OKLAHOMA
Office of Management
& Enterprise Services

Simulated Phishing Campaign Standard

Introduction

The State of Oklahoma utilizes simulated, simulated phishing campaigns as a training tool to ensure all state employees and contractors understand their role in protecting the confidentiality, integrity and availability of state data. Organizations use phishing training exercises to help employees defend against the phishing threats that get through automatic email filters, reducing potential compromise of information security for both the individual and their organization. These exercises use fake and realistic phishing emails to test employees' ability to detect the phish.

Purpose

This document establishes the simulated phishing campaign standard for the State of Oklahoma. The purpose of simulated phishing is to heighten cybersecurity awareness and reduce susceptibility to email-based social engineering attacks. Users should report phishing email using the **Phish Alert Report** button from the home tab in Microsoft Outlook. If this is a simulated phishing campaign, users will be congratulated for correctly reporting the email. Users who action on the simulated phishing email (reply, forward, or click on any hyperlinked content) fail the simulated phish and will receive immediate, targeted education to help them better identify and respond to phishing schemes.

Definitions

User – All State of Oklahoma employees, contractors, board members or other persons authorized to connect to the state network.

Phishing simulation – An internal control testing methodology which simulates a real-life phishing attempt. Pushed enterprise-wide to gather metrics on click rates/trends to better inform the focus of training efforts.

Standard

The state will conduct quarterly phishing simulations. By providing simulated phishing exercises, the state can obtain a direct measurement of employee understanding, as well as progress in user behavior. Continuous email phishing assessments can be effective by indicating patterns of phishing vulnerabilities within a department and identifying further awareness training needs.

Any users who fail simulated exercises are required to complete additional training. Repeated failures may result in loss of access, referral to the agency's HR department and potential termination.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- Security Awareness Training Standard.
- How to Report a Phishing Email.
- NIST, Scaling the Phish: Advancing the NIST Phish Scale.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 08/24/2023	**Review cycle:** Annually
Last revised: 08/24/2023	**Last reviewed:** 04/03/2024
Approved by: Joe McIntosh, Chief Information Officer	