Sample Phishing Playbook

<Company Inc>

TLP: Green / Clear

Document Control

Title:	Phishing Incident Response Playbook
Use Case:	Phishing
Revision:	v1.0
Date Revised:	March 14th, 2025
Owner:	<Owner>
Document Author:	*Thatguywiththeshirt*
Traffic Light Protocol:	Green / Clear
Additional Notes:	The author discloses the use of LLMs in the outline and drafting of this document.

Document Control History

Version	Date	Author	Summary of Changes
v1.0	03/14/25	*Thatguywiththeshirt*	Initial Release

1 Introduction & Purpose

1.1 Playbook Objectives & Scope

The primary objective of this playbook is to establish a comprehensive and actionable framework for the organization to effectively manage the persistent and evolving threat of phishing attacks. Its goals are multifaceted, aiming to minimize the potential impact of successful phishing attempts on the organization's operations, ensure a swift and efficient recovery process when incidents occur, and ultimately strengthen the overall cybersecurity posture against these prevalent social engineering tactics. This playbook is designed to serve as a central guide for all personnel involved in detecting, responding to, and preventing phishing incidents.

The scope of this playbook encompasses a wide spectrum of phishing attack types that the organization may encounter. This includes:

- Email phishing
- Spear phishing
- Whaling
- Vishing
- Smishing

This playbook applies to all company assets, including employee workstations, servers, mobile devices, cloud-based services, and the entire network infrastructure. It is designed to be consistent with industry-recognized standards and best practices for incident response, particularly aligning with the framework provided by the National Institute of Standards and Technology (NIST) SP 800-61, Revision 2 and Revision 3. The NIST framework emphasizes a continuous cycle of preparation, detection and analysis, containment, eradication, recovery, and post-incident activities. This approach ensures that the organization responds effectively to incidents and also learns from them to improve its defenses proactively.

Incident response playbooks, including this one, aim to provide clear and actionable steps for personnel to follow during various cybersecurity incident scenarios. These steps facilitate a consistent and effective response to commonly anticipated threats.

It is essential to recognize that this playbook is a living guide that will be periodically reviewed and updated to adapt to the evolving threat landscape and the organization's specific needs.

B. Intended Audience & Stakeholders

The primary audience for this playbook includes all individuals within the organization who play a role in managing and responding to phishing incidents. This encompasses Security Operations Center (SOC) analysts, who are often the first line of defense and triage. It also includes members of the Incident Response Team (IRT), who are responsible for in-depth

analysis, containment, eradication, and recovery activities. IT administrators, for implementing technical controls and assisting with system recovery. Specific sections of this playbook may be relevant to end-users, particularly those focusing on recognizing and reporting phishing attempts.

Beyond the primary responders, several key stakeholders will rely on this playbook to understand the organization's approach to managing phishing threats and their potential impact. Senior management will need to be informed of the playbook's objectives, scope, and the overall incident response process. The legal department will be involved in understanding legal and regulatory implications and reporting requirements. Human resources may need to be engaged in cases involving employee-related aspects of phishing incidents. The public relations team will be responsible for managing external communications in the event of a significant incident. Business unit leaders will need to understand how the playbook ensures the continuity of their operations in the face of phishing threats.

The roles and responsibilities within the Computer Security Incident Response Team (CSIRT) structure are the intended audience and ensure that each member understands their specific duties during a phishing incident. In certain situations, external stakeholders such as law enforcement agencies, forensic experts, and regulatory bodies may also need to be considered as part of the audience for specific communication and reporting protocols. By clearly outlining the roles and responsibilities for all involved parties, this playbook aims to generate a culture of cybersecurity within the organization, ensuring that all key stakeholders are aware of their contribution to a robust defense against phishing attacks.

C. Defining Phishing & Its Impact

Phishing is defined as a technique employed by malicious actors to acquire sensitive data, such as usernames, passwords, financial details, and other confidential information, by masquerading as a trustworthy entity in electronic communications. This social engineering tactic relies on manipulating human psychology to trick individuals into divulging information or taking actions that compromise their security or the security of the organization.

Phishing attacks can take various forms, each with its own characteristics and delivery methods.

- **Email phishing** involves sending fraudulent emails that appear to be from legitimate organizations or individuals.
- **Spear phishing** is a more targeted form of phishing that focuses on specific individuals or groups, often using personalized information to increase the likelihood of success.
- **Whaling** is a type of spear phishing that specifically targets high-ranking members of organizations, such as executives.
- **Vishing**, or voice phishing, uses phone calls or voice messages to deceive victims into revealing sensitive information.
- **Smishing** utilizes SMS or text messages to lure individuals into clicking malicious links or providing personal data.

The impact of successful phishing attacks on the organization can be substantial and far-reaching. Financial losses are a significant concern, arising from fraudulent transactions conducted using compromised credentials or from the payment of ransoms in the case of ransomware infections initiated through phishing. Data breaches are another serious consequence, where sensitive customer data, proprietary information, or employee records may be compromised, leading to regulatory fines, legal liabilities, and reputational damage. The organization's reputation and customer trust can suffer significantly following a successful phishing attack, potentially leading to long-term business impacts. Operational disruptions and downtime can occur if critical systems are compromised or infected with malware as a result of phishing.

Organizations may face legal and regulatory penalties depending on the type of data compromised and the applicable laws and regulations. It is crucial to understand that phishing often serves as an initial entry point for a multitude of other cyber threats, including the deployment of various forms of malware and ransomware. Therefore, a robust defense against phishing is a fundamental component of the organization's overall cybersecurity strategy.

II. Phishing Threat Landscape

A. Attack Types & Characteristics

1. Email Phishing

Email phishing, the most common form of phishing, is characterized by deceptive electronic messages designed to trick recipients into revealing sensitive information or performing harmful actions. These emails often exhibit several telltale signs. Suspicious sender email addresses, which may contain unusual domains or subtle misspellings of legitimate names, are a frequent indicator. Many phishing emails employ generic greetings, such as "Dear Customer," instead of addressing the recipient by name. Attackers often use urgent or threatening language to pressure recipients into acting quickly without thinking, claiming dire consequences if immediate action is not taken. Requests for sensitive personal or financial information, such as passwords, credit card details, or social security numbers, are a hallmark of phishing attempts. Spoofed or suspicious hyperlinks, where the visible text of a link differs from the actual URL it directs to or leads to an unexpected domain, are also common.

