

Phishing Incident Response Playbook

Title	Phishing Incident Response Playbook
Version	V1
Date issued	DD-MM-YYYY
Status	In progress
Document owner	Full Name
Creator name	Full Name
Creator organization name	<Organization Name>
Subject category	Phishing Incident Response
Access constraints	NA
Review cycle	Annually

1. Introduction

1.1. Incident Overview

Attackers often use emerging technologies and create convincing phishing emails to trick their targets. The employees of an organization may receive phishing emails from spoofed identities of their CEO, management, or vendors. The IH&R team must be prepared to track such emails and validate their original identity. Here, an employee of organization Z received a suspicious email from an unknown user with an unexpected attachment. This playbook describes different activities related to various stages of incident response for better implementation of incident response procedures in case of phishing incidents.

1.2 Purpose of Playbook

The main purpose of this playbook is to provide guidance for detecting and responding to phishing incidents within an organization. This playbook includes step-wise guidance for the IH&R team to implement mitigative actions and defend against phishing attacks in an organization.

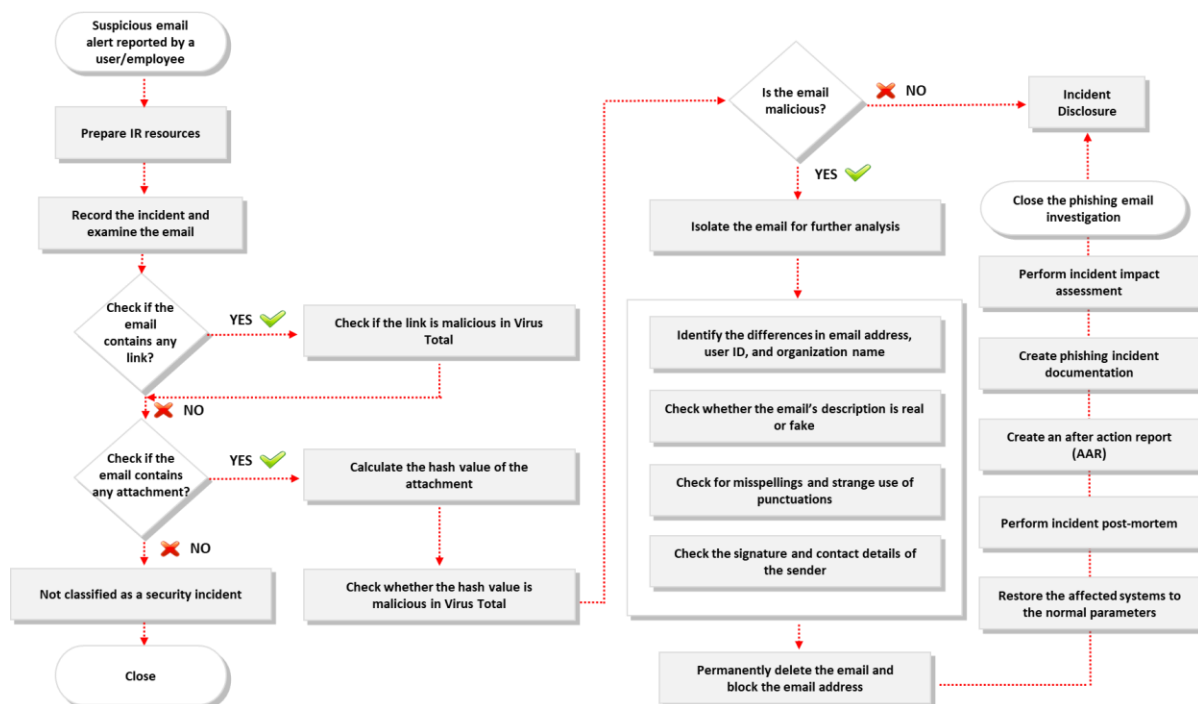
1.3 Scope

This playbook is developed for the use of incident responders to respond to phishing incidents in an organization. Additionally, this document must be used alongside the incident response plan of the organization. The scope of this document is listed below (not limited to):

