Network Programming

Q2. If you are a System admin, what preventions steps you will take to secure your PC?

Beware of email attachments from unknown people. Don't open unexpected email attachments from unknown persons. Just because an email message looks like it came from someone doesn't mean that it actually did. Scammers can "spoof" the return address, making it look like the message came from someone else.

Don't click on links embedded in email messages. It's usually safer to go to the company's website directly from your browser than by clicking on a link in an email message, unless you are absolutely certain that the email was actually sent by the person or company claiming to have sent the message.

Spear phishing is a type of phishing attack that appears to be from a colleague, employer or friend and includes a link or something to download. Spear phishing often targets senior executives at organizations that may have valuable information stored on their computers. These messages may be personalized with publicly available information about the recipient to make them look genuine.

Passwords. Passwords are frequently the only thing protecting our private information from prying eyes. Be sure to use a strong password computer's user account and your router or modem. Never use the default password that comes with a router or modem.

Account privileges. Do not log into a computer with administrator rights unless you must do so to perform a specific computer maintenance task. Running your computer as an administrator may leave your computer vulnerable to security risks.

Keep your software up-to-date. Computer hackers are always finding new ways to penetrate the defenses of your software programs. Software vendors respond with patches that close newly found security holes. To stay protected, you need to download and install patches for both your operating system and your software applications whenever they become available. Software patches or updates often address a problem or vulnerability within a program.

Shut it down. Shut it down, lock, log off, or put your computer to sleep before leaving it unattended. Make sure that your computer requires a secure password to start up.

Protect sensitive information. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email. Don't send sensitive information over the internet before checking a website's security.

Avoid social engineering attacks. Social engineering can be defined as the process of obtaining information from other people through the application of social skills. The objective of social engineering is to deceive the computer user into compromising his/her system and revealing sensitive information.

Back up all your data. While your computer may be an expensive asset, it is replaceable. However, the data and personal records on your computer may be difficult or impossible to replace. Whether or not you take steps to protect yourself, there is always the possibility that something will happen to destroy your data. One important risk to your data is **ransom ware**.

Encrypt files on your computer, laptop or portable device. Encryption is a way to enhance the security of a file or folder by scrambling the contents so that it can be read only by someone who has the appropriate encryption key to unscramble it.

Name:- Ankur Raj

Roll:- 171210012