Unsolicited attachments or requests to download files should always be treated with suspicion. While historically, grammatical errors and typos were strong indicators, the increasing use of artificial intelligence by attackers has made these less reliable. Inconsistent formatting or layout within the email can also be a red flag.

Typical email phishing scenarios include emails that mimic login pages of popular services, attempting to steal credentials when users enter their information. Bogus invoices or payment notifications are used to trick recipients into clicking malicious links or downloading infected attachments. Urgent account verification requests, often threatening account suspension if no action is taken, are another common tactic.

Attackers may also impersonate colleagues or supervisors, making unexpected or unusual requests. It is important to note that the sophistication of these emails is constantly increasing, with attackers leveraging AI to create more convincing and harder-to-detect phishing attempts. Relying solely on traditional indicators like grammar may no longer be sufficient for detection. Security awareness training must adapt to these evolving tactics, emphasizing the need for critical evaluation of all email communications.

2. Spear Phishing & Whaling

Spear phishing represents a more refined and targeted approach to phishing, focusing on specific individuals or groups within an organization. Unlike broad email phishing campaigns, spear phishing attacks often incorporate personalized information about the target, such as their name, job title, colleagues, or recent activities, to enhance the credibility of the message and increase the likelihood of a successful compromise.

This personalization requires attackers to conduct reconnaissance on their targets, often utilizing publicly available information from social media and other online sources. Due to the tailored nature of these attacks, they are often more convincing and can bypass generic security controls more effectively.

Whaling is a specific type of spear phishing that takes this targeted approach even further by focusing exclusively on high-level executives within an organization. These attacks often impersonate other senior executives, business partners, or trusted entities to solicit sensitive information, authorize fraudulent financial transactions, or gain access to highly privileged accounts.

The potential for significant damage resulting from successful whaling attacks is substantial, given the access and authority held by the targeted individuals. Compromised executive accounts can lead to significant financial losses, theft of critical intellectual property, and severe reputational damage. The attackers invest significant time and effort in researching their victims and crafting convincing messages to deceive them. Organizations must recognize the elevated risk posed by spear phishing and whaling and implement specific security measures and training to protect against these sophisticated threats.

3. Vishing & Smishing

Vishing, a combination of "voice" and "phishing," refers to phishing attacks conducted through phone calls or voice messages. Attackers often impersonate representatives from legitimate organizations, such as banks, government agencies, or IT support teams, to trick victims into divulging sensitive information, such as passwords, bank account details, or personal identification numbers. These calls frequently create a sense of urgency or fear to pressure victims into making hasty decisions without verifying the caller's identity. The rise of AI generated deepfake audio has further complicated the detection of vishing attacks, as attackers can now mimic the voices of trusted individuals, making the impersonation even more convincing.

Smishing, a combination of "SMS" and "phishing," involves phishing attacks carried out via SMS or text messages. These messages often contain malicious links that, when clicked, can lead to phishing websites designed to steal credentials or install malware on the victim's

device. Smishing attacks may also instruct victims to call a fraudulent phone number where they are further encouraged to reveal sensitive information.

The challenge in both vishing and smishing lies in the difficulty of verifying the authenticity of the communication channel. Caller ID can be easily spoofed in vishing attacks, and SMS messages can originate from seemingly legitimate numbers or use deceptive sender IDs. Organizations need to educate employees to be highly cautious of unsolicited phone calls or text messages asking for sensitive information or urgent actions.

B. Common Delivery Methods

1. Email

Email remains a primary vector for delivering phishing attacks due to its widespread use and the ability to easily disguise malicious content. Malicious attachments are a common method, where attackers embed malware within various file types such as executable files, documents containing malicious macros, or seemingly harmless PDFs. When a user opens an infected attachment, the malware can be silently installed on their system, granting attackers unauthorized access or control.

Malicious links embedded within the body of the email are another prevalent technique. These links often redirect users to fraudulent websites that mimic legitimate login pages or other sensitive data entry forms, allowing attackers to steal credentials and personal information. In some cases, clicking a malicious link can directly trigger the download of malware onto the user's device.

Email spoofing is a technique used to manipulate the sender information displayed in an email, making it appear as though the message originated from a trusted source, such as a company executive or a known vendor. This can significantly increase the likelihood that a recipient will trust the email and comply with its requests.

2. Social Media & Messaging

The increasing popularity and integration of social media and instant messaging platforms in both personal and professional communication have made them attractive avenues for phishing attacks. Attackers leverage these platforms to send direct phishing messages to users, often impersonating friends, colleagues, or legitimate organizations. These messages may contain malicious links that redirect victims to phishing websites designed to steal login credentials or other sensitive information.

Phishing attempts through instant messaging apps like WhatsApp, Slack, and Teams are also becoming more common. Attackers may exploit the trust that users often place in communications received through these platforms, especially if the message appears to come from a known contact whose account may have already been compromised. The ease with which attackers can create fake profiles or compromise existing accounts on social media and messaging apps makes these platforms a significant delivery vector for phishing attacks. The convergence of personal and professional interactions on these platforms can lead to a lapse in vigilance, increasing the risk of users falling victim to these types of attacks.

3. SMS & Voice Calls

SMS (Short Message Service) or text messaging is another common delivery method for phishing attacks, referred to as smishing. These attacks often involve sending text messages that contain shortened URLs, enticing recipients to click on them with promises of prizes, refunds, or urgent notifications. Clicking on these links can lead to phishing websites or trigger the download of malware onto the user's mobile device.

Voice calls, or vishing, are also used to deliver phishing attacks. Attackers often use social engineering tactics over the phone to impersonate trusted entities and trick victims into revealing sensitive information or performing certain actions, such as transferring money or providing access to their accounts. Caller ID spoofing allows attackers to mask their real phone number and display a number that appears legitimate, further enhancing the credibility of the vishing attempt. The immediacy and perceived authority associated with voice communication can make vishing attacks particularly effective.

C. Identifying Phishing Indicators (Signs & Symptoms)

Identifying phishing attempts requires vigilance and awareness of various indicators that can signal malicious activity. These indicators can be broadly categorized into signs, which are observable characteristics of a potential phishing attempt, and symptoms, which are user-reported or system-detected anomalies that may result from a successful attack.

