It makes native files such as PowerShell and WMI editable to enable malicious functions, making them recognized as legitimate and difficult to detect.

Social engineering attacks :

- **Phishing:** Attackers send fraudulent emails or messages impersonating legitimate sources to trick users into revealing sensitive information or downloading malware.
- **Spear Phishing**: Targeted phishing attacks aimed at specific individuals with authority or access to sensitive information.

- **Malvertising:** Malicious advertising containing harmful code that infects users' devices when they interact with the ad.
- **Drive-by Downloads:** Malware is automatically downloaded onto users' devices when they visit compromised websites.
- **Scareware Security Software:** Fake security software that deceives users into paying for unnecessary services or revealing financial information.
- **Baiting:** Placing infected physical devices, like USB drives, in locations where targets are likely to find and use them, leading to malware installation.
- **Vishing:** Voice phishing attacks conducted over the phone to manipulate targets into divulging personal or financial information.
- **Whaling**: Phishing attacks targeting high-profile individuals, such as CEOs or CFOs, to gain access to sensitive company data.

Distributed denial of service (DDoS):

- A DDoS (Distributed Denial of Service) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic.
- Unlike traditional DoS attacks where the attack comes from one source, DDoS attacks involve multiple compromised devices, often distributed across various locations.
- These devices, known as botnets, are controlled remotely by the attacker and coordinated to generate a massive volume of traffic towards the target.

Man-in-the-middle attack (MitM):

- When users or devices access a remote system over the internet, they assume they are communicating directly with the server of the target system.
- In a MitM attack, attackers break this assumption, placing themselves in between the user and the target server.
- Once the attacker has intercepted communications, they may be able to compromise a user’s credentials, steal sensitive data, and return different responses to the user.

MitM attacks include:

Session hijacking, Replay attack, IP spoofing, Bluetooth attacks

Password attacks:

A hacker can gain access to the password information of an individual by 'sniffing' the connection to the network, using social engineering, guessing, or gaining access to a password database.

Password attacks include:

- **Brute-force password guessing** — an attacker uses software to try many different passwords, in hopes of guessing the correct one. The software can use some logic to trying passwords related to the name of the individual, their job, their family, etc.
- **Dictionary attack** — a dictionary of common passwords is used to gain access to the computer and network of the victim. One method is to copy an encrypted file that has the passwords, apply the same encryption to a dictionary of regularly used passwords, and contrast the findings.

What is a virus? Explain virus with examples

- A computer virus is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works.
- A virus spreads between systems after some type of human intervention.
- Viruses replicate by creating their own files on an infected system, attaching themselves to a legitimate program, infecting a computer's boot process or infecting user documents.
- Virus can be a simple program that affects the computer system and allows the hacker to get into your files.
- Virus is nothing on its own and thus needs a host. The host helps the virus get into other systems and execute it when triggered.
- The common route is through emails, where the attachments contain the virus.
- Virus has the characteristics of self-replicating and being non-detectable, which makes it easier for hackers to make viruses to earn money illegally.

Common Signs of Computer Viruses

Speed of System

A computer system running slower than usual is one of the most common signs that the device has a virus. This includes the system itself running slowly, as well as applications and internet speed suffering. If a computer does not have powerful applications or programs installed and is running slowly, then it may be a sign it is infected with a virus.

Pop-up Windows

Unwanted pop-up windows appearing on a computer or in a web browser are a telltale sign of a computer virus. Unwanted pop-ups are a sign of malware, viruses, or spyware affecting a device.

Programs Self-executing

If computer programs unexpectedly close by themselves, then it is highly likely that the software has been infected with some form of virus or malware. Another indicator of a virus is when applications fail to load when selected from the Start menu or their desktop icon. Every time that happens, your next step should be to perform a virus scan and remove any files on programs that might not be safe to use.

Accounts Being Logged Out

Some viruses are designed to affect specific applications, which will either cause them to crash or force the user to automatically log out of the service.

