Table of Contents

Strategy and Concept

The purpose of the EIS Phishing Awareness Program is to:

- Reduce the likelihood that staff will fall for a phishing scam.
- Ensure that staff look for suspicious elements in every single email that they receive.
- Increase the number of staff that report suspicious emails.
- Improve the security culture of the enterprise

We do that by:

- Providing monthly simulations that are a safe way to practice the behavior that we want to see.
- Providing the Phish Alert Button (PAB) which is an easy and safe way to report suspected phishing attacks.
- Providing engaging refresher courses that increase retention of the content.
    - Refresher courses are not meant to be a punishment. They are meant to be enjoyable and brief.
- Providing manager engagement at each level to support staff if they are experience issues around phishing.

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?

1. Employees who have responded four or more times in a rolling 12-month period to simulated phishing emails will be considered Repeat Responders and assigned a phishing refresher training course.
    a. The notification of the training assignment comes in an email from the phishing tool **(not Workday)**, a sample notification email is provided in the appendix.
        i. The email contains instructions to login to Knowbe4 (training.knowbe4.com/ui/login) which the staff use to access the training.
    b. Employees are expected to complete the refresher course. We recommend that they save the completion certificate for their records.
2. Employees will be assigned an additional phishing refresher course assignment with each corresponding simulation response of four or more in a 12-month period.
3. Reminder notifications are auto-generated every 30 days until completion.

Manager/Direct Supervisor Engagement

What is the expectation of the manager/direct supervisor when the staff that they manage reach the Repeat Responder level in the phishing program?

1. An auto-generated email notification of the training assignment goes to the employee's manager/direct supervisor as well as the employee.
    a. The employee's manager/direct supervisor information (name and email) must be included in the agency's Active Directory data for notification of training assignment to be sent.
2. Managers/direct supervisors have access to each employees phishing and training data in their team through the "KB4 Team Dashboard".

   a. They can access the dashboard by logging in to Knowbe4 with their state of Oregon email address (training.knowbe4.com/ui/login).
3. The expectation of the employee's manager/direct supervisor is to have a conversation with the employee regarding continued phishing simulation responses.
   The goal of the employee and manager/direct supervisor 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 contact security.training@das.oregon.gov for additional phishing resources if needed.

Manager/Staff Phishing Awareness Repeat Responder talking points

1. Have you completed the assigned refresher training?
   a. Yes, that's great!
      i. Do you have any questions about it?
      ii. Did you print the certificate of completion for your records?
      iii. Would you like to review the "How to spot a phish" flyer with me or do you feel like you have a good understanding of the material?
      iv. Is there anything else that I can do to support you?
   b. No,
      i. Are you having trouble accessing the training?
         1. Staff can access the dashboard with their phishing data and any course assignments by logging in to Knowbe4 with their state of Oregon email address (training.knowbe4.com/ui/login).
      ii. Is there another reason that you haven't completed the training?
      iii. Let's set some time aside today and get that completed. It is a very short video/course. Let me know if you have any questions and be sure to save the certificate of completion for your records.

2. There are a lot of reasons why people fall for phishing scams. They are crafted in a way that tricks people into clicking. That is why we have the EIS Phishing Awareness Program; it allows you to have a safe environment to practice these skills.
3. We don't want you to feel bad because everyone is a potential victim of cyber-attack but want to do everything that we can to avoid falling for it in the future. It is important to pay attention to key items in every email that you receive. It only takes a few seconds, but it can prevent a security incident.

What to look for in every email we receive & how to respond:

1. Do I know the sender?
   a. Am I expecting this request from them?
   b. Is the signature block overly generic or doesn't follow company protocol?
   c. Does the sender address match the sender's name? if not, be suspicious.
2. Tone of the email – you know how your co-workers talk, does the tone sound strange?
   a. Watch out for emotions:
      i. Is there a sense of urgency?
      ii. Greed – are they offering you something?
      iii. Fear – is the email threatening or scary
      iv. Curiosity – scammers often take advantage of our curiosity, watch out for that.
3. Common indicators:
   a. Unusual attachments – if you're not expecting it, always verify with the sender by phone.
   b. Log-in pages – be suspicious of any email asking you to log in with credentials. Always use the official website to log in.
   c. Links – roll your mouse over a link to see the URL. Does it match what's in the email? If not, don't click.
4. Suspicious email on your mobile device:
   a. We don't recommend engaging with suspicious email at all with a mobile device. If you must then please delete the email without any other engagement.

i. Do not click on anything, open anything, enter anything, or reply.

b. Wait to hover over links until you are at your workstation – you are much more likely to click while using a mobile device.

c. The Phish Alert Button (PAB) is not available on your mobile device – wait until you're at your workstation so that you can report the suspicious email using the PAB.

5. If you see something, say something!

a. Report suspected phishing emails using the PAB on your Outlook toolbar.

b. If your staff have accidentally fallen for a phishing scam, it is imperative that they report it to your agency's IT team or to you, as their manager/direct supervisor. The faster that incidents are reported the faster they can be mitigated.

Note:

If staff do not trust that they are safe to report incidents when they happen, then we are part of the problem.
No one is immune to falling victim to phishing and it does no good to shame our colleagues when it happens.
In fact, it is counterproductive.

Phishing refresher course details

Staff will receive an assignment to the Phishing refresher course level 1 upon the 4th simulation failure. They will receive an additional refresher course assignment with each additional simulation failure.

