PHISHING EMAIL TRAINING – DESIGN DOCUMENT

Project Overview

- Project Name: Email Phishing Training Simulation
- Learning Objectives: Learners will identify common markers of phishing attacks in emails. Learners will respond appropriately to suspected phishing attacks.
- Target Audience: Mid-market- and enterprise-level employees doing regular training.
- Instructional Format: eLearning Module
- Tools/Technology: Articulate Storyline, Canva, Vyond

Content Outline

- Hook: Learner views a real-life scenario of a phishing attack and its consequences.
- Introduction
    - What are phishing emails?
    - What are the possible consequences?
    - Learning objectives of this course
- Common ways to identify phishing emails
    - Spot common red flags
        - Examples
            - Poor/Uncommon grammar and spelling, or grammar that sounds too formal
            - Unexpected or unusual senders
            - Multiple recipients or generic greetings
            - Social engineering
            - Embedded links in cloud-hosted documents
        - What to do
            - Don’t respond
            - Report to security team
        - Practice
            - Learners engage with several email examples to identify common red flags of phishing emails
    - Harder to spot
        - Examples
            - Impersonation of trusted brands or people
            - Social engineering tactics
            - Requests for unrecoverable assets

                - Requests for sensitive information
                - Suspicious links and URLs
            - What to do
                - Don’t respond
                - Take your time
                - Verify
                    - Go to website instead of clicking on link
                    - Reach out to known contact through other means rather than responding to email
                - Never send sensitive information over email
                - Never open links to shared documents that you are not expecting
                - If in doubt, report to security team
            - Practice
                - Learners engage with several email examples to identify suspicious emails that may be phishing emails
    - Application Practice
        - Learners engage with an email inbox to identify potential phishing emails AND respond appropriately
    - Summary
        - Phishing emails
        - Consequences
        - Tips
        - Further reading in resources ***
    - Closing

*** Include sidebar resources (see knowledge doc)

Script

** This script contains the content for the SME to verify but may not include aspects such as directions for interactions, accessibility adjustments, or whether the content is narrated or on-screen. **

ANIMATED VIDEO
SCENE: OFFICE - DAY
(Employee, TANYA, is typing when a new email pops up: Subject: “Quick Favor - From CEO”).
TANYA (reading aloud): ‘Hey Tanya, I need 6 gift cards for a last-minute client thank-you. Can you grab them and send the codes here ASAP? Can’t talk, heading into a meeting. - Jared’
(Tanya hesitates, then checks the email address.)
TANYA: jared.smith@gmail.com? Must be his personal email. It sounds urgent…
(Tanya pulls out company card and types in card number to generic gift card site. She navigates back to the email, clicks reply, and starts typing in card codes.)
SCREEN TEXT OVERLAY: 30 minutes later…
TANYA (on call): Did you get the gift card codes in time? (audio static) The email you sent me asked for gift cards… (audio static) You didn’t send that email?!
NARRATOR (V.O.): Tanya was tricked into sending $600 in unrecoverable gift cards, money gone forever. While this isn’t much money, it shakes the company’s faith in Tanya and identifies the company as an easy target for other attackers.
NARRATOR (pops up on screen): Tanya was just trying to stay on top of her tasks when an urgent email popped up, supposedly from the CEO. But the request wasn’t real. It was a phishing attack.

CONTENT PRESENTED FOR USERS TO CLICK THROUGH
[Slight pause for emphasis]
Phishing is a type of cyber-attack where scammers impersonate trusted contacts or organizations in order to trick you into clicking malicious links, opening harmful attachments, or giving up sensitive information like your passwords or financial details. Phishing emails are often designed to look real, create a sense of urgency, and pressure you to act quickly.

[Serious but reassuring tone]
The consequences of phishing can be severe: identity theft, financial loss, data breaches, reputational damage, and even legal penalties for your organization.
But the good news?
Attacks like this are **completely avoidable.**

In this training, you'll learn how to spot common red flags in email phishing attempts, how to respond appropriately when you suspect a phishing email, and how to apply best practices to protect both yourself and your organization from risk. While phishing can happen through phone calls, text messages, and even physical mail, this course will focus specifically on email-based phishing attacks.

