EIS Phishing Awareness Program updates for 2024-2025

The EIS Phishing Awareness Program is a service provided by the Human Risk Management (HRM) program in Cyber Security Services (CSS) to all executive branch agencies. This program allows us to simulate phishing emails that can be sent to staff. Conducting these types of phishing attack simulations helps empower staff to make better decisions around email and can also help reduce organizational risk by identifying potential gaps in our training and/or communication.

Most recent updates include:

1. **Access to a Learner and Team Dashboard:** All staff are able to log on to Knowbe4.com with their state email address to view their phishing data; managers are able to access a dashboard for their team.
    a. **Monthly awareness content** will be available in the messages tab of the learning dashboard starting March 2024.
2. **New hybrid Phish Alert Button (PAB):** All staff should have a PAB installed on their Outlook toolbar. The PAB is your first step after identifying a suspicious email. It will confirm if an email is a simulation or not and will forward valid (non-simulation) emails to the appropriate IT department.
3. **Clarifying agency expectations:**
    a. Agencies are required to cooperate with Cyber Security Services (CSS) to allow successful delivery of phishing simulations and phishing email notifications within their environment.
    b. Agencies shall ensure that staff and management continually understand the ongoing expectations of the program,
    c. Agencies that choose to send their reported phishing emails to the CSS SOC “ReportAPhish” inbox must have an assigned POC for responding to agency staff if needed.
4. **Simulations use phishing templates selected by KnowBe4’s Artificial Intelligence Driven Agent (AIDA)** which selects the most relevant and challenging template for each user.
5. **Forwarding has been added as a simulation failure type.** Forwarding a potentially malicious email is not recommended and we cannot prevent scanning of suspicious links once they are inside our environment. Staff are

directed to use the PAB to report suspicious email. They should follow the same process whether they believe they've received a real or simulated phishing email.

More information about the EIS Phishing Awareness Program can be found on the CSS website:
https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-phishing-awareness-program-expectations.pdf

https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-phishing-awareness-program-learner-and-team-dashboard-overview.docx

https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-phishing-hybrid-Phish-Alert-Button-info.pdf

Questions? please contact security.training@das.oregon.gov