Talking points

"Protect your Information and mine"
The phishing awareness program will help State of Oregon employees become even better stewards of State data.
The phishing awareness program allows us to "self-phish" and identify how we can better protect state data.
The phishing awareness program provides useful, relevant, and actionable training for State of Oregon employees.

FAQ

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.

Why is this program happening?
This program will help increase information security for the State of Oregon by teaching employees how to identify a malicious phishing email and take appropriate action. As a result of the training, State of Oregon Employees will be even better stewards of Oregonian's data.

What happens if I click on a link?
When an employee responds to a phishing simulation email, they will be directed to 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.

What is the difference between a phishing simulation email and a regular phishing email?
The difference is Enterprise Information Services (EIS) phishing simulation emails will not harm our staff or expose the state's data in any way. They are designed to increase awareness and provide training. This program will help us identify how many employees are responding to phishing emails by clicking on potentially malicious links and how many report the suspicious emails.

What do I do when I receive a suspicious email?
When you receive a suspicious email, real or simulation, use the Phish Alert Button (PAB) on your Outlook toolbar. If you do not have the PAB, please contact security.training@das.oregon.gov

Who is receiving the phishing simulation emails?
Eventually, all Executive Branch agencies will be receiving the phishing simulation emails. The rollout of the program began in Q3 2019 with EIS and then extends to all other state agencies. The program is being rolled out in the following phases:

- Phase 1: Q3 2019 – EIS
    - July: CSS pilot
    - August-September: all of EIS
- Phase 2: Q4 2019 – DAS
- Phase 3: Q1 2020 - Selected agencies
- Phases will continue until all Executive Branch agencies are included

What are the consequences if I click on a link in one of the phishing simulation emails?
Employees that continue to respond to multiple phishing simulation emails will receive increased training and feedback to help raise their awareness of phishing threats. No punitive action will be taken by CSS.
It is up to the agency to consider limiting phish-prone users' access to certain applications or websites and increasing their security configurations and security-related applications if they continue to prove to be a vulnerable employee.

How will the increased training be administered?
We have an automated training campaign that will assign your repeat responders additional security training. The training is delivered to employees directly from Knowbe4 immediately following the 4th click/fail and with each additional click/fail.
A notification of the training assignment will be automatically sent to the manager if the manager information is in your agency's Active Directory data. The staff & manager will receive a reminder every 30 days until the training is complete.

How long will this be going on?
Once the program is rolled out to all Executive Branch agencies, the training program will be ongoing.

Will the results of the program be recorded somewhere?
CSS Information Security Awareness and Training Coordinator will be providing quarterly reports to all agency directors and CIOs that identify the risks within their agency related to phishing.

What is included in the report?
The reporting will include the phish prone % for each agency by campaign/month.

A phishing campaigns phish-prone percentage is calculated based on the number of total failures (clicks, attachment opens, data entry, replying) divided by the total number of emails delivered in that campaign.

For example, if 100 people received emails, and 52 of them clicked a link in the email and eight of those users also entered data into the landing page, the Phish-failure Percentage for that campaign would be 60%.

Staff and manager/supervisors can login to Knowbe4 at training.knowbe4.com/ui/login using their state of Oregon email address to access their own and their staff's phishing and phishing training data.

One staff member designated by the agency Director may be granted Knowbe4 reports access. Please contact security.training@das.oregon.gov to get that set up.