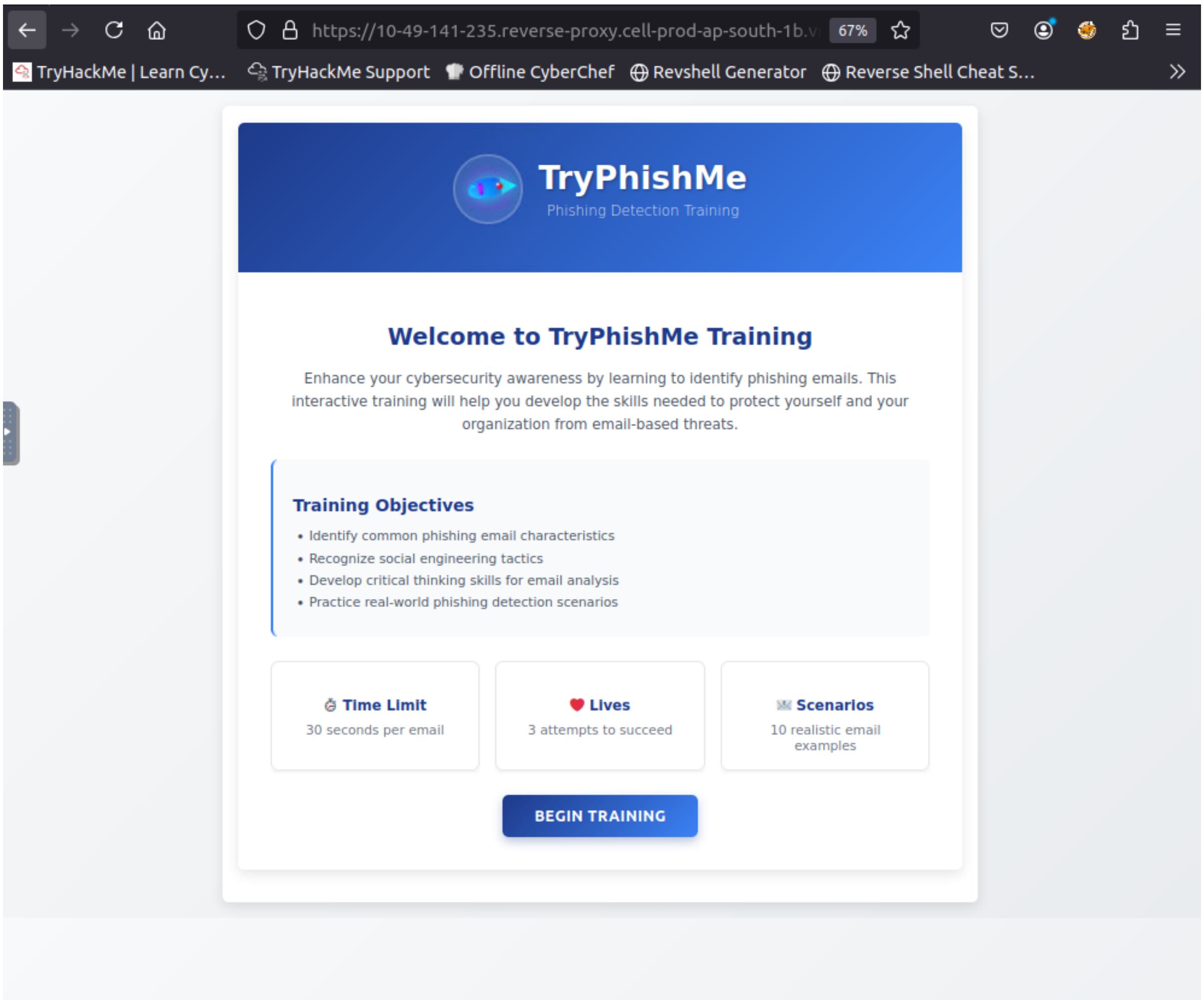
Write-Up: The Phishing Pond (TryHackMe).

Task: Store the interactive training of TryPhishMe by identifying phishing emails and legitimate messages correctly.

Introduction

In the online module that link from TryHackMe provided, TryPhishMe, 10 real email examples were thrown down. We were to examine sender addresses, domains, urgency vibe, and the links particularly to determine whether an email was a Safe (Not Phishing) or a Malicious (Phishing) one. The introduction page that can be found at the beginning of the site appears as it is shown below.



