Corrigendum

Std - 9

Subject : computer Studies

Medium : English

As per the instruction by the Government of Gujarat and the Gujarat State Secondary and Higher Secondary Education Board, some additional information regarding 'Cyber Security, its Threats and Solution' has been presented at the end of chapter 14 in this new edition of textbook for 2021. In present time, the excess use of Internet has arised the threatful issue like 'Cyber Attack'. The measures of security have been discussed in these points. And also some questions regarding it, have been included in exercise.

Cyber Security, Its Threats and Solutions

Today most of us use Internet for one or another purpose. Even our homes, infrastructure, vehicles and home appliances are getting connected to Internet. The excessive sharing of data and interconnectivity of different things have brought a new threat called cyber attacks. Cyber attacks is an activity wherein a person sitting anywhere in the world with the use of Internet is able to target a persons or an organizations IT infrastructure with an intention to harm them or steal from them. It is an intentional and malicious effort by an organization or an individual to break into the systems of another organization or individual. The attacker's motives here may include data theft, information theft, financial gain, espionage, or sabotage. Though many cyber attacks exist, most of them result into the one of the following attacks.

Phishing: It refers to the use of deceptive means usually in form of a fake website page or web link to trick individuals into responding to the e-mail and disclosing sensitive information. For example one might receive an email stating that he or she has won a prize worth lakhs of rupees based on a game that he played on a particular website. To claim the prize money the user needs to provide details of his bank by clicking on a link. The message subjects are very lucrative and at times even a person who knows about spamming does fall in trap. The phishing attacks and spams are normally launched using e-mail systems that have been compromised.

Malware: Malware refers to "malicious software," that include viruses, worms, trojan horses, and spyware. These softwares are capable of creating a havoc on IT infrastructure as they can be used to control machine, access information, monitor activity, log keys and perform other malicious actions. The attackers are taking advantage of e-mail to transfer malware from one place to another easily. The attacks although not successful always if happens may allow the attacker to take control of our email account, machine, data and other sensitive information.

Ransomware: It involves the hacker locking the access to victim's computer or files. The attacker in this case holds the acquired information for ransom. The victim to get back access to what is legitimately his property needs to pay the attacker. Ransomware spreads through phishing emails or unknowingly visiting an infected website.

Data Exposure: It is becoming a major cyber security threat today. Here the attackers tries to get access to database information of an applications like banking, social media, university or any other applications that store data. Data exposure occurs in a different ways. Hackers might be able to steal login details of a user through social engineering or use malware to gain access. Accidental sharing of data also at times lead to data exposure. Accidental sharing usually occurs as a result of human error. A simple action of "Reply All" to an email can cause data exposure.

These attacks have given rise to term called, Cybersecurity. Cybersecurity is application of certain mechanisms that are used to protect a computer system from the theft or damage of computer's hardware, software, or electronic data. It also intends to protect the services that the computer systems provide. With virtually everything getting connected with each other with the use of Internet, cybersecurity has never been more critical.

Few steps mentioned here will help organizations and individual put better protection in place. The steps if followed properly will help in protection against cyber attacks.

- While using computer systems like servers, personal computers, laptops or mobile devices install a good anti-virus or anti-malware software.
- Ensure that the anti-virus software or anti-malware software installed on the devices is up to date. Every day, new set of viruses and malware appear in market. Thus it becomes important for individuals and businesses to remain protected from these viruses.
- Use a firewall to protect a computer or networks that you use. As malware can spread using multiple means other than email it becomes important to control the data that moves on the network. Firewall monitors traffic entering and leaving the network. Similarly user computers such as home personal computers or laptops, should install a personal firewall to ensure that the computer is protected.
- All incoming and outgoing emails should be filtered for computer viruses. The filters should ideally installed at entry points of networks such as a router or an access points.
- All the users should be educated about the best practises of using computers. For example one must ensure not to open an attachment or to click on a link in an email they are not expecting.

