Document Reference:	PIRP-1	Effective Date:	17 December 2023
Document Name:	Phishing Playbook	Expiry Date:	17 December 2024

Phishing Incident Response Playbook

Redback Operations

Document Owner:	Indiah Smith	Last Modified By:	Indiah Smith
Next Review Date:	17 June 2023	Last Modified on:	17 December 2023

Version	Modified By	Approver	Date	Changes made
1.0	Indiah Smith	Ben Stephens	17 December 2023	

Table of Contents

1 Introduction

1.1. Overview

A cyber incident must be responded to effectively by the organisation and an appropriate response mechanism must be executed to protect the systems, data and reputation of the company. The incident response playbook will provide assistance to incident response teams and stakeholders to ensure a consistent response and approach is used for rectification purposes following a cyber incident.

The playbook will provide guidance to the Cyber Incident Response Team (CIRT) in adherence with the (Cyber Incident Response Plan) CIRP.

It will describe the activities of the CIRT to effectuate a tailored response to phishing attacks.

1.2. Purpose

The purpose of the Phishing Incident Response Playbook is to provide guidance on executing an efficient and timely response to a phishing incident. It establishes the key stakeholders involved in the response and the activities that should be carried out in the detection, investigation and resolution phases.

1.3. Definition of Phishing

Phishing is a technique used by cyber criminals to provide personal information such as login details and credit card details through making their identity by acting as a legitimate business or person. Spear Phishing is used by attackers through acquiring information about employees and the company to provide an element of realism to their attack.

1.4. Scope

This playbook covers phishing attacks that directly impact the organisation through targeting associated affiliates and stakeholders such as employees and customers. This playbook does not cover cyber threats such as malware, data theft, virus outbreak, denial of service, unauthorised access, elevation of privilege, root access, improper usage or recovery playbooks. Please refer to each individual playbook for the appropriate tools and techniques to deal with the relevant attack.

1.5. Stakeholders and audience

This playbook shall be provided to the CIRT and may be used by the CIRT in addition to IT staff and other relevant personnel. Relevant stakeholders may include the SEMT, legal and compliance teams, HR teams, customer support teams and external customers. This playbook establishes the lines of communication and methods to effectively collaborate during the event of a phishing incident.

2 Phishing Summary

2.1. Phishing attacks

There are a variety of forms that phishing attacks may take. These include:

2.1.1. Spear phishing

Spear phishing refers to malicious emails that are sent to a specified person. Cybercriminals will already have access to personal details about a victim such as a name, employer, job title, email address and specific information about their role. These attacks are difficult to detect and can have detrimental effects such as theft of intellectual property or compromising assets.

2.1.2. Email phishing

Email phishing occurs when a cybercriminal registers a fake domain to replicate a real organisation through techniques such as character substitution or using reputable business names in their email addresses. They send generic requests via email that appear to be genuine.

2.1.3. Whaling

Whaling attacks are targeted at senior management using subtle techniques such as masking their identity by acting as management asking employees to carry out instructions. This plays on their willingness to do this without questioning the sender and their authority. Attackers carry out this attack to gain access to confidential information or execute fraudulent action with financial, legal and reputational effects.

2.1.4. Smishing and vishing

This attack method involves the use of telephones to communicate with victims. Smishing involves the use of text messages by attackers and vishing involves the use of a telephone

conversation. Attackers may use a text message including a link which will direct the victim to a website creature asking for banking credentials. Vishing involves the attacker imitating a bank employee asking for the victim's credentials through the use of phone calls.