

Phishing Playbook

**Authorised by** **:**

**Date issued or last reviewed/revised** **:**

**Date last exercised** **:**

# Table of Contents

[1. Table of Contents 2](#_Toc210211428)

[2. Document Control 3](#_Toc210211429)

[2.1 Document Revision 3](#_Toc210211430)

[3. Assumptions & Disclaimer 4](#_Toc210211431)

[3.1 Assumptions 4](#_Toc210211432)

[3.2 Disclaimer 4](#_Toc210211433)

[4. Background 5](#_Toc210211434)

[5. Objectives 8](#_Toc210211435)

[5.1 Proactive Response 8](#_Toc210211436)

[5.2 Quick Containment 8](#_Toc210211437)

[5.3 Effective Remediation 8](#_Toc210211438)

[6. Readiness 9](#_Toc210211439)

[6.1 General Readiness 9](#_Toc210211440)

[6.2 Prepare Phase Readiness 9](#_Toc210211441)

[6.3 Detect Phase Readiness 10](#_Toc210211442)

[6.4 Analyse Phase Readiness 10](#_Toc210211443)

[6.5 Contain Phase Readiness 10](#_Toc210211444)

[6.6 Eradicate Phase Readiness 10](#_Toc210211445)

[6.7 Recover Phase Readiness 11](#_Toc210211446)

[6.8 Post-Incident Handling Phase Readiness 11](#_Toc210211447)

[7. NIST Incident Handling Categories 12](#_Toc210211448)

[7.1 NIST Framework Incident Response Life Cycle 12](#_Toc210211449)

[7.2 Prepare 14](#_Toc210211450)

[7.3 Detect 16](#_Toc210211451)

[7.4 Analyse 19](#_Toc210211452)

[7.5 Contain 23](#_Toc210211453)

[7.6 Eradicate 26](#_Toc210211454)

[7.7 Recover 27](#_Toc210211455)

[7.8 Post-Incident 29](#_Toc210211456)

[8. Glossary 33](#_Toc210211457)

# Document Control

## Document Revision

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Issue Date | Changes |
| 0.1 | Name | XX/XX/2025 | Initial Draft |
| 0.2 |  | XX/XX/XXXX | Draft Review |
| 1.1 |  | XX/XX/XXXX | Final release |

# Assumptions & Disclaimer

## Assumptions

* This playbook must be followed by an experienced Incident Response Team
* This playbook is reviewed and updated as part of the post-incident review exercise at the end of each similar incident
* This playbook must be approved by the relevant stakeholders
* This playbook is accessible by the Incident Response Team
* Perform a continuous impact assessment during the incident treatment
* Additional logs collection might be required throughout the incident treatment

## Disclaimer

This playbook is to be followed by an experienced Incident Response Team. The steps defined in this document, in the different workflows available in the NIST incident handling categories section, are presumed to be validated and approved by the appropriate stakeholders in the organisation. In case of an incident falling under this playbook category, the Incident Response Team will follow the process described below and will presume that their actions are approved in applying the appropriate security control to reduce the threat identified.

Incident Response Teams must maintain their knowledge of products, processes, and systems and ensure access to systems is adequate and accessible in the event of an incident.

The organisation following this playbook must be aware of the applicable laws, regulations, and compliance obligations such as GDPR, PCI and NDB schemes etc.

# Background

Phishing is a variant of social engineering conducted over email and is considered a cybercrime. It is defined as a fraudulent attempt to obtain the target’s PII or other sensitive information, e.g., usernames, passwords, credit card details or other personal details. The attack occurs when an email is sent to the targeted recipients urging them to provide the above information by clicking on a malicious link, downloading an attachment that contains malicious content or sending a reply. Similar phishing attacks can also occur via text message (smishing) or over the phone.

Phishing emails may contain some of the features below[[1]](#footnote-1):

* Sense of urgency
* Hyperlinks
* Attachments
* Unusual sender
* Generic, non-specific topic of engagement, e.g. An invoice needs to be paid, but no mention of the terms or company involved

Phishing emails occur regularly, and organisations should review phishing attempts to determine if their staff are being specifically targeted or if the phishing emails are part of expected levels of unsolicited spam and opportunity-driven phishing campaigns.

This playbook should be followed once the organisation has determined that the impact of the phishing emails has warranted a security incident.

