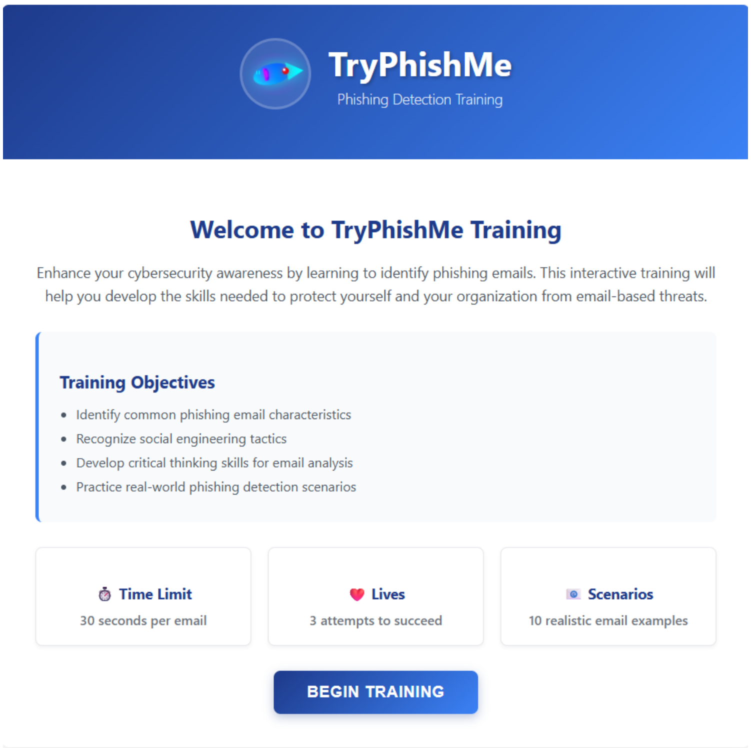
## Introduction

The Phishing Pond is designed to build practical phishing-detection skills through a set of real-world email examples. The room teaches how attackers craft deceptive messages and which red flags to look for when reviewing suspicious emails. It focuses on the most common phishing tactics, including urgency in subject lines, look-alike domains, display-name impersonation, malicious attachments, compromised sender accounts, and offers that attempt to gather personal or financial information.

## Starting the Phishing Analysis



TryPhishMe

Phishing Detection Training

Welcome to TryPhishMe Training

Enhance your cybersecurity awareness by learning to identify phishing emails. This interactive training will help you develop the skills needed to protect yourself and your organization from email-based threats.

Training Objectives

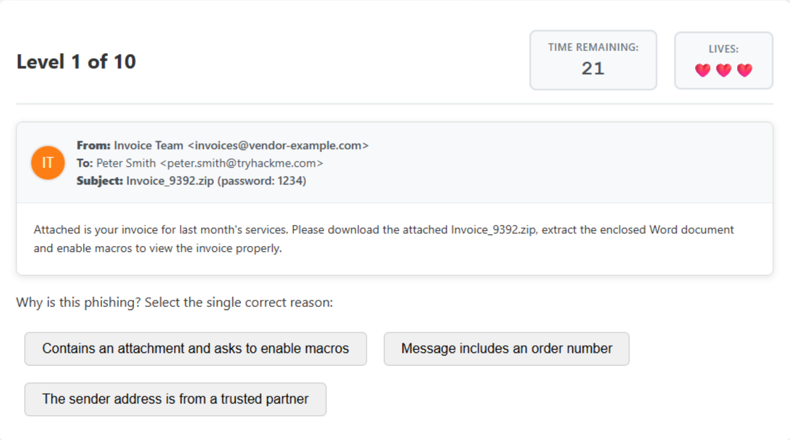
- Identify common phishing email characteristics
- Recognize social engineering tactics
- Develop critical thinking skills for email analysis
- Practice real-world phishing detection scenarios

⏱ Time Limit
30 seconds per email

❤ Lives
3 attempts to succeed

Scenarios
10 realistic email examples

## Level 1



Level 1 of 10

TIME REMAINING: 21

LIVES: ❤❤❤

IT

From: Invoice Team <invoices@vendor-example.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Invoice_9392.zip (password: 1234)

Attached is your invoice for last month's services. Please download the attached Invoice_9392.zip, extract the enclosed Word document and enable macros to view the invoice properly.