[Friendly, confident tone]
Not all phishing emails are sophisticated. In fact, many have common red flags that make them easy to spot—if you know what to look for.
These warning signs often show up in the email's sender, language, format, or content.
Let's go over some of the most common ones:

1. Social Engineering Tactics.
Scammers try to manipulate emotions, creating urgency, fear, or curiosity. If the email pressures you to act quickly: slow down. That's a red flag. Most phishing emails will use some sort of social engineering tactic, but there are other common red flags to look out for.

2. Poor or Unusual Grammar and Spelling.
Many phishing emails contain typos, awkward phrasing, or odd formatting. On the flip side, if the writing feels overly polished or too formal (especially from someone you know) it's worth a second look.

3. Unexpected or Unusual Senders.
If you get an email from someone you don't recognize, or a strange message from someone you do, it could be a phishing attempt.

4. Multiple Recipients or Generic Greetings.
Watch out for emails addressed to "Dear Customer" or "Hi User," especially if you're one of many recipients unrelated to your role.

5. Embedded Links in Cloud-Hosted Documents.
Attackers often use platforms like DocuSign, SharePoint, or Adobe Sign to deliver malicious links that can't be detected by email security software. Never open shared documents you weren't expecting.

[Reassuring tone]
Spotting even just one of these signs is a good reason to pause and verify. The more red flags you recognize, the better you'll be at staying one step ahead.

PRACTICE OPPORTUNITY
Now that you're familiar with some of the most common red flags, let's put your skills to the test to identify potential phishing emails. Keep in mind: not every suspicious email is a phishing attempt, but when in doubt, it's always better to double-check.

**Emails will be presented in a random order and users will be asked first to identify if it is "safe" or "suspicious" then (if suspicious) asked to click in the email (hotspots) to identify a red flag they noticed. **

Safe Email #1
Subject: Team Meeting Rescheduled to Thursday
From: jasmine.lee@company.com
To: Aisha Patel
Hi Aisha,
Just a heads-up that the team meeting has been moved to Thursday at 10 a.m. to accommodate James's schedule. The updated calendar invite should be in your inbox.
Thanks!
– Jasmine
Feedback (safe): Correct! This is a legitimate work email. It's specific, relevant to your schedule, and comes from a known internal address.
Feedback (suspicious): Not quite. While it's good to be cautious, this email has no red flags. It's from a known colleague, includes expected info, and doesn't ask for any sensitive action.

Safe Email #2
Subject: Benefit Enrollment Portal Now Open
From: hr@company.com
To: All Employees
Hello Team,
Our annual benefits enrollment period is now open. Please log into the employee portal by Friday, May 31 to review and update your selections.
Let us know if you have any questions.
– HR Team
Feedback (safe): You got it! This is a standard HR communication. It's from the company's official HR address and doesn't ask for credentials or include suspicious links.
Feedback (suspicious): That's incorrect. This is a safe message. It provides general info and directs employees to the official company portal, not an unknown site.

Safe Email #3
Subject: Q2 Sales Report – Final Review
From: marcus.evans@company.com
To: Javier Morales
Hi Javier,
Here's the final draft of the Q2 report. Thanks again for pulling together the regional numbers. Let me know if you spot anything that needs fixing before we send it to leadership.

Best,
Marcus
Feedback (safe): Correct! This email is routine and expected. It's directly from a colleague about work you've been collaborating on.
Feedback (suspicious): Not quite. This one's safe. The sender and content are consistent with internal workflows and there are no urgent requests or red flags.

Phishing Email #1 – Poor/Unusual Grammar and Spelling
Subject: You account will be Terminate soon!
From: IT-Support@company.com
To: Lena Chen
Dear user,
We detected suspicious activity on your account. You must verify it now to avoid loosing access. Click here to confirm credentials: [https://account-support.company.com.tinyurl.com/]
This urgent.
– IT Team
Feedback (safe): Oops! Watch out for misspellings and awkward grammar. Those are often signs the message isn't coming from your real IT team.
Feedback (suspicious): Yes! This email is full of red flags: bad grammar, spelling mistakes, and pressure to click a suspicious link.
Feedback 2 (correctly identifies red flag): Great eye! That is a common red flag in phishing emails. Spotting things like suspicious links, urgent language, or unfamiliar senders helps protect you and your organization.
Feedback 2 (incorrectly identifies red flag): Not quite. That part of the email isn't necessarily suspicious. Take another look. Watch for things like strange sender addresses, unexpected attachments, or pressure to act fast.