The following factors should be considered:

* Phishing emails originating from:
  + Internal staff to external parties
  + Internal staff to other internal staff
  + Trusted 3rd parties, partners, suppliers, and vendors to internal staff
* Phishing emails sent to:
  + Executives
  + Finance teams
  + HR teams
* If multiple staff have clicked on the links in the email
* If multiple staff have opened any attachments in the email
* If multiple staff have provided any corporate credentials while interacting with the email

According to NIST Special Publication 800-61 rev 2, an incident response process contains four main phases: preparation, detection and analysis, containment/eradication/recovery, and post-incident activity. Descriptions for each are included below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Prepare** | **Detect & Analyse** | **Contain, Eradicate & Recover** | **Post-Incident Handling** |
| The initial phase is where organisations will perform preparatory measures to ensure that they can respond effectively to incidents if and when they are uncovered.  This should also include regular testing of playbooks to ensure they are robust, easy to follow and incorporate any recent learnings | The second phase is where organisations should strive to detect and validate incidents rapidly because infections can spread through an organisation within a matter of minutes.  Early detection can help an organisation minimise the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organisation sustains as a result of the incident. | The third phase, containment, has two major components: stopping the spread of the attack and preventing further damage to systems. An organisation needs to decide which methods of containment to employ early in the response. Organisations should have strategies and procedures in place for making containment-related decisions that reflect the level of risk acceptable to the organisation. | Because the handling of Phishing incidents can be extremely expensive, it is particularly important for organisations to conduct a robust assessment of lessons learned after major Phishing incidents to prevent similar incidents from occurring. |

The Incident Response Plan (IRP) may contain references to the organisation-defined playbooks. The playbooks will define the steps to follow in case of a specific incident, in this playbook (Phishing). In case of an incident, it is recommended to refer to the IRP. If an incident response is covered in a playbook, the use of the playbook takes priority on the IRP.

This playbook will not cover the areas below that might already be available in the IRP.

The IRP may cover the areas below:

* Data Categories for Tracking Incidents
* Types of Incident Detection Channels
* Incident prioritisation matrix and triage process
* Incident Response Workflow
* Incident Root-cause Framework
* Incident response Lifecycle
* Incident Response Checklist (During)
* Post-Incident checklist (After)
* Incident Response Performance Metrics
* Incident Response Process/Procedures/Playbook List
* Roles and responsibilities
* Incident Response Team
* Incident Response Team Organisational Structures
* The communication process in case of an incident
* Checklist for Communicating with Media
* Incident Communication Memo to Employees - Template
* Sample Customer Notification Letter - Template
* Response Plan for Compromise of Personal Information - Template
* Incident evidence collection log

For any information related to the above, please refer to the Incident Response Plan.

# Objectives

## Proactive Response

A playbook helps security teams optimise their actions for efficiency and productivity. Your security team can plan and prioritise their actions in a methodical and repeatable fashion. Following a playbook, your team will have the best chance to respond and contain incidents when and where they occur.

## Quick Containment

Time and speed are crucial in assessing the environment and risk in the context of your business. Playbooks give a complete view of the necessary tasks to capture the data needed to support proper recovery and forensics. The efficiency a playbook brings to a security team allows for quick responses to finding the source of the attack, following lateral movement across the organisation, and taking the proper steps to mitigate damage.

## Effective Remediation

Playbooks facilitate security processes, mitigation plans, and smooth communication between multiple departments. By working methodically through data collection, analysis, and communications, you improve the odds for effective eradication, recovery with integrity, and forensic-quality reporting.

# Readiness

Incident Response Teams function in a state of constant readiness. A security incident can occur at any time of day or night so Incident Response Teams should always be prepared to respond.

A state of readiness involves checking their processes, procedures, tools, and access in the downtime to ensure that when an incident occurs, they are familiar with the processes and tools involved to reduce wasted time and effort.

## General Readiness

* Ensure that the organisation has an Incident Response Plan (IRP) that is up to date, reviewed, approved by the appropriate stakeholders, authorised by the appropriate executive, and communicated to the appropriate teams (Incident Response Teams, IT Support Team, IT Team).
* Ensure that the required playbooks to support the IRP exists or are being developed.
* Ensure that the playbooks and all required processes and procedures in responding to an incident are referred to in the IRP.
* Ensure that the organisation has a functioning knowledge base tool.
* Ensure that the required users have access to the organisation’s knowledge base.
* Ensure that the organisation has a training plan in place to upskill the employees in the required area that will speed up their reaction in dealing with a threat.

