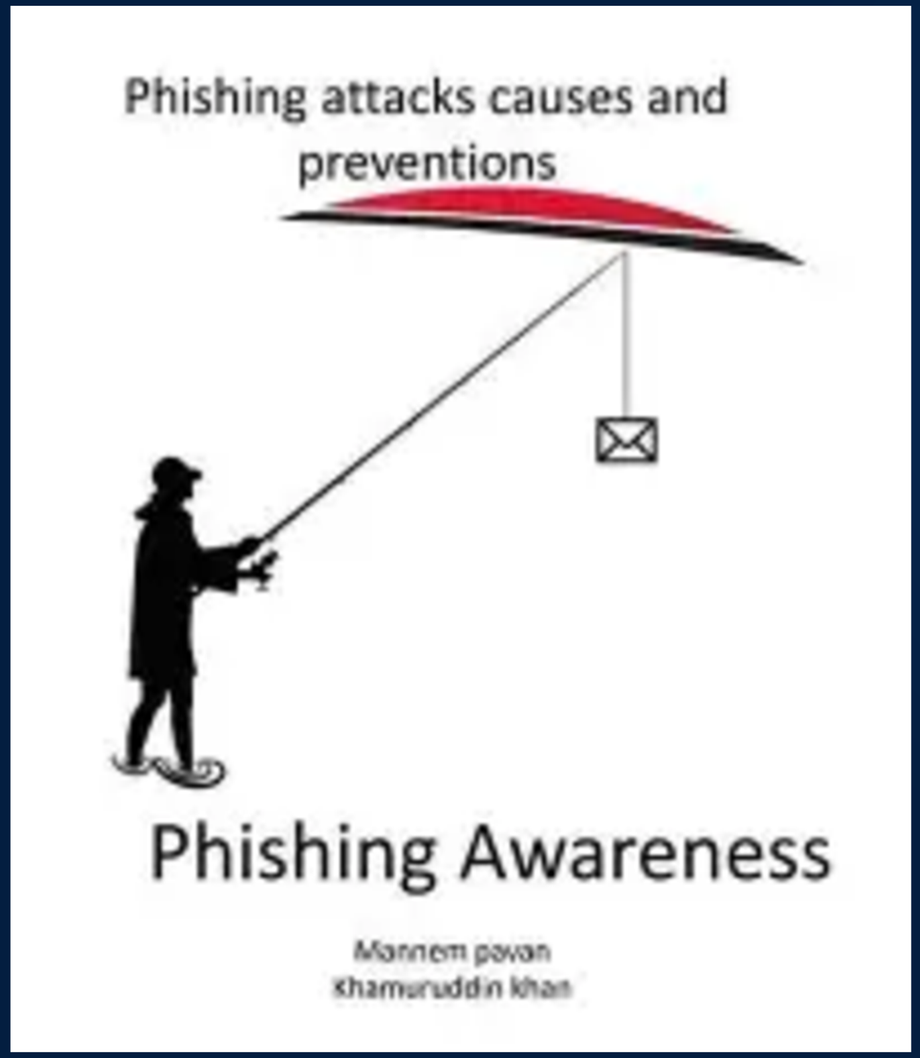
PHISHING
AWARENESS

Presented by: Omar Ahmed



What is Phishing?

🎣 Definition: Phishing is a cyber attack where attackers trick individuals into revealing sensitive information.

📧 Often comes in the form of fake emails, websites, or messages.

🎯 Goal: Steal credentials, data, or install malware.

Common Phishing Techniques

- Email Spoofing: Looks like it’s from a trusted source.
- Fake Websites: Clone of real websites to steal login info.
- Urgency and Fear: “Your account will be suspended!”
- Social Engineering: Pretending to be HR, IT, or a bank.

Spot a Phishing Email

🔍 Check the sender’s email (e.g., support@amaz0n.com)

🚨 Look for spelling/grammar mistakes

🔗 Hover over links – do they go to real domains?

📎 Beware of unexpected attachments

🧠 Ask: Was I expecting this email?

Examples of Phishing Emails

To: Your email

Subject: Apple Facetime Information Disclosure

National Security Department

A vulnerability has been identified in the Apple Facetime mobile applications that allow an attacker to record calls and videos from your mobile device without your knowledge.

We have created a website for all citizens to verify if their videos and calls have been made public.

To perform the verification, please use the following link:

Facetime Verification

This website will be available for 72 hours.

National Security Department

Fake Website Example

Social Engineering Tactics

🤝 Impersonation: CEO fraud, IT support scam

📞 Vishing: Phone calls pretending to be banks or IT

💬 Smishing: Fake SMS messages with malicious links

🧠 Psychological Pressure: “Act now or lose access!”

Best Practices to Stay Safe

✅ Don’t click links or download files from unknown sources

✅ Always verify with the sender via another channel

✅ Use 2FA (Two-Factor Authentication)

✅ Keep software and antivirus updated

✅ Report suspicious emails to your IT/security team

What to Do if You Suspect Phishing

🛑 Stop and think

📤 Do NOT respond, click links, or open attachments

🧹 Delete the message after reporting

Real-World Examples

2020: Twitter employees tricked via phone (vishing) → Hackers gained admin access

2016: John Podesta email → Led to DNC data breach

Emphasize how simple mistakes can lead to huge consequences.

Phishing Drill: Train Before the Threat Hits

✅ Goal: Build a culture of alertness, not fear.

🟦 Simulated Phishing Tests
Regularly send fake phishing emails to employees.
Identify who clicks or responds – no blame, only learning.
Provide instant feedback and training if someone falls for it.

🎓 Interactive Learning
Use short e-learning modules (2–5 min).
Include realistic examples and clickable simulations.

🏆 Gamify Security
Reward teams with the highest awareness.
Leaderboards, certificates, or small incentives.

Final Tips

📌 Stay alert – phishing constantly evolves

💬 When in doubt, ask your IT team

🧠 Think before you click

🔐 Cybersecurity is everyone’s responsibility

THANK YOU