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

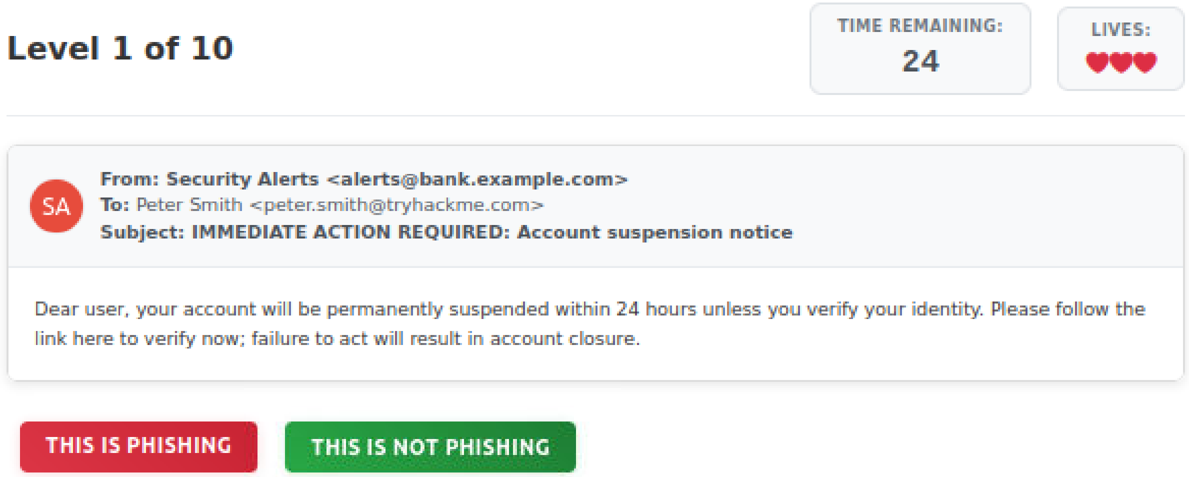
Scenarios: 10 realistic email examples

BEGIN TRAINING

Scenario Analysis (Levels 1-10)

Level 1: Suspension of account warning.

Answer: THIS IS PHISHING



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.

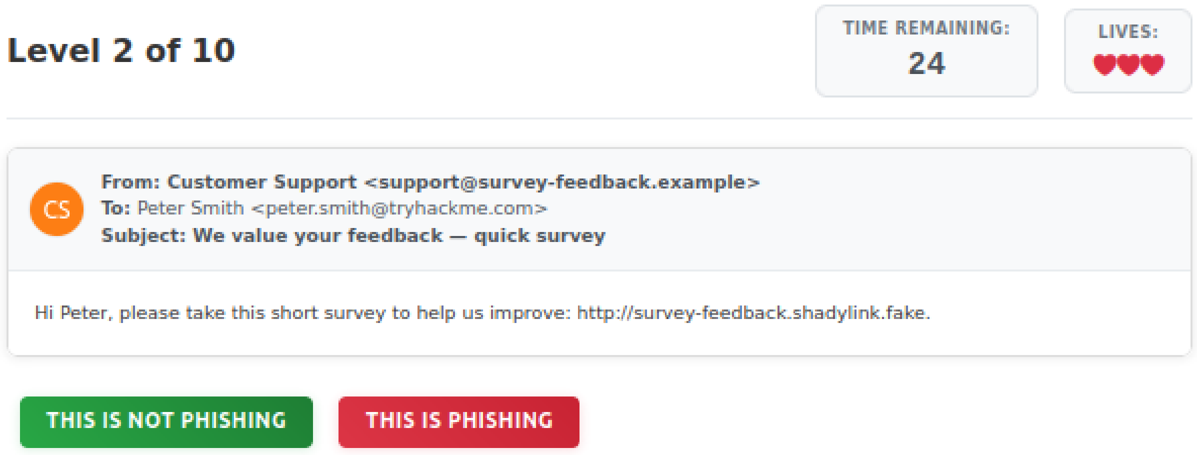
Sense of urgency: The subject line is caps, and it is threatening permanent suspension within 24 hours (IMMEDIATE ACTION REQUIRED). They give time to get you to panicking.

Generic Greeting: The email includes a simple message which states that it addressed you as Dear user, not by your name.

Red Flag: Banks and legitimate services do not request that you verify identity via direct link in an email very often.