- Determine the total number of users affected by a phishing email

- Understand and document various user actions associated with the phishing email; for example:
User 1: Downloaded the attachment
User 2: Opened the spoofed link
- Identify any related activities by checking the following:
 - Any suspicious email
 - Any email containing unknown URL
 - Social media activities
 - Any non-deliverable email
 - Any sign of suspicious activity
- Analyze suspicious emails
- Recover from the incident

1.4 Workflow Diagram



Workflow diagram for phishing incident response

2. Preparation

2.1 Objectives

The main objective of the preparation phase is to prepare an organization to respond to phishing incidents in an effective and timely manner. Another objective of this phase is to define the roles of employees, along with their reporting mechanisms, to mitigate phishing incidents.

2.2 Activities Involved

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Prepare for incident response:
 - Prepare, review, and practice the incident response procedures in accordance with the incident response plan
 - Configure email filtering tools such as MailWasher Pro and N-able Mail Assure to filter and block all malicious emails transmitted across the network
 - Incorporate threat intelligence into the existing security capabilities to feed them with the latest risks, vulnerabilities, and common patterns
 - Provide easy access to the required documentation such as incident response plan and network architecture to respond to a phishing incident. Links of important documents are given below:
 - Link 1:
 - Link 2:
 - Link 3:
 - Deploy email monitoring tools such as Teramind and Inbound Shield to check for malicious attachments, links, messages, and sensitive data in both incoming and outgoing emails
 - Identify and define the key indicators and patterns of a phishing incident and map them with the available SIEM or other security solutions
 - Employ email log analysis tools such as Tracemail and Mailgun to extensively analyze all incoming and outgoing emails in the network
 - Prepare a list of questions to be asked by tech support from the complainants to identify the type of email incident
 - Establish email-independent communication channels such as telephone, message, and VOIP to report incidents and send data to the incident response team and other authorities
 - Develop and implement an acceptable email usage policy to define the satisfactory behavior of employees while using their official email
 - Configure email clients or servers to create regular archives and backups of all emails

- Inform the employees:
 - Conduct regular training and awareness programs related to phishing, malicious emails attacks, ransomware, and other email security incidents
 - Create a proper format for reporting and registering complaints
 - Ensure that training and awareness sessions are mandatory for employees handling critical data and systems of the organization
 - Provide proper contact information of personnel who can be contacted by users in case of an email security incident

2.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Prepare for incident response ○ Create incident response processes and procedures ○ Define roles and responsibilities ○ Review recent incident reports ○ Incorporate threat intelligence ○ Maintain network architecture and data flow diagrams ○ Define threat indicators and incorporate alerting solutions	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Service Desk	Email, Phone, Text Message
	Service Delivery Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	Federal Agency	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
Inform the employees	Information Security Manager	Email, Phone, Text Message

○ Conduct training and awareness campaigns related to phishing incidents	IT Manager/Director	Email, Phone, Text Message
	HR Manager/Director	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

2.4 Additional Information (if any)

Note: Refer to the following templates and checklists to fill the necessary details:

- a. Preparation to Handle Email Security Incidents.docx
- b. IH&R Plan Template.docx

3. Detection and Notification

3.1 Objectives

The main objective of the detection phase is to perform initial investigation on suspected emails and determine whether they are phishing emails.

3.2 Activities Involved

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Detect the phishing email:
 - Check for unexpected attachments from unknown users, clients, vendors, or peers
 - Check for attachments with unusual or unrecognized formats
 - Check the authenticity of the email address
 - Check for differences in the sender email ID and their display name
 - Check for incomplete or incorrect organization names or names containing numbers instead of letters
 - Check if the email message contains generic greetings such as “Dear users” or “Dear customers”
 - Check if the email message contains unusual links or attachments
 - Hover on the links in the email message and check whether a different website or URL is displayed; moreover, check whether the URL of links in the email message displays an incorrect name or domain

