International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 03 | Mar 2021 www.irjet.net p-ISSN: 2395-0072

Security Issues in the Information System and Solution of the Security Issues

Miss. Suchitra Shantaram Poskar[1], Miss. Ruchita Rajesh Khamkar[2]

[1]Student of M.Sc.I.T. , D.B.J. College Chiplun, Ratnagiri , Maharashtra, 415605.
[2]Student of M.Sc.I.T. , D.B.J. College Chiplun, Ratnagiri , Maharashtra, 415605.

Abstract:- The purpose of this paper to discuss security issues in information system. In today's, people can collect amount of data their business, there is chance to hack data so there is need to secure this data. But there is lots of issues in security are occurs. Security is become most important issue in information system. In this we can see the issues of the security and why it is important. Also we will cover some solution of that issues.

Keywords: Security issues, current security issues, Solutions of the security issues in IS, why security in information system is important?

Introduction

The problems are occurs in the information system is either computer viruses or threats or abuse. Since the current generation are depends upon the information system, problems are threatening information system also daily activities. The current issues are of security is jamming spoofing, hacking malicious software, etc.

Internet allows a creativity including black market, so cyber criminals are carefully discovers a new path to commit illegal act , tapping sensitive internet network in the world. Therefore protecting data is the growing challenge.

Before information systems invented the information are stored in the paper files only and in certain departments where many people's would not have access to the data. In the evolution of the information system the big amount of data are store the electric format rather that paper format so users can viewed the amount of data . Also more users can access the large amount of data electronically rather that manually. But there is more susceptible to the threat of cyber crime.

Security Issues

Now a days, every day launch new technology or gadgets. Many times it access internet but there is no planning for security. Because of weak security there is chance of risk. One of the current computer crime is spamming, spamming means sending intrusive emails to threat the people using information system. Spammers are rarely punished since law are hardly enforced.

Next is hacking . everyone knows about hacking, hacking means illegal user attempt to access private information and misuse it .Jamming is also another computer crime. It is not one of the most common and easiest way to threatening information system.

Identity theft can occurs someone use another person private information and commit fraud to gain benefits from financially, medically, etc. once criminal access this information they may use it to commit identity theft.

Current Security Issues in Information System

1) Hacking
2) Spamming
3) Sniffing
4) Viruses and Malicious Software
5) Jamming
6) Identity Theft

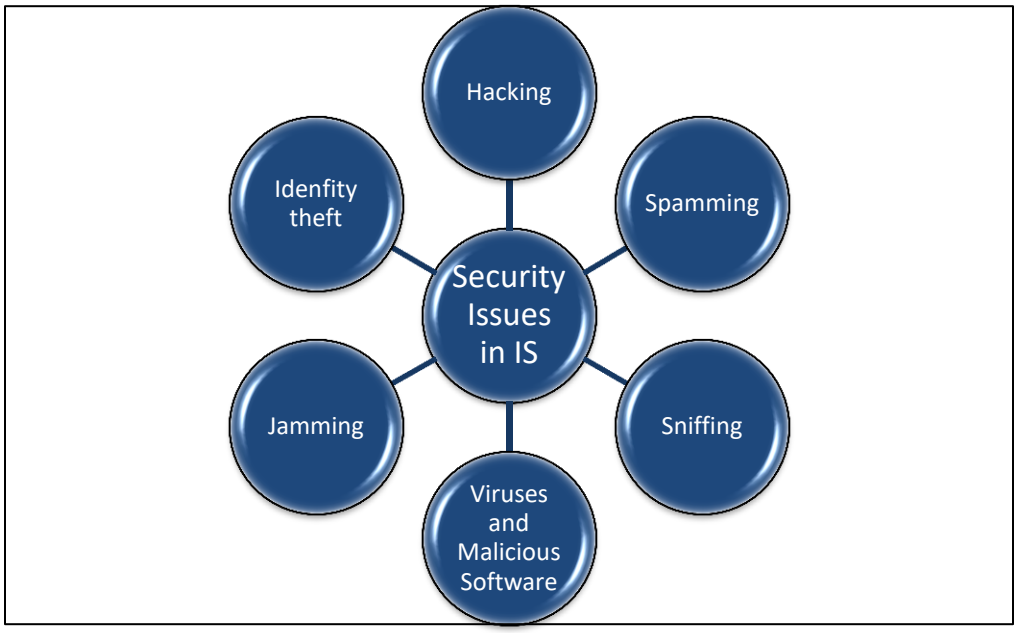

Fig:-security issues in IS

1)Hacking

Hacking means gaining unauthorized access to data in user's computer. Hacking is used to by-pass security control to gain unauthorized data to access a system. Once hackers can gain access the data then they can do whatever they can want. Some common activities are-

