



# Cybersecurity

Protecting the Digital World

Asst. Professor Sachin Singh



# Introduction to Cybersecurity

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. It is crucial in today's digital age as cyber threats are increasing in frequency and complexity. Understanding the key areas such as network security, data protection, and endpoint security enables organizations to strengthen their defenses against potential breaches.

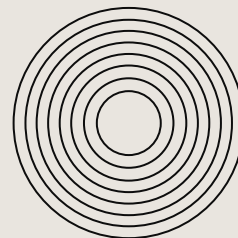




01

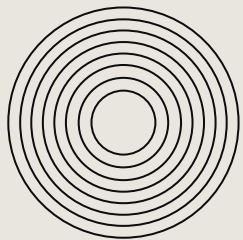
+

# Threats



+

.....



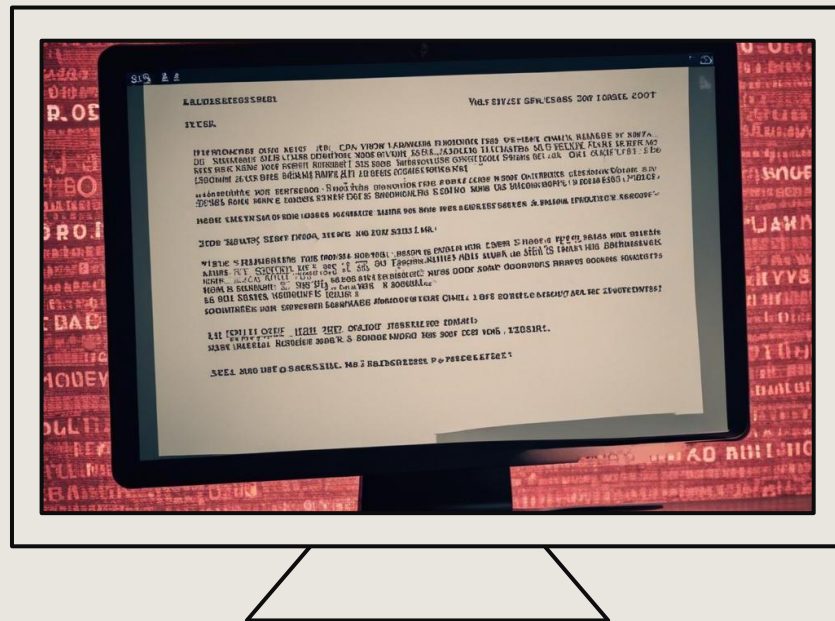
# Phishing Attacks

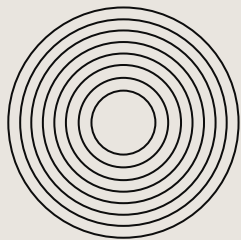
Phishing is a cyber attack that involves tricking individuals into providing sensitive information, such as login credentials or financial details, typically through deceptive emails or websites. Attackers often impersonate legitimate organizations to increase the likelihood of success. Phishing can lead to identity theft and significant financial losses for victims.



# Malware & Ransomware

Malware is malicious software designed to harm or exploit any programmable device or network. Ransomware is a particular type of malware that encrypts files on a victim's device, demanding payment for the decryption key. These attacks can disrupt operations, compromise sensitive data, and result in significant costs for recovery and mitigation.





+

# Social Engineering

Social engineering is a manipulation technique that exploits human psychology to gain confidential information or access. Attackers use various tactics, such as impersonation, to deceive individuals into divulging personal or organizational data. Common forms of social engineering include pretexting, baiting, and tailgating. Educating individuals about these tactics can significantly reduce susceptibility to such attacks.

⋮

+

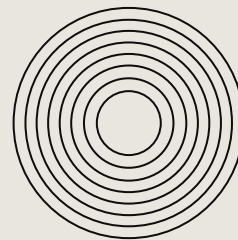




02

+

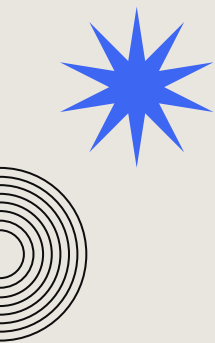
# Best Practices



.....

+





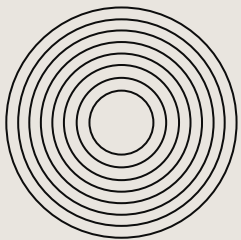
+

# Strong Passwords & MFA

Using strong passwords is vital for cybersecurity. Passwords should be complex, incorporating uppercase letters, numbers, and symbols. Multi-factor authentication (MFA) adds an extra layer of security by requiring multiple forms of verification before granting access. This significantly reduces the risk of unauthorized access even if a password is compromised.







+

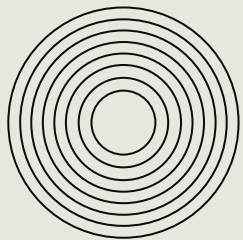
# Software Updates

Regularly updating software ensures that any vulnerabilities are patched, protecting systems from exploitation by attackers. Software updates often include security enhancements that address potential threats. It is important not to ignore update prompts and to enable automatic updates whenever possible to maintain security integrity.

⋮



+



# Identifying Suspicious Emails

Recognizing suspicious emails is crucial in preventing phishing attacks. Indicators of phishing emails include unknown senders, misspellings in the domain name, urgent calls to action, and generic greetings. Training individuals to scrutinize email content and verify the sender's identity can prevent falling victim to scams and data breaches.





# Conclusions

In conclusion, enhancing cybersecurity requires awareness of various threats such as phishing and social engineering, along with implementing best practices like strong passwords and timely updates.

Educating everyone about these measures is essential in creating a safer digital environment. Staying informed and vigilant is the key to protecting oneself online.