- Check if the email message contains attractive information such as the user winning a lottery, competition, free subscription, or vacation and job offers
- Check if the email message contains any message that arouses a sense of urgency; for example, asking the user to immediately transfer funds to help them
- Check if the message contains information asking the user to reveal sensitive information, log in to their accounts using the provided links, or install updates
- Check for spelling errors in the email message
- Check the company logo and identify mistakes (if any)
- Check the complete signature and contact details of the sender
- Escalate the phishing incident to higher authorities with the proper escalation procedure
- Gather the following information from initial investigation:
 - Type of incident
 - Location of incident
 - Who, how, and when was the incident reported
 - List of users/employees who received the phishing email
 - Identify the causes behind the incident
 - Determine the number of employees who opened the email and downloaded or accessed malicious links or attachments
 - Identify if the downloaded files contain malicious content such as virus, trojan, or worm
 - Number of systems affected
 - Impact on business operations

3.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Detecting the incident <ul style="list-style-type: none"> ○ Monitor security solutions ○ Respond to manual and automated alerts ○ Escalate the incident via the ticketing system (if not escalated) 	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Initial investigation <ul style="list-style-type: none"> ○ Collect initial evidence data ○ Classify and prioritize the incident 	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Head of IT	Email, Phone, Text Message
Notification of the incident <ul style="list-style-type: none"> ○ Follow the defined IH&R plan to notify the incident 	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message

3.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- c. Email Security Incident Detection and Analysis Template.docx
- d. Checklist for Identifying Phishing and Spam Emails.docx
- e. Phishing Examples.docx

4. Containment

4.1 Objectives

The main objective of the containment phase is to identify the systems affected by the phishing email and isolate them from the network.

4.2 Containment Steps/Activities

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Activities to contain the phishing incident:
 - Identify the system(s) affected by the phishing mail
 - Identify user accounts compromised by the phishing link (if any)
 - Isolate the affected systems from the network to prevent the malware from spreading
 - Check whether users downloaded the attachment, clicked on the link, and provided the requested information
 - Identify active sessions related to the email from the affected system and close them
 - Remove internet connection from the system to disconnect remote access (if any)
 - Report and block malicious links and IP addresses on servers, network devices, and across all security solutions
 - Reduce the impact of the phishing email on other employees by identifying the key objectives of the email and implementing filters to block emails with a similar signature
 - Block all identified indicators of compromise (IoCs) in the email system and endpoint security solutions
 - Reset the password of all affected email accounts and systems
 - Enable two-factor authentication for all employees
 - Scan the affected systems using antivirus or antimalware software such as TotalAV, Bitdefender Antivirus Plus, and Kaspersky Anti-Virus

- Update and patch the email security software
- Block automatic email forwarding to remote unknown domains
- Enable the mailbox auditing feature
- Communicate the progress:
 - Regularly inform the stakeholders about the status of the incident handling process

4.3 Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Containment activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

4.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- f. Containment of Email Security Incidents Checklist.docx
- g. Incident Containment Checklist.docx
- h. Incident Containment Template.docx

