Q1. Define following terms

Cybercrime, also known as computer crime, refers to any illegal activity that is committed through the use of a computer or a computer network. This can include a wide range of activities, such as hacking into computer systems, spreading malware, stealing personal information, and engaging in online financial fraud. Cybercrime can also include activities such as cyberstalking, online harassment, and the distribution of illegal or harmful content. Because the internet and digital technology are constantly evolving, new forms of cybercrime are constantly emerging.

Cyber law, also known as internet law, refers to the legal principles and regulations that govern activities on the internet and other digital networks. It is a complex and rapidly evolving area of law that covers a wide range of issues, including intellectual property rights, privacy, data protection, e-commerce, and online speech.

Cyber law is necessary as Cyber crime is increasing day by day and many countries are making laws to prevent the cybercrime, to protect the citizens and the organization from cyber attacks. Cyber law plays a crucial role in helping to ensure that the internet and other digital networks remain safe, secure, and trustworthy for everyone.

Cyber law is necessary as there is a lack of regulation in cyberspace, and it is essential to keep up with the ever-evolving technologies and the ways in which they are being used.

Cybersecurity refers to the practice of protecting internet-connected systems, including hardware, software and data, from attack, damage, or unauthorized access. It also involves the measures and technologies that are used to detect and prevent cyber threats, such as hacking, phishing, and malware. Cybersecurity is important for individuals, businesses, and organizations of all sizes, as well as government agencies and critical infrastructure providers.

Some examples of cybersecurity practices include:

- Firewall, antivirus and intrusion detection/prevention systems to protect against unauthorized access and malware.
- Encryption to protect sensitive data in transit and at rest.
- Regular software updates and patch management to fix vulnerabilities.

Q2. Explain Identity Theft and provide security measures

Identity theft is a fraud involving another person's identity for an illicit purpose. This occurs when a criminal uses someone else's identity for his/her own illegal purposes.
Examples – fraudulently obtaining credit, stealing money from the victim's bank account, using the victim's credit card number

Security Measures	Brief of Description

Monitor your credit closely	The credit report contains information about your credit accounts and bill paying history so that you can be tipped off when someone is impersonating you. Watch for suspicious signs such as accounts you did not open. You can also consider identity protection services, which range from credit monitoring to database scanning, for extra security
Keep records of your financial data and transactions	Review your statements regularly for any activity or charges you did not make
Install security software	Install security software (firewall, antivirus and anti-Spyware software) and keep it up to date as a safety measure against online intrusions
Use an updated Web browser	Use an updated web browser to make sure you're taking advantage of its current safety features
Be wary of E-Mail attachments and links in both E-Mail and instant messages	Use caution even when the message appears to come from a safe sender as identity information in messages can easily be spoofed.
Store sensitive data securely	Just as you keep sensitive paper documents under lock and key, secure sensitive online information. This can be done through file encryption software
Shred documents	It is important to shred the documents that contain personal or financial information (both paper and electronic) before discarding them. This prevents dumpster diving and in the online world, the ability for hackers to bypass information that has not been permanently deleted from your system

Q3. Explain Phishing and provide security measures

The word Phishing comes from the analogy that Internet scammers are using E-mail lures to fish for passwords and financial data from the sea of Internet users.
The E-mail will usually ask the user to provide valuable information about himself/herself or to "verify" information that the user may have provided in the past while registering for online account. To maximize the chances that a recipient will respond, the phisher might employ any or all of the following tactics:

