CYBER SECURITY

MADE BY

Daljeet Raj

VLE CSC

216737550017

What is cyber security?

Computer security, cybersecurity, or information technology security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. Cyber-attacks can be considered as an exploitation of resources, unauthorized access to the systems, ransomware attacks to encrypt data and extract money.

What Are the Elements of Cyber security?

- **Application security.** *Website applications are common ground for cybercriminals and its' vulnerability may cause a lot of trouble. Organizations that run a business on the websites must ensure their safety to protect their customers, their financials and personal information.*
- **Network security.** *It is the process of protecting servers and solving security issues in servers, hosts, devices, and internet services. Network security is done by protecting the usability and integrity of data on the network.*
- **Operational security.** *It protects the organization's main functions. Operational security is important to track critical information and the assets that interact with it to identify vulnerabilities.*

Threats to Computer

A. Theft means stealing of information or hardware for using the data for wrong purposes.

B. Viruses are computer programs that can damage the data and software programs or steal the information stored on a computer.

Theft

These maybe of three types:

- Physical: Where a person may steal your desktop computer or laptop.
- Identity: Where a hacker steals your personal information and assumes your identity. Using this false identity, the hacker can gain access to your account information or perform illegal activity.

- Software Piracy: This is stealing of software and includes using or distributing unlicensed and unauthorized copies of a computer program or software.

Viruses

Major types of viruses are Worms and Trojan Horse.

- **Worms :** These are viruses that replicate themselves and spread to all files once they attack a computer. This makes it very difficult to remove them.
- **Trojan Virus :** A Trojan Horse disguises itself i.e., it appears to be a useful software program but once it reaches a computer it starts behaving like a virus and destroying data.

- **Online Predators :** Online predators are people who trap you into inappropriate relationships. They may be older people posing to be your age, bullying you into doing illegal activities online.

➢ Reasons for Security Break

Security break is leakage of information stored in a computer.

Personal information can be lost or leaked in two ways:

1. We are not careful in giving out personal information over the Internet. For example, we share our account details and password on unsecure sites.

2. A person gets unauthorized access to our computer. This can happen in the office if we leave are computer without logging out. Computer security and privacy is about measures we can take to restrict access to personal data stored in a computer.

Best practices for cyber security

- Use strong passwords
- Encrypt your data
- Keep your username and password private.
- Don't share personal info
- Use antivirus and antispyware software
- Clear cookies frequently
- Install firewalls

- Always use secure sites
- Disk fragmentation
- Backup your data

Using strong passwords

Use strong passwords, a combination of alphanumeric and special characters could be used for creating a password that is not so easy to crack or guessed by other users.

Points to be considered while creating passwords: -

i. Change your password frequently at least 2 or 3 weeks so that your account information remains secure.

ii. Using strong passwords can lower the risk of a security breach; effectiveness of a password depends on the security mechanism of the software and users' involvement in generating a strong password.

iii. Keep the length of the password at least 12-14 characters if permitted.

iv. Avoid keeping passwords based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, etc.

v. Use capital and lower-case letters.

vi. Avoid using the same password for multiple sites or purposes.

vii. Avoid using something that the public or workmates know you strongly like or dislike.

viii. Use random password generators if possible. Example of a strong password: u1vX:4Hd{] $

Use data encryption: This is usually done by banks and companies in which important customer information is stored. They can encrypt their entire hard disk using encrypting feature in Windows (Bit locker). This would force users to use a decryption password (or key) before starting the computer thus preventing unauthorized usage.

Install antivirus and antispyware software: Antivirus and Antispyware programs offer real-time protection monitoring your computer for any changes by malware software. Keep your Antivirus and Antispyware software always up to date, this can help in protecting your computer from recent threats.

Use firewalls: Firewalls could be software or hardware and can assist in keeping a computer and a network secure. Firewalls analyze the network traffic and determine if the traffic should be allowed or not.

Clear browser cookies frequently: Cookies are programs that are created on your local computer when you visit websites. Though cookies are meant for storing data based on your activity performed during your earlier visit such as logon details, details of a shopping cart, visited pages in a website, etc. they could also be tracked by unauthorized users and possibly gain access to your personal information.

Never install software from unknown sources: As they might not be trustworthy; download only from well-known or reputed websites. Verify the source if it is legitimate by searching the internet or referring to comments from other users before downloading them; understand the nature and the purpose of the software before attempting to download and install them.

CONCLUSION

Cyber security is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so it is crucial to learn how to defend from them and teach others how to do it too.

THANKYOU