Phishing Email #2 – Unexpected or Unusual Sender
Subject: Important: Review Your Payroll Info
From: payroll-update@companyalerts.net
To: Emily Nguyen
Hi Emily,
There was a discrepancy in your recent payroll entry. Please review and confirm your account details immediately: [https://account-details.company-alerts.net.dyytjh37291hh1vyvieowz093874.bitly.url/ref?=afyeybenn323983ruyruownuwuco3kljcygzjnermla]
– Payroll Department
Feedback (safe): Not quite. Even though the message sounds professional, the email comes from a non-company domain. Always double-check the sender!

Feedback (suspicious): Good catch! The sender address isn't from the company's domain, which is a strong indicator this is a phishing attempt.
Feedback 2 (correctly identifies red flag): Great eye! That is a common red flag in phishing emails. Spotting things like suspicious links, urgent language, or unfamiliar senders helps protect you and your organization.
Feedback 2 (incorrectly identifies red flag): Not quite. That part of the email isn't necessarily suspicious. Take another look. Watch for things like strange sender addresses, unexpected attachments, or pressure to act fast.

Phishing Email #3 – Multiple Recipients or Generic Greetings
Subject: Action Required – Employee Survey
From: surveys@internal-tools.com
To: Omar Haddad + 30 other external addresses
Dear Employee,
Please take a moment to complete our mandatory employee experience survey. Your feedback is important!
Click *here (hyperlink)* to take the survey!
Thank you.
Feedback (safe): Be careful. Emails with "Dear Employee" and multiple unrelated recipients are a common phishing tactic.
Feedback (suspicious): Correct! Legitimate company surveys are usually personalized and sent directly, not in bulk with generic greetings.
Feedback 2 (correctly identifies red flag): Great eye! That is a common red flag in phishing emails. Spotting things like suspicious links, urgent language, or unfamiliar senders helps protect you and your organization.
Feedback 2 (incorrectly identifies red flag): Not quite. That part of the email isn't necessarily suspicious. Take another look. Watch for things like strange sender addresses, unexpected attachments, or pressure to act fast.

Phishing Email #4 – Social Engineering Tactics
Subject: CONGRATULATIONS!!! YOU'VE WON A FREE iPHONE 16
From: prizecenter@w1n-free-now.biz
To: Malik Thompson

Dear Lucky Winner,
You have been randomly selected to receive a brand new iPhone 16 as part of our Employee Loyalty Giveaway!
All you need to do is click the link below and enter your full name, shipping address, and company ID.

(Due to compliance, we are unable to ship to PO boxes. If you don't have another address to use, please send us an email explaining the situation and we can send you a link to purchase it yourself through the Apple store.)
Claim Your FREE Prize Now! (hyperlink)
This offer is only valid for the next 30 minutes, so don't wait!
Act fast—your FREE iPhone is just a click away!

Sincerely,
The Rewards Department
Feedback (safe): Incorrect. Free prizes and urgent requests for info are classic phishing tactics. Always be cautious.
Feedback (suspicious): Correct. This is a phishing scam. The prize, urgency, and request for sensitive info are all red flags.
Feedback 2 (correctly identifies red flag): Great eye! That is a common red flag in phishing emails. Spotting things like suspicious links, urgent language, or unfamiliar senders helps protect you and your organization.
Feedback 2 (incorrectly identifies red flag): Not quite. That part of the email isn't necessarily suspicious. Take another look. Watch for things like strange sender addresses, unexpected attachments, or pressure to act fast.

Phishing Email #5 – Embedded Links in Cloud-Hosted Documents
Subject: FYI – Updated contract from legal
From: no-reply@dropbox.com
To: Jake Thompson
Hey,
The legal team just uploaded the new vendor contract. Please review:
[https://www.dropbox.com/l/scl/AABwt6h8XVIhNyhk0ngWmYB6BU4kw0PrUTBA]
Let me know when you've signed it.
– Rebecca
Feedback (safe): Not quite. Be wary of unexpected cloud file links, even if they look legit. Always verify before clicking.
Feedback (suspicious): Great job spotting this one! The link to a shared document you weren't expecting is suspicious and could contain malware.
Feedback 2 (correctly identifies red flag): Great eye! That is a common red flag in phishing emails. Spotting things like suspicious links, urgent language, or unfamiliar senders helps protect you and your organization.
Feedback 2 (incorrectly identifies red flag): Not quite. That part of the email isn't necessarily suspicious. Take another look. Watch for things like strange sender addresses, unexpected attachments, or pressure to act fast.

