Technical Talk-1

**Report: Cyber Security at the Workplace**

Resource Person : Mr. Sagar. R. Pujar Date: 4th July, 2025

Time: 11:00 AM

* Introduction

**Cyber Security** refers to the practice of protecting systems, networks, programs, and data from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

* Types of Cyber Security

1. **Operations Security (OpSec):** Operations Security (OpSec) is a risk management process that identifies critical information and then takes steps to protect it from adversaries. Originally developed by the military, OpSec is now widely used in cybersecurity and business environments to safeguard sensitive data and operations.
2. **Application Security:**Focuses on keeping software and devices free of threats. This protection can be done by **constantly updating the apps** to ensure they are secure from attacks.
3. **Identity Management:** Controls user access within the organization.It deals with the procedure for determining the **level of access** that **each individual has within an organization.**
4. **Mobile Security:** It involves securing the organizational and **personal data stored** on mobile devices such as **cell phones**, **computers**, **tablets**, and **other similar devices against various malicious threats**.
5. **Cloud Security:** It involves in **protecting the information stored in the digital environment** or cloud architectures for the organization.

It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.

1. **Network Security:** Network Security refers to the strategies, technologies, policies, and practices used to protect the integrity, confidentiality, and accessibility of computer networks and data.Protects computer network from intruders, whether they are targeted attackers or opportunistic malware
2. **Threat Assessment:** Threat assessment is the process of identifying, analyzing, and evaluating potential threats that could harm an organization's assets, operations, people, or reputation. It is a crucial part of risk management and cybersecurity planning.

* Types of Cyber Security Threats

Cyber threats are malicious acts aimed at stealing data, damaging systems, or disrupting digital operations. Common threats include:

* Malware
* Insider Threats
* Ransomware
* Phishing
* Ransomware
* SQL Injection
* Data breaches
* Major Cyber Security Tips for the Workplace

**1**. **Think Before You Click**

Avoid clicking on suspicious links—common phishing trick is clickjacking.

**2**. **Use Strong and Unique Passwords**

Follow guidelines from NIST. Use combinations of characters, and change passwords frequently.

**3. Use a Password Manager**

Tools like KeePass, LastPass, or Dashlane help manage passwords securely.

**4. Enable Multi-Factor Authentication (MFA)**

Adds an extra layer of protection by requiring additional verification.

**5. Check CERT-In Updates**

Monitor alerts from India’s Computer Emergency Response Team for cybersecurity news and incidents.

**6. Keep Systems Updated**

Regular updates reduce vulnerability to cyberattacks.

**7. Use Firewalls and Antivirus Software**

Implement and maintain tools like Norton, McAfee, or NGFW to block threats.

**8. Avoid Using Debit Cards Online**

Prefer safer options like PayPal or credit cards for online transactions.

**9. Recognize Phishing Scams**

Look out for suspicious email content, links, and sender details.

**10. Avoid Unfamiliar Websites**

Untrusted websites can trigger drive-by download attacks.

**11. Limit Downloads**

Only download essential files from trusted sources; use custom installation.

**12. Be Cautious on Social Media**

Oversharing can make you an easy target for attackers.

**13. Regular Data Backup**

Always keep a secure copy of your data to restore in case of cyber incidents.

**14. Avoid Public WiFi Without VPN**

Use VPNs to encrypt connections when on public networks.

**15. Secure Data Using Encryption**

Use strong encryption for digital assets and limit access through proper control mechanisms

* **Tools & Hands-On Activities**

1. **Footprinting & Port Scanning:** Using tools like Nmap and Google Hacking Techniques.
2. **Advanced Google Operators:** intitle:, inurl:, filetype: etc. for information gathering.
3. **Phishing Identification:** Google’s Phishing Quiz platform.
4. **Dark Web & Privacy Exploration:** TOR Browser.
5. **Password Cracking Practice:** EC-Council’s Skillpacks.

* **Use Strong and Varied Passwords**

1. To make your passwords strong and secure, you can refer to the password policy guidelines of the National Institute of Standards and Technology and consider the following:
2. Use passwords with **more than 8 characters** and a **maximum of 64 characters**
3. Never make use of the same password **twice**
4. **Use at least one u**ppercase letter, one **l**owercase letter, one **n**umber, and a **few symbols** other than &, #, \_, @, etc.
5. Use passwords that are easy to remember and also, **do not leave clues** in the open or make them available to the public
6. Change your **password often** and **reset it.**

* **Avoid Online use of Debit Cards**

1. One of the most useful Cyber Security measures that you can take is regarding online transactions and payments.
2. When you purchase services or products online, try to avoid paying through debit cards or any other payment method that is connected to your bank account directly.
3. Rather, you can make use of applications like PayPal or credit cards, which will provide more protection to your bank account

* Cyber Security Activities

**Activity 1:** Google Hacking

Using advanced search operators (e.g., intitle:, inurl:, filetype:) to gather OSINT (Open Source Intelligence) from web pages.

**Activity 2:** Phishing Awareness

Identifying phishing and legitimate emails using interactive platforms like Google Phishing Quiz.

**Activity 3:** Tools for Ethical Hacking

Tor Browser – For anonymous browsing.

Nmap – For network mapping and port scanning.

Citizen Evidence – Analyzing media for authenticity.

Password Cracking Labs – Online cybersecurity training on password security.

* Conclusion

Maintaining cyber security in the workplace is essential in today’s digital age. Employees must stay informed, follow best practices, and use the right tools to defend against an ever-evolving threat landscpes.