Phishing Awareness Program Expectations

2020-2021

Table of Contents

Phishing Awareness Program

The CSS Information Security Awareness and Training (ISAT) program hereinafter referred to as ISAT will oversee the implementation of the 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, Labor, etc.) prior to onboarding their agency.

*Includes all state agencies within the Executive department as defined in ORS 174.11 includes but is not limited to agencies, state organizations, boards and commissions, hereinafter referred to as Agency.

1. What is phishing?

“Phishing” is a social engineering attack using email or a messaging service to send messages 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 type of phishing attack simulations help identify which end users or programs are responsive and provides 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 and program behaviors. Phishing simulations will progress over time 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:

1. Providing an established training process that can be implemented monthly as part of a more mature information security awareness program.
2. Allowing for targeted phishing campaigns using unique scenarios or variables (e.g., attachments, embedded links, or requests for personal information) for high-risk end user groups (e.g., new employees, staff dealing with financial transactions or employee records, stewards handling highly sensitive data, IT staff with admin privileges).
3. 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).
4. Minimizing risk by training a broader population to be more aware of current phishing scams or threats and understand how to respond appropriately.
5. Identifying end users frequently taking "undesired actions" and using that information to deliver targeted training where it is most needed, when it is needed.
6. 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.
7. Providing end users with real-time, tangible feedback.
8. Offering end users a sense of accountability (i.e., cybersecurity is everyone's responsibility) and helping everyone be prepared for potential cyberattacks.

1.3. How to gauge the effectiveness of the Phishing Awareness Program?

In order to gauge the effectiveness of the Phishing Awareness Program we must not only look at click rate and reporting but also at the security culture of our organizations and the enterprise as a whole. Security culture is defined as the ideas, customs, and social behaviors that impact the security of your organization.

We track click rates and reporting as an indicator of positive behavior change. We track security culture in order to see how including phishing awareness has impacted the security culture of your organization.

A survey is used to measure security culture. It is sent to all staff in an organization 90 days after initial implementation of the Phishing Awareness Program and annually thereafter. This information is used to establish a baseline for your security

culture, to make changes as necessary, and to track the way your culture evolves over time.

The results of the survey will provide a breakdown of the seven dimensions that make up your agency's security culture, as well as an overall security culture score for your organization.

The seven dimensions are:

- Attitudes
- Behaviors
- Cognition
- Communication
- Compliance
- Norms
- Responsibilities

More information on security culture can be found in the program documents.

2. Communications

What are the communication expectations for ISAT and participating agencies?

2.1. Communication expectations

1. Agency Directors and Chief Information Officers (CIOs) will be provided with access to program documents to ensure successful implementation prior to the phishing awareness campaign start date as per the Phishing Awareness Program Expectations.
2. Agency Directors and CIOs will announce the official start of the Phishing Awareness Program to all agency employees prior to onboarding their agency into the Phishing Awareness Program. Employees will be informed prior to their agency being on-boarded into the program of what the program entails, how they will be affected and why this type of awareness program is necessary.
3. All additional statewide communications from ISAT will be reviewed by EIS Communications and the Department of Administrative Services (DAS) Communication Officers. ISAT sends communication concerning initial implementation and any significant changes to the Phishing Awareness Program to the CIO Council Chair executive assistant to be disseminated to the CIO Council members who will distribute the information within their agency using their standard communication methods.

4. Prior to implementation of the Phishing Awareness Program at participating agencies, the ISAT will coordinate with agency Directors, CIOs, and/or leadership and agency help desks for any upcoming phishing simulation campaigns to ensure the simulation vendor is whitelisted and to ensure help desks are aware of the potential influx of calls or emails.

   Agencies will whitelist following instructions from the phishing vendor for any and all spam filtering appliances and web filters in use. Agency will revisit whitelisting at the time of any updates to said systems.

5. A security culture survey and phishing simulation emails will be sent to employees at participating agencies from the enterprise phishing simulation tool. The 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**
ISAT	CIOC	Program documents and updates	Prior to initial implementation; Program updates; As needed;
ISAT	CIO/Director/ leadership	Introductory email to coordinate implementation, program documents are located at: https://www.oregon.gov/das/OSCIO/Pages/Securityresources-ag.aspx#securityresources8	Prior to implementation
Agency communications team/channel	Management group	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
ISAT	All agency staff	Security culture survey	90 days after implementation and annually thereafter

Agency communications team/channel	All agency staff	Reminder	3 days prior to implementation
Agency IT Helpdesk	ISAT	Traffic report (total number of tickets attributed to phishing including simulation campaign)	Monthly
ISAT	Agency leadership & CSS leadership	Security culture report	Annually
ISAT	CSS leadership	Enterprise phishing report	Quarterly
ISAT	Agency leadership	Agency phishing report	Quarterly
ISAT	Manager of repeat responder(s)	Email notification of online training course enrollment	As needed

2.2. Program documents

- Phishing Awareness Program Expectations
- Phishing program kick off PowerPoint presentation
- Email template: CIO to management
- Talking points/FAQ
- How to spot a phish poster
- Phishing one pager
- Email template: Director to staff
- Phishing program PowerPoint presentation for staff

Located at: https://www.oregon.gov/das/OSCIO/Pages/Securityresources-ag.aspx#securityresources8

3. Implementation

The Phishing Awareness Program will be implemented in phases.

- Phase 1 (Q3 2019): Monthly phishing emails sent to EIS employees for testing purposes.
- Phase 2 (Q4 2019): Monthly phishing 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 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 will follow the M365 implementation schedule until all executive branch employees receive monthly phishing 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.

4. Strategy and Concept

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

4.1. Phishing simulation email traits

- Slightly above what is considered SPAM
- Used for monthly testing
- All new and existing employees receive them
- Simulations will vary in complexity

5. Employee Engagement

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

5.1. First through fourth responses

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 phishing simulation email, provides information on how they could have detected it, and how to avoid these types of emails in the future.

Staff are directed to **follow their agency's current reporting process.** They should

follow the same process whether they believe they've received a real or simulated phishing email.

5.2. Fourth response

Employees who have responded to four or more phishing simulation emails in a rolling12-month period will be assigned an online training course. If the manager information is included in the Active Directory Integration data an email notifying the employee's manager of the employee's training requirement will be sent. This information is also available in the reports console of the phishing tool.

The employee's manager shall have a conversation with the employee regarding phishing attempts. 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.

It is up to the discretion of the agency to enter completion of phishing trainings in the agency's Learning Management System of record.

6. Reporting

6.1. ISAT responsibility

- ISAT will provide agency data to agency leadership and enterprise data to CSS leadership quarterly.
- ISAT will include data from agency help desk phishing reports as well as reports sent to ReportAPhish@oregon.gov with the quarterly data provided to CSS leadership and agencies.

6.2. Agency responsibility

- Agency will notify ISAT immediately of any filtering that would impact the phishing data.
- Agency help desks will track the number of phishing reports received.
- Agencies will provide help desk phishing report data to ISAT monthly.
- Specified agency staff will have access to their agency's reporting console in the phishing tool.

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 GRC Director

_____ _____

[NAME], Agency CIO or comparable

_____ _____

[NAME], Agency Director or comparable