- Stealing sensitive information
- Spying user action using installing apps that allows attackers.
- Defacing website

2) Spamming-

Spamming means any king of unwanted, intrusive digital communication through emails, calls. It purposely used for commercial advertisement. But criminals used for threatening. Unfortunately, in 2018 many email spam very much in problems, many business who fall victim to spam year after year. About only 55% contain legitimate data that means almost half of the email content is spam.

3) Sniffing

Sniffing means monitoring and capturing all data packets through the network. Sniffers are used by network to monitor and create the traffic. Atttakers are used sniffer to caputer data packets through the network for containing sensative information such as user's personal account information, password, etc. Sniffers can install hardware or software in the system. They are placing a packet sniffer in a network and capture malicious intruder and analyzed all traffic network. There are two types of sniffer, first one is active sniffer and second one is passive sniffer. In active sniffer , that sniffer conducted switch network means two devices connected in network. These switch uses a MAC (media access control) to forward information to their destination ports. Attackers take advantage to create network traffic into LAN to enable sniffing. The second is passive sniffers, in this sniffer uses hub instead of switches. It perform like switch only they used Mac address to read their destination ports of data. Attackers simply connected to the LAN and they are able to sniff all data traffic in the network.

4) Viruses and Malicious software

Now a day's use of internet are increasing rapidly, because of these risk are increased in the computer network that are affected by malicious software or programs such as viruses. Malicious software is a software that uses for to harm or hack the user's personal information or business information. Computer viruses are the small part of computer code that is inserted into another program and lies inactive account until triggered by unsuspecting person. This trigger means opening a file or downloading a file using internet. Most of the companies installed anti-virus software but most sophisticated anti-virus software cannot keep with increasing number of viruses and malicious software or program. Attacker's motive of the creating viruses is seeking profile , misuse of sending messages etc it demonstrate that vulnerability in the software for denial of service to explore security issues.

5)Jamming

Jamming is another cyber crime that are used to threat a information system. It is not one of the common way but it is a easiest to accomplish. Jamming means attacker that attempts interface with the broadcast communications. Behind the purpose of jamming is finding a way to tied up a line to a computer is the central brain behind the website. Once lines are tied up, legitimate users can access the website, therefore lines are 'jammed' with illegal user.

6)identity theft

Identity theft also called as identity fraud. It is a crime that criminal obtain personal information such as user's name, their social security number, credit or debit card number to commit a fraud or other crimes. Identity theft occurs most of the business or organizations when illegal users used to stole electronic records from employer. Identity theft access to computer to hack into IS of the business or organization. Once they information illegally accessed, the result will be harmful for the victim.

Solutions of the security issues in IS

1)Hacking:-

- Don't access personal or financial data on the public wifi this may caused harmful. Using personal information such as back account with credit using public wifi ,it may not secure. It is best to do those things on secure connection
- Hackers can hack your information ,location or connection when users GPS connection is on instead of that when we need GPS just turn them on otherwise off.
- Use password or any encryption code while opening a device or file and never use auto complete feature for encryption code. This can protect person's private data or information.
- Don't use link or do not open link or attachment if not sure about that source

2)Spamming

- Most of the spam messages are fraud emails send by unknown person or sources. The hacker who hack the information through the sources of their victim. So never respond such type of spam message because spammer will know that email address is always active thus it increase the chance to target the email by the spammer.
- Everyone can easily access internet , spammer are also sneaking on internet and finding the email addresses which they will send spam emails. So newer post email addresses on publicly they can send spam emails on that account or it is not good using weak password the hacker will hack the account.
- Download anti-virus software or spam filtering tool , it can help to scan the email that received for malicious program.
- Do not any personal or business email address because many spammers are sneaking on internet to find such type of group of email list to collecting new email addresses

3)Sniffing

- Installing antivirus tool like *Avast free antivirus* it can protect computer devices from the sniffers. Hackers will use viruses and worms to target a computer for sniffing but strong antivirus tool can prevent these attacks.