CONTENT PRESENTED FOR USERS TO CLICK THROUGH

Now you know how to identify some common red flags in phishing emails, but what do you do when you spot one?
If you come across an email that seems suspicious, don't respond, even if you're sure it's a scam. Replying only confirms to attackers that your account is active and being regularly checked.
Never enter personal or sensitive information into links or forms from an unexpected message. Legitimate organizations won't ask for sensitive information through email. Instead, report the email to your security team right away. It's always better to report something that turns out to be safe than to ignore a real threat. Many companies will have a "Phishing" button to easily report emails that are suspected as phishing.
When in doubt, play it safe: don't click, don't respond, and report it.

Not all phishing emails are obvious. In fact, some are designed to look *exactly* like the real thing—and that's what makes them dangerous. It is important to remember that even emails that seem legitimate at first glance often use social engineering tactics to create a sense of fear or urgency. Always take the time to assess an email carefully before taking action.

Let's look at some more sophisticated examples of phishing techniques and what you can do to avoid a phishing attack.

1. Impersonation of Trusted Brands or People.
Attackers may spoof a familiar email address or use slight name changes to pose as a coworker, a manager, even a C-level executive. They may also copy branding and logos to make the message look legit. If something feels off, trust your instincts and verify through another channel.

Subject: Immediate Action Required: Security Update for Company Email
From: it-admin@companyaccess.net
To: Anika Desai
Hi Anika,
As part of our routine security updates, all employees are required to re-authenticate their accounts to maintain secure access to internal systems.
Please log in to your portal using the secure link below to complete the update:
Secure Login Portal (hyperlink)
Failure to complete this by end of day may result in temporary suspension of your email access.
Let us know if you run into any issues.

Thanks,
James Carter

IT Support Specialist
Tech Company
(Email includes fake footer with branding and IT contact info)

This email raises a potential security concern, so it's important not to ignore it. While you recognize and trust your IT provider, the request is both urgent and unexpected, two common red flags. The best course of action is to report the email as phishing. In the worst case, your IT team will confirm it's legitimate and appreciate your caution. You can also log into your company portal directly (without using the email link) to check for any notifications about re-authenticating your account.

2. Requests for Unrecoverable Assets.
No one at your company should ever ask for gift cards, cryptocurrency, or other non-refundable items via email. These kinds of requests are a huge red flag. Let's take another look at Tanya's email from beginning of this training.

Subject: Quick Favor
From: jared.smith@gmail.com
To: Tanya Henderson

Hey Tanya,

I need 6 gift cards for a last-minute client thank-you. Can you grab them and send the codes here ASAP?
Can't talk, heading into a meeting.

-Jared

You probably don't want to ignore a message from your CEO, even if it seems unusual. Always verify unexpected requests by calling or messaging them directly through a trusted channel like Teams or Slack. Never respond to the email unless you've confirmed the request is legitimate. As always, report the email to your IT team if you cannot verify the request.

3. Requests for Sensitive Information.
Be cautious if you're asked to verify passwords, update billing info, or share personal details. Legitimate companies won't ask for this through email, especially out of the blue.
Subject: Urgent: Update Your Billing Information to Avoid Service Disruption
From: billing@officeplus-updates.com
To: Emily Parker

Dear Emily,
We've been unable to process your recent payment due to outdated billing information. To avoid any interruption in your office supply deliveries, please update your billing details by clicking the link below:
Update Billing Information (hyperlink)
Please complete this update within 48 hours to ensure your account remains active.
Thank you for your prompt attention.

Best regards,
Billing Department
OfficePlus Supplies
(Includes company logo and contact details)

If you handle office supply orders for your company, you shouldn't ignore this email. However, you should never enter billing or sensitive information by clicking a link in an email. Instead, log into your account directly or call the support number on the company's official website, not the one in the email. If you find no billing issues with your account, be sure to report this suspicious email to your IT team.