Crashing of the Device

System crashes and the computer itself unexpectedly closing down are common indicators of a virus. Computer viruses cause computers to act in a variety of strange ways, which may include opening files by themselves, displaying unusual error messages, or clicking keys at random.

Mass Emails Being Sent from Your Email Account

Computer viruses are commonly spread via email. Hackers can use other people's email accounts to spread malware and carry out wider cyberattacks. Therefore, if an email account has sent emails in the outbox that a user did not send, then this could be a sign of a computer virus.

Examples of Computer Viruses

The web contains millions of computer viruses, but only a few have gained popularity and infect record numbers of machines. Some examples of widespread computer viruses include:

- **Morris Worm –** One of the earliest and most pervasive computer virus examples, this self-replicating computer program spread through the early Internet in 1988, slowing down or crashing many machines.
- **Nimda –** This particular type of worm targeted web servers and computers running Microsoft Windows operating systems, spreading through multiple infection vectors in 2001.
- **ILOVEYOU –** A highly destructive worm that spread via email, disguised as a love confession and caused widespread damage in 2000 by overwriting files.
- **SQL Slammer –** A fast-spreading computer worm that exploited a vulnerability in Microsoft SQL Server, causing network congestion and disrupting Internet services in 2003.
- **Stuxnet –** A sophisticated worm designed to target and sabotage industrial control systems, particularly Iran’s nuclear program, by exploiting zero-day vulnerabilities in 2010.

- **CryptoLocker** – This ransomware Trojan, which infected hundreds of thousands of computers in 2013, encrypted victims' files and demanded a ransom for their decryption.
- **Conficker –** Emerging in 2008, this worm exploited vulnerabilities in Windows operating systems, creating a massive botnet and causing widespread infection.
- **Tinba –** First discovered in 2012, this banking Trojan primarily targeted financial institutions, aiming to steal login credentials and banking information.
- **Welchia –** A worm that aimed to remove the Blaster worm from infected systems and patch the exploited vulnerability but caused unintended network congestion in 2003.
- **Shlayer –** A macOS-specific Trojan that primarily spreads through fake software updates and downloads, delivering adware and potentially unwanted programs since 2018.

Explain basic terminologies related to cyber security.

1. **Unauthorized Access:** When someone gains access to a system, server, or data without proper authorization or using someone else's credentials.
2. **Hacker:** A person who seeks to exploit weaknesses in computer systems or networks for various reasons, including financial gain, activism, or personal challenge.
   Hacker Slang:
   • Hacker: An expert on a particular system who seeks to learn more about it by understanding its weaknesses and flaws.
   • White Hat Hacker: Ethical hackers who report system flaws to the vendor, often hired for penetration tests.
   • Black Hat Hacker (Cracker): Gains unauthorized access to cause harm, steal data, or disrupt systems.
   • Gray Hat Hacker: Engages in potentially illegal activities but may not have malicious intent.
3. **Threat**: Any potential danger or harmful event that could compromise the security or integrity of a system or data.
4. **Vulnerability:** A weakness or flaw in a system's design, implementation, or configuration that could be exploited by attackers to compromise security.
5. **Attack:** An intentional action or assault on a system's security, typically carried out by individuals or automated tools to exploit vulnerabilities and breach defenses.
6. **Antivirus or Antimalware:** Software designed to detect, prevent, and remove malicious software (malware) from computers and networks.
   • Trojan virus — tricks a user into thinking it is a harmless file. A Trojan can launch an attack on a system and can establish a backdoor, which attackers can use.
   • Ransomware — prevents access to the data of the victim and threatens to delete or publish it unless a ransom is paid. Learn more in our guide to ransomware prevention.
   • Wiper malware — intends to destroy data or systems, by overwriting targeted files or destroying an entire file system. Wipers are usually intended to send a political message, or hide hacker activities after data exfiltration.
   • Worms — this malware is designed to exploit backdoors and vulnerabilities to gain unauthorized access to operating systems. After installation, the worm can perform various attacks, including Distributed Denial of Service (DDoS).
   • Spyware — this malware enables malicious actors to gain unauthorized access to data, including sensitive information like payment details and credentials. Spyware can affect mobile phones, desktop applications, and desktop browsers.