5. Analysis

5.1 Objectives

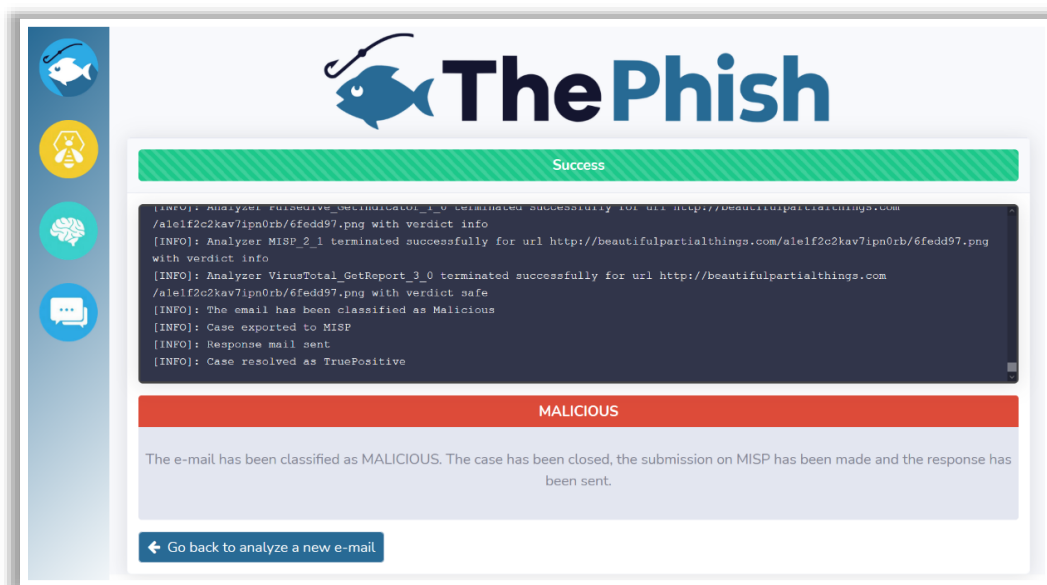
The main objective of this phase is to analyze the security incident and determine its scope. Another objective of this phase is to detect and report the incident impact to establish forensic investigation requirements and develop an effective mitigation strategy based on analysis results.

5.2 Activities Involved

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Analyze the scope of the phishing incident:
 - Identify if any sensitive data are compromised

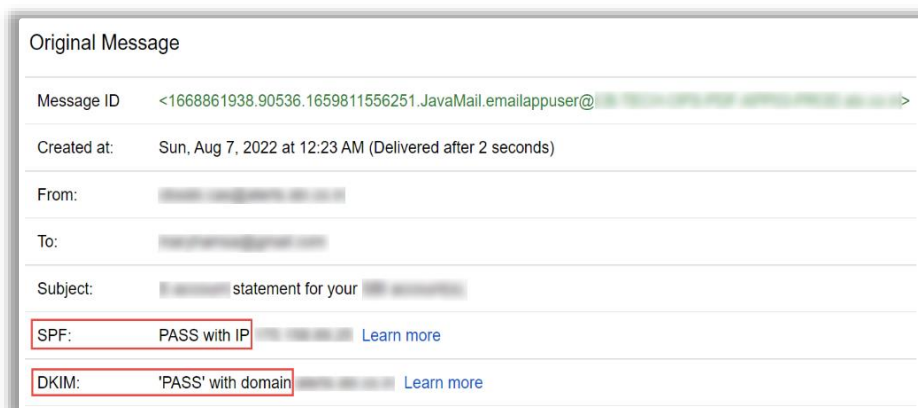
- Identify if the safety of any employee is at risk
- Identify if any organizational service or operation is affected
- Identify if you have control over critical systems across the organizational network
- Check for evidence to identify the adversary
- Identify if there is any internal knowledge about the phishing incident
- Identify unpatched accounts and systems that can be fixed after the analysis
- Identify the indicators of the phishing incident
- Check for unauthorized access to personal or sensitive corporate data
- Analyze the email message:
 - Always use a safe system to analyze phishing emails
 - Use tools such as ThePhish and Netcraft to analyze the suspected phishing email and obtain the necessary details for further investigation



Screenshot of ThePhish case closure window showing malicious email in the results

