**Phishing Incident Response Playbook**

**Developed by: Nikhil Makwana**

**Version: 1.0**

This document provides a structured approach for identifying, analyzing, and responding to phishing incidents in a corporate environment.

9/20/2024

**Introduction:**  
  
At XYZ Corp, phishing is one of the prevalent forms of cyber threats that my organization experiences. Phishing is a type of cyber fraud where the attackers try to lure employees into providing personal information such as passwords and account numbers. In this recent attack, the attackers used phishing emails that looked like they were from internal personnel, making the targets open a link. This action exposed personal data and credentials that are sensitive to our corporate security and at risk of being compromised.  
  
The attackers used such strategies as posing as official representatives of businesses and conveying the impression of urgency to make employees perform actions without questioning the credibility of the messages. These are some of the deception methods that are in concordance with the general idea of phishing that mostly uses emotional appeal to compel users lacking the kind of knowledge the phishing attack wants into making a wrong decision.

Typical phishing attack types are as follows:

* **Spear Phishing**: Specific and deliberate acts of violence against one or several people, or representatives of certain structures.
* **Whaling:** A specific kind of spear phishing assault aimed at the company’s top management or other key personnel.
* **Extortion Attacks:** These attacks leverage data stolen in a breach for the purpose of extorting money, although they may not necessarily contain links or attachments.
* **SPAM:** E-mails sent with the intention of getting a response without necessarily being malicious, but are sent in bulk.

**Analysis and Detection**

Phishing attacks are frequently discovered using a variety of methods:

* **User Reports:** Users forward emails that they deem to be suspicious to the IT security teams or through a phishing reporting mechanism.
* **Automated Systems:** Anti-phishing systems used in Office 365 are programs that offer the user alerts according to the contents or activity of the received emails
* **Direct Detection:** Employees in the IT department may receive phishing emails themselves.

Detection is important because the phishing attacks are known to go viral very soon. These incidents have to be addressed as soon as possible in order to evaluate their potential and the level of danger they pose.

**Information Acquisition (Level 1 Reaction)**

Security teams should collect the following information to categorize and address phishing incidents:

* **Scope of the Attack:** How many persons received the phishing e-mail? Are they from certain categories for instance students or staff?
* **Source of the Email:** Is the email sent from a genuine internal user’s account or is it from a malicious attacker?
* **Target of the Phish:** Is the phishing message being sent to people in a higher authority of the targeted organization?
* **Content and Intent:** Is there a message that has links or an attachment that looks rather dubious? Is this a case of job scam or is it another type of scam?

**Classification of Phishing Attacks**

The severity of phishing incidents can be used to classify them:

**Minor:** Few and easily recognizable phishing messages, unlikely to lead to significant losses. These incidents may be partially addressed by automation tools, lack of malware, or are not from inside accounts.

**Moderate:** Spam that is infectious or contains phishing links with a broader circulation that may contain malware or originate from an inside account. These are more likely to cause a financial or reputational loss.  
  
**Major:** Advanced persistent phishing attacks can cause significant disruption to operations by tricking a large number of users and are difficult to stop.

**Decisions on Escalation**

Escalation is determined by how serious the phishing attack is:

* **Minor Incidents:** Can be resolved at Level 1 or 2 without the involvement of the IT management.
* **Moderate to Major Incidents:** Should be forwarded to the IT management. In some cases, the IT incident response team may be called upon to help in the management of the situation.
* **Extreme Incidents:** In some circumstances, the IT incident response team may call upon the EOCG to come into play to handle the problem.

**Mitigation and Containment**

Depending on how serious the incident is, the following steps can be taken to lessen phishing incidents:

|  |  |  |
| --- | --- | --- |
| Consideration | Action | Severity |
| Inside Compromise | Disable compromised accounts and block suspicious IP addresses. | Minor |
| Identified Compromised Users | Deactivate compromised accounts right away. | Minor |
| Distribution of Malicious Content | Using Office 365’s feature of “search and destroy” to remove phishing emails from users’ inboxes. | Minor |
| Communication to Affected Users | Send email notifications or use IT ticket systems to alert users. | Moderate |
| Broader Communication | Put up notices on the intranet, IT portals, and on social networking sites like (Twitter, and LinkedIn). | Moderate |
| Internal IT Response | When a high-severity incident arises, activate the virtual war room and notify the IT leadership immediately. | Major |

**Pre-approved Communication Templates**

**User Response to Reported Phishing Attempt**

Subject: Phishing Attempt Reported  
  
Hello,  
Thank you for contacting the IT department. The message you reported is indeed a phishing attempt. It can be safely deleted. Please remember that phishing emails are generally harmless unless you click a malicious link or provide sensitive information.  
Here are a few tips to identify phishing messages:  
  
1. Any legitimate mass communications from the IT department will always be sent in form of official bulletins.

2. Phishing emails have language errors such as grammatical errors or even wrong information.

3. Phishing links often look different, for example, when the mouse is hovered over the link, it leads to a suspicious web address.

If you have further questions, feel free to reach out.

**Broad Communication to Users**

Subject: Beware of Phishing Alert: Take Quick Action!

Dear [Audience],

There have been numerous reports of phishing emails going around. These emails might ask you to confirm your account or click on links. Should you come across such correspondence, kindly remove it right away**.**

As a reminder:

* Never open any attachments from people you do not know or trust or click on any links that look suspicious to you.
* Avoid getting carried away with employment offers that you never expected or any strange request for payments.
* Check the authenticity of the sender as the email addresses used by the sender may be fake.
* Many scams contain elements of time pressure, so as with the previous tip, don’t rush into anything.

Thank you for your attention to this matter.  
Best regards,

**Business Continuity**

For XYZ Corp, this phishing incident did not reach the level where our company email services had to be disabled or business operations halted. The employees were informed immediately and email filters were modified to prevent the entry of any more such messages. Therefore, there were no serious inconveniences to the daily activities due to the efficient implementation of the plan. Nevertheless, if the situation had been more critical, we could have proceeded with more enhanced measures such as the suspension of access to certain systems to deal with the threat.

**Recuperation and Return to Regular operations**

After the mitigation of the phishing threat at XYZ Corp, there were no other steps in the recovery process that needed to be taken. Consequently, the incident response team conducted the analysis later to ensure that there were no more active threats. Weekly newsletters were prepared and delivered to all employees regarding phishing and encouraging them on the need to report any emails suspected to be phishing. These updates together with common security awareness campaigns will go a long way in preventing future incidences of phishing.