7. **Social Engineering:** The manipulation of individuals through psychological techniques to trick them into divulging confidential information, providing access, or performing actions that compromise security.
8. **Virus:** A type of malicious software that infects a computer or device by replicating itself and spreading to other files or systems, often causing harm or unwanted actions.
9. **Firewall:** A security measure, either hardware or software-based, that monitors and controls incoming and outgoing network traffic based on predetermined security rules, helping to prevent unauthorized access and protect against cyber threats.

How to protect yourself from the cyber crime

- Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems.
- These are tips for protecting yourself against cybercrime. :

Keep software and operating system updated

- Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.
- Software updates often include patches or fixes for security vulnerabilities that have been identified since the previous version was released.
- By installing updates promptly, you ensure that your system is equipped with the latest defenses against known security threats.

Use anti-virus software and keep it updated

- Antivirus software is designed to detect and prevent malware infections on your computer. It scans files, programs, and other data for known malware signatures and behavioral patterns associated with malicious activity.
- Many antivirus programs offer real-time protection features that continuously monitor your system for suspicious activity.
- These features can detect and block malware in real-time, preventing it from executing and causing damage to your computer.

Use strong passwords

- Using strong passwords is crucial for protecting your accounts and sensitive information from unauthorized access.
- Strong passwords are harder for attackers to guess or crack using automated tools. By using strong passwords, you greatly reduce the risk of unauthorized access to your accounts and the potential compromise of your personal or sensitive information.
- Brute force attacks involve trying every possible combination of characters until the correct password is found. Strong passwords, especially those with a combination of letters, numbers, symbols, and uppercase and lowercase characters, significantly increase the complexity and difficulty of these attacks.

Never open attachments in spam emails

- Malicious actors often use email attachments as a vector to distribute malware, such as viruses, ransomware, or trojans.

- These attachments may appear harmless at first glance but can contain executable files or scripts designed to infect your computer when opened.
- Email attachments can also be used in phishing attacks, where attackers impersonate legitimate entities to trick recipients into opening malicious attachments.
- In addition to delivering malware, email attachments may also be used to steal sensitive information from unsuspecting victims.

Contact companies directly about suspicious requests

- If you are asked for personal information or data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal.
- Ideally, use a different phone to make the call to ensure that the line is not compromised by cybercriminals who could intercept the call.

Manage your social media settings

- Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points.
- For instance, if you post your pet's name or reveal your mother's maiden name, you might expose the answers to two common security questions.

Know what to do if you become a victim:

- If you believe that you've become a victim of a cybercrime, you need to alert the local police and, in some cases, the FBI and the **Federal Trade Commission**.
- This is important even if the crime seems minor. Your report may assist authorities in their investigations or may help to thwart criminals from taking advantage of other people in the future.

What is Internet Fraud? How internet fraud works?

- Internet fraud involves using online services and software with access to the internet to defraud or take advantage of victims.
- The term "internet fraud" generally covers cybercrime activity that takes place over the internet or on email, including crimes like identity theft, phishing, and other hacking activities designed to scam people out of money.
- Cyber criminals use a variety of attack vectors and strategies to commit internet fraud. This includes malicious software, email and instant messaging services to spread malware, spoofed websites that steal user data, and elaborate, wide-reaching phishing scam.

Internet fraud can be broken down into several key types of attacks, including:

1. **Phishing and spoofing :**

- Phishing is a technique used to gain personal information for the purpose of identity theft.
- Phishing involves using a form of spam to fraudulently gain access to people's online banking details.
- Typically, a phishing email will ask an online banking customer to follow a link in order to update personal bank account details.
- If the link is followed the victim downloads a program which captures his or her banking login details and sends them to a third party.