Signs of a suspicious message

Signs of a potential phishing attempt may include common tactics such as:

- A suspicious sender email address, which may use an unusual domain or contain misspellings of legitimate names.
- Generic greetings, such as "Dear Customer," instead of a personalized address
- Attackers often employ urgent or threatening language to pressure recipients into immediate action.
- Requests for sensitive personal or financial information, which is not solicited via email
- Spoofed or suspicious hyperlinks, where the displayed link text does not match the actual URL or redirects to an unexpected website.
- Unsolicited attachments or requests to download files
- Grammatical errors and typos.
- Inconsistent formatting or layout within the message can also raise suspicion.
- Unexpected or unusual requests from known contacts.
- In the context of smishing, suspicious phone numbers or sender IDs are red flags.
- Promises of prizes or rewards that appear too good to be true are often associated with phishing scams.

Symptoms

Symptoms that may indicate a successful phishing attack include:

- Unusual login attempts or other suspicious activity on user accounts or reports of unauthorized access to accounts.
- Unexpected password reset requests or account lockouts can also be a symptom of compromise.
- The unexplained installation of unauthorized software or malware.
- Data exfiltration or loss.
- In cases where ransomware is deployed via phishing.
- An increase in spam or phishing emails being sent from an employee's account could indicate that the account has been compromised and is being used as part of a larger campaign.
- Unusual network traffic or connections to suspicious IP addresses or domains may also be detected by security monitoring tools.
- Endpoint protection software on a user's system is found to be malfunctioning or has been disabled

A comprehensive security awareness training program should educate users on both these observable signs and potential symptoms to foster a multi-layered approach to phishing defense.

III. Detection & Triage

A. Monitoring Tools & Techniques

1. Anti-Phishing Software & Filters

Anti-phishing software and email security gateways play a crucial role in the initial detection and prevention of phishing attacks. These tools analyze incoming and outgoing email traffic, identifying patterns and characteristics associated with known phishing campaigns. They often utilize sophisticated algorithms, reputation scoring, and threat intelligence feeds to detect and block malicious emails before they reach the user's inbox. URL filtering and reputation services are integrated into many of these solutions, enabling them to identify and block access to websites known to host phishing pages or distribute malware. It is critical to ensure that these anti-phishing tools and filters are consistently updated with the latest threat intelligence, including newly identified malicious domains, URLs, and email patterns.

Properly configured email security gateways can also implement email authentication protocols like SPF, DKIM, and DMARC to verify the legitimacy of email senders and prevent email spoofing, a common tactic used in phishing attacks. Furthermore, endpoint detection and response (EDR) solutions deployed on user workstations can also contribute to phishing

detection by monitoring user behavior and system activity for suspicious actions that might indicate a successful phishing compromise.

2. DNS & URL Analysis

Analyzing Domain Name System (DNS) queries and the characteristics of Uniform Resource Locators (URLs) can provide valuable insights into potential phishing activity. When a user clicks on a link in a phishing email, their computer sends a DNS query to resolve the domain name to an IP address. Monitoring these DNS queries can reveal if users are attempting to access domains known to be associated with phishing or other malicious activities.

Anomalous patterns in DNS traffic, such as a sudden increase in queries to newly registered or obscure domains, can also be indicative of a potential compromise. Examining the structure and characteristics of URLs themselves can aid in detection.

Attackers often use techniques like typosquatting, where they register domain names that are very similar to legitimate ones with slight variations or misspellings, hoping that users will not notice the difference. Analyzing URLs for these subtle variations, as well as for suspicious path structures or the use of URL shortening services, can help identify potentially malicious links. Integrating threat intelligence feeds that contain lists of known malicious domains and URLs into DNS and web traffic analysis tools can further enhance the detection capabilities.

3. SIEM & Threat Intelligence

Security Information and Event Management (SIEM) systems are essential tools for detecting phishing attacks by aggregating and correlating log data from various security devices and systems across the organization's IT infrastructure.

SIEM systems can collect logs from firewalls, intrusion detection systems, antivirus software, email servers, web proxies, and endpoint devices, and then analyze this data to identify patterns of activity that may indicate a phishing attempt or a successful compromise. For example, a SIEM might detect a user clicking on a suspicious link in an email followed by unusual network traffic to an external IP address or the execution of an unknown process on their workstation. The integration of threat intelligence feeds into SIEM systems significantly enhances their ability to detect known phishing indicators. These feeds provide up-to-date information on malicious IP addresses, domains, URLs, and email addresses associated with phishing campaigns.

By correlating log data with this threat intelligence, the SIEM can generate alerts when users interact with known malicious infrastructure or receive emails from known phishing sources. Continuous monitoring and analysis of logs by the SIEM, coupled with timely threat intelligence updates, are crucial for early detection of phishing attacks and minimizing their potential impact.

4. User Reporting & Awareness

Despite the advancements in automated detection tools, user reporting remains a critical component of an effective phishing detection strategy. Many sophisticated phishing attacks are designed to bypass automated security controls by exploiting human psychology and trust.

Security awareness training plays a vital role in educating users on how to recognize the signs of a phishing email, message, or call. This training should cover various phishing tactics and provide users with practical guidance on what to look for, such as suspicious sender addresses, urgent requests, and unusual links or attachments.

Equally important is establishing clear and easy-to-use reporting mechanisms that empower users to quickly report any suspected phishing attempts to the security team. This could include a dedicated email address for reporting suspicious emails or a reporting button integrated into the email client.

Encouraging a culture where users feel comfortable reporting potential threats, even if they are unsure, is essential for early detection and preventing successful compromises. Tools like KnowBe4 and Cofense can be used to deliver phishing simulations and cybersecurity training, further enhancing user awareness and reporting habits.

B. Indicator of Compromise (IOC) Analysis

1. Email Header & Content Examination

When a potential phishing email is reported or flagged by security tools, the first step in analysis often involves a thorough examination of the email header and content. Email headers contain a wealth of information about the email's origin, path, and authentication status. Analyzing these headers can reveal discrepancies in the sender's information, such as inconsistencies between the "From" address and the actual sending server, or failures in email authentication protocols like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication Reporting and Conformance (DMARC). These failures can indicate that the email is spoofed and did not originate from the purported sender's domain.