- Do not visit unauthorized access site, it if we visit it will affect harmful for computer device. Visit HTTPS site S means secure, browser can show the padlock icon next to the URL means those sites are secure. HTTPS are encrypted that's why it can protect from those website until you're there. It protects us only at that specific website that are encrypted.
- Antivirus tool and encryption are protect from sniffer

4) Viruses and Malicious software

- One of the most easiest way to protect against malicious program is to install anti-virus software. This software protect device from viruses that threat to the system. It can scan the device and clean the unwanted files that affect on device and malware. And also it provide automatic update to protect against newly creating files or viruses.
- Regularly update anti-virus software, when installed anti-virus software ,it ensure that it regularly updated to stop attacker to attack to access computer device through the vulnerabilities.
- Don't click on unknown link or open any suspicious site or emails, they are trick into people to fool them or to force them to open that link that way is called phishing. It is the easiest way for hacker to install malicious software on the device. These type of link may infect computer with viruses, if it is doubtful site , do not click it.
- Install firewall that protect device from malware. It stops the malicious attack by unauthorized person who access the private computer network. It provide extra barrier against viruses and prevent the chance of attack.

5)Jamming

- Jamming attacks caused because of transmission of radio network communication. Regularly check source on the site. Most of the user not regularly check the sources of the most of the traffic site, there is chance of traffic jam.

6)Identity theft

- Protect computer device or Smartphone with security software.. if computer device or smartphone are infected with viruses, other safeguards are little help to prevent those viruses but criminal definitely attack online action because they have key to access the device.
- Use strong password, because of weak password hacker can hack the device and damage user's system.
- Stay alert and watch the identity theft action such as false information, missing bills or mails, receiving call about past bill for product that you didn't buy.

Why security in information system is important?

A security in computer device works as a barrier, or a shield, between your PC and cyber space. It reduced the risk of attacks in the IT systems. By apllying security to protect sensitive information or data from unauthorized user also it can protect denial-of-service attacks.

Now a days everyone used internet so it is possible to stole the information by hacker, the security system and our awareness protect devices or data from attacker, viruses and malicious program.

References

security issues-

https://en.wikibooks.org/wiki/Introduction_to_Information_Technology/Cybersecurity

https://courses.lumenlearning.com/wm-introductiontobusiness/chapter/reading-security-issues-in-electronic-communication/

Current security issues in information system:-

https://www.guru99.com/mis-ethical-social-issue.html

https://link.springer.com/article/10.1023%2FA%3A1010064007816

https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types

https://www.greycampus.com/opencampus/ethical-hacking/active-sniffing-attacks

https://pchtechnologies.com/what-is-malicious-software/

https://its.unl.edu/security/identity-theft/#A.

Solution or prevention of the security issues:-

https://www.chubb.com/us-en/individuals-families/resources/6-ways-to-protect-yourself-from-hackers.html

https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/5-simple-ways-you-can-fight-spam-and-protect-yourself

https://www.avast.com/c-sniffer

https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing_tools.htm

https://www.webroot.com/in/en/resources/tips-articles/how-can-i-protect-myself-from-identity-theft-online

Why security in information system is important?

https://www.redteamsecure.com/blog/why-is-information-security-important#:~:text=Reducing%20the%20risk%20of%20data,unauthorized%20access%20to%20sensitive%20information.&text=Ensuring%20business%20continuity%20through%20data,information%20safe%20from%20security%20threats.

https://www.iticollege.edu/the-importance-of-information-systems-security/

Biographies:-

Miss. Suchitra Shantaram Poskar,
Student of M.Sc.I.T. ,
D.B.J. College Chiplun, Ratnagiri,
Maharashtra, 415605.

Miss. Ruchita Rajesh Khamkar,
Student of M.Sc.I.T. ,
D.B.J. College Chiplun, Ratnagiri,
Maharashtra, 415605.