1. Strategy and Concept

The EIS Phishing Awareness Program does not report a list of names of individuals who respond to simulated phishing attacks. This enterprise program is non-punitive, with all employee intervention occurring one on one between staff and manager/direct supervisor only.

Employees and managers need to be aware of and follow any internal agency policies and procedures they have in place, as they relate to phishing.

The purpose of this program is to:

- Teach staff to recognize phishing.
- Teach staff to look for suspicious email elements in every single email that they receive.
- Teach staff to 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 will hopefully increase retention of the content.
  - They are not meant to be a punishment.
  - We want them to be enjoyable.
  - We want them to be brief.
- Providing manager engagement at each level to support staff if they are experience issues around phishing.

2. 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?

Employees who have responded four or more times to simulated phishing emails will be considered Repeat Responders and assigned a phishing refresher training course. 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. The email contains a password-less link (unless your agency has opted to use the Learner Dashboard) which the staff use to access the training.

Employees are expected to complete the refresher course. We recommend that they save the completion certificate for their records.

Employees will be assigned an additional phishing refresher course assignment with each corresponding simulation response of four or more.

3. Manager/Direct Supervisor Engagement

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

An email notification of the training assignment goes to the employee's manager/direct supervisor as well as the employee. 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. Managers/direct supervisors in agencies that have enabled the Learner Dashboard have access to each employees phishing and training data in their team through the "KB4 Team Dashboard".

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.

If your agency does not have the Learner Dashboard enabled and your staff member doesn't remember engaging with a simulation four or more times please feel free to email security.training@das.oregon.gov and we can provide you a spreadsheet with the details of the staff's simulation engagement as well as a record of training completions.

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. There is a direct link to the refresher training in the email that was sent to staff. If it has expired, please contact security.training@das.oregon.gov to have a new one sent.
        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 this 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.

   Here are some tips that we want to think about with every single email that we receive:
   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.
      d. Tone of the email – you know how your co-workers talk, does the tone sounds strange?
   2. Watch out for emotions:
      a. Is there a sense of urgency?
      b. Greed – are they offering you something?
      c. Fear – is the email threatening or scary
      d. 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. 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.

4. Reporting

If you see something, say something!

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

2. 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.

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.

5. 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 Andrew's 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: 2022 Social Engineering Red Flags – 15 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.

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

6. Appendix

6.1 Samples of manager/direct supervisor notification emails:

a. Agencies using Learner Dashboard

Dear [[DISPLAY_NAME]],

You are receiving this email because you are listed as the manager in your agency's Active Directory for the employee(s) listed below.
If this email has reached you in error please contact your **agency's IT help desk** to correct the manager information for this employee.

As per the EIS Phishing Awareness Program Expectations, employees who have responded to four or more simulated phishing emails will be considered Repeat Responders and assigned a phishing refresher training course.

[[user_list_count]] employees were added to a phishing refresher training campaign: [[training_campaign]]
This phishing refresher training is **NOT located in Workday Learning.** The following information is provided in the event that your staff comes to you for assitance with their login or completion.

The notification of the training assignment comes in an email to the staff from the phishing tool (not Workday). The email contains a log-in link which the staff use to access the training.The first time they login they will need to do the following in order to select a password for their login.

- Click on "reset password"
- Knowbe4 will send a password reset email to the staff
- Select a password that is at least 12 characters long
- Return to the login screen
- Enter the password to access the learner dashboard
- The list of incomplete refresher trainings is located at the bottom of the screen

Staff must allow the refresher training to play to the end for the system to mark it complete. They will see a screen congratulating them on completing the training. We recommend that staff either screenshot that screen or save the certificate of completion for their records.

The expectation of the employee's manager is to have a conversation with the employee regarding continued phishing simulation responses.
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.

Please refer to the security resources website and the program documents for phishing resources if needed. https://www.oregon.gov/das/OSCIO/Pages/Securityresources-ag.aspx

The EIS Phishing Awareness Program does not report the names of individuals who respond to simulated phishing attacks.
This enterprise program is non-punitive, with all employee intervention occurring one on one between staff and manager only.

Employees and managers need to be aware of and follow any internal agency policies and procedures they have in place, as they relate to phishing.

Employee List:
[[user_list]]

Employee Names:
[[user_fullname_list]]

Employee Emails:
[[user_email_list]]

If you need additional support with this please contact security.training@das.oregon.gov with questions.