## Prepare Phase Readiness

* Ensure access to the breached systems.
* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incident are included in the knowledge base.
* Ensure access to the RACI matrix to identify the point of escalations.
* Ensure access to escalation paths.
* Ensure access to contact details (email, phone number) of the stakeholders designated as points of escalation.
* Ensure access to contact details (email, phone number) of the appropriate contact in the legal team.
* Ensure access to contact details (email, phone number) of the appropriate contact in the Governance and Compliance Team (GRC).
* Ensure access to contact details (email, phone number) of the appropriate contact in the marketing/communication team.
* Ensure access to contact details of vendors for the tools used and authority to engage vendor support teams where applicable and escalation contact details.

## Detect Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incidents are included in the knowledge base.
* Ensure that detection tuning learnings from previous incidents have been updated in the appropriate toolsets.
* Ensure toolsets are up to date.

## Analyse Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure toolsets are up to date.

## Contain Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure good functioning of firewalls and other network devices.
* Ensure that tools such as SIEM, IDS, Scanners, and Antiviruses are updated.
* Ensure that firewall rules are documented.
* Ensure access to the organisation’s risk framework, process, and acceptance criteria.
* Ensure access (read and write) to the organisation’s asset register to update the status of the affected assets.

## Eradicate Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the Incident Response Team is aware of the communication plan in the event of incidents.

## Recover Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incident are included in the knowledge base.
* Ensure that tools such as SIEM, IDS, Scanners, and Antiviruses are updated.
* Ensure that cloud services and other data stores are synchronised.
* Ensure that any network changes are documented.
* Ensure any existing related risks are reviewed, reassessed, and updated.
* Create any risk items identified.

## Post-Incident Handling Phase Readiness

* Ensure the required access and training in the tools needed in this phase to handle the incident.
* Ensure work instructions/processes/procedures required in this phase are up to date.
* Ensure that the learnings from the previous similar incident are included in the knowledge base.

# NIST Incident Handling Categories

## NIST Framework Incident Response Life Cycle

[[2]](#footnote-2)Lifecycle diagram from NIST Computer Incident Handling Guide SP 800-61 Revision 2

**Preparation**[[3]](#footnote-3)

Incident response methodologies typically emphasise preparation—not only establishing an incidentresponse capability so that the organisation is ready to respond to incidents, but also preventing incidentsby ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs.

**Detection & Analysis**[[4]](#footnote-4)

In the event of an incident, the Incident Response Team must detect and identify the type of incident occurring. In addition, it is necessary to collect the relevant data (logs, files, information) to be analysed. Once the above is completed, it is required to document the incident, prioritise it then communicate it to the appropriate authorities. The legal team of the organisation should be notified in the case of an event occurring that falls under the Notifiable Data Breaches (NDB) scheme.

**Containment, Eradication & Recovery**[[5]](#footnote-5)

Once the incident is identified, the Incident Response Team should be able to plan a strategy to stop the breach and reduce the risk of the threat spreading, therefore starting the recovery phase.

**Post Incident Activity**[[6]](#footnote-6)

Once an incident is resolved, the next step for the team is to go back to the beginning and prepare for the next incident; input from each new incident should help inform the preparation process, whether by adding new information about new threats or simply as a means of fine-tuning procedures that are part of the incident management process. Post-Incident Review is one of the main activities of this phase, and it includes the review and update of the incident playbook and the update of the knowledgebase.

Periodic risk assessments of systems and applications should determine what risks are posed by combinations of threats and vulnerabilities. This should include understanding the applicable threats, including organisation-specific threats. Each risk should be prioritised, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasise monitoring and response activities for those resources.[[7]](#footnote-7)

The objectives of using the NIST Framework are the following:

* A better understanding and management of cybersecurity risks
* A decrease in cybersecurity risks
* Prioritisation of cybersecurity activities
* Prioritisation in cybersecurity investments and maximisation of the impact of each dollar spent on cybersecurity
* Define a common language to communicate inside and outside an organisation
* Improvement of communications, awareness, and understanding between and among IT, planning, and operating units, as well as senior executives
* Defined cybersecurity posture

## Prepare

The initial phase is where organisations will perform preparatory measures to ensure that they can respond effectively to incidents when they are uncovered.

The organisation should have an Incident Response Plan (IRP) well documented, thoroughly explaining the roles and responsibilities of the employees/teams involved in the incident handling process. The plan must be tested to assure that your employees will perform as they were trained.