2. **Spyware:**

- Spyware is generally considered to be software that is secretly installed on a computer and takes things from it without the permission or knowledge of the user.
- Spyware may take personal information, business information, bandwidth or processing capacity and secretly gives it to someone else.

3. **Lottery Fee Fraud**

- Another common form of internet fraud is email scams that tell victims they have won the lottery. These scams will inform recipients that they can only claim their prize after they have paid a small fee.
- Lottery fee fraudsters typically craft emails to look and sound believable, which still results in many people falling for the scam.
- The scam targets people's dreams of winning massive amounts of money, even though they may have never purchased a lottery ticket. Furthermore, no legitimate lottery scheme will ask winners to pay to claim their prize.
-

4. **Credit Card or Bank Loan Scam:**

- Credit card fraud typically occurs when hackers fraudulently acquire people's credit or debit card details in an attempt to steal money or make purchases.
- To obtain these details, internet fraudsters often use too-good-to-be-true credit card or bank loan deals to lure victims.
- For example, a victim might receive a message from their bank telling them they are eligible for a special loan deal or a vast amount of money has been made available to them as a loan.

5. **NIGERIAN 419 SCAMS:**

- Nigerian scams, also called 419 scams, are a type of fraud and one of the most common types of confidence trick.
- The number “419” refers to the article of the Nigerian Criminal Code dealing with fraud.
- The scheme begins once a consumer receives a letter concerning the “request for urgent business transaction” usually the transfer of millions of dollars, are being sent out to consumers and business’ via mail, email and fax transmission.
- The writer of the letter will normally ask for an upfront processing fee and in some cases arrange for a meeting to discuss the transfer of funds.

Explain 3 areas for bidding frauds in detail.

- Online auctions, such as eBay, can be a wonderful way to find merchandise at very good prices.
- Auction fraud broadly refers to any type of fraud that occurs through online auction sites. Though it can occur on both sides of the platform, it is more commonly associated with sellers than buyers.

The Federal Trade Commission and Auction Fraud:

- The FTC also lists three other areas of bidding fraud that are growing in popularity on the Internet:
  - Shill bidding
  - Bid shielding
  - Bid siphoning

Shill Bidding:

- Shill bidding is a deceptive practice where sellers or their associates create fake accounts to bid on their own items in online auctions.
- These fake bids artificially inflate the bidding price, creating the illusion of high demand and driving up the final sale price.
- Shill bidding can be difficult to detect since the fake bids may appear legitimate, making it challenging for genuine bidders to distinguish between genuine and fake bids.
- **Risk:** Buyers may lose their money, especially in organized fraud schemes where the seller disappears after collecting funds from multiple auctions.
- **Preventive Measures**: Setting a maximum bid limit and avoiding bidding wars can help prevent overpaying for items due to shill bidding.

Bid Shielding:

- Bid shielding is an unethical practice of trying to block others from bidding.
- The goal is to intimidate other bidders into withdrawing from the auction, allowing the fraudulent bidder to win the item at a lower price.
- Many of the major auction sites, such as eBay, have taken steps to prevent bid shielding
- **Detection and Prevention**: Bid shielding can be detected by monitoring bidding patterns and identifying suspicious behavior, such as unusually high bids followed by retractions.

- Auction platforms can implement safeguards to prevent bid shielding, such as restricting bid retractions after a certain point in the auction or penalizing users who engage in fraudulent bidding practices.

Bid Siphoning:

- Bid siphoning is when someone puts a real item up for auction on a real auction website, but then they add links in the item description that take buyers to other websites that are not part of the auction site.
- These external sites are not part of the official auction platform and may be set up with the intention of perpetrating fraud or scams.
- The unaware buyer who follows those links might find himself on an alternative site that is a “setup” to extract bank credentials or some sort of fraud.
- **Purpose and Impact**: The primary aim of bid siphoning is to divert potential buyers away from the legitimate auction process and onto fraudulent websites
- Bid siphoning undermines the integrity of the normal auction process, which is based on principles of capitalism and democracy.