Incident Response Playbook – Phishing Scenario (Checklist)

Phase	Task	Evidence Examples	Owner	Status
Preparation	Conduct phishing awareness training & simulations	Training logs, LMS records	Compliance	Not Started
Detection	Identify/report suspicious email or alert in SIEM	Sentinel alert screenshots, reported email headers	Security Analyst	Not Started
Containment	Isolate compromised accounts, block malicious senders	Entra ID logs, Defender quarantine reports	IT Security	Not Started
Eradication	Remove malicious messages, reset user credentials	Quarantine reports, password reset logs	IT Security	Not Started
Recovery	Restore mailbox, monitor systems for reinfection	Recovery logs, monitoring dashboards	Security Ops	Not Started
Lessons Learned	Conduct post-incident review & tabletop exercise	IR report, meeting notes, action items	Compliance / CISO	Not Started