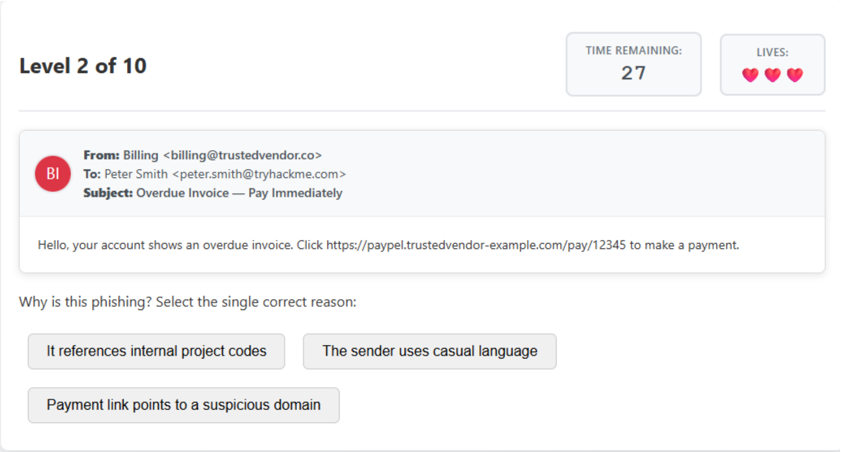
Why is this phishing? Select the single correct reason:

Contains an attachment and asks to enable macros
Message includes an order number
The sender address is from a trusted partner

*Figure 1 – Phishing Email*

Reason: It contains an attachment and asks to enable macros

## Level 2



Level 2 of 10

TIME REMAINING: 27

LIVES: ♥ ♥ ♥

**From:** Billing <billing@trustedvendor.co>
**To:** Peter Smith <peter.smith@tryhackme.com>
**Subject:** Overdue Invoice — Pay Immediately

Hello, your account shows an overdue invoice. Click https://paypel.trustedvendor-example.com/pay/12345 to make a payment.

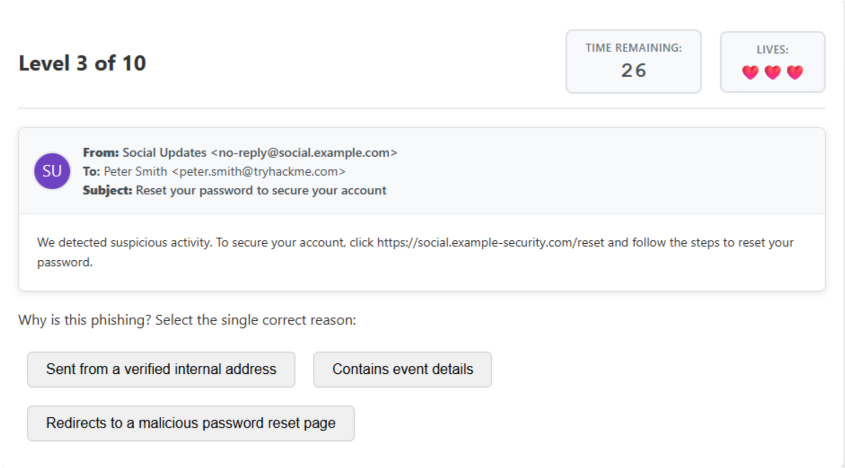
Why is this phishing? Select the single correct reason:

BI
It references internal project codes
The sender uses casual language
Payment link points to a suspicious domain

*Figure 2 – Phishing Email*

Reason: The payment link points to a suspicious domain

## Level 3



Level 3 of 10

TIME REMAINING: 26

LIVES: ♥ ♥ ♥

**From:** Social Updates <no-reply@social.example.com>
**To:** Peter Smith <peter.smith@tryhackme.com>
**Subject:** Reset your password to secure your account

We detected suspicious activity. To secure your account, click https://social.example-security.com/reset and follow the steps to reset your password.

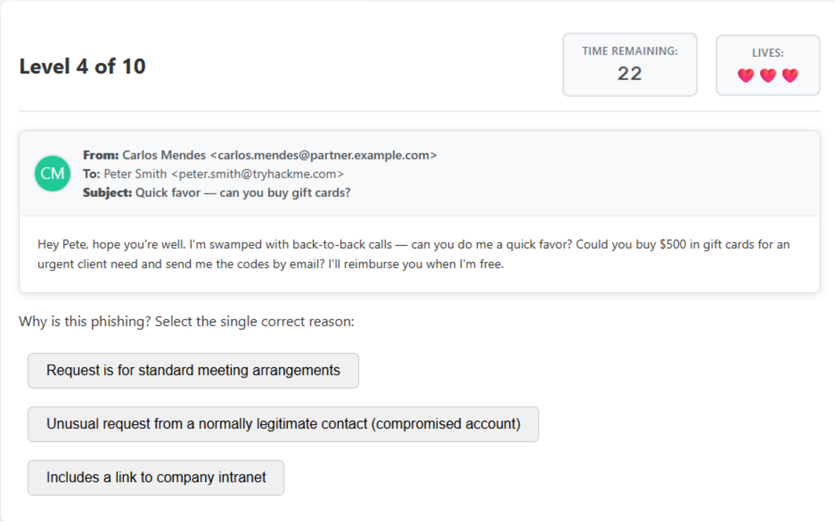
Why is this phishing? Select the single correct reason:

