ENTERPRISE
information services

EIS Phishing Awareness Program

2024-2025

Table of Contents

Contents

EIS Phishing Awareness Program

The Cyber Security Services (CSS) Human Risk Management (HRM) - Information Security Awareness and Training (ISAT) program hereinafter referred to as HRM will oversee the implementation of the EIS Phishing Awareness Program and will coordinate with appropriate stakeholders (e.g., Data Center Services (DCS), the CSS Security Operations Center (SOC), *Agency Director(s), CIO(s), IT management and helpdesks, Human Resources, etc.) prior to onboarding their agency.

*Includes all state agencies within the Executive department as defined in ORS 174.112 includes but is not limited to agencies, state organizations, boards, and commissions, hereinafter referred to as Agency.

1.0 What is phishing?

"Phishing" is a social engineering attack using email intended to trick individuals into taking an action, such as clicking on a link, opening an attachment, or providing information. Phishing remains the number one attack method for cybercriminals because it often leads to success. Oregon state government employees are a target because they have access to sensitive and confidential information and access to information systems.

1.1 What is a phishing awareness program?

A phishing awareness program, also known as a phishing simulation program, phishing assessment program or self-phishing, is a customizable training and awareness program used by security awareness professionals in various industries.

This program allows Enterprise Information Services (EIS) / Cyber Security Services (CSS) to simulate phishing emails that can be sent to end users. Conducting these types of phishing attack simulations helps empower end users to make better decisions around email and can also help identify which end users are responsive in order to provide the opportunity for more focused training opportunities to help reduce organizational risk.

Phishing simulations can provide immediate feedback to the end user and produce reports and analytics about employee behaviors. Phishing simulations will progress over time with the use of Artificial Intelligence (AI) to challenge employees and keep them aware of relevant and emerging threats.

1.2 Why have a phishing awareness program?

A phishing awareness program is one of the few information security training techniques that can be easily measured and provides data to track behavior change over time.

The benefits include:

- Providing an established training process that can be implemented monthly as part of a more mature information security awareness program.
- Establishing a baseline for all end users and developing metrics that best suit the enterprise culture (e.g., click rates—how many click on the message and fall for the scam, how many report suspicious emails).
- Minimizing risk by training a broader population to be more aware of current phishing scams or threats and understand how to respond appropriately.
- Identifying end users frequently taking “undesired actions” and using that information to deliver targeted training where it is most needed, when it is needed.
- Leveraging end-user responses and metrics to identify gaps in existing security awareness materials and tailor materials to fit the training needs of the enterprise.
- Providing end users with real-time, tangible feedback.

- Offering end users, a sense of accountability (i.e., cybersecurity is everyone’s responsibility) and helping everyone be prepared for potential cyberattacks.

2.0 Agency Responsibility

2.1 Prior to Implementation

- Agencies will implement the Active Directory Integration (Provisioning).
- Agencies will implement the most recent method of allow listing approved by CSS and DCS for this program.
- Agencies will implement the Phish Alert Button for reporting suspicious emails.

  The Phish Alert Button (PAB):

  - Forwards the emails to an agency determined email address (retaining all header information so that the IT team can do analysis which is NOT retained when staff send the email directly).
  - Gives staff automatic feedback informing them whether the email they are reporting the EIS simulated phishing attack or a real phishing email.
  - Moves the email from their mailbox to their deleted folder.
  - Allows us to automate collection of data on phishing reports.
- Agencies will communicate with all staff about the upcoming program. Communication expectations details below.

2.2 Ongoing

- Agency will notify HRM immediately of any email filtering that would impact the phishing data.
- Agency will allow list all 10 Oregon Knowbe4 domains in any security service in your environment prior to deployment of said

service.

- Agency will notify HRM immediately of any plan for changes to email domains or any other changes that could impact the successful delivery of the simulated phishing emails.
- Agency IT teams will cooperate with HRM to trouble-shoot delivery issues of phishing simulations in their environment.
- Agency help desk will assist staff when staff cannot locate training assignment emails within the agency's environment.
- Agency will ensure that staff and management continually understand the ongoing expectations of the Phishing Awareness Program.
- Agencies who choose to use ReportAPhish must have an assigned POC for responding to agency staff if needed.
    - ReportAPhish is an email mailbox used for reporting suspicious emails and is monitored by the Security Operations Center.

