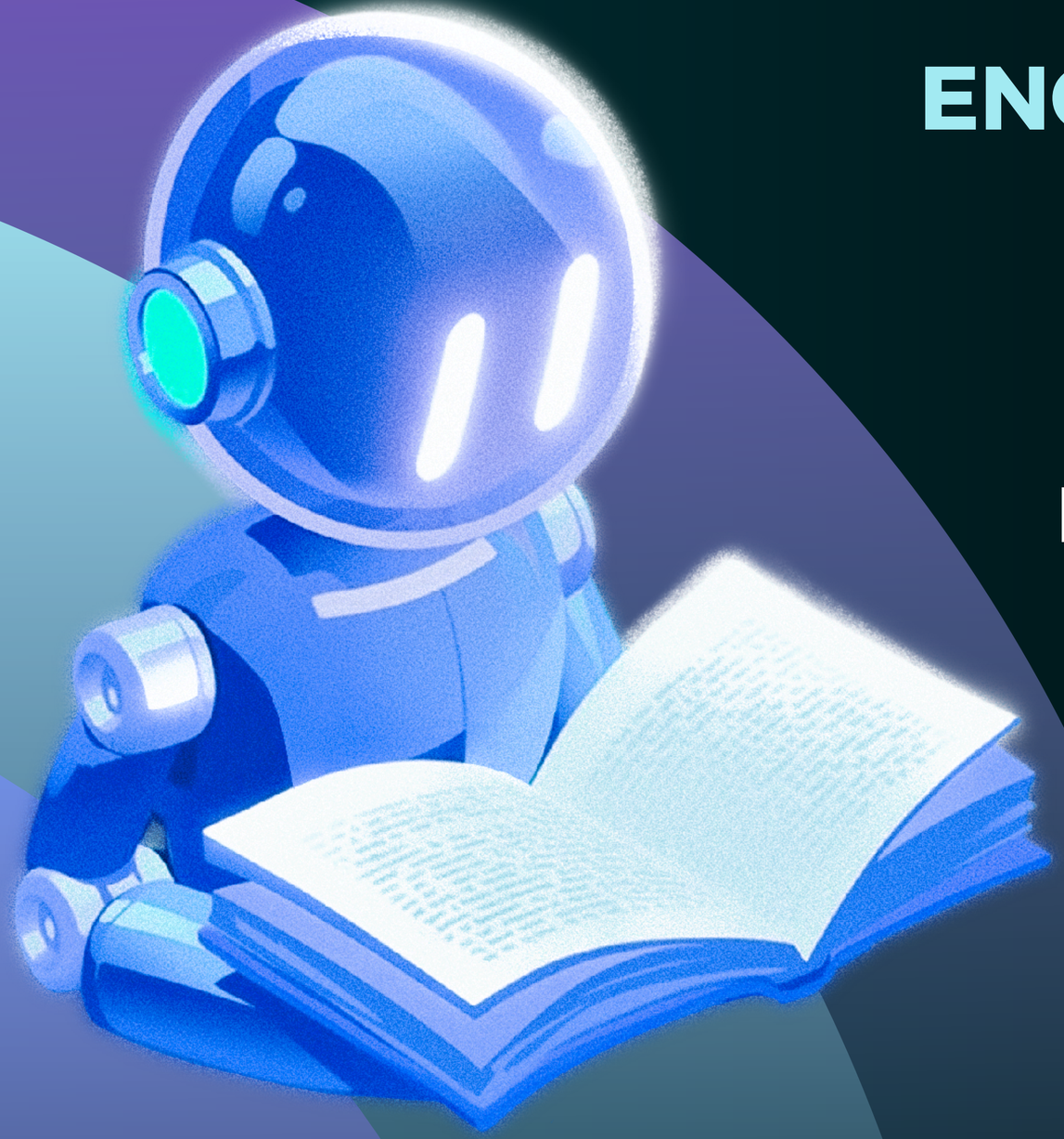


PHISHING & SOCIAL ENGINEERING AWARENESS TRAINING

SECURING THE HUMAN ELEMENT IN CYBERSECURITY

Presented by: G.Lavanya
CodeAlpha Internship

WHAT IS PHISHING?

- Phishing is a cyber attack where attackers impersonate trusted sources.
- It is used to steal passwords, banking details, and personal data.
- Over 90% of cyber attacks begin with phishing.

MALWARE

Harmful software such as viruses, ransomware, and spyware.