Scrutinizing the email content is equally important. Analysts look for suspicious language, such as urgent or threatening tones, unusual requests, or grammatical errors; however, savvy threat actors can use AI to reduce the errors. Utilizing IoC information provided by security platforms can help check if the log files of defensive infrastructure contain communication with known malicious entities.

2. Attachment & Link Scrutiny

A crucial aspect of phishing incident analysis involves the detailed scrutiny of any attachments or links included in the suspicious communication. File attachments should undergo both static and dynamic analysis.

Static analysis involves examining the file's characteristics without executing it, looking for known malicious signatures, metadata, and other indicators.

Dynamic analysis, often performed in a sandboxing environment, involves executing the file in a controlled and isolated environment to observe its behavior and identify any malicious actions it may attempt to perform, such as installing malware, establishing network connections to suspicious hosts, or modifying system files.

Similarly, links found in phishing emails or messages need to be carefully examined. Analysts should verify the destination URL and check its reputation using online tools and services that aggregate information about known malicious websites. These tools often provide insights into whether a URL has been previously associated with phishing, malware distribution, or other malicious activities. It is also important to identify if a link redirects the user through multiple websites before reaching its final destination, as this can be a tactic used by attackers to obfuscate the true nature of the link. Inspecting the source code of webpages associated with suspicious URLs can sometimes reveal hidden scripts or malicious content that may not be immediately visible to the user.

3. Network Traffic & DNS Queries

Analyzing network traffic and DNS queries can provide valuable forensic evidence in phishing investigations. Monitoring network traffic for connections originating from potentially compromised systems to known malicious IP addresses or domains identified through threat intelligence feeds can help confirm a successful compromise. Unusual outbound traffic patterns, such as large amounts of data being transferred to unfamiliar locations, can also be indicative of data exfiltration following a phishing attack.

Examining DNS queries can reveal if a user's system has attempted to resolve the domain names of known phishing sites or command-and-control servers used by malware. Network Intrusion Detection and Prevention Systems (NIDS/NIPS) play a vital role in this by continuously monitoring network traffic for suspicious patterns and known attack signatures. Alerts generated by these systems, such as those indicating connections to blacklisted IP addresses or the detection of known malware communication protocols, can be correlated with user reports of suspicious emails to build a comprehensive picture of the incident.

C. Incident Prioritization & Classification

Establishing a clear and consistent process for prioritizing and classifying phishing incidents is essential for ensuring that the security team can effectively allocate resources and respond to threats based on their potential impact and severity. Several factors should be considered when prioritizing a phishing incident. The number of users targeted or potentially affected by the phishing campaign is a key consideration, as a wide-reaching attack has a greater potential for causing widespread disruption and compromise. The sensitivity of the data that could be compromised if the attack is successful also plays a crucial role in prioritization. Incidents that target systems or data deemed highly confidential or critical to business operations should be given higher priority. The potential functional impact on business operations is another important factor.

A phishing attack that leads to the disruption of critical services or prevents employees from performing essential tasks will require a more urgent response. Indicators of successful

compromise, such as a user having entered their credentials on a fake website or downloaded a malicious attachment, elevate the priority of the incident. Finally, phishing attempts that specifically target high-value individuals, such as executives, should be prioritized due to the potential for significant damage resulting from the compromise of their accounts.

Based on these prioritization criteria, a classification system should be developed to categorize phishing incidents into different severity levels, such as low, medium, and high. This classification helps the security team determine the appropriate level of response and the urgency with which actions need to be taken. For instance, a low-severity incident might involve a small number of users targeted with a generic phishing email and no indication of successful compromise, while a high-severity incident could involve a targeted attack on senior executives with evidence of account compromise and potential data exfiltration. NIST SP 800-61r2 recommends prioritizing incidents based on their functional impact, information impact, and recoverability. To provide a clear and consistent framework for incident triage, the following Incident Prioritization Matrix can be utilized:

Severity Level	Number of Users Affected	Data Sensitivity	Potential Impact	Indicators of Compromise	Target
High	Multiple users	Highly Confidential / Critical	Critical service outage, Data breach	Confirmed	Executives, High Value
Medium	Several users	Confidential / Proprietary	Significant disruption	Suspected	General Employees
Low	Single user	Public / Internal	Minor disruption	None	General Employees

This matrix provides a guideline for quickly assessing and categorizing the severity of phishing incidents, ensuring that the most critical threats receive the immediate attention and resources required to mitigate their impact effectively.

IV. Incident Response Procedures

A. Team Roles & Responsibilities (CSIRT Structure)

A well-defined Computer Security Incident Response Team (CSIRT) with clearly established roles and responsibilities is crucial for effectively handling phishing incidents.

- **The Incident Response Manage**r is responsible for the overall coordination of the response effort, ensuring that all team members are aware of their roles, and maintaining clear communication throughout the incident lifecycle.
- **Security Analysts** are tasked with the initial investigation and analysis of the reported phishing attempt, determining its scope and potential impact, and implementing containment measures.
- **Forensic Analysts** may be involved in more complex incidents requiring in-depth evidence collection and analysis to understand the attacker's techniques and the extent of the compromise.
- **IT Administrators** play a critical role in system isolation, remediation efforts such as removing malware and restoring systems, and updating security controls.
- **The Communication Lead** is responsible for managing both internal and external communications related to the incident, ensuring that accurate and timely information is disseminated to relevant stakeholders.
- **Legal Counsel** provides guidance on legal and regulatory considerations, including data breach notification requirements and potential legal ramifications.
- **Human Resources** may need to be involved in incidents that involve employee actions or potential policy violations.

Clear communication channels and well-defined escalation paths within the CSIRT are essential for a coordinated and efficient response to phishing incidents. NIST provides several considerations for selecting an incident response model, including the need for 24/7 availability and the required expertise of the team members.

B. Immediate Actions (Upon Notification)

1. Initial Assessment & Scope Determination

Upon notification of a suspected phishing incident, the immediate priority is to conduct an initial assessment to verify the legitimacy of the report and determine the potential scope and impact of the incident. This involves gathering as much information as possible from the reporting user or system, analyzing email headers and content, and checking against known threat intelligence.

The security team needs to quickly determine the number of users who received the suspicious communication, the systems that might be affected, and the type of information that could be at risk if the attack is successful. This initial assessment helps in prioritizing the incident and determining the appropriate level of response. NIST emphasizes the importance of effective detection and analysis in minimizing the impact of security incidents.