Level 2: Survey Feedback

Answer: THIS IS PHISHING



Level 2 of 10

TIME REMAINING: 24

LIVES: ❤❤❤

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

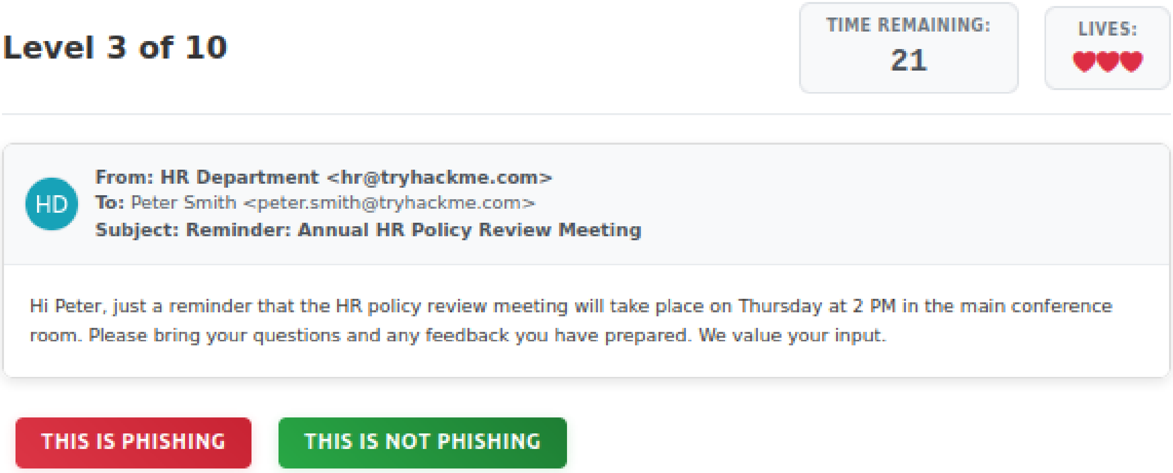
Hi Peter, please take this short survey to help us improve: http://survey-feedback.shadylink.fake.

Malicious Domain: The malicious link in the messsge goes to a site, which is:http: survey-feedback.shadylink.fake. The domain name has even fake and shadylink which are red flags.

Sender Mismatch: The sender is Customer Support, and the domain does not belong to any trusted organization.

Level 3: HR Policy Meeting

Answer: THIS IS NOT PHISHING



Level 3 of 10

TIME REMAINING: 21

LIVES: ♥♥♥

From: HR Department <hr@tryhackme.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Reminder: Annual HR Policy Review Meeting

Hi Peter, just a reminder that the HR policy review meeting will take place on Thursday at 2 PM in the main conference room. Please bring your questions and any feedback you have prepared. We value your input.

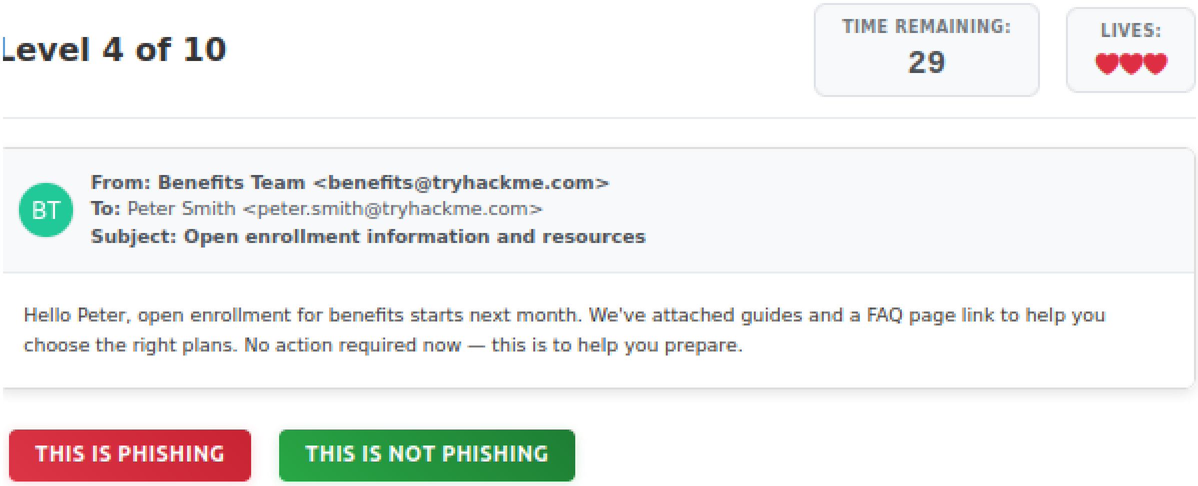
Internal Sender: The email itself is sent by the email address of the person who works in the HR department of tryhackme.com to peter.smith@tryhackme.com- pure internal communication.

