WhatsApp Phishing System

Date: 10 July 2024

Key Components Delivered By:

EVVO LABS	**DEVELOPER**
Phishing test template: Specially designed WhatsApp messages that will be sent to the employee.	A **fake website** hosted on **OZT.SG.**
	Tracking mechanism (refer to Track mechanism section below)
	Report: After the phishing test campaign, we will need to generate report on the test performance of the organisation. (refer to Reporting section below)

Steps to Engage Client

1) We will ask them about their commonly used websites (eg. google workspace, the HR portal, etc)
2) Ask client to provide a list of employees, their role, mobile number.
3) Ask client to have all employees sign an acceptance form where they agree to receive phishing test WhatsApp messages. This should be done about 1 month before the actual test.
4) We will inform the client that Whatsapp messages coming from a new company will be prompt the user to accept or report/block the number (this safeguard is activated when the security option is turned on in the WhatsApp setting)

Tracking Mechanism

- When employee click on a url of the WhatsApp phishing message, he will be redirected to this website (https://ozt.sg). We will record that as a "fail-clicked" in the database.
- When employee enters the credentials on the fake website, it will be recorded as "fail-responded" in the database.

To track which employee has clicked the phishing link and entered information on the fake website, you need to implement a method to uniquely identify each employee's interactions. Here's a detailed approach to achieve this:

1) Unique identifier in the phishing message
2) Hosting of fake website to prompt for credentials

Unique Identifier in the Phishing Message [This is for Internal Use. Developer use this for information to understand the full context of this system)

Each phishing message sent to an employee should contain a unique identifier embedded in the URL. This identifier will allow you to track the specific actions of each employee (which will be recorded in the database of the fake website)

Steps:

1. Create a unique identifier (unique-ID) for each employee.
2. Append this identifier to the phishing URL as a query parameter (e.g., `https://ozt.sg/login?id=unique-id`).
3. The unique URL will be shortened (using for example bit.ly) as https://bit.ly/login-xx (where xx is the unique ID of that employee)
4. Create a customized message for each employee

First Name	**Unique-ID**	**Whatsapp Phishing Message**
Alex	01	Hello Alex, we noticed some unusual activity on your account. Please verify your account by clicking on the link: **https://bit.ly/login-01**

Hosting Fake Website

Hosting the fake website with unique domain name (https://ozt.sg)

1) Create a portal where the user can enter their credentials. This website will ask employees to enter a username and password.
    a. [Developer] You can provide the basic login screen for us to test the functionality. When client provides the actual design requirement, we will request you to make that change. We will get input from the client regarding the design. Eg, we may provide the same look and feel of office.com login page.

2) The website will have a database which will capture the following information
    a. id: this is the unique ID of that employee (The unique ID is captured from the source URL https://ozt.sg/login?id=unique-id ; For example https://ozt.sg/login?id=01 the unique ID will be 01)
    b. failed-click date/time: when the employee first landed on the website because he clicked on the Whatsapp message link.
    c. failed-responded date/time: when the employee entered something into the credential text fields and pressed enter.

Reporting

- Create a reporting page in https://ozt.sg.com/admin-report
- In this page, allow the admin to download the report in CSV format (press a button to download)
- Generate the report using the information captured on the website database where each line will consist of (id, failed-click date/time, failed-responded date/time).

id	Failed-click date/time	failed-responded date/time