SU
Sent from a verified internal address
Contains event details
Redirects to a malicious password reset page

*Figure 3 – Phishing Email*

Reason: It redirects to a malicious password reset page

## Level 4



Level 4 of 10

TIME REMAINING:
22
LIVES:
❤❤❤
CM

**From:** Carlos Mendes <carlos.mendes@partner.example.com>
**To:** Peter Smith <peter.smith@tryhackme.com>
**Subject:** Quick favor — can you buy gift cards?

Hey Pete, hope you're well. I'm swamped with back-to-back calls — can you do me a quick favor? Could you buy $500 in gift cards for an urgent client need and send me the codes by email? I'll reimburse you when I'm free.

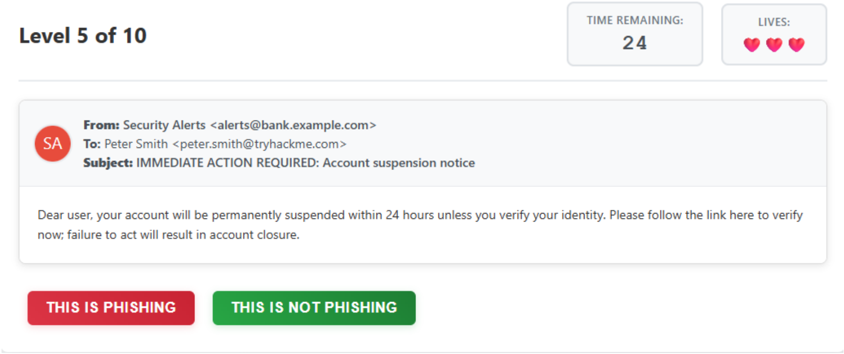
Why is this phishing? Select the single correct reason:

Request is for standard meeting arrangements
Unusual request from a normally legitimate contact (compromised account)
Includes a link to company intranet

*Figure 4 – Phishing Email*

Reason: It is an unusual request from a normally legitimate contact (compromised account)

## Level 5



Level 5 of 10

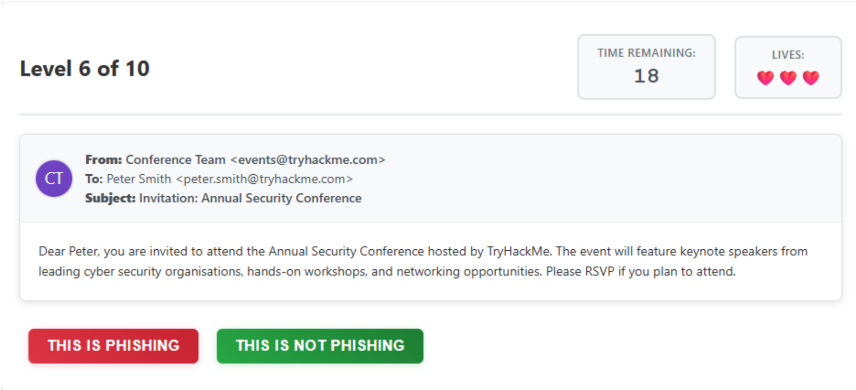
**From:** Security Alerts <alerts@bank.example.com>
**To:** Peter Smith <peter.smith@tryhackme.com>
**Subject:** IMMEDIATE ACTION REQUIRED: Account suspension notice

Dear user, your account will be permanently suspended within 24 hours unless you verify your identity. Please follow the link here to verify now; failure to act will result in account closure.