Additional procedures might be followed according to the organisation’s systems and service structure.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.2.1 | Determine Core Ops Team & Define Roles | Define roles and responsibilities in case of an incident and define the points of escalation | Incident Response Team and IT Team and Leadership team (CISO, CIO, CTO…etc) |
| 7.2.2 | Review and maintain a timeline | Create and maintain a timeline of events | Incident Response Team |
| 7.2.3 | Determine Extended Team & Define Roles | Define teams that are involved in the phishing Incident | Incident Response Team  IT Team |
| 7.2.4 | Define Escalation Path | Determine the list of stakeholders in case of escalation and define types of escalations | Incident Response Team |
| 7.2.5 | Request relevant logs and information | Collect the logs and relevant evidence related to the incident to identify its origin | Incident Response Team |

## Detect

The second phase is where organisations should strive to detect and validate incidents rapidly because infections can spread through an organisation within a matter of minutes. Early detection can help an organisation minimise the number of infected systems, which will lessen the magnitude of the recovery effort and the amount of damage the organisation sustains as a result of the incident.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| - | Define Threat Indicators | Decision box to illustrate the two paths possible (follow standard threat indicator or custom threat indicators) | Incident Response Team |
| 7.3.1 | Standard | An Indicator represents an atomic piece of information that has some intelligence value. There is a standard threat indicator that is predefined and makes the process smoother  Sub steps: 7.3.1.1 – 7.3.1.5 | Incident Response Team |
| 7.3.2 | Custom | An Indicator represents an atomic piece of information that has some intelligence value. There are custom threat indicators according to the type of incident or threat  Sub steps: 7.3.2.1 | Incident Response Team |
| 7.3.3 | Gather statistics on impacted recipients | Gather information on the phishing incident such as the list of employees impacted | Incident Response Team |
| 7.3.4 | Obtain copies of phishing emails including headers | Identify the phishing email causing the incident | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.3.1.1 | Unknown or unexpected network traffic from the store and headquarter locations | Detect any abnormal network traffic from the organisation’s sites, locations, stores, or headquarters | IT Team (Network Team)  Incident Response Team |
| 7.3.1.2 | Unknown or unexpected outgoing internet traffic | Detect any abnormal outgoing internet traffic | Incident Response Team  IT Team |
| 7.3.1.3 | Unknown or unexpected services and applications configured to launch automatically on system boot | Detect any abnormal services and applications programmed to launch on system boot | Incident Response Team  IT Team |
| 7.3.1.4 | Antivirus programs malfunctioning or becoming disabled for unknown reasons | Identify and list the antivirus installed that are not functioning properly or being disabled without the security team being notified | Incident Response Team  IT team |
| 7.3.1.5 | Degraded processing capability (increased CPU utilisation) | Check the CPU capability | Incident Response Team  IT team |
| 7.3.2.1 | Custom Indicators | An Indicator represents an atomic piece of information that has some intelligence value. There are custom threat indicators according to the type of incident or threat | Incident Response Team  IT Team |

## Analyse

During this phase, collected data and information is analysed to confirm the incident scope and impact and determine possible containment and eradication techniques and tasks.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| - | Define risk factors | Decision box to illustrate the two paths possible (follow standard risk factors or custom risk factors) | Risk Management Team (GRC)  Incident Response Team |
| 7.4.1 | Standard | Define standard risk factors according to the organisation’s risk management process and acceptance criteria that have a privacy impact, a business impact, and technical impact  Sub steps: 7.4.1.1 – 7.4.1.8 | Risk Management Team (GRC)  Incident Response Team |
| 7.4.2 | Custom | Define custom risk factor  Sub steps: 7.4.2.1 – 7.4.2.4 | Risk Management Team (GRC)  Incident Response Team |
| 7.4.3 | Research IOC (Indicators of Compromise) | Collect the sender’s email address, collect sending server details, collect URLs in the body of the malicious email, collect email attachments, collect and search for hash | Incident Response Team |
| 7.4.4 | Analyse (open) attachments included in phishing emails in a sandbox environment | Ensure to use of sandbox environment while dealing with malicious attachments | Incident Response Team |
| 7.4.5 | Analysis of evidence | Collect evidence of the incident and perform an analysis | Incident Response Team |
| - | Is the content of the email malicious | Decision box to illustrate the two paths possible | Incident Response Team |
| 7.4.6 | Go to the post-incident phase | Move to the post-incident phase if the email analysed does not contain malicious content | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.4.1.1 | IP is at risk of being exposed | Define if IP has been exposed | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.1.2 | PII is at risk of being exposed | Define is PII has been exposed | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.1.3 | Customers are affected by this incident | Identify customers that are affected | Risk Management Team (GRC)  Incident Response Team  IT Team |
| 7.4.1.4 | Public safety is affected | Identify if public safety is affected | Governance and Compliance team  Legal Team |
| 7.4.1.5 | Personnel safety is not affected | Check that personnel safety is not affected | Risk Management Team (GRC)  Incident Response Team  The leadership team (C level) |
| 7.4.1.6 | This act could be exploited for criminal activity | Make sure that the information exposed is not used for criminal activity | Risk Management Team (GRC)  Incident Response Team  The leadership team (C level) |
| 7.4.1.7 | This could harm the public brand | Document the incident and communicate it to the appropriate stakeholder and define the communication and legal approach | Legal Team  Communication Team  The leadership team (C level) |
| 7.4.1.8 | Products, goods, or services are affected by this outbreak | Detect and list the assets affected by the outbreak | Legal Team  Governance and Compliance Team |
| 7.4.2.1 | Business | Define business impact due to the incident | Risk Management Team (GRC)  Incident Response Team |
| 7.4.2.2 | Operational | Define operational impact due to the incident | Risk Management Team (GRC)  Incident Response Team |
| 7.4.2.3 | Compliance | Define the impact on the governance and compliance team due to the incident | Risk Management Team (GRC)  Incident Response Team |
| 7.4.2.4 | Industry | Define industry impact due to the incident | Risk Management Team (GRC)  Incident Response Team |

