Phishing Awareness Training

Security Insights for Teams

What is Phishing

Social Engineering to steal credentials

- Phishing leverages manipulation tactics to trick individuals into revealing usernames, passwords, and other confidential data.

Often appears legitimate

- Messages often impersonate trusted entities like IT departments, banks, or company executives to gain user trust.

Common in emails, SMS and even phone calls

- Attackers use various channels - emails, text, and voice-to distribute phishing content and . maximum success

Phishing Red Flags

15

MINS

How to Respond

- **Tips:**

- Don’t click unknown links
- Report to IT/SOC
- Check sender carefully
- Use official login portals only

Insight From Our Phishing Awareness Drill

- **25% Clicked Suspicious Link:** A quarter of participants interacted with a phishing simulation mail, highlighting real vulnerabilities.
- **15% Reported the Threat:** Only a small fraction useed proper reporting channels to alert IT/SOC, indicating a need for reinforcement.
- **60% Ignored the Message:** Majority took no action–neither engaging nor reporting–underscoring awareness gaps.
- **Next Steps: Continuous Training:** Plan for quarterly phishing simulations and microlearning to boost resilience.

Any questions? Ask away!

Give your audience space to resolve immediate questions or concerns.