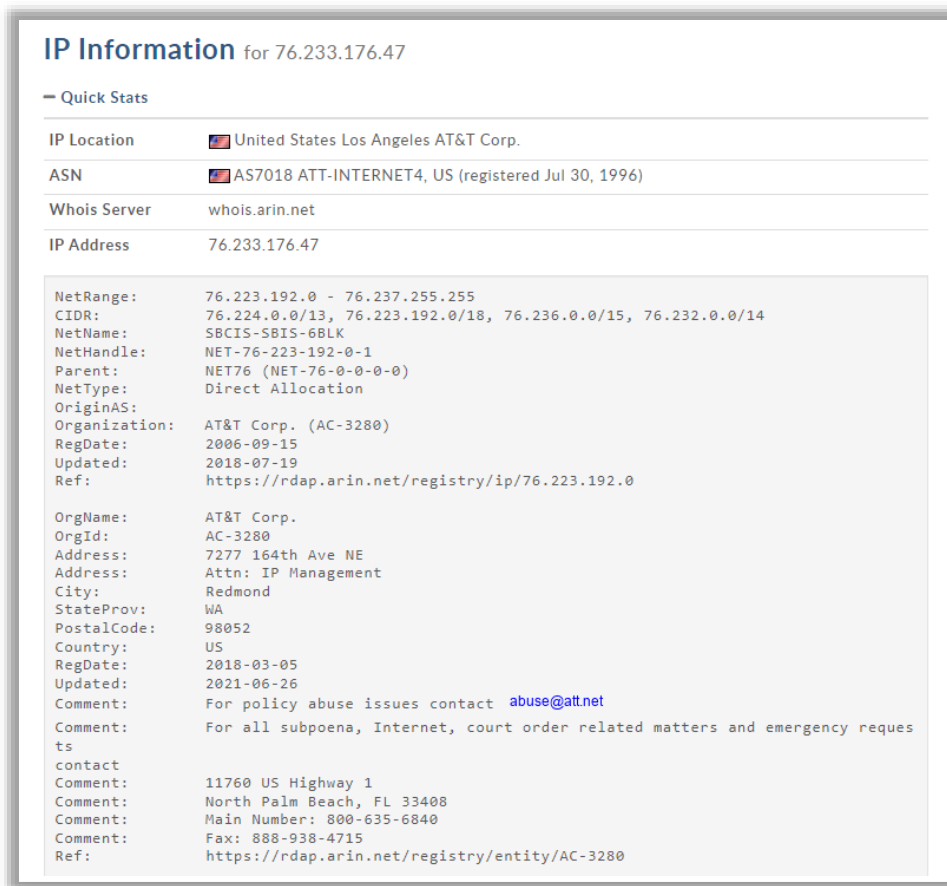
- Document the results to further analyze the email
- Analyze the email header:
 - Gather the following supporting evidence from the email header using tools such as MxToolbox and E-Mail Header Analyzer and track the suspect:
 - Return path
 - Recipient email address
 - Name of email server

- Type of email sending service
 - IP address of sending server
 - Unique message number
 - Date and time when the email was sent
 - Sender Policy Framework (SPF)
 - Domain Keys Identified Mail (DKIM)
 - Information related to attachment files
- Analyze the email header in **Gmail** by clicking on the “More” option (three vertical dots) at the top-right corner of the message, followed by clicking on the “Show original” option to view email header details
- Check the **SPF** and **DKIM** credentials of the email to verify its authenticity



Screenshot of SPF and DKIM fields

- Analyze the validity of the suspected email:
 - Use tools such as Email Dossier and Hunter's Email Verifier to check the validity of received emails
- Analyze the originating IP address of the suspected email identified from the email header using the WHOISLookup Search tool



Screenshot displaying geographic address in the WHOIS database

- Analyze links and attachments present in the email:
 - Use the OSINT tool to identify the associated domains for obtaining other registration data
 - Use the VirusTotal tool to submit the suspected links or attachments received with the email
 - Submit these links and attachments to any malware sandbox such as Joe Sandbox for further investigation
- Analyze email logs:
 - Check system logs to verify the email path
 - Check the network equipment logs of routers, switches, firewalls, and servers to retrieve details of the traffic they allow or deny, source and destination IP addresses, URLs, and types of transmission
 - Examine router and firewall logs to verify the timeline and IP addresses contained within the email
 - Check email logs using tools such as EventLog Analyzer to detect traces of abnormal or malicious emails