2. User Account Security (Credentials Reset)

If the initial assessment indicates a high likelihood of a successful phishing attack, especially one that aimed to steal user credentials, immediate steps must be taken to secure potentially compromised user accounts. This typically involves immediately resetting the

passwords of the affected accounts. Users should be instructed to choose strong, unique passwords that are not used for any other services.

Enforcing multi-factor authentication (MFA) on these accounts, if not already in place, is a critical step to prevent unauthorized access even if the password has been compromised. Additionally, any active sessions associated with the compromised accounts should be revoked to prevent attackers from continuing to use them. A thorough investigation of the account activity should be conducted to identify any unauthorized access or actions that may have occurred before the credentials were secured. NIST's response to a phishing scam includes disabling compromised accounts as an immediate action.

C. Containment & Quarantine

1. Blocking Malicious Sources (Senders, URLs)

Once a phishing attack has been identified and verified, immediate containment measures must be implemented to prevent further harm. This includes blocking the malicious sources associated with the attack. If the attack was delivered via email, the sender's email address and domain should be blocked at the organization's email gateway to prevent future emails from the same source from reaching other users.

Any identified malicious URLs that were part of the phishing attack should also be blocked at the web proxy or firewall to prevent users from accidentally or intentionally accessing them.

Sharing this threat intelligence, such as the blocked sender addresses and malicious URLs, with other relevant security tools and platforms within the organization can further enhance the containment efforts. NIST recommends containment strategies that include blocking network traffic from malicious sources.

2. System & Network Isolation

In cases where a phishing attack has resulted in a system compromise or the potential for malware infection, isolating the affected systems from the network is a critical containment step. This prevents the potential spread of malware or the attacker's lateral movement to other systems within the organization's network.

Network segmentation can be employed to further limit the attacker's ability to move across different segments of the network. If the phishing attack involves malicious emails, these emails should be quarantined in user inboxes to prevent other users from falling victim. NIST's incident response guidelines emphasize the importance of isolating affected systems during the containment phase.

D. Communication & Escalation Protocols

1. Internal Notifications (Management, Users)

Establishing clear internal communication protocols is vital for managing phishing incidents effectively. Relevant management personnel, including senior leadership and IT management, should be promptly notified about the incident, including its severity, potential impact, and the ongoing response activities. This ensures that they are aware of the situation and can provide necessary support and guidance. Guidelines and templates are below and in the appendix

Guidelines:

- **Timeliness**: Immediate notification is crucial for high-severity incidents. For medium and low-severity incidents, notifications should be provided within a reasonable timeframe (e.g., within 1-2 hours).
- **Clarity**: Communication should be clear, concise, and avoid technical jargon that may confuse non-technical recipients.
- **Accuracy**: Ensure all information is verified before dissemination to prevent misinformation.
- **Channels**: Utilize appropriate communication channels (e.g., email, instant messaging, phone calls) based on the urgency and nature of the incident.
- **Escalation**: Define clear escalation paths and procedures for notifying higher levels of management or specialized teams when necessary.
- **Documentation**: Maintain a log of all communications related to the incident, including timestamps, recipients, and content.

Management Communication Template

Subject: *Urgent: Potential Phishing Incident - [Incident Severity]*
To: *[Management Recipients]*
Date & Time: *[Date] [Time]*

Incident Summary: *A potential phishing incident has been detected/reported.*
Severity: *[High/Medium/Low]*
Description: *[Brief description of the incident, including the type of phishing attack, potential impact, and number of users affected.]*
Current Status: *[Outline the actions taken so far, including initial assessment, containment, and investigation.]*
Next Steps: *[Describe the planned actions, including further investigation, remediation, and recovery.]*
Potential Impact: *[Outline the potential impact on business operations, data, and reputation.]*
Contact: *[Name and contact information of the incident response manager.]*
Updates: *Regular updates will be provided as the situation evolves.*

Users Communication Template

***Subject**: Important Security Alert: Potential Phishing Attempt*

***To**: All Employees*

***Date & Time:** [Date] [Time]*

***Attention:**A potential phishing attempt has been identified.*

***Description**:[Brief description of the phishing attempt, including examples of suspicious emails, messages, or calls.]*

Recommended Actions:
- Do not click on any links or open any attachments from suspicious senders.
- If you have already clicked on a link or opened an attachment, immediately report it to *[Security Team Contact].*
- If you have entered any credentials, immediately change your password and enable multi-factor authentication.
- Be vigilant and report any suspicious activity to *[Security Team Contact].*

***Contact**: [Security Team Contact Information]*

Thank you for your cooperation in maintaining our organization's security.

2. External Reporting (Providers, Authorities)

In certain circumstances, external reporting of phishing incidents may be necessary. This includes situations where a data breach involving personal information has occurred, triggering legal and regulatory reporting requirements. The playbook should outline the specific procedures for reporting incidents to relevant authorities, such as law enforcement agencies and data protection authorities. Contact information for these entities should be readily available.

Guidelines:

- **Legal Compliance:** Ensure all external reporting complies with applicable laws and regulations (e.g., GDPR, HIPAA, PCI DSS).
- **Accuracy**: Provide accurate and verified information to external parties.
- **Timeliness**: Report incidents within the required timeframes.
- **Authorization**: Obtain necessary authorization before disclosing sensitive information to external parties.
- **Documentation**: Maintain detailed records of all external communications and reporting activities.
- **Single Point of Contact:** Designate a single point of contact for external communications to ensure consistency.

External Reporting Template (Providers):

***Subject**: Security Incident Notification - <Company Inc>*

***To**: [Provider Contact]*

***Date & Time:** [Date] [Time]*

Incident Details:
[Brief description of the incident, including the type of phishing attack and its potential impact on the provider's services.]

Affected Services:
[List the specific services or systems that may be affected.]

Actions Taken:
[Outline the actions taken by the organization to contain and mitigate the incident.]

Request for Assistance:
[Specify any assistance required from the provider, such as blocking malicious traffic or providing log data.]

Contact:
[Name and contact information of the organization's representative.]

