Managing Cybersecurity Risks...

Definitions

- Malware: Malicious software that disrupts or damages a user's computer.

- Phishing: Deceptive email scams aiming to steal sensitive information.

- Spoofing: Fake identity tricks to gain unauthorized access.

- Supply Chain Attack: Breaches through third-party vendors.

- Insider Threat: Risks from malicious or negligent employees.

- DoS Attacks: Denial of Service attacks that overwhelm networks.

- Identity-Based Attacks: Exploits using compromised credentials.

- Code Injection Attacks: Insertion of malicious code into software.

- DNS Tunneling: Abuse of the Domain Name System to pass malware or stolen information.

- IoT-Based Attacks: Exploiting vulnerabilities in Internet of Things devices.

Phishing is a type of cybercrime where individuals are contacted by someone posing as a legitimate institution via email, telephone, or text message to lure them into providing sensitive data such as personal information, banking and credit card details, and passwords. This information can then be used for identity theft or financial loss.

The term "phishing" is a play on the word "fishing," as it involves using deceptive emails or messages as lures to "fish" for information from individuals. To protect against phishing, it is important to be cautious with unsolicited communications and to verify the authenticity of requests for personal information.

Training Video:
https://youtu.be/JlQovysQBn0?si=GW3k1o8bdIC2dus2

Types of Attacks...

Pharming: Redirecting users from legitimate websites to fraudulent ones using malicious code.

Whaling: Targeted phishing attacks aimed at senior executives.

Evil Twin: A fake Wi-Fi network that mimics a legitimate one to capture user data.

Website Spoofing: Creating fraudulent websites that appear legitimate to deceive users.

Man-in-the-middle Attack: Intercepting communication between two parties to steal or manipulate data.

Spear Phishing: Highly targeted phishing attacks that impersonate trusted sources.

HTTPS Phishing: Using a secure link that leads to a malicious website.

Email Phishing: Sending deceptive emails that appear to be from reputable sources.

Angler Phishing: Posing as customer service agents on social media to deceive individuals.

Clone Phishing: Creating a nearly identical version of a legitimate email to trick users.

Vishing: Phishing conducted over the phone.

Watering Hole Phishing: Compromising a popular website to target its users.

Pop-up Phishing: Using adware or scare tactics through pop-up messages.

Deceptive Phishing: Email spoofing to impersonate legitimate organizations.

Search Engine Phishing: Creating fake product pages that appear in search engine results.
Image Phishing: Using malicious image files to execute an attack.