Context: It is simply a meeting reminder in a particular date and location.

Safe Content: No malicious links, attachments or data requests.

Level 4: Benefits Enrolment

Answer: THIS IS NOT PHISHING



Level 4 of 10

TIME REMAINING: 29

LIVES: ❤❤❤

From: Benefits Team <benefits@tryhackme.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Open enrollment information and resources

Hello Peter, open enrollment for benefits starts next month. We've attached guides and a FAQ page link to help you choose the right plans. No action required now — this is to help you prepare.

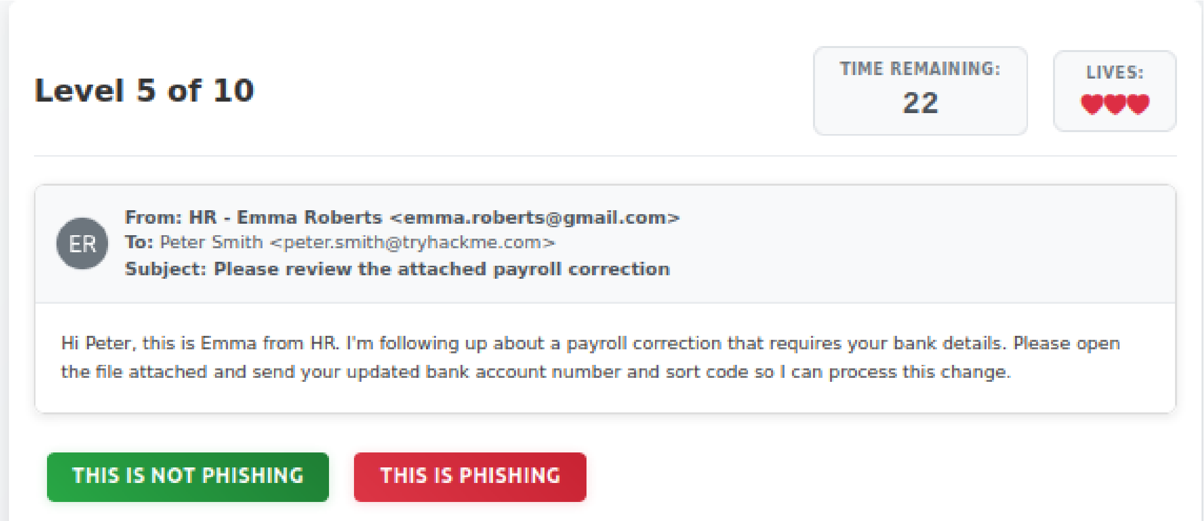
None of the Call to Action: It reads, no action yet to be taken. Real phishing mailings always demand action.

Internal Source: The message is sent by benefits, benefits@tryhackme.com, which is the company domain.

Information: The mail does not require credentials but provides you with resources (guides/FAQs).

Level 5: Payroll Correction

Answer: THIS IS PHISHING



From: HR - Emma Roberts <emma.roberts@gmail.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Please review the attached payroll correction

