TYPES OF CYBER THREATS

NAME : JANHVI

COURSE NAME : CYBER SECURITY

DATE: 13 JULY

GUIDER’S NAME: MR. RUSHIKESH DINKAR

What is cybersecurity?

- It's the practice of protecting computer systems ; Networks, Software and Data, from Digital Attacks, or Unauthorized Access or Theft.
- It involves a Combination of technologies, Processes and Practices such as;
- It prevent Attacks;
- It detect threats so we can urgently fix them before any sort of mishappening , so its like an advantage for it .
- It respond to incidents.
- It recovers from damage; as in case anything we lose such as data; we immediately can backup or recover it .

DEFINITION OF CYBER THREATS

- These are malicious Attempts to damage, disrupt, or gain unauthorized access to computer systems, or data. These threats come from different or various sources such as Hackers, Criminal Organisations, etc.
- There are many types of cyber threats such as;
- Malware
- Man in the middle (MitM) attacks
- Denial of service
- SQL Injection
- Zero day Exploits
- Advanced Persistent Threats (APTs)

What is MALWARE?

- It’s a Malicious Software.
- It includes Viruses, Worms, Spyware, Ransomware and Adware.
- Let’s take an example of Malware; A Ransomware Attack that encrypt your Files and Demands Payment to unlock them for Misuse.
- Types are Trojan Horse , Spyware, Rootkits, Keyloggers.
- You can prevent by use firewalls and enable real time protection or update software regularly, avoid random clicks.

What is PHISHING?

- It’s a Fraudulent Emails or Messages tricking Users into Revealing personal or financial Information.
- Lets take an example; An Email pretending to be from your personal bank account asking for your login credentials.
- Includes a malicious link or attachment
- Clicking it leads to a fake login page or downloads malware.
- Types are Email Phishing, Spear Phishing, Whaling, Smishing, Vishing.

What is RANSOMWARE?

- A TYPE OF MALWARE THAT LOCKS OR ENCRYPTS DATA AND DEMANDS A RANSOM TO RELEASE IT.
- LETS TAKE AN EXAMPLE; IN MAY 2021 IRELAND'S PUBLIC HEALTH SYSTEM KNOWN AS HSE WAS HIT BY A SERIOUS RANSOMWARE ATTACK, IT CAUSED A NATIONWIDE HEALTHCARE CRISIS.

What are APTs? (Advanced Persistent Threat)

- It is highly skilled, long term cyberattack carried out by well funded and organized groups often linked with government or cyber criminal organizations.
- It's more like cyber spy mission but not a quick hack.
- The common targets are; govt. and Military Networks.
- Large companies, Healthcare or research organizations, critical infrastructure.
- And few examples are; APT1 China and Stuxnet.

How to protect against cyber threats

- ANTIVIRUS
- FIREWALLS
- REGULAR UPDATES
- STRONG PASSWORDS
- EMPLOYEE TRAINING

CONCLUSION

- Cyber threats are becoming increasingly sophisticated, frequent, and damaging in today's digital world.
- From malware and phishing to APTs , Attackers use various methods to exploit vulnerabilities and gain access to sensitive data.
- Understanding the types of threats is the first step towards building stronger defense system's and promoting cyber awareness.
- Individuals and organizations must stay Updated, adopt proactive security measures, and promote a culture of cybersecurity to stay protected.
- Cybersecurity is not just a technical issue; but it is a shared RESPONSIBILITY.

THANK YOU FOR YOUR TIME AND ATTENTION !

If you have any questions or query , feel free to ask .

Janhvi [janhviiprajapati@gmail.com]