# Phishing Incident Response – NIST 800-61 Scenario

## Overview
This scenario outlines the response to a phishing attack that results in a user entering credentials into a spoofed login page. The attacker gains unauthorized access to the organization's email environment and attempts further internal compromise.

# 1. Preparation
- Ensure MFA is enforced for all accounts.
- Maintain updated email security filtering rules.
- Train employees on identifying phishing emails.
- Confirm logging for:
  - Email security gateway
  - Authentication logs (AD/Azure AD)
  - Endpoint protection/EDR
- Validate IR communication channels (Slack/Teams war-room, phone tree).
- IR toolkit available: email header analyzer, Sysinternals, Wireshark, URL scanners, sandbox.

# 2. Detection & Analysis

## Initial Indicators
The incident may be reported or detected through:
- User reports receiving suspicious email.
- Email security tool flags malicious URL attachment.
- SIEM alert for unusual login location.
- MFA push notifications user did not request.

## Evidence Collection
- Copy original phishing email.
- Extract email headers.
- Retrieve malicious URL, domain, and hosting IP.
- Review authentication logs for:
  - Impossible travel
  - Multiple failed logins
  - Login from new geographic region
- Check mailbox rules for signs of compromise.

## IOC Examples
Indicator Type	Value

URL	http://secure-login-authenticate[.]com
IP Address	185.244.36.12
File Hash (If Attachment)	SHA256: (example placeholder)
User Behavior	Login from Russia, 3:14 AM

## Triage Severity
Medium → High depending on:
- Successful login by attacker
- Mailbox manipulation
- Lateral movement attempts

# 3. Containment

## Short-Term Containment
- Disable the compromised user account.
- Revoke all active sessions.
- Block malicious URL/domain at firewall and web filter.
- Inform user not to interact with the email further.

## Long-Term Containment
- Reset user’s password and enforce MFA re-registration.
- Remove malicious inbox rules (forwarding/auto-delete).
- Patch any exploited vulnerabilities (browser/email client).

# 4. Eradication
- Delete phishing email from all inboxes using admin tools.
- Remove any malicious files downloaded by the user.
- Run endpoint malware scan.
- Ensure no persistence mechanisms exist (scheduled tasks, startup items).
- Remove unauthorized OAuth tokens from user account.

# 5. Recovery
- Re-enable user account after securing it.
- Confirm authentication logs show normal behavior.
- Monitor mailbox for 48–72 hours.
- Reinforce email security filtering if needed.
- Notify IT/security leadership of final status.

# 6. Lessons Learned
- Identify why the phishing email bypassed filters.
- Update rules for URL and attachment scanning.
- Provide additional user training if needed.
- Document the updated IR process.
- Add new IOCs to blocklists and SIEM rules.

# MITRE ATT&CK Mapping

Technique	ID	Description
Phishing	T1566	User deception via email
Valid Accounts	T1078	Attacker uses stolen credentials
Command & Control	T1071	Browser-based communication
Credential Harvesting	T1056	Fake login page

# Final Reporting Checklist
- Summary of event timeline
- All collected IOCs
- Impact assessment
- Containment actions taken
- Recovery verification
- Recommendations for prevention