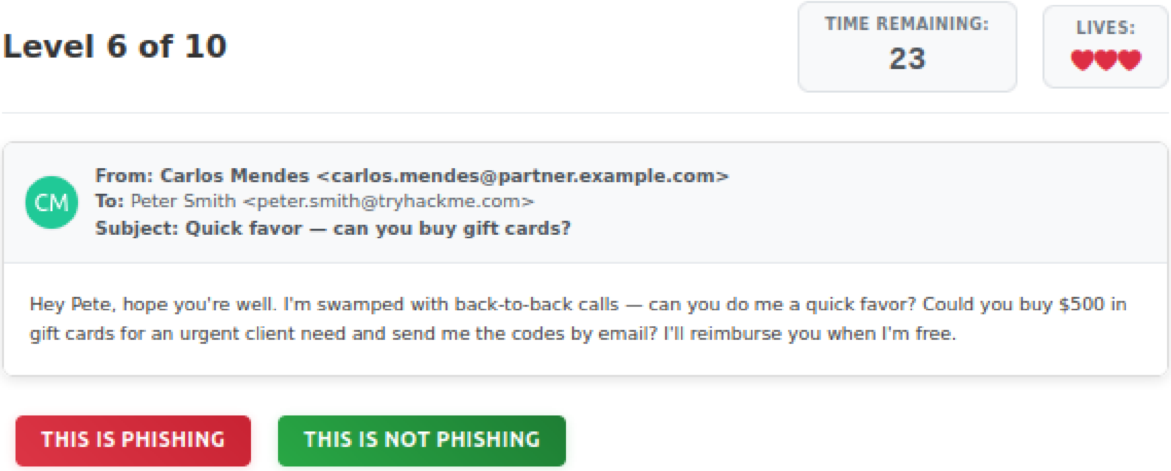
Hi Peter, this is Emma from HR. I'm following up about a payroll correction that requires your bank details. Please open the file attached and send your updated bank account number and sort code so I can process this change.

Public Domain: The sender identifies him/herself as HR - Emma Roberts but the email address is a generic, non-corporate, one, that is, an Emma.roberts@gmail.com.

Sensitive Data Request: It requests an updated bank account number, the request presented in the form of an attached file. A secure portal would be utilized by real HR and not email attachments. Also, the real HR doesn’t need to ask for your bank account number since they already have it.

Level 6: CEO Fraud (Gift Cards Scam)

Answer: THIS IS PHISHING



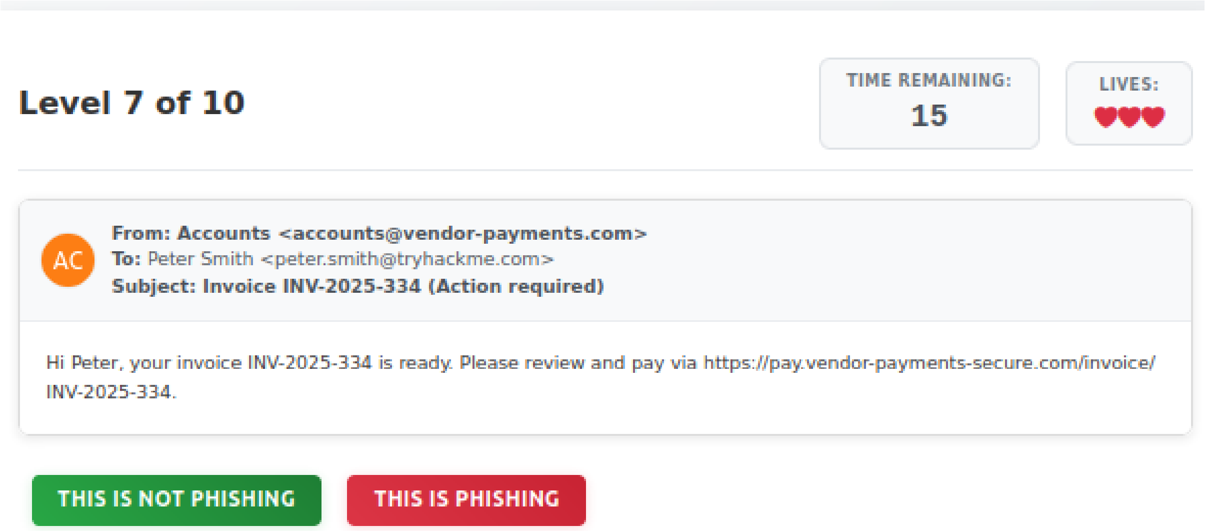
From: Carlos Mendes <carlos.mendes@partner.example.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Quick favor — can you buy gift cards?

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.

The "Gift Cards" Pointer: They would like you to purchase through 500 gift cards. This is what a BEC (Business Email Compromise) scam is characterized by. Gift cards are not used by legitimate companies. Instead, the sender gives an excuse that they are too busy answering phone calls, and you cannot confirm.