*Figure 5 – Phishing Email*

Reason: It requests verification via a link and use urgent and threatening language

## Level 6



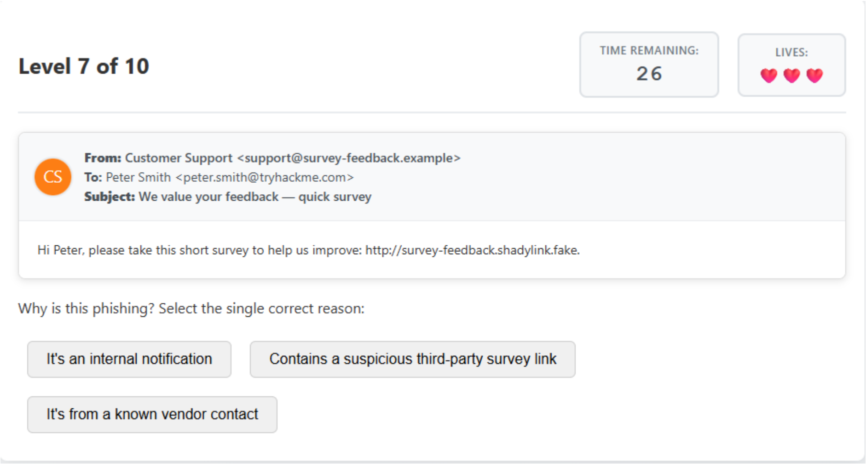
Level 6 of 10

**From:** Conference Team <events@tryhackme.com>
**To:** Peter Smith <peter.smith@tryhackme.com>
**Subject:** Invitation: Annual Security Conference

Dear Peter, you are invited to attend the Annual Security Conference hosted by TryHackMe. The event will feature keynote speakers from leading cyber security organisations, hands-on workshops, and networking opportunities. Please RSVP if you plan to attend.

*Figure 6 – Not a Phishing Email*

## Level 7



Level 7 of 10

TIME REMAINING:
26
LIVES:
❤ ❤ ❤

**From:** Customer Support <support@survey-feedback.example>
**To:** Peter Smith <peter.smith@tryhackme.com>
**Subject:** We value your feedback — quick survey

Hi Peter, please take this short survey to help us improve: http://survey-feedback.shadylink.fake.

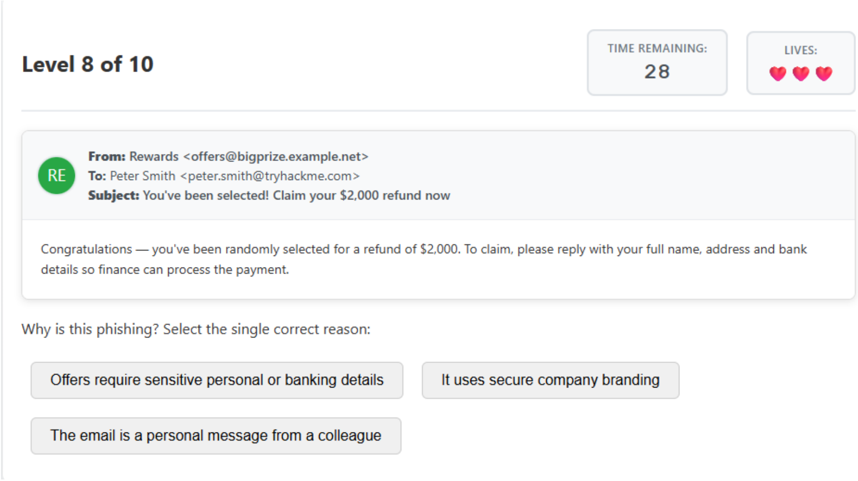
Why is this phishing? Select the single correct reason:

CS
It's an internal notification
Contains a suspicious third-party survey link
It's from a known vendor contact

*Figure 7 – Phishing Email*

Reason: It contains a suspicious third-party survey link

## Level 8


Level 8 of 10

TIME REMAINING:
28
LIVES:
❤ ❤ ❤
RE

**From:** Rewards <offers@bigprize.example.net>
**To:** Peter Smith <peter.smith@tryhackme.com>
**Subject:** You've been selected! Claim your $2,000 refund now

Congratulations — you've been randomly selected for a refund of $2,000. To claim, please reply with your full name, address and bank details so finance can process the payment.