External Reporting Template (Authorities):

***Subject**: Security Incident Report - <Company Inc>*

***To**: [Authority Contact]*

***Date & Time:** [Date] [Time]*

***Incident Details:** [Detailed description of the incident, including the type of phishing attack, the date and time of occurrence, and the number of individuals affected.]*

***Data Compromised:** [Specify the types of data that may have been compromised, such as personal information, financial data, or intellectual property.]*

***Impact**: [Outline the potential impact of the incident, including financial losses, reputational damage, and legal implications.]*

Actions Taken: *[Describe the actions taken by the organization to contain, investigate, and remediate the incident.]*

Contact*: [Name and contact information of the organization's representative.]*

Supporting Documentation:
[List any supporting documentation that will be provided, such as forensic reports or log

E. Investigation & Analysis

1. Forensic Data Collection & Tools

When responding to a phishing incident that has led to a potential compromise, the ability to collect and analyze digital evidence is paramount. A variety of tools are available to aid in this process. These tools help security analysts and forensic investigators to acquire, preserve, and examine data in a forensically sound manner. Here are some common categories and examples of tools used in forensic data collection:

Disk Imaging Tools: These tools create bit-by-bit copies (images) of storage devices, ensuring that all data, including deleted files and unallocated space, is preserved for analysis. Examples include:

- *FTK Imager:* A free tool used to acquire data and create forensic images.
- *Autopsy*: An open-source digital forensics platform with imaging capabilities.

Memory Forensics Tools: These tools capture and analyze the contents of a computer's RAM, which can contain valuable information about running processes, network connections, and even malicious code. Examples include:

- *Volatility*: An open-source memory forensics framework.
- *Redline*: A free endpoint security tool with memory analysis capabilities.

Log Collection and Analysis Tools: These tools help gather and analyze logs from various systems and devices, providing insights into events that occurred during the incident. Examples include:

- *SIEM* (Security Information and Event Management) Systems: While primarily for detection, SIEMs also play a role in collecting and centralizing logs for analysis .
- *Syslog*: A standard protocol for event logging in Unix-like systems.
- *Event Viewer*: A built-in log management tool in Windows operating systems.

Network Analysis Tools (Packet Sniffers and Protocol Analyzers): These tools capture and analyze network traffic, which can reveal communication patterns, malicious connections, and data exfiltration attempts. Examples include:

- *Wireshark:* A widely used open-source packet analyzer.
- *tcpdump*: A command-line packet capture tool.

- *Endpoint Detection and Response (EDR) Solutions:* Many modern EDR solutions have built-in forensic capabilities, allowing for the collection and analysis of endpoint data in the context of incident response.

Mobile Forensics Tools: If the phishing attack involved mobile devices (smishing, social media phishing), specialized tools may be needed to collect data from these devices.

The selection of specific tools will depend on the nature of the phishing incident, the systems involved, and the organization's existing security infrastructure and forensic capabilities. It's also important to ensure that personnel handling forensic data are properly trained in the use of these tools and follow established best practices to maintain the integrity of the evidence.

Chain of Custody

Maintaining a meticulous chain of custody is critical in forensic investigations to ensure the integrity and admissibility of digital evidence. The chain of custody is a chronological record that documents the seizure, custody, control, transfer, analysis, and disposition of evidence. It provides a detailed history of who handled the evidence, when, where, and what was done with it. Any break in the chain of custody can compromise the credibility of the evidence in legal proceedings or internal investigations.

A comprehensive chain of custody record should include the following information :

Case Information: Case name or number, date and time of the incident.
Evidence Details: Description of the evidence (e.g., specific computer, server, email).
Identifying information (e.g., serial number, asset ID, hostname, file name).
Date and time of collection.
Location of collection.
Method of collection (how the evidence was acquired).
Condition of the evidence at the time of collection (e.g., powered on/off, physical state).
Custody Log: A chronological record of each transfer of custody:
Date and time of transfer.
Name and signature of the person releasing the evidence.
Name and signature of the person receiving the evidence.
Purpose of the transfer (e.g., storage, analysis, transport).
Storage Information: Location where the evidence is stored, storage conditions, and security measures in place.
Analysis Information: Details of any examinations or analyses performed on the evidence, including the date, time, examiner, and tools used.
Final Disposition: Information on the final outcome of the evidence (e.g., returned to owner, retained for legal proceedings, securely destroyed).

Here is a template for a Chain of Custody Form:

Chain of Custody Form

Case Information:

Case Name/Number: _____
Date of Incident: _____
Investigating Officer: _____
Agency/Department: _____
Evidence Details:

Item Number: _____
Description of Item: _____
Evidence Type (e.g., Computer, Email, USB Drive): _____
Identifying Information (Serial #, Hostname, File Name, etc.):_____
Date and Time of Collection: _____
Location of Collection: _____
Collected By (Name/Signature): _____
Method of Collection: _____
Condition of Evidence at Collection: _____

Date & Time	***Released by***	***Received by***	***Reason for transfer***	***Remarks / Condition***

2. Root Cause Determination

A key objective of the investigation is to determine the root cause of the phishing incident. This involves identifying the initial point of entry, such as the specific phishing email or message, and understanding the vulnerabilities that allowed the attack to succeed. Analyzing the attacker's tactics, techniques, and procedures (TTPs) provides valuable insights into their methods and motivations. It is also crucial to determine if any data was compromised or exfiltrated as a result of the attack.

3. Compromise Assessment

A comprehensive compromise assessment is necessary to determine the full extent of the phishing incident. This involves identifying all affected systems, user accounts, and data.

Security teams will analyze logs and network traffic for any signs of further malicious activity, such as unauthorized access attempts, lateral movement within the network, or communication with suspicious external hosts.

F. Eradication & Recovery

1. Removal of Malicious Content

The eradication phase involves removing all malicious content associated with the phishing incident from affected systems and networks. This includes deleting malicious emails from user inboxes and email servers, removing any malware that may have been installed on compromised systems using anti-malware tools or manual removal techniques, and disabling any compromised user accounts.

2. System Restoration

The recovery phase focuses on restoring affected systems to a clean and operational state. This may involve restoring systems from clean backups to ensure that any malware or malicious modifications have been removed. It is crucial to verify the integrity of the restored systems and data before returning them to production.

3. Security Control Updates

To prevent similar phishing attacks from occurring in the future, it is essential to update security controls based on the findings of the incident investigation. This may involve updating firewall rules, enhancing email filtering configurations, updating anti-malware signatures, and implementing patches to address any vulnerabilities that were exploited during the attack.