1. Names of legitimate organizations

2. "From" a real employee

3. URLs that "look right"

4. Urgent messages

Security Measures	Brief of Description
Keep antivirus up to date	Important aspect is to keep antivirus software up to date because most antivirus vendors have signatures that protect against some common technology exploits. This can prevent things such as a Trojan disguising the web address bar or mimicking the secure link (i.e., HTTPS)
Do not click on hyperlinks in E-mails	It should always be practiced that, in case an E-mail has been received from unknown source, clicking on any hyperlinks displayed in an E-mail should be avoided. This may lead to either the link taking the victim to the website created by the phisher or triggering a Malicious Code installation on the system. Instead, to check out the link, manually retyping it into a web browser is highly recommended.
Take advantage of antispam software	Anti-Spam software can help keep Phishing attacks at a minimum. A lot of attacks come in the form of Spam and by using anti-spam software, many types of phishing attacks are reduced because the messages will never end up in the mailboxes of end-users
Verify https (SSL)	Ensure the address for displays " https://" rather than past "http://" along with a secure lock icon that has been displayed at the bottom right hand corner of the web browser while passing any sensitive information such as credit cards or bank information. One may like to check by double clicking the lock to guarantee the third-party SSL

Q4. Write note on email spoofing

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value. Unless they inspect the header more closely, users see the forged sender in a message. If it's a name they recognize, they're more likely to trust it. So they'll click malicious links, open malware attachments, send sensitive data.
Email spoofing is possible due to the way email systems are designed. Outgoing messages are assigned a sender address by the client application; outgoing email servers have no way to tell whether the sender address is legitimate or spoofed.

How Email spoofing works and Example
The goal of email spoofing is to trick users into believing the email is from someone they know or can trust—in most cases, a colleague, vendor or brand. Exploiting that trust, the attacker asks the recipient to divulge information or take some other action.
As an example of email spoofing, an attacker might create an email that looks like it comes from PayPal. The message tells the user that their account will be suspended if they don't click a link, authenticate into the site and change the account's password. If the user is successfully tricked and types in credentials, the attacker now has credentials to authenticate into the targeted user's PayPal account, potentially stealing money from the user.
More complex attacks target financial employees and use social engineering to trick a targeted user into sending millions to an attacker's bank account.
To the user, a spoofed email message looks legitimate, and many attackers will take elements from the official website to make the message more believable.

Spoofed emails mimic, or spoof, an email from a legitimate sender, and ask you to take some sort of action. Well-executed spoofs will contain familiar branding and content, often from a large well-known company such as PayPal or Apple. **Common email spoofing spam messages include:**

1. A request for payment of an outstanding invoice
2. A request to reset your password or verify your account
3. Verification of purchases you didn't make
4. Request for updated billing information
5. Tech support scams

Q5. Write a note on Malware

Malware, short for malicious software, refers to any type of software specifically designed to harm or exploit computer systems. Malware can take many forms, such as viruses, worms, trojan horses, ransomware, and spyware.

Some of the common characteristics of malware include:

1. The ability to replicate itself and spread to other systems
2. The ability to hide itself from detection by security software
3. The ability to cause harm to the infected system, such as by stealing personal information or disrupting the normal functioning of the computer
4. The ability to use the infected system to attack other systems

Virus: is a type of malware that attaches itself to a legitimate program or file in order to spread to other computers. Once a virus infects a computer, it can replicate itself and spread to other systems.

Worm: is a type of malware that can replicate itself and spread to other computers without needing to attach itself to a legitimate program or file.

Trojan: is a type of malware that disguises itself as a legitimate program in order to gain access to a computer system. Once it is installed, it can be used to steal personal information, install additional malware, or gain remote access to the infected system.

Ransomware: is a type of malware that encrypts a victim's files, making them inaccessible. The attackers typically demand a ransom payment in exchange for the decryption key.

Spyware: is a type of malware that is specifically designed to collect personal information from an infected computer, such as by monitoring the victim's browsing habits or logging keystrokes.

Rootkits: Rootkits is a software system that consists of one or more programs designed to obscure the fact that a system has been compromised.

Backdoors: Backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plain text and so on while attempting to remain undetected

Overall, malware is a serious threat to computer security and can cause significant harm to both individuals and organizations. It is important to use anti-virus and anti-malware software, keep your software updated, and practice safe browsing in order to protect yourself from these types of attacks.