Below is a list of the course names and course lengths associated with each level:

Level 1 – 4 failures
Course title: To Click or Not to Click – 3 minutes
Level 2 – 5 failures
Course title: How to Spot Phishing Scams – 3 minutes
Level 3 – 6 failures
Course title: Phish Catcher Game – 7 minutes
Level 4 – 7 failures

Course title: Phishing Your Inbox – 10 minutes

Level 5 – 8 failures

Course title: Basics of Phishing (with Quiz)

Level 6 – 9 failures

Course title: Phishing Foundations – 15 minutes

Level plus – 9+ failures

Course title: Social Engineering Red Flags with Jenny Radcliffe – 17 minutes

The course list above is for reference only.
Courses are subject to change at any time.
They are replaced in campaigns when they are set to retire by the vendor.

Managers can view the above courses in Workday for reference without a course assignment.

Viewing of a refresher course in Workday does NOT remove a course assignment in the Knowbe4 platform. Always advise staff to follow the instructions in the notification email to access their refresher course assignments in the Knowbe4 platform.

We are all in this together.
By supporting each other with understanding we can build a stronger security culture in the state of Oregon.

For more information, please contact security.training@das.oregon.gov

Appendix

Links to sample EIS Phishing Awareness Program notification emails:

Notification to staff – New employee (2 weeks after being added to the agency's Active Directory)
https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-phishing-awareness-program-new-employee-notification-email.pdf

Notification to staff – New course assignment
https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-phishing-awareness-program-new-assignment-staff-email.pdf

Notification to staff – Reminder of past due assignment
https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-phishing-awareness-program-assignment-reminder-staff-email.pdf

Notification to manager – New course assignment
https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-phishing-awareness-program-new-assignment-manager-email.pdf

Notification to manager – Reminder of past due assignment
https://www.oregon.gov/eis/cyber-security-services/Documents/eis-css-phishing-awareness-program-assignment-reminder-manager-email.pdf

How to spot a phish printable:

How to Spot a Phish

Finding the phish 101 with Professor Troy

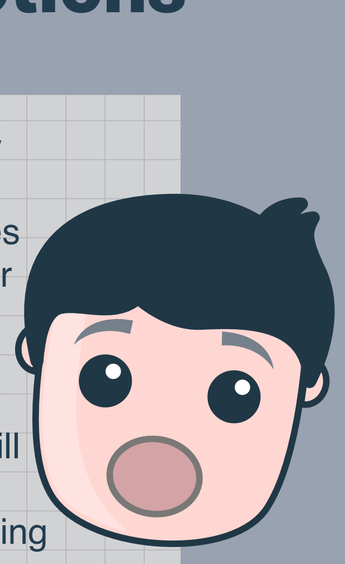
Lesson 1: Watch out for emotions

Greed

Phishing emails often dangle a financial reward of some kind if you click a link or enter your login information. If an email offers you something that seems too good to be true, it probably is.

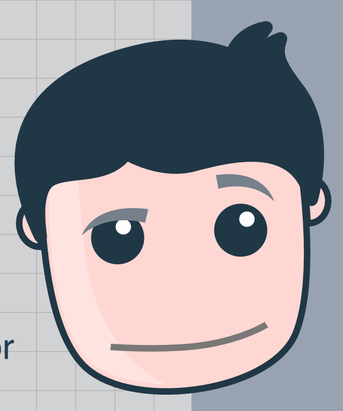
Urgency

If an email provides a strict deadline for performing an action -- be suspicious. Phishing emails will try to fluster recipients by creating a sense of urgency.



Curiosity

People are naturally curious, and phishers take advantage of this by sending emails that promise to show us something exciting or forbidden.



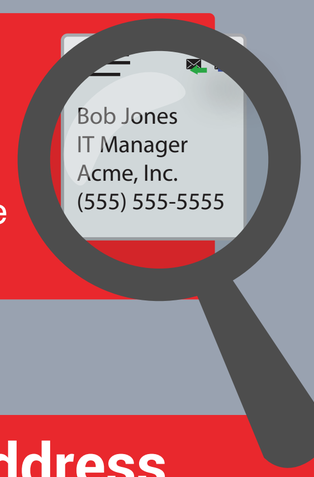
Fear

Scaring recipients is a common tactic in phishing emails. Emails that threaten you with negative consequences or punishment should be treated with suspicion.

Lesson 2: Examine these items closely

Email Signatures

A signature block that is overly generic or doesn't follow company protocols could indicate that something is wrong.

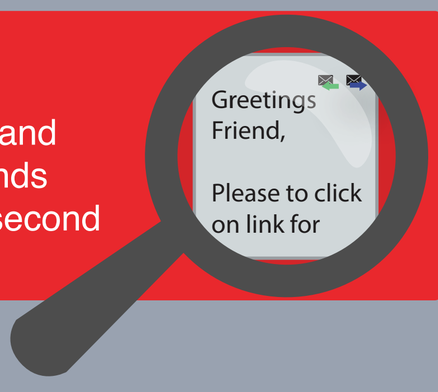


Sender Address

If the address doesn't match the sender name, be suspicious of the entire email.

Email Tone

We know how our co-workers and friends talk, so if an email sounds strange, it's probably worth a second look.



Lesson 3: Look for common indicators of a phish

Attachments

If you receive an unexpected or unusual attachment, always verify with the sender via phone.

From: Joe Smith
To: Troy Foster
Subject: WebMail Migration

Attachment -- Webmail_Migration.pdf

Troy,

This is to inform you that we are in the processing of m
to the Windows 2003 platform, which includes an exci
e-mail.

Attached is a document outlining the benefits of the m
migration we request you to enter your Windows password before 8 PM on Tuesday.
Failure to do so will result in being locked out of your email account!

Please click here to update your password.

Thank You,
John Smith

Log-in Pages

Spear phishers will often spoof websites to look legitimate in order to steal your credentials.

Links

Roll your mouse pointer over the link and see if what pops up matches what's in the email. If they don't match, don't click.

If you see something, say something!

Report suspected phishing emails to the information security team

COFENSE