- Analyze SMTP logs to determine failures or inconsistencies in the server
- Examine DNS logs to verify whether the attacker used IP spoofing to hide their identity
- Examine DHCP logs to verify the hosts associated with malicious IP addresses
- Analyze email sever logs to retrieve information such as the number of affected systems, email message IDs, and associated IP addresses
- Check threat intelligence feeds to determine whether the phishing email targeted a single person or group of individuals
- Document the results obtained
- Protect the evidence for further legal actions
- Determine the attack type:
 - Categorize the attack type based on the obtained results to implement appropriate mitigative strategies
- Determine the severity of the phishing incident:
 - Create an attack severity matrix considering the incident scope

5.3 Stakeholders Involved

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Analyze the scope of phishing incident	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Initiate evidence gathering and forensic analysis	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Analyze the email message and report potentially compromised data	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

5.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- i. Email Security Incident Detection and Analysis Template.docx
- j. Email Header Analysis Template.docx
- k. Checklist for Handling the Forensic Evidence Properly.docx
- l. Evidence Gathering and Forensic Analysis Form.docx

6. Eradication

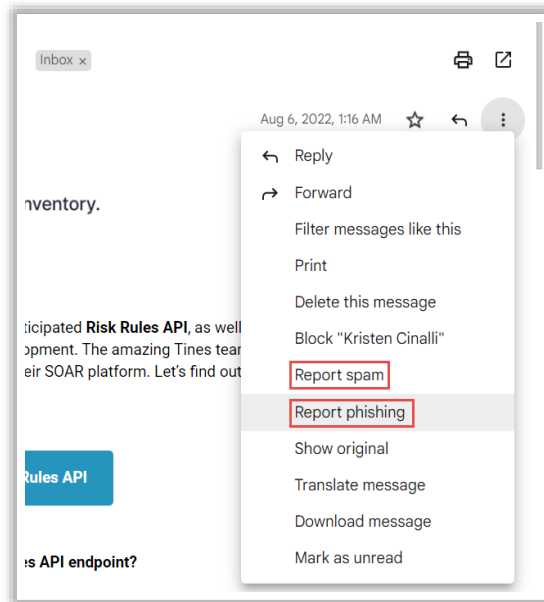
6.1 Objectives

The main objective of this phase is to take appropriate measures to eradicate the incident and prevent the occurrence of such incidents in future.

6.2 Eradication Steps/ Activities

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Perform the following activities to eradicate the phishing incident:
 - Use anti-phishing and antispam tools such as SPAMfighter, SpamTitan, and MailWasher to prevent similar incidents in future
 - Identify common patterns and signatures from the emails and block them on the SMTP server
 - Implement DNS blackholing to block IP addresses used to send malicious emails
 - Blacklist malicious websites and disable automatic downloading across all systems and devices
 - Blacklist emails using signatures, sender addresses, or other details of malicious emails
 - Scan all affected systems using antivirus solutions to ensure the removal of all malware-related artifacts
 - Block and remove the impacted accounts and re-issue new accounts to employees
 - Use encryption or VPNs to communicate using emails
 - Reinforce the security of email servers and clients
 - Train employees to check the email headers of emails asking for immediate action such as financial transactions
 - Implement multiple verification policies for financial transactions
 - Install browser extensions and tools to detect and prevent phishing attacks
 - If the system is infected by malware, patch the vulnerabilities exploited by the malware
 - Perform root cause analysis on the incident
 - Report the phishing email to the service provider
- To report the suspected phishing email → In Gmail, open the suspicious mail and click on the “More” button (three vertical dots) at the top-right corner; then, select the “Report spam” or “Report phishing” option based on the type of email incident you want to report



“Report spam” and “Report phishing” options in Gmail

6.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Develop an eradication plan <ul style="list-style-type: none"> Perform technical and business analyses and create a prioritized eradication plan Establish a communication strategy based on the eradication plan 	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Internal/External Communications Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Eradication activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

6.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- m. Eradication of Email Security Incidents Checklist.docx
- n. Incident Eradication Template.docx
- o. Incident Eradication Checklist.docx

7. Recovery

7.1 Objectives

The main objective of this phase is to recover the affected systems, network, and other resources from the incident impact and maintain business continuity.