## Contain

The third phase, containment, has two major components: stopping the spread of the attack and preventing further damage to systems. It is important for an organisation to decide which methods of containment to employ early in the response. Organisations should have strategies and procedures in place for making containment-related decisions that reflect the level of risk acceptable to the organisation.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.5.1 | Additional Information Gathering | Identify the systems that have been affected, the data compromised, the IT services being impacted, the means through which malware gained access, the vulnerability is exposed, and the ways the attack spread  Sub steps: 7.5.1.1 – 7.5.1.7 | Incident Response Team  IT Team |
| 7.5.2 | Identify the staff who has access to malicious URL | List of employees targeted by the malicious email | Incident Response Team  IT Team |
| 7.5.3 | Identify the staff who opened malicious attachments | List of employees that have opened the malicious attachment | Incident Response Team  IT Team |
| 7.5.4 | Block malicious URLs on Web proxy | Ensure the blocking of the malicious URLs | Incident Response Team  IT Team |
| 7.5.5 | Consider email filtering based on IOC gathering | Proceed to email filtering to ensure the rejection of the malicious emails | Incident Response Team |
| 7.5.6 | Determine the level of communication | Consider the type and level of communication according to the spread and impact of the incident in the organisation | Incident Response Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.5.1.1 | Server | Check, isolate, and list servers that have been compromised | Incident Response Team  IT Team |
| 7.5.1.2 | Desktop | Check, isolate, and list desktops that have been compromised | Incident Response Team  IT Team |
| 7.5.1.3 | Laptop | Check, isolate, and list laptops that have been compromised | Incident Response Team  IT Team |
| 7.5.1.4 | Mobile | Check, isolate, and list mobiles that have been compromised | Incident Response Team  IT Team |
| 7.5.1.5 | VM | Check, isolate, and list virtual machines that have been compromised | Incident Response Team  IT Team |
| 7.5.1.6 | Layered controls | Containment steps can occur at the network, host, or application layer to obtain containment. E.g., firewall rules, host configuration changes, or application of a patch | Incident Response Team and IT Teams |
| 7.5.1.7 | Antivirus | Implemented and updated | IT Team |

## Eradicate

The fourth phase, eradicate, refers to the removal of the threat and its immediate recurrence.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.6.1 | Consider password rest | Impacted users must change their corporate credentials. They should also consider changing the password to personal accounts such as social media, banking, or email if they were accessed from the same workstation | Incident Response Team |
| 7.6.2 | Consider full AV scan | Perform a full antivirus scan | Incident Response Team  IT Team |
| 7.6.3 | Remove malicious email from contaminated recipient’s mailbox | Eradicate the malicious emails from contaminated mailboxes | Incident Response Team  IT Team |