3.0 Communications

What are the communication expectations for HRM and participating agencies?

3.1 Communication Expectations

- Agency leadership will be provided with access to program documents to ensure successful implementation prior to the phishing awareness campaign start date.
- Prior to onboarding their agency into the EIS Phishing Awareness Program, agency leadership will announce the following information to all employees:
    - Official start date of the EIS Phishing Awareness Program,
    - Program details,
    - How staff will be affected,
    - The necessity of this type of awareness program,

- Staff and Manager expectations.

- All statewide communications from HRM are reviewed by EIS Communications.

HRM communicates significant changes to the EIS Phishing Awareness Program by either making an announcement at Chief Information Officer Council (CIOC) or sending information to the CIOC Chair executive assistant to be disseminated to the CIOC members who will distribute the information within their agency using their standard communication methods.

3.2 New Employee Communication

- New employees will receive an automatic email notification of the EIS Phishing Awareness Program from the phishing vendor tool 2 weeks following their information being added to the agency's Active Directory.

3.3 Simulation Cadence

- Simulated phishing attack emails will be sent to employees at participating agencies from the phishing vendor tool. The simulated phishing attack emails will be sent once a month at random times during normal business hours 8:00am – 5:00pm Monday – Friday.

Sender	**Audience**	**Communication Type**	**Frequency**

HRM	CIOC	Program documents and updates	Prior to initial implementation;
			Program updates;
			As needed;

HRM	Director/ Agency leadership/ CIO	Introductory email to coordinate implementation, program documents can also be found on the CSS website.	HRM

		A private TEAMS channel is set up for each agency with all related documents as well.	
Agency communications team/channel	Management staff	EIS Phishing Awareness Program documents and CIO to manager email	2 weeks prior to implementation
Agency communications team/channel	All agency staff	Director to staff email and any communications documentation deemed necessary	1 week prior to implementation
Agency communications team/channel	All agency staff	Reminder of program start.	3 days prior to implementation
Phishing Tool auto notification	New agency staff	New employee notification of EIS Phishing Awareness Program	2 weeks following information added to Active Directory
HRM through phishing tool	All agency staff	Phishing simulations	monthly
HRM	CSS leadership	Enterprise phishing report	Quarterly
HRM	Agency leadership	Agency phishing report	Quarterly
Phishing Tool auto notification	Repeat Responders - Staff who have 4 or more responses to	Email notification of online training course enrollment. This notification (and refresher assignment) comes from the phishing tool – not Workday.	As refresher training is assigned; Reminder of incomplete assignment every

	phishing simulations		30 days
Phishing Tool auto notification	Manager of repeat responder(s) in Active Directory	Email notification of online training course enrollment. This notification (and refresher assignment) comes from the phishing tool – **not Workday**.	As refresher training is assigned; Reminder of incomplete assignment every 30 days

3.4 Program Documents

- EIS Phishing Awareness Program document – Agency Leadership signs this document as program acknowledgment and returns to HRM prior to implementation.
- EIS Phishing Awareness program kick off PowerPoint presentation.
- Email template: CIO to management
- Manager/Direct Supervisor Resource document
- Talking points/FAQ
- Learner/Team Dashboard Overview
- How to spot a phish printable
- Phishing one pager
- Email template: Director to staff
- Phishing program PowerPoint presentation for staff

4.0 Enterprise Implementation

The EIS Phishing Awareness Program has been implemented in phases.

