Phishing Attack Response Documentation Sample

1. Incident Overview

Report Date	YYYY-MM-DD
Detection Source	[e.g. Employee Report, Email Filter]
Reported By	[Name / Department]
Assignee	[Name / Team]

2. Description of the Incident

Summary:
Brief overview of the phishing attack.

Phishing Method:
[Email / SMS / Other]

Phishing Content:
Short description or sample of the phishing message.

3. Initial Actions Taken

- Incident reported to IT/security team.
- Identified potentially affected users.
- Preserved original phishing email/message.
- Email/Account quarantine procedures initiated.

4. Impact Assessment

- Number of recipients: [Number]
- Number of users who clicked: [Number]
- Number of credential submissions: [Number]
- Sensitive data at risk: [Description]

5. Containment & Mitigation Steps

- Blocked malicious email sources/domains.
- Reset passwords for affected users.
- Removed phishing emails from inboxes.
- Monitored accounts for suspicious activity.
- Refreshed spam and phishing filters.

6. Communication

- Notification sent to affected users.
- Internal communications to management/staff.
- External communication (if required): [Describe]

7. Lessons Learned & Recommendations

- User awareness/training suggestions.
- Security control enhancements.
- Policy/procedure updates recommended.

8. Appendix

- Sample phishing email (redacted as necessary).
- Indicators of compromise (IOCs).
- Incident ticket references.