

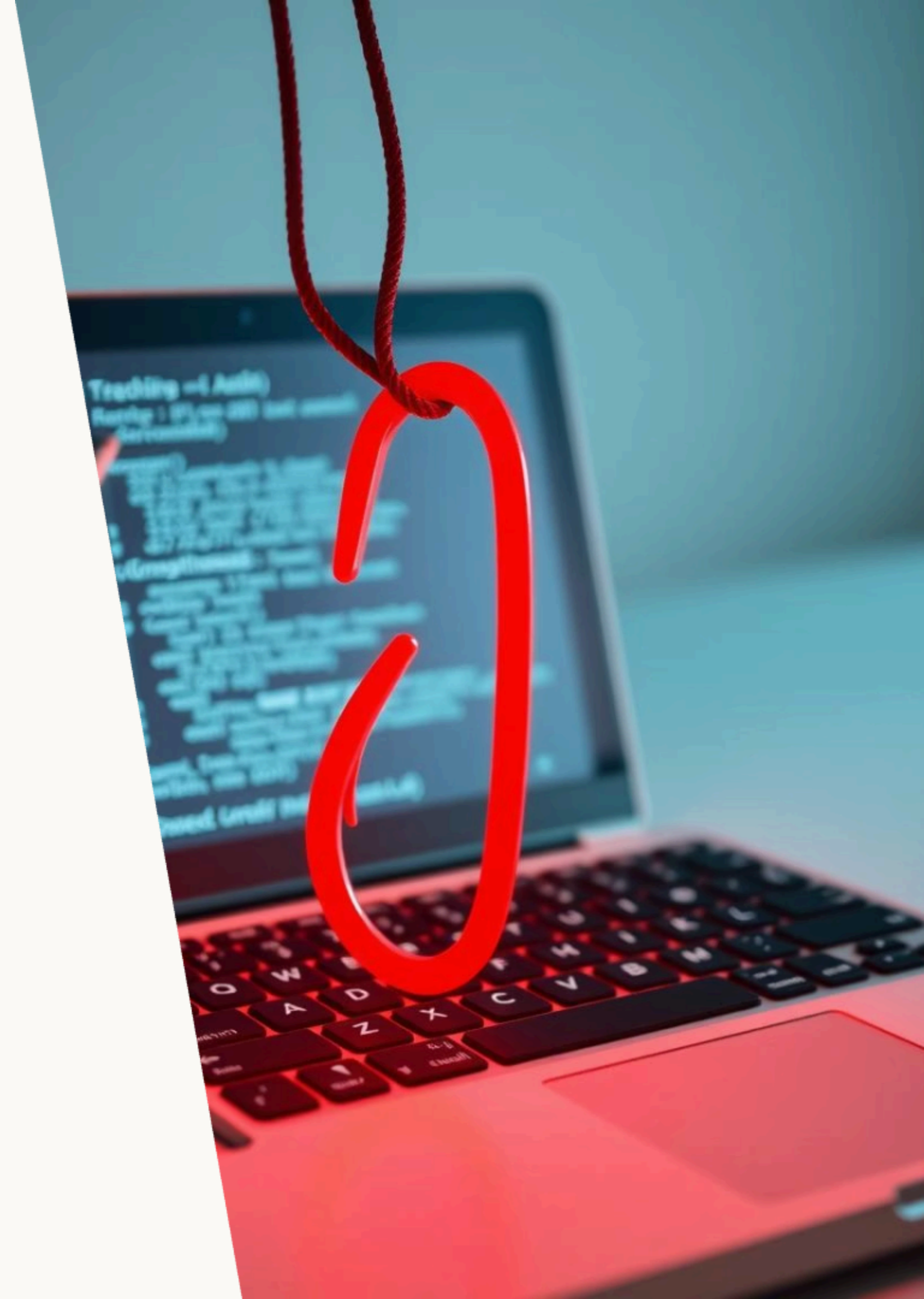
presentation about phishing attacks

Presented By

MATURI JASWANTH SAI MADHU MOHAN

Phishing Exposed: Defending Against Cyber Deception

Phishing threatens individuals and organizations by exploiting trust. It tricks victims into revealing sensitive data and credentials.



What is Phishing?

Understanding the Threat Landscape

Deceptive Emails

Fake messages pretending to be trustworthy sources.

Fraudulent Websites

Look-alike sites designed to steal login credentials.





Social Engineering

Manipulating emotions to gain confidential information.





Spotting the Bait: Identifying Phishing Emails

-  **Check Sender Details**
Look for misspelled or strange email addresses.
-  **Beware of Urgency**
Phishers create pressure to act quickly and fearfully.
-  **Hover Over Links**
Reveal URLs before clicking to detect suspicious sites.
-  **Avoid Unexpected Attachments**
Attachments can contain malware or ransomware.


Fake or Real? Recognizing Deceptive Websites

Legitimate Website

- Secure HTTPS connection
- Correct domain spelling
- Professional design and branding
- Privacy policy easily found

Fake Website

- Suspicious or missing HTTPS
- Misspelled or unusual URLs
- Low-quality imagery or layout
- Absence of contact information



Social Engineering: The Art of Manipulation

1

Building Trust

Attackers act friendly or authoritative to gain confidence.

2

Creating Urgency

Pressuring victims to respond quickly without thinking.

3

Exploiting Emotions

Using fear, curiosity, or sympathy to manipulate actions.

Real-World Examples: Phishing Attacks in Action

CEO Fraud

Scammers impersonate executives to request wire transfers.

Credential Harvesting

Email links lead to fake sites stealing passwords.

Spear Phishing

Personalized attacks targeting specific individuals or roles.

Defense Strategies: Protecting Yourself and Your Data



Use Multi-Factor Authentication



Verify Links and Senders



Install Anti-Phishing Software



Educate and Train Regularly





Stay Vigilant: Resources and Best Practices

Stay Updated

Follow cybersecurity news and alerts.

Report Suspicious Activity

Notify IT or use phishing reporting tools.

Regular Password Changes

Use strong, unique passwords and change periodically.

Participate in Security Training

Engage in ongoing phishing awareness programs.