- Phase 1 (Q3 2019): Monthly phishing simulation emails sent to EIS employees for testing purposes.
- Phase 2 (Q4 2019): Monthly phishing simulation emails sent to all DAS employees for testing purposes. Emails staggered within one week each month to all DAS employees.
- Phase 3 (Q1 2020): Monthly phishing simulation emails sent to agencies as determined. Emails staggered across each month, ongoing for all included agency staff.
  - Phased implementation was interrupted due to COVID and vendor change.
- Subsequent phases follow the M365 implementation schedule until all executive branch employees receive monthly phishing simulation emails on an ongoing basis.
  - Agencies outside of the executive branch but within state of Oregon government can be included in the EIS Phishing Awareness Program at the discretion of CSS leadership.

5.0 Strategy and Concept

Employees will receive phishing simulation emails that resemble real phishing attacks.

5.1 Phishing Simulation Email Traits

- Used for monthly testing.
- All new and existing employees receive them.
- Simulations will vary in complexity. Simulations may use AIDA Selected phishing templates. This feature uses data from KnowBe4's Artificial Intelligence Driven Agent (AIDA) to select the most relevant and challenging template for each user. AIDA Selected templates are chosen based on a user's training history, phishing events, and performance metrics, such as their Phish-prone

percentage. Simulations will spoof managers, leadership, and the organization.

6.0 Employee Engagement

What happens when an employee responds to a phishing simulation email by clicking on a link, opening an attachment, replying, forwarding or providing information?

6.1 Every time staff responds.

When an employee responds to a phishing simulation email, they will be directed to a landing page and provided with feedback. The feedback informs the employee they responded to a simulated phishing attack email, provides information on how they could have detected it, and how to avoid falling for these types of attacks in the future.

Staff are directed to **use the Phish Alert Button to report suspicious email.** They should follow the same process whether they believe they've received a real or simulated phishing email.

6.2 Fourth response

Employees who have responded four or more times to simulated phishing emails will be considered "Repeat Responders" and assigned a phishing refresher training course. The notification of the training assignment comes in an email from the phishing tool **(not Workday)**. The email contains a link which the staff use to access the training. Staff may also log in to their Learner Dashboard at Knowbe4.com.

An email notification of the training assignment goes to the employee's manager as well. The employee's manager information must be included in the agency's Active Directory data for notification of training assignment to be sent.

Managers have access to each individual's phishing and training data in their team through the “Knowbe4 Team Dashboard”. Managers can log in to Knowbe4.com to access their Team Dashboard.

The expectation of the employee’s manager is to have a conversation with the employee regarding continued phishing simulation responses. The goal of the employee and manager engagement is to better understand why the employee is still responding to potential phishing emails as well as to provide additional best practices around phishing. Please refer to the CSS website and the program documents for phishing resources if needed.

Employees and managers need to be aware of and follow any internal agency policies and procedures they have in place, as they relate to phishing.

6.3 Learner/Team Dashboard

- All staff can login at Knowbe4.com to access their phishing data via the Learner Dashboard. Information can be located on the attached Learner/Team Dashboard Overview document.
- Any individual in a supervisory position may access their direct reports phishing data through the Knowbe4 Team Dashboard. Please review the Learner/Team Dashboard Overview document for more information.

7.0 Reporting

- HRM will provide aggregate agency data to agency leadership and enterprise data to CSS leadership quarterly.
    - HRM does not release phishing data to any other entity(s). All requests for phishing data shall be directed to agency leadership directly.
    - HRM includes data from the Phish Alert Button with the quarterly data provided to CSS leadership and agencies.

- HRM will be providing emailed reports to agency leadership on a request only basis. Please have agency leadership contact security.training@das.oregon.gov for a request form.
- HRM permits Knowbe4 reports access to one user per agency, designated by the agency Director. Please have agency leadership contact security.training@das.oregon.gov to designate agency reports user.

ACKNOWLEDGEMENT
[Agency Name]

By signing below, I acknowledge that I fully understand the information concerning the DAS EIS/CSS ISAT Phishing Awareness Program in the attached document and agree to comply with the communication plan and agency requirements therein.

Signature: **Date:**

______________________________ ______________

[NAME], EIS/CSS Risk & Governance Director

______________________________ ______________

[NAME], Agency CIO or equivalent

______________________________ ______________

[NAME], Agency Director or equivalent