## Recover

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact of a cybersecurity incident. Examples of outcome Categories within this Function include Recovery Planning; Improvements.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.7.1 | Consider education campaign | Promote education campaign | Incident Response Team |
| 7.7.2 | Consider organisation security awareness training | Organise security awareness training  Sub steps: 7.7.2.1 – 7.7.2.2 | Incident Response Team |
| 7.7.3 | Validation & Assurance | The following assurance considerations should be considered during the recovery phase:   * Perform a baseline vulnerability scan * Perform penetration testing * Ensure configuration adheres to best practice * Perform a code review if relevant * Document the findings gathered from the assessment above   Update the risk and issue registers with the findings and prioritised them | Incident Response Team  IT Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.7.2.1 | Prepare security awareness training material | Define the content of security awareness training with a focus on phishing | Incident Response Team |
| 7.7.2.2 | Define security awareness training schedule | Prepare a security awareness training schedule | Incident Response Team |

## Post-Incident

Because the handling of phishing incidents can be extremely expensive, it is important

for organisations to conduct a robust assessment of lessons learned after major phishing incidents to prevent similar incidents from occurring.



Below are the detailed descriptions of the steps referred to in the diagram above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.8.1 | Incident review | It is necessary to include an incident review in the Incident management process  Sub steps: 7.8.1.1 – 7.8.1.2 | Incident Response Team (IRP) |
| 7.8.2 | Lessons uncovered | Identify the items that require improvements such as policy updates, new controls to implement, new standards or frameworks to implement, etc  Sub steps: 7.8.2.1 – 7.8.2.4 | Incident Response Team |
| 7.8.3 | Lessons applied | Determine what worked well in the organisation’s incident response plan and opportunities for improvement. Lessons learned from both mock and real events will help strengthen systems against future attacks.  Sub steps: 7.8.3.1 – 7.8.3.3 | Incident Response Team |
| 7.8.4 | Response workflow updated | Check that the new configurations are in place via the performance of internal audits and following a continuous improvement process | IT Team  Incident Response Team |
| 7.8.5 | Update of the knowledgebase | Add the new processes or procedures used in this incident to the organisation knowledgebase | IT Team  Incident Response Team |
| 7.8.6 | Update Risk Register | Update the risk register to define the new level of the risk and define its new status | Incident Response Team  GRC Team |

Below is the second layer of the steps described above:

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Step** | **Description** | **Ownership/Responsibility** |
| 7.8.1.1 | Electronic Personal Health Information (ePHI) compromised? | Identify if Electronic Personal Health Information has been compromised as a consequence of this type of incident | Incident Response Team  IT Team |
| 7.8.1.2 | Sensitive information compromised? | Identify if sensitive information has been compromised as a consequence of this type of incident | Incident Response Team  IT Team |
| 7.8.2.1 | Discovery meeting | Once the investigation is complete, hold an after-action meeting with all Incident Response Team members and discuss what was learned from the phishing incident | Incident Response Team |
| 7.8.2.2 | Policy updates defined | Define the uplift required to improve the organisation’s security policies to embed them in the organisation | Incident Response Team  IT Team  Governance & Compliance Team  Leadership Team (C-Level) |
| 7.8.2.3 | Process updates | Update processes to ensure the inclusion of the new steps identified as missing to ensure an improved security posture | All organisation |
| 7.8.2.4 | Configuration updates defined | Implement the configuration updates as required to strengthen systems against future attacks | Incident Response Team  IT Team |
| 7.8.3.1 | Policies implemented | Once policies are updated, these have to be implemented and communicated within the organisation. Owners should be defined for each policy, and the review date should be determined | Policy Owners |

|  |  |  |  |
| --- | --- | --- | --- |
| 7.8.3.2 | Process changes implemented | Implementation of the uplifted or updated processes | Policy Owners  Organisational Change management Team  The project team in charge of the process update project |
| 7.8.3.3 | Configurations applied | Check that the new configurations are in place and following a continuous improvement process | IT Team |

# Glossary

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CTO: Chief Technology Officer

GRC: Governance Risk & Compliance

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

IR Team: Incident Response Team

IRP: Incident Response Plan

IT: Information Technology

LDAP: Lightweight Directory Access Protocol

Malware: Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network

MB: Megabyte

NDB: Notifiable Data Breach

NIST: National Institute of Standards and Technology

Procedure: A document written to support a specific process

Process: A series of actions or steps taken to achieve a specific end state

SIEM: Security Information and Event Management

SOC: Security Operation Centre

VM: Virtual Machine

1. <https://www.phishing.org/what-is-phishing> [↑](#footnote-ref-1)
2. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-2)
3. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-3)
4. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-4)
5. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-5)
6. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-6)
7. NIST Computer Incident Handling Guide SP 800-61 Revision 2: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [↑](#footnote-ref-7)