Holy Phish!

Phishing Attack Response Plan

The Facts Were These: An employee (we’ll call him Timmy, because that’s his name) receives a phishing email that mimics the company’s IT department asking him to reset his password. Timmy clicks the link and enters his credentials.

Below is a breakdown of each phase of the plan and a rough estimate of the timeline starting from the detection of the threat to the recovery stage.

Immediate Actions (0-30 minutes)

Detection

User reports suspicious email or IT detects phishing indicators.
Security team validates the threat.
Determine if credentials were compromised.

Initial Response

Don’t forward or screenshot the phishing email.
Isolate the affected user's account immediately.
Reset compromised credentials.
Revoke active sessions for the affected user.

Containment (30 minutes - 2 hours)

Email Security

Search for and quarantine similar emails across all mailboxes.
Block sender domains/IPs at email gateway.
Update email security rules to prevent similar attacks.

Protect Credentials

Force password reset for compromised accounts.
Enable MFA if not already active.
Review and revoke any suspicious OAuth applications.
Check for any unauthorized access or data exfiltration.

Investigation (2-24 hours)

Log Analysis

Review email logs for delivery and interaction data.
Analyze authentication logs for suspicious logins.
Check file access logs for unauthorized data access.
Review VPN and network access logs.

Scope Assessment

Identify all users who received the phishing email.
Determine which users clicked links or entered credentials.
Assess potential data exposure or system compromise.

Recovery (24-72 hours)

System Restoration

Restore user access with new credentials.
Verify system integrity and remove any malware.
Update security awareness training materials.
Implement additional email security controls.

Communication

Notify affected users about the incident.
Provide guidance on recognizing phishing attempts.
Report to relevant authorities if required.
Update senior management on incident status.

Post-Incident

Conduct user security awareness training.
Review and update email security policies.
Implement additional technical controls (DMARC, SPF, DKIM).
Schedule follow-up security assessments.