# Social Engineering Awareness for Staff

Defending the Human Element of Cybersecurity

Presented by: Shah Durrani

Equipping IT professionals with the knowledge to recognize and combat social engineering attacks.

# Understanding Social Engineering

### Definition

Exploiting human behavior for unauthorized access.

### IT as a Target

High-value targets due to admin rights and privileged access.

### Attack Vector

Social engineering is an entry point for initial access.


# Common Attack Vectors

## Phishing

Credential harvesting, malware delivery.

## Vishing (Voice Phising)

Impersonating vendors or leadership.

## Pretexting

Fake support calls, supplier impersonation.

## Insider Manipulation

Shoulder surfing, tailgating.

# Advanced Techniques

### Spear-Phishing & BEC

### Social Media Reconnaissance

LinkedIn stalking for information gathering.

### MFA Fatigue Attacks

### AI-Generated Lures

Use of AI for realistic and convincing lures.

# Case Studies

1

### Breach Breakdown

Technical overview of known breaches.

2

### Manipulation Tactics

How attackers manipulated IT workflows/tools.

3

### Preventive Measures

What went wrong and how to prevent it.

# Detection & Response

### Monitor Logins

Abnormal login patterns, MFA behavior.

### Analyze Emails

Headers and attachments analysis.

### Sandbox Testing

Test suspicious files in safe environments.

# Hardening IT Operations

### Least Privilege

Enforce least privilege principles.

### Role-Based Access

Implement RBAC.

### Update Helpdesk

Enhance identity verification steps.

### Device Lockdown

Secure unattended devices.

# Escalation Procedures

### Escalate Attempts

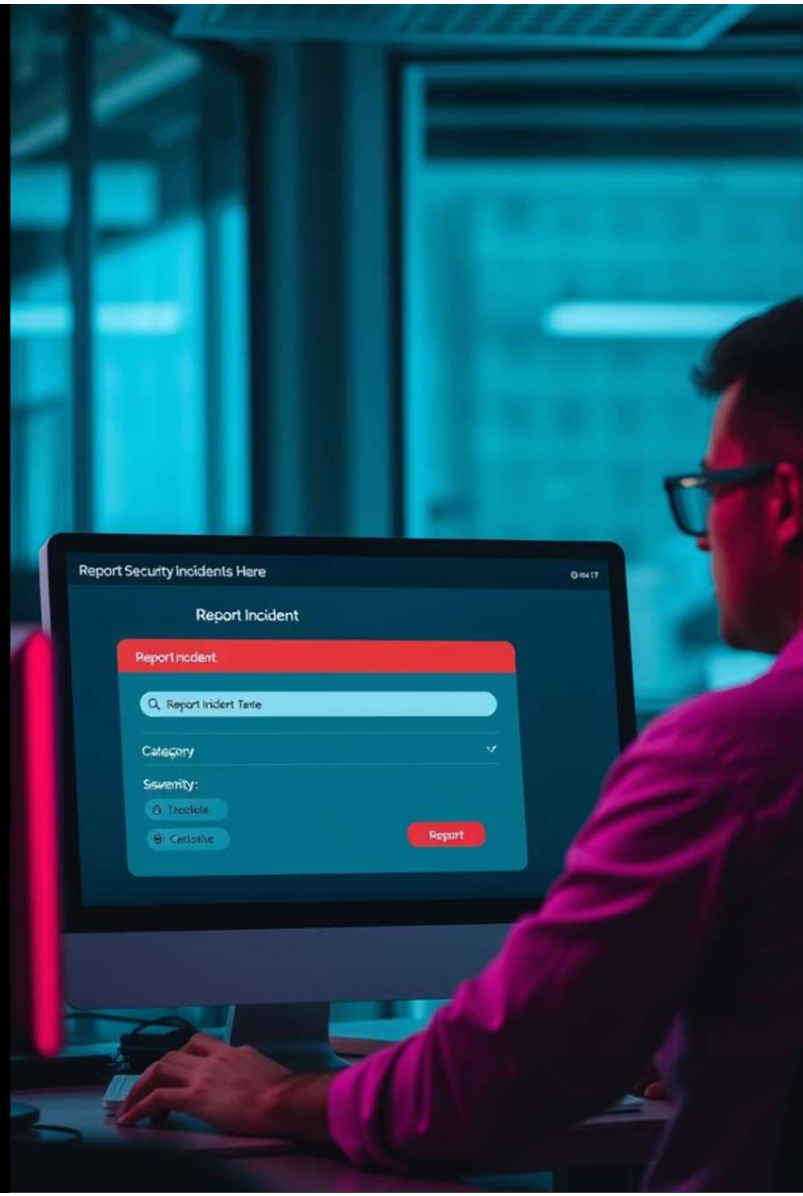
Report suspected social engineering.

### Reporting Tools

Use phishing report buttons.

### Regular Drills

Conduct tabletop exercises.



# Final Reminders & Q&A

### Human Firewall

Humans are the first line of defense.

### Critical Thinking

Think critically and verify information.

### Stay Informed

Stay alert and up-to-date.