

Tabletop Experience:

Unmasking Phishing and Whaling Attacks

Overview

Phishing attacks manipulate employees into compromising security by exploiting emotions like fear, helpfulness, or respect for authority. This activity focuses on a specific, highly targeted form of phishing known as “Whaling,” or “CEO Fraud.” In these attacks, criminals impersonate high-level executives, such as the CEO or CFO, to exploit authority bias and trigger an urgent emotional response.

Modern threat actors frequently use generative artificial intelligence (AI) to produce phishing emails with exact organization logos and no grammatical errors. While participants should still keep an eye out for obvious spelling or branding mistakes, this session challenges them to understand that they can no longer rely solely on these surface-level phishing clues.

Roles

Facilitator:

Controls exercise pace, guides discussions, and ensures full participation.

Participants:

Openly discuss their thought processes and respond to scenarios according to the exercise rules.

Introduction

Give the participants the scenario: Summit View Logistics is expanding its operations into Europe. The CEO, Marcus Vance, has been traveling in Germany all week to secure a major warehouse lease. Everyone in the organization knows this deal is a massive priority. The CFO, Elena Smith, is on a 10-hour flight back to headquarters and is currently unreachable. Taylor Reese, Accounts Payable Manager, receives a suspicious email.

Part 1: Signs Annotation

 **Duration:** 15 minutes

Materials:

- Timer or stopwatch
- Scenario handouts
- Pens or pencils

Instructions:

- Divide the room into small groups.
- Hand out the email prints and pens or pencils to each group.
- Instruct groups to underline elements that build false trust. Examples include accurate email signatures, mentions of real internal projects, or an authentic executive tone.
- Direct groups to **circle** behavioral warning signs. Examples include extreme urgency, demands to keep the request a secret, or instructions to bypass standard payment portals.
- Give the groups 15 minutes to read the email, discuss, and annotate.

Part 2: Discussion

 **Duration:** 10 minutes

Questions:

- Which false trust indicators did you spot, and how much did they impact your trust in the email?
- What specific behavioral warning signs gave the scam away?
- How are those behavioral triggers designed to make you feel or react?

Possible answers/prompts:

- False trust indicators: Phishing scammers scrape LinkedIn or corporate websites for real project names to make the email look authentic.
- Warning signs: The phishing email asks the employee to bypass standard procedures. The sender demands secrecy from the employee's direct manager.
- The core takeaway: The authentic-looking elements are just a smokescreen. The behavioral warning signs are the actual danger.

Conclusion

 **Duration:** 5 minutes

Wrap up the exercise by connecting the concepts directly to your organization's reality. Explain that spotting a behavioral warning sign is only the first step in the defense; the second is taking the correct action by following the organization's procedures.

Take the opportunity to answer any questions participants may have about how to report this type of scam internally and about the tools, channels, and documentation available for reporting these incidents.

Attachment – Scenario Handout

 Compose

-  Inbox
-  Drafts
-  Sent
-  Starred
-  Spam
-  Trash
-  Archive
-  All Mail

 Archive  Spam  Delete  More  Reply  Forward

From: Marcus Vance <m.vance@summitview-logistics-internal.com>
To: Taylor Reese
Subject: **URGENT: Berlin Warehouse Deposit**

Hi Taylor,

I am sitting with the brokers in Berlin. We are ready to sign the warehouse lease we discussed at Monday’s all-hands meeting.

We have a major problem. Another firm just put an offer on the facility. The broker said if we do not clear the €50,000 security deposit in the next hour, they are giving the lease to the other company.

Elena Smith is on a flight, and I cannot wait for her approval. The broker is not in our vendor portal yet, and that will take too long.

I need you to process a direct wire to the account details attached below right now. Keep this between us until Elena lands so people don’t panic about the deal falling through. Let me know the second the wire is confirmed.

Best,
Marcus

 Attachment: Wire_Transfer_Details.pdf

False Trust Indicators: Sender location (Berlin); mentions a real project (warehouse lease / all-hands meeting); knows the CFO’s status and name (Elena is on a flight).

Behavioral Warning Signs: Extreme urgency (next hour / other company will get it); bypassing procedures (not in the vendor portal); isolation (keep this between us).