4. Suspicious Links and URLs.
Phishing emails often hide dangerous links behind text that looks normal. Hover over the link before clicking. If the destination doesn't match or looks strange, don't click it. Watch out for lookalike domains like *micr0soft.com* instead of *microsoft.com*.

Subject: Action Required: Confirm Your Account Details
From: support@microsoft-secure.com
To: jordan.smith@company.com

Hello Jordan,

We've detected unusual activity on your Microsoft account. Please verify your account details immediately to avoid suspension.
Click the link below to review and confirm your information:
Verify Your Account (hyperlink, on hover shows http://micr0soft-security.com/verify)
If you don't take action within 24 hours, your account will be locked for your protection.

Thank you,
Microsoft Security Team

While this message doesn't directly ask for sensitive information, the sense of urgency is a red flag. Slow down and verify its legitimacy. Hover your mouse over the link: in this case,

the “o” in “Microsoft” has been replaced with a zero. Phishing sites often mimic legitimate ones using lookalike characters that are hard to spot. Always report suspicious links or URLs to your IT team.

Now it’s your turn to apply what you’ve learned.
In this practice activity, you’ll explore a sample email inbox for Sofia Rossi. Apply what you have learned about common red flags to spot potential phishing attempts. For each message, decide whether it’s safe or suspicious. If it’s suspicious, choose the best way to respond.
Take your time, trust your instincts, and remember: when it comes to phishing, it’s always better to verify than to guess. Ready to get started?

ACTIVITY
** Interactive email inbox. Each email entry will show the subject and from information. Users can click on each entry to view the email and choose from the response options. Once a response has been chosen, the email entry will turn grey (marked as read) but users could click on it again to change their answers. Feedback will be given for all email entries on next slide and final score will be recorded. Emails will be presented in a random order**

Safe Email # 1
Subject: Team Meeting Rescheduled
From: jessica.lam@company.com
To: Sofia Rossi, Diego Morales, Svetlana Petrov, Jalen Thompson, Mei Lin Zhang

Hi everyone,
Just a quick note that our team meeting has been moved from Tuesday to Thursday at 10 AM. The updated invite is on your calendar.
Let me know if you can’t make it!

Thanks,
Jessica

Response and Feedback

- Safe, respond to Jessica.
    - Feedback: Great job! This email doesn’t ask you to input sensitive information or click on any links. It is important to note that if you don’t recognize the sender or other recipients or know that there is not a meeting scheduled, you should not respond. Otherwise, this email is safe to respond to.
- Suspicious, verify with Jessica through Teams.

    - Feedback: Not quite. While it is better to be safe when it comes to phishing, this email is most likely safe. Unless you don't recognize the sender or other recipients or know that there is not a meeting scheduled, this email should be safe to respond to.

Safe Email #2
Subject: Timesheet Reminder
From: payroll@company.com
To: Sofia Rossi

Hi Sofia,
This is a reminder to submit your timesheet by Friday at 5 PM. You can access the payroll portal through the intranet.
Thanks!
Best,
Payroll Team

Response and Feedback

- Safe, submit your timesheet through the payroll portal.
    - Perfect! This email doesn't ask you to input sensitive information, click on any links, or respond at all. It directs you to take an action on your company portal. This is a safe email.
- Suspicious, respond to email asking why you are getting this email.
    - Not quite. If you suspect an email is suspicious you should never respond to it. However, this email is likely safe since it doesn't ask you to input sensitive information, click on any links, or respond at all.

Safe Email #3
Subject: RE: Q2 Metrics
From: jordan.chen@company.com
To: Sofia Rossi

Hey Sofia,
Yep, here's the link to the deck in Drive:
https://drive.google.com/file/d/1XyZ2ExampleLink
Let me know if you need anything else!
—Jordan

<Sofia Rossi wrote>
Hey Jordan,

Do you have that Q2 metrics deck handy? I want to include some of the numbers in tomorrow's client call.
Thanks!
Sofia

Response and Feedback

- Safe, click to open the document.
    - Great job! This email is a coworker responding to you and sending you the document you requested in a method you expected. If a coworker sends you a document that you are not expecting then you should be cautious, but in this case it's not phishing.
- Suspicious, report as phishing.
    - Not quite. Since Jordan is responding directly to your request for a document this email is not phishing.