G. Post-Incident Activities & Reporting

Following the eradication and recovery phases, a thorough review of the phishing incident should be conducted. This includes documenting the incident timeline, the actions taken during the response, and any lessons learned. A detailed incident report should be prepared for management and other relevant stakeholders, outlining the findings of the investigation, the impact of the incident, and the steps taken to contain and remediate it.

The post-incident review should identify any areas for improvement in the incident response plan and existing security controls. Based on the lessons learned, the phishing playbook and other relevant security policies should be updated to reflect any necessary changes and improvements.

V. Communication & Coordination

A. Internal Communication Strategies

1. Management Reporting

A well-defined process for reporting phishing incidents and the corresponding response activities to senior management is essential for maintaining organizational awareness and securing necessary support. The reporting should be timely and provide a clear overview of the incident, including its nature, scope, potential impact, and the actions taken or planned by the incident response team. The frequency of these reports should be determined based on the severity and duration of the incident, with initial notifications being immediate for high-impact events and regular updates provided as the response progresses.

Key metrics and information to be included in management reports may involve the number of users targeted and affected, the sensitivity of any data potentially compromised, the functional impact on business operations, the estimated cost of the response, and the anticipated timeline for recovery.

2. User Notifications & Guidance

Effective internal communication also involves providing timely and relevant information to users about ongoing phishing campaigns and offering clear guidance on how to identify and avoid these threats. Developing pre-approved templates for user notifications can ensure consistent and accurate messaging. These notifications should alert users to specific phishing tactics that are currently circulating, provide examples of what to look for, and reiterate best practices for handling suspicious emails, messages, or calls.

Clear channels should be established for users to receive updates on the status of any significant phishing incidents and to understand any actions they may need to take, such as changing passwords or reporting suspicious activity. Regular security awareness training plays a crucial role in preparing users to recognize and respond appropriately to phishing attempts.

B. External Communication Strategies

1. Customer & Partner Notifications

In the event of a phishing incident that may potentially affect customers or business partners, establishing clear procedures for external notification is crucial for maintaining transparency and trust. This is particularly important in cases involving a data breach where customer or partner data may have been compromised, or if attackers are impersonating the organization to target external entities.

Developing pre-approved communication templates and guidelines for these external notifications ensures that the messaging is consistent, accurate, and provides the necessary information without causing undue alarm.

Guidelines:

- **Transparency:** Be open and honest about the incident and its potential impact.
- **Empathy:** Acknowledge the concerns of affected customers.
- **Clarity:** Use clear and concise language, avoiding technical jargon.
- **Actionable Advice:** Provide specific steps customers can take to protect themselves.
- **Contact Information**: Offer clear channels for customers to ask questions or report concerns.
- **Legal Compliance:** Ensure the notification complies with all applicable privacy laws and regulations.

External Reporting Template (Customers):

Subject: Important Security Notice: Potential Data Security Incident

Dear Valued Customer,

We are writing to inform you of a potential data security incident that may affect some of our customers.

What Happened:

On *[Date]*, we detected *[Brief description of the incident, e.g., unauthorized access to our systems].* We immediately launched an investigation and took steps to secure our systems.

What Information May Be Affected:

[Specify the types of customer information that may have been affected, e.g., names, email addresses, payment information].

What We Are Doing:

- We have taken immediate steps to secure our systems and prevent further unauthorized access.
- We are conducting a thorough investigation to determine the full scope of the incident.
- We are working with cybersecurity experts to enhance our security measures.
- We are notifying relevant authorities.

What You Can Do:

- Change your password for your <Company Inc> account immediately.
- Enable multi-factor authentication (MFA) on your account.
- Be vigilant for any suspicious emails, calls, or text messages.

- Monitor your financial accounts for any unauthorized activity.
- If you notice any suspicious activity, please report it to us immediately at *[Contact Information].*

Our Commitment to You:

We understand the importance of protecting your personal information, and we sincerely apologize for any concern this incident may cause. We are committed to taking all necessary steps to prevent similar incidents in the future.

For More Information:

If you have any questions or concerns, please contact us at *[Contact Information]* or visit our website at *[Website Address].*

Sincerely,

The <Company Inc> Team

2. Legal & Regulatory Compliance

Phishing incidents, especially those resulting in data breaches, may trigger specific legal and regulatory reporting requirements. The playbook should clearly specify these requirements, such as data breach notification laws in relevant jurisdictions. It should also outline the process for engaging with legal counsel to ensure full compliance with all applicable regulations and reporting obligations. This includes determining the specific information that needs to be reported, the timelines for reporting, and the appropriate authorities to notify. Maintaining accurate records of the incident and the response activities is crucial for demonstrating compliance.

VI. Continuous Improvement & Learning

A. Post-Incident Review & Analysis

1. Lessons Learned & Process Adjustments

Establishing a formal process for conducting post-incident reviews following every significant phishing incident is crucial for continuous improvement. These reviews should involve all relevant stakeholders from the incident response team and potentially other departments. The primary goal is to document key findings from the incident, thoroughly analyze the root causes that contributed to its occurrence and impact, and critically evaluate the effectiveness of the incident response procedures that were followed.

Based on this analysis, necessary adjustments should be identified and implemented to the incident response plan, as well as to broader security policies and procedures.

2. Playbook & Policy Updates

To ensure that the phishing playbook remains a relevant and effective guide, a regular review and updates should be undertaken as part of the post incident report. This review process should involve key stakeholders from the security team and other relevant departments. Lessons learned from past phishing incidents, as well as changes in the broader threat landscape, should be incorporated into the playbook and related security policies. This includes updating procedures based on new attack techniques, incorporating information about emerging threats identified through threat intelligence monitoring, and refining communication and escalation protocols as needed.

B. Ongoing Security Enhancements

1. Control & Countermeasure Improvements

Continuously evaluating and improving existing security controls and countermeasures is essential for strengthening the organization's defenses against phishing attacks. This may involve enhancing email filtering capabilities, implementing more advanced threat protection solutions, deploying or optimizing endpoint detection and response (EDR) systems, and strengthening network security controls. The organization should also stay informed about new security technologies and practices and implement them as appropriate to bolster its defenses against evolving phishing tactics.