PHISHING

Fraudulent attempts to obtain sensitive information.

DATA BREACHES

Unauthorized access to confidential data.

DENIAL OF SERVICE (DOS)

Attacks that overwhelm systems, making them unavailable.

HOW A PHISHING ATTACK WORKS ?

1. ATTACKER SENDS A FAKE EMAIL/MESSAGE
2. VICTIM CLICKS A MALICIOUS LINK OR ATTACHMENT
3. SENSITIVE DATA IS CAPTURED
4. ACCOUNT OR SYSTEM GETS COMPROMISED

ANATOMY OF A PHISHING EMAIL

HOW TO IDENTIFY PHISHING EMAILS?

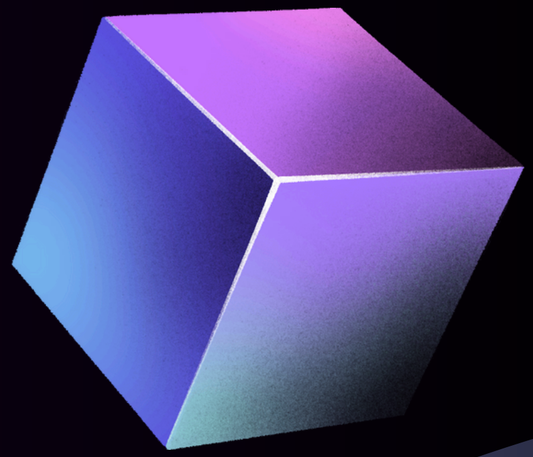
- MISMATCHED OR SUSPICIOUS SENDER ADDRESS
- GENERIC GREETINGS LIKE “DEAR CUSTOMER”
- URGENT LANGUAGE DEMANDING IMMEDIATE ACTION
- UNEXPECTED LINKS OR ATTACHMENTS

IDENTIFYING FAKE WEBSITES

SPOTTING FAKE WEBSITES

- Check for spelling mistakes in the URL
- HTTPS does not guarantee legitimacy
- Poor design or broken links
- Fake login pages that mimic real brands

SOCIAL ENGINEERING TECHNIQUES



- PRETEXTING: FAKE SCENARIOS (IT SUPPORT, HR CALLS)
- BAITING: MALWARE-INFECTED USB DRIVES OR FREE DOWNLOADS
- QUID PRO QUO: REWARDS IN EXCHANGE FOR INFORMATION

REAL-WORLD PHISHING SCENARIO

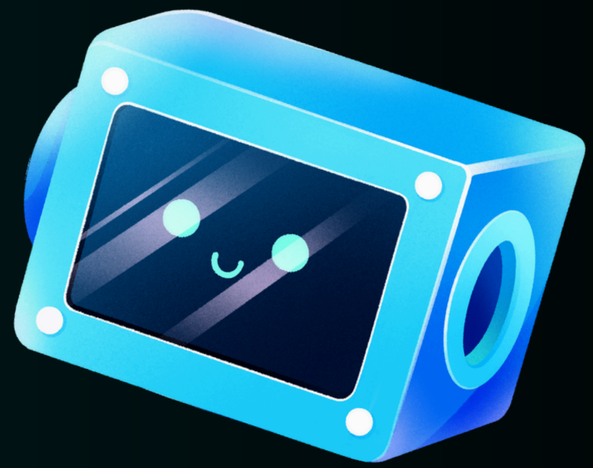
- Employee receives an “Urgent Invoice” email
- Attachment contains malware or ransomware
- Opening it compromises the system

BEST PRACTICES TO PREVENT PHISHING

HOW TO STAY SAFE

- Think before clicking on links
- Enable Multi-Factor Authentication (MFA)
- Verify requests using official contact methods
- Use password managers and updated security tools

WHAT IF YOU CLICKED A PHISHING LINK?



Incident Response Steps

1. Disconnect from the internet immediately
2. Change passwords from another device
3. Inform IT/Security team
4. Scan the system for malware

QUICK QUIZ

Question:

You receive a text saying:
"Your Amazon package is stuck.
Pay ₹2 to release it."

Options:

A) Pay the fee
B) Click the link
C) **Delete and check the official Amazon app** ✅

CONCLUSION

Content:

- Phishing targets human trust
- Awareness is the strongest defense
- You are the Human Firewall

Final Tip:

When in doubt — report it.

THANK YOU