7.2 Recovery Steps/Activities

[Activities may differ based on organizational policies, but they are not limited to the following.]

- Activities to recover from phishing attack:
 - If the phishing email is attempting to spoof a bank or financial institution, inform the concerned institutions about the attack and block compromised accounts
 - Restore the affected business-critical systems to normal parameters
 - Restore systems based on business impact analysis
 - Change the password of all affected emails accounts
 - Restore the affected systems using a trusted backup
 - File a complaint with the cybercrime department
 - Contact law enforcement and brief them about the incident
 - Take complete backups and update the software
 - Recover deleted emails using recovery tools such as EaseUS Email Recovery Wizard and SysTools Outlook Recovery, if required
 - Perform complete vulnerability analysis and patch the identified vulnerabilities
 - Restart suspended services
 - Use email security tools such as Gpg4win, Proofpoint Email Protection, and Barracuda Email Protection to monitor further suspicious activities

7.3 Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Recovery activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

7.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- p. Incident Recovery Procedure Template.docx
- q. Incident Recovery Checklist.docx

8. Post-incident Activities

8.1 Objectives

The main objective of this phase is to create the necessary phishing incident reports such as incident documentation, lessons learned, and incident impact assessment. Another objective of this phase is to close the phishing investigation and disclose its details to respective stakeholders.

8.2 Activities Involved

- Perform phishing incident post-mortem or incident review to detect the root causes
- Create an after action report (AAR) that includes information such as what worked effectively, areas of improvement, and strategies for enhancing the response in case of similar phishing incidents
- Conduct a lessons learned meeting to document all details of the incident; ensure that the following questions are answered in this meeting:
 - When and who detected the phishing email?
 - What happened exactly?
 - What caused the phishing incident?
 - To whom was the phishing incident reported?
 - Was the organization adequately prepared to handle the phishing incident?
 - How was the phishing incident contained?
 - How were the impacted systems sanitized?

- What procedures were followed during recovery?
- Were the documented procedures followed by the response team?
- How well did the incident response team and management perform in resolving the phishing incident?
- How should the incident response team and management respond to mitigate similar phishing incidents in future?
- Were there any gaps in communicating the phishing incident?
- Was the right amount of information shared with the right personnel?
- What are the tools and resources required to detect, analyze, and prevent similar phishing incidents in future?
- Create concise and clear phishing incident documentation in a standard format and get it reviewed by an editor
- Create an incident impact assessment report to determine all types of losses caused by the phishing incident; this report must address the following, if required:
 - Financial losses incurred owing to leakage of confidential information
 - Legal costs for investigating the case, lawyer's fees, etc.
 - Costs pertaining to analyzing the phishing incident and recovering and installing software and hardware
 - Implementation costs
 - Costs related to the damage of goodwill as well as loss of customer trust and reputation
- Officially close the phishing email investigation by informing the management and securely retain investigation reports considering the retention policy of the organization
- Disclose incident details to the respective stakeholders by consulting with the legal department of the organization

8.3 Stakeholders Involved/Communication Established

Activities	Stakeholders Involved	Communication Mode/Channel
Conduct lessons learned meeting	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create incident documentation	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create an incident impact assessment report	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Officially close the investigation	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Senior Management	Email, Phone, Text Message
Disclose incident details to the respective stakeholders	Information Security Manager	Email, Phone, Text Message
	Manager – Information Governance	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	CISO	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	Human Resource	Email, Phone, Text Message
	Media	Email, Phone, Text Message
	Vendors	Email, Phone, Text Message
	Customers and General Public	Email, Phone, Text Message
	Business Partners	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

8.4 Additional Information (if any)

Note: Refer to the following documents to fill the necessary details:

- r. Incident Documentation Template.docx
- s. Incident Impact Assessment Report Template.docx
- t. Incident Closure Letter.docx
- u. Incident Disclosure Form.docx

9. Appendix (if any)