**To**: [AGENCY NAME] Employees

**From**: [AGENCY DIRECTOR OR CIO]

**Subject**: Phishing Awareness Program

The State of Oregon takes information security very seriously. To help ensure our staff understand agency expectations, and what they can do to help protect themselves and our organization, the [AGENCY NAME] will be expanding their security awareness and training program to include a phishing awareness program.

**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 to increase staff awareness around suspicious emails. It’s designed to help individuals identify and change risky behavior.

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.

Beginning in [MONTH], our employees will begin receiving simulated phishing emails that resemble the same malicious emails the cyber criminals are sending every day.

**What’s the difference?**

The difference is that the phishing simulation emails will not harm our staff in any way. They are designed to increase awareness and provide education. This training 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 to expect**

When you receive a phishing email, follow the steps below:

1. Don’t respond to the email or click any links.
2. Follow your current agency process for reporting suspicious emails.
3. Delete the email

It’s that easy!

For a refresher on how to spot a potential phishing email, check out the poster below.

***Questions?***

*Contact Enterprise Information Services (EIS), Cyber Security Services (CSS) by emailing* *security.training@oregon.gov**.*