- We should not download and run programs of unknown origin without first getting proper information of the download source.
- Ensure that regular backup of important files and folders are taken. One must keep this backup either on removable media such as portable drives. For added security, the backup should be stored securely on another location.
- Where possible, try to use access control mechanisms and restrict end user permissions. The end users of the organization should not be given administrative privileges on their devices.
- Design network security policies within an organization and propagate them to all the users.

Common Threats while using an E-mail System

An e-mail system today has become integral part of communication mode in organization. It is used to expedite the process of sending and receiving information. An e-mail system is generally made up of two components, a server and a client. These components are known as mail server and mail clients. Users can read, compose, send, and store e-mails using mail clients. The mail client sends the email using the underlying network infrastructure to a mail server. The mail server then delivers, forwards, and stores e-mail messages. Thus it becomes mandatory to protect all components involved in proper working of an email system. We need to protect the mail clients, servers as well as the devices and the infrastructure that is part of email systems.

Attackers can try to exploit the usage of e-mail system to cause hindrance in the organizational or personal activity. They may try to access confidential information, disrupt IT access to resources, or gain control over an organization. Some of the common threats that are observed people when using emails are Malware, Spam, Phishing, Social engineering, Unauthorized access to resources and Information leak. Let us have a more detailed understanding of how these threats can affect an individual or an organization.

Spam: Unsolicited commercial or non commercial e-mails found in our mailbox are commonly known as spam. Spams have tendency to disrupt user productivity, and consume computer resource like disk space, memory or processor. Further it can also be used as a tool to distribute malware. Email systems today provide a separate folder named "Spam" and a filter rules that can be applied to mark an email as spam.

Social engineering: Social engineering refers to tricking people into handing over access to ones or organization's sensitive information. E-mail spoofing is a common social engineering attack, here a person or a program successfully pretends to be an official user by falsifying the sender information. For example an IT department of an organization may receive a message from its Accounts Officer (attacker using the account officers credentials) which states that he or she has forgotten the password of a crucial application and would like it to be reset.

Unauthorized access to resources: An attacker or an insider with malicious intent may use email as a tool to gain unauthorized access to resources through a successful attack on a mail server.

Information Leak: People use emails from different location and devices. This practise of using the emails from multiple location at times lead to unintentional information leak.

Also note that the Malware and Pishing attacks discussed in earlier section can also be easily launched using an email.

With the use of emails increasing day by day, it becomes necessary to take precautions when using email for communications. The steps mentioned here provides a general guideline for organizations and user for precautionary usage of email.

- Make sure that the mail server application of the organization is secured.
- Make sure that the mail clients that you use are secured.
- Make sure that the transmission lines used for tranfering mails are secured.
- Secure the supporting hardware and operating environment.
- Do not open any emails from untrusted sources.
- Never open unexpected attachments without scanning.
- Choose a strong password for your mail accounts.
- Use updated anti-virus software on the computers from where you access emails.
- Do not access emails from public Wi Fi places like restaurants, malls and other places.
- Try not to leave your machines accessible to others.

EXERCISE

1. What is Cyber security?
2. List and explain the threats that can crop up when using an email.
3. What do you mean by data exposure? How can organizations protect themselves from it?
4. Define the following terms:

   (a) Spam (b) Ransomware (c) Malware (d) Phishing

5. **Choose the most appropriate option from those given below :**

   (1) Deceptive means usually in form of a fake website page or web link to trick individuals into responding to the e-mail and disclosing sensitive information is an example of which of the following?

   (a) Cyber Bullying (b) Cyber Grooming (c) Phishing (d) Spam

   (2) Which of the following refers to the hacker locking the access to victim's computer or files?

   (a) Malware (b) Spam (c) Phishing (d) Ransomware

   (3) Which of the following threat are encountered while accessing an email?

   (a) Social Engineering (b) Phishing (c) Spam (d) All of these