PHISHING Incident Response Procedure

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX..

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to Employees 3

1.3.1 Applicability to External Parties 3

1.3.1 Applicability to Assets 3

1.4 Related Documents / References 3

2. Procedure Statements 4

3. Procedures Steps 5

3.1 Identification 5

3.2 Investigation 5

3.3 Remediation 6

4. Procedure Compliance & Enforcement 8

4.1 Compliance Measures 8

4.2 Enforcement 8

5. Glossary / Acronyms 9

5.1 Glossary / Acronyms 9

6. Document Management 10

6.1 Document Revision Log 10

6.2 Document Ownership 10

6.3 Document Coordinator 10

6.4 Document Approvers 10

6.5 Distribution 10

# Introduction

## Document Definition

This document is a Procedure.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Objective

The objective of this procedure is to list out the steps the XXXX will take to detect, contain, remove and recover from a Phishing attack

## Scope

### Applicability to Employees

XXXX refers to XXXX. as well as its majority-owned subsidiaries and joint ventures (if applicable). This Procedure applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Procedure statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Procedure applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework.*
* *XXXX-PRC-ALL-006 - Incident Response Plan*

# Procedure Statements

Phishing remains one of the most well-known forms of Cyber-attacks to date. Although this form of threat has been in existence for a long time, the Cyber attacker of today has become very stealthy in their approaches. There are different variants of a Phishing attack, but in general, it can be defined as follows:

“Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, XXXXing, and credit card details, and passwords.

The information is then used to access important accounts and can result in identity theft and financial loss.”

Either the victim is sent a malicious attachment (such as a .XLS or .EXE file extension), or a malicious link to click on. It is important to note here that Phishing attacks have also become highly specialized, such as those of Spear Phishing and Business E-Mail Compromise (BEC). In these instances, a certain individual, or groups of individuals are specifically targeted.

However, whomever the target is, once the damage is done, efforts need to be taken to mitigate the damage and try to find ways so that these types of attacks don’t happen again.

The critical and sensitivity of the incident is determined in accordance with *XXXX-PRC-ALL-006 - Incident Response Plan and appropriate risk rating will be applied*

# Procedures Steps

## Identification

* Users report a suspected case of phishing attack to IT by calling extension 1234 or sending a mail to helpdesk @xxxx.com. This could also be discovered by periodic information security monitoring and reported to IT help desk
* The following information is collected about the suspected email/link:
* The E-Mail address of the sender;
* The intended recipient of the E-Mail;
* The Subject Line of the particular E-Mail;
* Carefully examine the E-Mail message, and if there is an attachment with it, make sure that you do not download it and if there is a link do not click on it.
* Triage:

If the above investigation discovers that an actual Phishing attack is underway, then the following steps must be accomplished:

* The specific kind of Phishing E-Mail it is. For example, is it a:
* BEC (Business Email Compromise)
* Spear Phishing (where one particular individual or individuals are targeted);
* Clone Phishing (where an original E-Mail message has been transformed into a malicious one);
* Whaling (this is similar to BEC, but primarily C-Level Executives are specifically targeted);
* Link Manipulation (this where a spoofed website is involved);
* Website Forgery (this is where JavaScript code is used to alter the URL bar maliciously);
* Covert Redirect (this when a website address looks genuine and authentic, but the victim is taken to a spoofed website);
* Social Engineering (this occurs typically in a business environment where lower-ranking employees [such as administrative assistants] are targeted and conned to give out corporate secrets);
* SMS (in these instances, wireless devices, primarily Smartphones are targeted, and malicious text messages are sent instead).

## Investigation

At this phase, the actual E-Mail message/ link and its contents need to be examined carefully, the and degree of damage needs to be ascertained. Regarding the former, the following must be investigated:

* Analysis of the E-Mail Header:
* The From Field: This will contain the name of the sender;
* X-Authenticated User: This will contain the E-Mail address of the sender (such as [johndoe@anywhere.com](mailto:johndoe@anywhere.com));
* The Mail Server IP Address: This will contain the actual TCP/IP address of the E-Mail server from where the Phishing E-Mail was sent. It is important to keep in mind as well that the physical location of the E-Mail server does not necessarily imply that the Cyber attacker is located in that geographic as well. Many times, they will be in a separate location from that of the E-Mail server.
* Analysis of the E-Mail message:
* At this phase, the actual contents of the E-Mail message need to be examined carefully, as there are many tell-tale signs which can be difficult to spot at first glance.
* Analysis of the Domain Link:
* If the Phishing E-Mail contains a suspicious link, as stated before, carefully examine the spoofed website, and determine where the data on the website is actually posted (such as the determining the TCP/IP address of the Web server that hosts the spoofed website, etc.).

With regards to the latter point in this part, the level and/or severity of the damage needs to be ascertained and ultimately determined. Examples of this include the following:

* The total number of impacted employees and systems
* What actions were carried out by the employees with regards to the Phishing E-Mail, for instance:
* Did they download an attachment;
* Alternatively, did they go to a spoofed website and unknowingly submitted their personal information, or even sensitive business login information.
* What was impacted:
* Servers;
* Workstations;
* Wireless Devices;
* The Network Infrastructure;
* Other aspects of the IT Infrastructure.

## Remediation

This is deemed to be one of the most critical phases; as this is where the damage of the Phishing attack will be contained. This will involve the following:

* After determining whom the impacted employees are, immediately change their passwords;
* After determining the impacted points in the IT Infrastructure, also immediately change login credentials of the people who have access to those particular resources as well;
* If the impacted points include Smartphones, immediately execute the “Remote Wipe” command to those affected Smartphones, so that any sort of sensitive information/data that resides on them will be deleted and cannot be accessed. In these instances, have your employees return the affected Smartphones back, and issue new ones with usernames and passwords;
* Run an anti-malware scan of the environment
* Infected systems that cannot be cleaned should be reformatted
* Continue to monitor all systems within your IT Infrastructure and all User Accounts for any misuse, or for any unusual anomalies that may be occurring.
* Prepare an incident report for the Security Committee

# Procedure Compliance & Enforcement

## Compliance Measures

Not applicable.

## Enforcement

All staff of XXXX must comply with all Information Security Procedures. Failure to comply with these procedures may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Glossary / Acronyms

## Glossary / Acronyms

|  |  |
| --- | --- |
| XLS | Excel |
| EXE | Executable file |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Procedure is owned by the YYYY

## Document Coordinator

This Procedure is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Distribution

* *IT*