2. Security Awareness Training

Ongoing security awareness training for all employees is a critical component of a proactive phishing defense strategy. This training should educate employees about the latest phishing threats, including new attack techniques and social engineering tactics, and provide them with clear guidance on how to identify and report suspicious communications. Regular phishing simulation exercises should be conducted to test employee awareness and identify areas where further training or reinforcement is needed..

C. Proactive Security Practices

1. Regular Playbook Reviews

To ensure its continued effectiveness, the phishing playbook should be subject to regular reviews, ideally on an annual basis or more frequently if significant changes occur in the threat landscape or the organization's infrastructure. These reviews will involve key stakeholders from the security team and other relevant departments to gather feedback and identify areas for improvement.

2. Threat Intelligence Monitoring

Continuously monitoring threat intelligence feeds is a proactive security practice that helps the organization stay ahead of emerging phishing tactics, techniques, and campaigns. By staying informed about the latest threats, the organization can proactively update its security controls, refine its detection rules, and adapt its security awareness training to address these new risks.

3. Simulation & Exercise Drills

Conducting regular simulation and exercise drills, such as tabletop exercises and simulated phishing attacks, is crucial for testing the effectiveness of the incident response plan and the preparedness of both the security team and employees. These exercises help identify any gaps or weaknesses in the plan, as well as areas where the team's response can be improved. They also serve as valuable training opportunities for employees, reinforcing their ability to recognize and report phishing attempts.

VII. Appendices

A. Messaging Templates

Management Communication Template

Subject: *Urgent: Potential Phishing Incident - [Incident Severity]*
To: *[Management Recipients]*
Date & Time: *[Date] [Time]*

Incident Summary: *A potential phishing incident has been detected/reported.*
Severity: *[High/Medium/Low]*
Description: *[Brief description of the incident, including the type of phishing attack, potential impact, and number of users affected.]*
Current Status: *[Outline the actions taken so far, including initial assessment, containment, and investigation.]*
Next Steps: *[Describe the planned actions, including further investigation, remediation, and recovery.]*
Potential Impact: *[Outline the potential impact on business operations, data, and reputation.]*
Contact: *[Name and contact information of the incident response manager.]*
Updates: *Regular updates will be provided as the situation evolves.*

Users Communication Template

Subject*: Important Security Alert: Potential Phishing Attempt*

To*: All Employees*

Date & Time: *[Date] [Time]*

Attention:*A potential phishing attempt has been identified.*

Description*:[Brief description of the phishing attempt, including examples of suspicious emails, messages, or calls.]*

Recommended Actions:
- Do not click on any links or open any attachments from suspicious senders.
- If you have already clicked on a link or opened an attachment, immediately report it to *[Security Team Contact].*
- If you have entered any credentials, immediately change your password and enable multi-factor authentication.
- Be vigilant and report any suspicious activity to *[Security Team Contact].*

***Contact**: [Security Team Contact Information]*

Thank you for your cooperation in maintaining our organization's security.

External Reporting Template (Providers):

***Subject**: Security Incident Notification - <Company Inc>*

***To**: [Provider Contact]*

***Date & Time:** [Date] [Time]*

Incident Details:
[Brief description of the incident, including the type of phishing attack and its potential impact on the provider's services.]

Affected Services:
[List the specific services or systems that may be affected.]

Actions Taken:
[Outline the actions taken by the organization to contain and mitigate the incident.]

Request for Assistance:
[Specify any assistance required from the provider, such as blocking malicious traffic or providing log data.]

Contact:
[Name and contact information of the organization's representative.]

External Reporting Template (Authorities):

***Subject**: Security Incident Report - <Company Inc>*

***To**: [Authority Contact]*

***Date & Time:** [Date] [Time]*

***Incident Details:** [Detailed description of the incident, including the type of phishing attack, the date and time of occurrence, and the number of individuals affected.]*

***Data Compromised:** [Specify the types of data that may have been compromised, such as personal information, financial data, or intellectual property.]*

***Impact**: [Outline the potential impact of the incident, including financial losses, reputational damage, and legal implications.]*

Actions Taken: *[Describe the actions taken by the organization to contain, investigate, and remediate the incident.]*

Contact*: [Name and contact information of the organization's representative.]*

Supporting Documentation:
[List any supporting documentation that will be provided, such as forensic reports or log

External Reporting Template (Customers):

Subject: Important Security Notice: Potential Data Security Incident

Dear Valued Customer,

We are writing to inform you of a potential data security incident that may affect some of our customers.

What Happened:
On *[Date]*, we detected *[Brief description of the incident, e.g., unauthorized access to our systems].* We immediately launched an investigation and took steps to secure our systems.

What Information May Be Affected:
[Specify the types of customer information that may have been affected, e.g., names, email addresses, payment information].

What We Are Doing:
- We have taken immediate steps to secure our systems and prevent further unauthorized access.
- We are conducting a thorough investigation to determine the full scope of the incident.
- We are working with cybersecurity experts to enhance our security measures.
- We are notifying relevant authorities.

What You Can Do:
- Change your password for your <Company Inc> account immediately.
- Enable multi-factor authentication (MFA) on your account.
- Be vigilant for any suspicious emails, calls, or text messages.
- Monitor your financial accounts for any unauthorized activity.
- If you notice any suspicious activity, please report it to us immediately at *[Contact Information].*

Our Commitment to You:
We understand the importance of protecting your personal information, and we sincerely apologize for any concern this incident may cause. We are committed to taking all necessary steps to prevent similar incidents in the future.

For More Information:

If you have any questions or concerns, please contact us at *[Contact Information]* or visit our website at *[Website Address].*

Sincerely,

The <Company Inc> Team

B. Checklist & Forms

Chain of Custody Form

Case Information:

Case Name/Number: _____
Date of Incident: _____
Investigating Officer: _____
Agency/Department: _____
Evidence Details:

Item Number: _____
Description of Item: _____
Evidence Type (e.g., Computer, Email, USB Drive): _____
Identifying Information (Serial #, Hostname, File Name, etc.):_____
Date and Time of Collection: _____
Location of Collection: _____
Collected By (Name/Signature): _____
Method of Collection: _____
Condition of Evidence at Collection: _____

Date & Time	Released by	Received by	Reason for transfer	Remarks / Condition