Phishing Email #1
Subject: URGENT – Password Expiring in 24 Hours
From: security-alert@company.com
To: Sofia Rossi

Hi Sofia,
Your email password will expire in 24 hours. Log in to the company portal or click the link below to update your sign-in information.
myaccount.company.com (on hover displays myaccount.company.com.login.73k3k9s982k1ls9x6733.bly.zx)
– IT Security Team

Response and Feedback

- Safe, click the link and reset your password.
    - Poor choice. This email looks urgent, but you should never click a link in an email and enter sensitive information such as your password. You should log into your company portal through the browser to check if your password needs to be reset. There is a good chance this email is phishing.
- Suspicious, report as phishing.
    - Great choice! This email is most likely phishing since it asks you to click a link and enter sensitive information. Your company will appreciate your diligence in maintaining security. If this request turns out to be legitimate your security team will let you know that it is safe.

Phishing Email #2
Subject: Request for Immediate Action Required
From: michael.richards.team@gmail.com
To: Sofia Rossi

Dear Miss Rossi,

I trust this message finds you in excellent health and high spirits. I am writing to inform you of a discrepancy that has been detected in your recent payroll disbursement. It is imperative that you confirm your identity and verify your employee credentials at your earliest convenience.

Kindly click the secure link below to access the validation portal:
http://employee-verification-secure.info

Failure to comply within the next 12 hours may result in temporary suspension of your employee account. We appreciate your cooperation in this urgent matter.

Warm regards,
Michael Richards
Payroll Coordination Officer
Human Resources Division

Response and Feedback

- Safe, click the link to verify.
    - Poor choice. This email looks urgent. However, it sounds overly formal, and you should never click a link in an email and enter sensitive information. There is a good chance this email is phishing.
- Suspicious, report as phishing.
    - Great choice! This email is most likely phishing since it asks you to click a link and enter sensitive information. Your company will appreciate your diligence in maintaining security. If this request turns out to be legitimate your security team will let you know that it is safe.

Phishing Email # 3
Subject: Unusual sign-in activity on your Microsoft Teams account
From: Microsoft Teams no-reply@msteams-security.com
To: Sofia Rossi

Your account was used to sign in on a new device.

We detected a sign-in to your Microsoft Teams account from a new device. If this was you, you can safely ignore this email. If not, we recommend reviewing your recent activity.

Sign-in Details:

- Account: sofiarossi@company.com
- Location: Moscow, Russia
- Device: Windows 10 – Chrome Browser
- Time: May 27, 2025, 9:39 AM (UTC)

If this wasn't you, please secure your account immediately.
Review Activity (http://secure-msteams-check.com/verify)

This link will expire in 24 hours for your protection.
Thanks,
The Microsoft Teams Security Team

Security tip: *Microsoft will never ask for your password via email. Always verify suspicious activity directly from your Microsoft account.*

Response and Feedback

- Safe, click the link to report activity as suspicious.
    - Poor choice. This email looks urgent, but you should never click a link in an email and log into an account. There is a good chance this email is phishing. If you are worried that someone has accessed your Microsoft account, you can log login from your browser and make sure that there is no suspicious activity.
- Suspicious, sign into your Microsoft account through your browser.
    - Great choice! This email is most likely phishing since it asks you to click a link and enter sensitive information. From your account you can check for any suspicious activity. If there is, you can safely address the concern. If not, make sure to also report the email as phishing. Your company will appreciate your diligence in maintaining security.

CONTENT
By completing this training, you've just taken a big step toward protecting yourself, and your organization, from phishing attacks. Let's quickly review what we've covered.
Phishing emails are designed to trick you into taking an action: like clicking a link, sharing sensitive information, or opening harmful attachments. These attacks can lead to serious consequences, including data breaches, identity theft, and financial loss.
But the good news is that many phishing emails have warning signs. Throughout this training, you've learned to recognize common red flags, such as:

- Unusual grammar or overly formal tone
- Unexpected or unfamiliar senders
- Generic greetings or multiple recipients
- Attempts to create urgency or fear
- Suspicious links or lookalike URLs

When you spot something that doesn't seem right, don't click or reply. Instead, report the message to your IT or security team. It's always better to double-check than to take a risk.
If you'd like to explore this topic further, be sure to check out the Resources tab to the left for additional information and best practices.
Thanks for completing this training, and remember, staying alert is one of the best ways to protect yourself and your organization.