We are happy to go over the expectations and provide resources so that you can support your staff in the best way possible.
We are all in this together.

b. Agencies NOT using the Learner Dashboard

Dear [[DISPLAY_NAME]],

You are receiving this email because you are listed as the manager in your agency's Active Directory for the employee(s) listed below.
If this email has reached you in error please contact your **agency's IT help desk** to correct the manager information for this employee.

[[user_list_count]] employees were added to a training campaign: [[training_campaign]]

As per the EIS Phishing Awareness Program Expectations, Employees who have responded to four or more simulated phishing emails will be considered Repeat Responders and assigned a phishing refresher training course.

This phishing refresher training is **NOT located in Workday Learning.** Your staff must **click on the password-less link in the email notification** that they received to access the training.
The following information is provided in the event that your staff contact you for assistance.

The notification of the training assignment comes in an email from the phishing tool (not Workday).
The email contains a password-less link (unless your agency has opted to use the Learner Dashboard) which the staff use to access the training.

Staff must allow the refresher training to play to the end for the system to mark it complete. They will see a screen congratulating them on completing the training. We recommend that staff either screenshot that screen or save the certificate of completion for their records.

The expectation of the employee's manager is to have a conversation with the employee regarding continued phishing simulation responses.
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.

Please refer to the security resources website and the program documents for phishing resources if needed. https://www.oregon.gov/das/OSCIO/Pages/Securityresources-ag.aspx

The EIS Phishing Awareness Program does not report the names of individuals who respond to simulated phishing attacks.
This enterprise program is non-punitive, with all employee intervention occurring one on one between staff and manager only.

Employees and managers need to be aware of and follow any internal agency policies and procedures they have in place, as they relate to phishing.

Employee List:
[[user_list]]

Employee Names:
[[user_fullname_list]]

Employee Emails:
[[user_email_list]]

If you need additional support with this please contact security.training@das.oregon.gov with questions.
We are happy to go over the expectations and provide resources so that you can support your staff in the best way possible.
We are all in this together.

6.2 How to spot a phish poster

How to Spot a Phish

Finding the phish 101 with Professor Troy

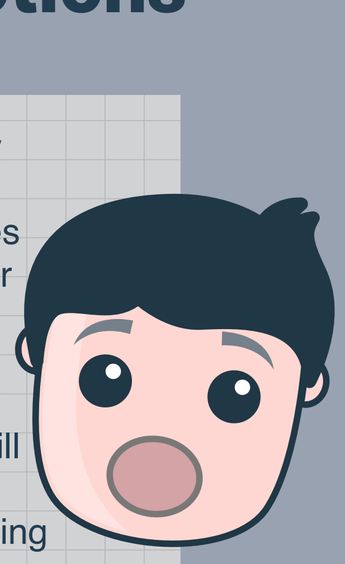
Lesson 1: Watch out for emotions

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.

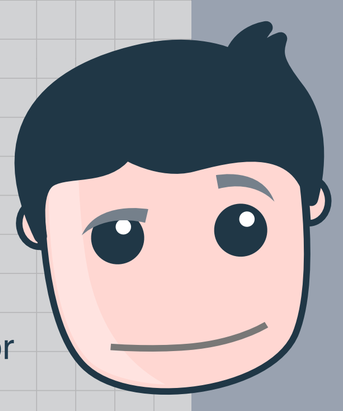
Urgency

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.



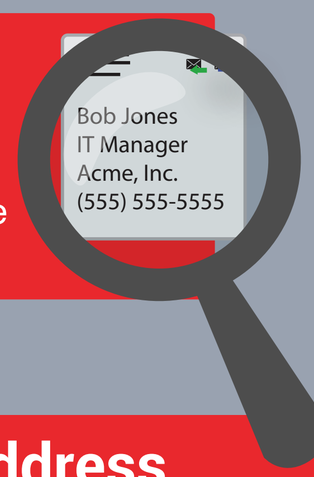
Fear

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.

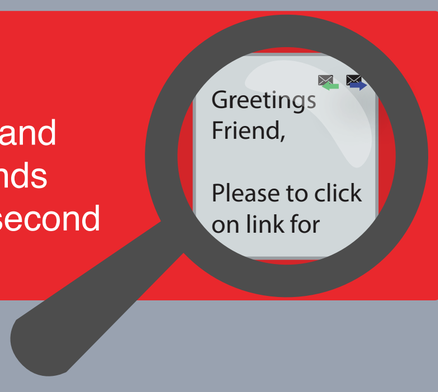


Sender Address

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