# **Incident Response Playbook: Phishing Email**

**Use Case:** A user receives a phishing email containing a malicious link or attachment designed to steal credentials or install malware.

## **1. Detect and Analyze**

**Objective:** Identify and confirm the phishing attempt.

**Actions:**

* User reports suspicious email to the IT or Security Operations Center (SOC).
* Analyze email headers for anomalies (e.g., mismatched From and Reply-To, failed SPF/DKIM/DMARC checks).
* Inspect embedded URLs and attachments using sandbox analysis or services like VirusTotal.
* Check browser history and file system for evidence of user interaction (e.g., link clicked, file downloaded).
* Examine system logs for suspicious activities, such as PowerShell execution or macro-enabled document execution.
* Capture and analyze a memory dump using tools like Volatility to identify malicious processes, scripts, or injected code.
* Document all indicators of compromise (IoCs), including:  
  + Malicious domains and IP addresses
  + Hashes of dropped files
  + Suspicious registry keys
  + Command-line arguments used by malicious processes

## **2. Contain**

**Objective:** Prevent the attack from spreading or escalating within the environment.

**Actions:**

* Immediately isolate the affected endpoint from the network.
* Temporarily disable the user’s account to prevent potential misuse.
* Block known malicious domains and IP addresses at the firewall, proxy, or DNS level.
* Use email gateway tools to search for and remove the phishing message from other users’ mailboxes.
* Notify IT security and relevant stakeholders of containment actions and impact.

## **3. Eradicate**

**Objective:** Remove the threat and all associated artifacts from the affected system(s).

**Actions:**

* Delete all files associated with the phishing payload (e.g., downloaded malware, scripts).
* Remove persistence mechanisms such as registry Run keys, scheduled tasks, or startup scripts.
* Run a comprehensive antivirus/malware scan using up-to-date definitions.
* Use forensic tools (e.g., Volatility, Autopsy) to validate system state and confirm full removal of malicious components.

## **4. Recover**

**Objective:** Restore normal system operations in a secure manner.

**Actions:**

* Restore the system from a known good backup or reimage the affected machine.
* Reset the user’s passwords for local accounts, email, and any other potentially exposed services.
* Reconnect the system to the network only after confirming it is fully remediated.
* Monitor endpoint and network activity for signs of reinfection or continued suspicious behavior.
* Notify the user and provide guidance to avoid similar threats in the future.

## **5. Post-Incident Activity**

**Objective:** Document the incident thoroughly and improve defenses based on lessons learned.

**Actions:**

* Conduct a post-incident review with the incident response team and affected parties.
* Update the incident response playbook to reflect lessons learned and any process improvements.
* Produce and submit a comprehensive incident response report including:  
  + Incident summary
  + Timeline of events
  + Root cause analysis
  + Remediation steps taken
  + IoCs identified
* Implement improved email security controls (e.g., enhanced filtering, sandboxing).
* Conduct security awareness training for employees focusing on phishing identification and reporting procedures.

**NIST Incident Response Framework Evaluation Report**

## **1. Preparation Assessment**

The current playbook requires significant enhancements to meet NIST's preparation standards, based on NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide. While it identifies basic response roles and tools, it lacks a comprehensive asset inventory that classifies systems by criticality and sensitivity, that is why it delegates the responsibility to other frameworks and practices. According to NIST guidelines, the playbook should document all networks, servers, and endpoints with their relative importance to prioritize response efforts. The playbook would benefit from establishing monitoring baselines for normal email traffic patterns and user behavior, which are currently absent. Additionally, it needs to define specific security event thresholds that trigger investigations, along with more detailed response procedures for various phishing scenarios. These preparation elements are essential for effective incident response but are not adequately addressed in the current version.

**2. Detection and Analysis Evaluation**

The playbook's detection approach partially aligns with NIST requirements by including multiple data sources such as email headers and user reports. However, it could be strengthened by incorporating additional detection methods from security tools and external threat intelligence as recommended by NIST. The analysis procedures effectively examine email artifacts but would benefit from more robust baseline comparisons to identify deviations from normal activity. While the playbook documents indicators of compromise well, it could improve by including precursor identification to detect potential attacks before they occur. The correlation of related events across systems needs enhancement to better understand the full scope of incidents as prescribed by NIST guidelines.

## **3. Containment, Eradication and Recovery Review**

The containment strategies in the playbook follow NIST principles by aiming to stop attacks quickly, but they lack the tiered approach recommended by the framework. NIST emphasizes that containment should consider damage potential and service availability needs, suggesting temporary solutions for critical systems and permanent fixes for less essential ones. The playbook would benefit from including specific procedures to identify attacking hosts and validate IP addresses, which are crucial NIST requirements. While eradication steps effectively remove malware, they could be enhanced with more comprehensive host identification procedures. Recovery procedures align well with NIST's emphasis on restoring operations securely, though they could better document measures to prevent repeat attacks on the same assets.

## **4. Post-Incident Activity Assessment**

The playbook's post-incident process includes basic documentation but needs expansion to fully meet NIST standards. NIST requires thorough reviews answering specific questions about what happened, response effectiveness, and needed improvements. The current version would benefit from adding structured questions about timing, process adherence, information gaps, and any response mistakes. It should include more detailed analysis of whether staff could have responded differently or shared information better. The playbook currently lacks the comprehensive approach to identifying new precursors and indicators that NIST recommends. Additionally, it needs clearer procedures for implementing lessons learned, including specific tools or resources required to prevent future incidents and how findings feed back into preparation activities.