



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

BEGIN TRAINING

Level 1 of 10

TIME REMAINING:

7

LIVES:



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.

THIS IS PHISHING

THIS IS NOT PHISHING

This is not phishing because the email is internal, same company names and contains no urgent requests, asks for no sensitive information, and comes from a legitimate company domain.

Level 2 of 10

TIME REMAINING:

12

LIVES:



From: HR - Emma Roberts <emma.roberts@gmail.com>

To: Peter Smith <peter.smith@tryhackme.com>

Subject: Please review the attached payroll correction

Hi Peter, this is Emma from HR. I'm following up about a payroll correction that requires your bank details. Please open the file attached and send your updated bank account number and sort code so I can process this change.

Why is this phishing? Select the single correct reason:

Display name looks familiar but the email address doesn't match the organisation

It only asks for non-sensitive confirmation

The attachment is a benign PDF

Phishing. The display name looks familiar ("HR - Emma Roberts"), but the email address is a personal Gmail (@gmail.com), not an official company domain. It also asks for sensitive bank details via an attachment.

Level 3 of 10

TIME REMAINING:
21

LIVES:




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.

Why is this phishing? Select the single correct reason:

Uses urgent scare language to force action

Includes detailed account activity history

Comes from your manager

Phishing. Uses urgent scare language (“IMMEDIATE ACTION REQUIRED”) and threatens account suspension to rush the recipient into clicking a link without verification.

Level 4 of 10

TIME REMAINING:
9

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://paypal.trustedvendor-example.com/pay/12345> to make a payment.

Why is this phishing? Select the single correct reason:

The sender uses casual language

It references internal project codes

Payment link points to a suspicious domain

Phishing. The payment link points to a suspicious domain (paypal.trustedvendor-example.com), which is a misspelling of “PayPal” designed to deceive.

Level 5 of 10

TIME REMAINING:
15

LIVES:
❤️❤️❤️



From: Accounts <accounts@vendor-payments.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Invoice INV-2025-334 (Action required)

Hi Peter, your invoice INV-2025-334 is ready. Please review and pay via <https://pay.vendor-payments-secure.com/invoice/INV-2025-334>.

Why is this phishing? Select the single correct reason:

Link uses a deceptive domain to mimic a payment portal

Includes accurate invoice numbers

Sender uses correct business signage

Phishing. The link uses a deceptive domain (vendor-payments-secure.com) that mimics a legitimate payment portal to trick users into entering payment information.

Level 6 of 10

TIME REMAINING:
13

LIVES:
❤️❤️❤️



From: Microsoft Support <security@rnmicrosoft.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.rnmicrosoft.com> to avoid interruption.

Why is this phishing? Select the single correct reason:

Sender domain is a look-alike (e.g., rnmicrosoft.com vs microsoft.com)

The message includes personalised details

It's sent from a known internal address

Phishing. The sender domain is a look-alike

Level 7 of 10

TIME REMAINING:
16

LIVES:
❤️❤️❤️



From: Jane Doe <jane.doe@tryhackme.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Lunch Plans for Tomorrow

Hey Peter, do you want to grab lunch tomorrow at noon at the new Italian restaurant downtown? They have good reviews and a quieter back room for conversations. Let me know if that works for you.

THIS IS NOT PHISHING

THIS IS PHISHING

Not Phishing. This is a casual, non-urgent email from a colleague at the same company domain (tryhackme.com), with no request for sensitive data or suspicious links.

Level 8 of 10

TIME REMAINING:
10

LIVES:
❤️❤️❤️



From: IT Helpdesk <it-support@service-update.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Mandatory security re-login required

Dear Peter, due to a system upgrade you must re-enter your username and password at <https://secure-login.example.com> within 48 hours to retain access.

Why is this phishing? Select the single correct reason:

Contains a link to a credential-collecting page

Comes from a senior manager

It's a casual invite to an event

Phishing. Contains a link to a credential-collecting page disguised as a legitimate login portal, urging quick action due to a “system upgrade.”

Level 9 of 10

TIME REMAINING:
12

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:

It's an internal notification

Contains a suspicious third-party survey link

It's from a known vendor contact

Phishing. Contains a suspicious third-party survey link (shadylink.fake) that could lead to malware or data harvesting.

Level 10 of 10

TIME REMAINING:
22

LIVES:




From: Recruitment <jobs@career-opps.example.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Exciting job opportunity — immediate start

Congratulations! We reviewed your profile and you'd be perfect for a new role. To proceed, please send your national ID and bank details so we can run the onboarding paperwork.

Why is this phishing? Select the single correct reason:

Comes from an internal HR alias

Asks for sensitive personal identification and banking details

Includes calendar invites

Legitimately phishing. Asks for highly sensitive personal identification and banking details under the guise of onboarding, which is not standard practice for legitimate job offers.

Congratulations!

You completed the game successfully!

Your flag: **THM{i_phish_you_not}**

Lives remaining: 3

Total time: **8m 31s**

 Play Again