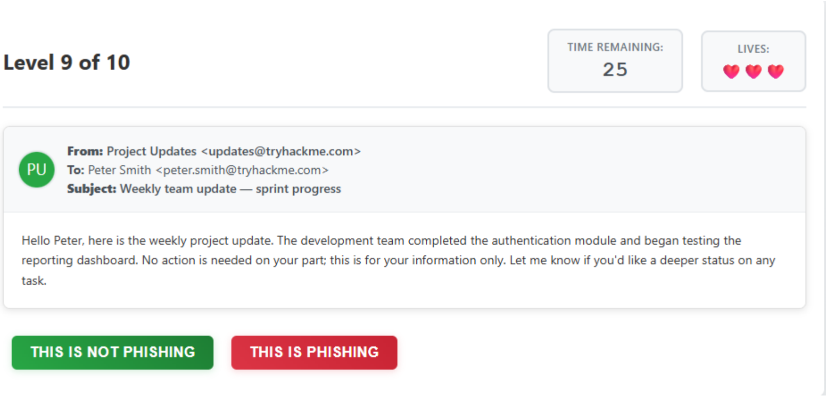
Why is this phishing? Select the single correct reason:

Offers require sensitive personal or banking details
It uses secure company branding
The email is a personal message from a colleague

*Figure 8 – Phishing Email*

Reason: Its offers require sensitive personal or banking details

## Level 9

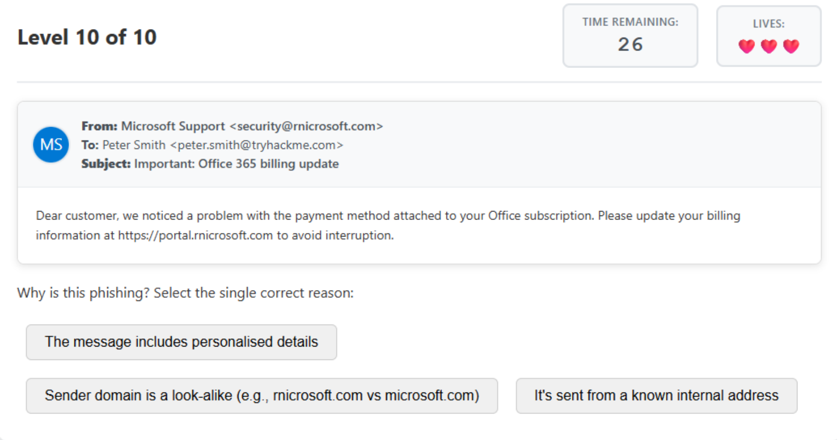

Level 9 of 10

**From:** Project Updates <updates@tryhackme.com>
**To:** Peter Smith <peter.smith@tryhackme.com>
**Subject:** Weekly team update — sprint progress

Hello Peter, here is the weekly project update. The development team completed the authentication module and began testing the reporting dashboard. No action is needed on your part; this is for your information only. Let me know if you'd like a deeper status on any task.

*Figure 9 – Not a Phishing Email*

## Level 10



Level 10 of 10

TIME REMAINING: 26

LIVES: ❤ ❤ ❤

MS

**From:** Microsoft Support <security@rnicrosoft.com>
**To:** Peter Smith <peter.smith@tryhackme.com>
**Subject:** Important: Office 365 billing update

Dear customer, we noticed a problem with the payment method attached to your Office subscription. Please update your billing information at https://portal.rnicrosoft.com to avoid interruption.

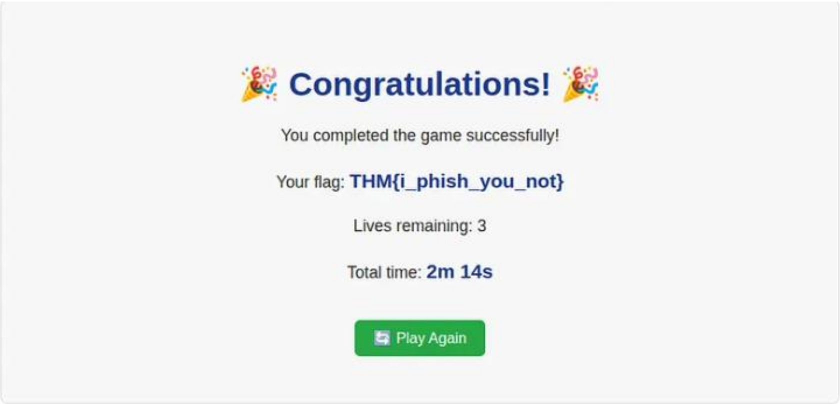
Why is this phishing? Select the single correct reason:

The message includes personalised details
Sender domain is a look-alike (e.g., rnicrosoft.com vs microsoft.com)
It's sent from a known internal address

*Figure 10 – Phishing Email*

Reason: Sender domain is look-alike (eg., rnicrosoft.com vs microsoft.com)

## Flag



🎉 Congratulations! 🎉

You completed the game successfully!

Your flag: **THM{i_phish_you_not}**

Lives remaining: 3

Total time: **2m 14s**

= THM{i_phish_you_not}