Level 7: Invoice Payment

Answer: THIS IS PHISHING



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

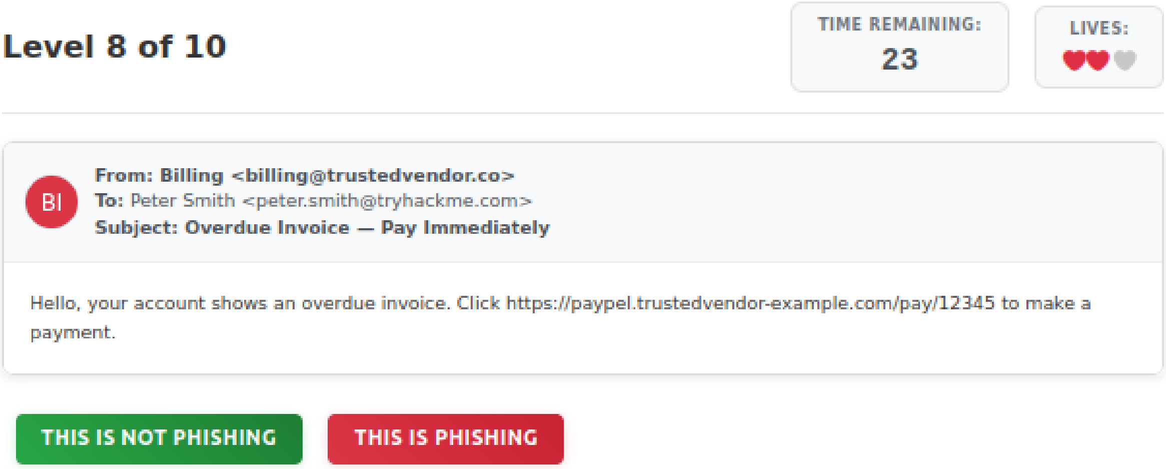
Hi Peter, your invoice INV-2025-334 is ready. Please review and pay via https://pay.vendor-payments-secure.com/invoice/INV-2025-334.

Domain Spoofing: The mailer is accounts.vendor-payments.com, and the URL is pay.vendor-payments-secure.com. Adding -secure is the time-honoured look-a-like technique.

Unsolicited Invoice: Unsolicited invoices are one of the prevalent patterns of credit card theft or malware.

Level 8: Overdue Invoice (Typosquatting)

Answer: THIS IS PHISHING


Level 8 of 10

TIME REMAINING:
23

LIVES:
♥♥♥

BI

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

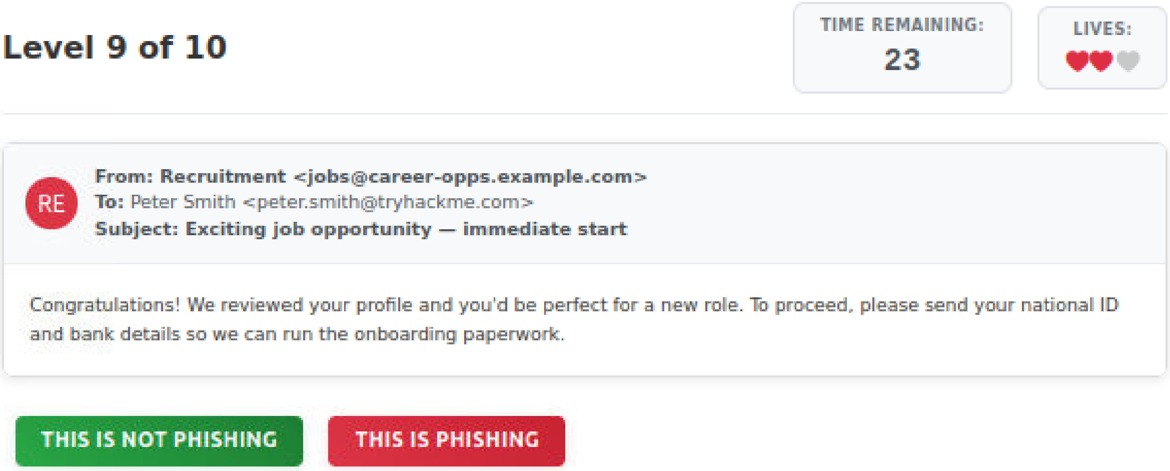
Hello, your account shows an overdue invoice. Click https://paypel.trustedvendor-example.com/pay/12345 to make a payment.

Typosquatting: The connection is to https://paypel.trustedvendor.... There is a visual trick, the misspelling of Paypel (PayPal).

Threat: The topic Pay Immediately attempts to fear your critical thinking.

Level 9: Job Recruitment

Answer: THIS IS PHISHING



Level 9 of 10

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

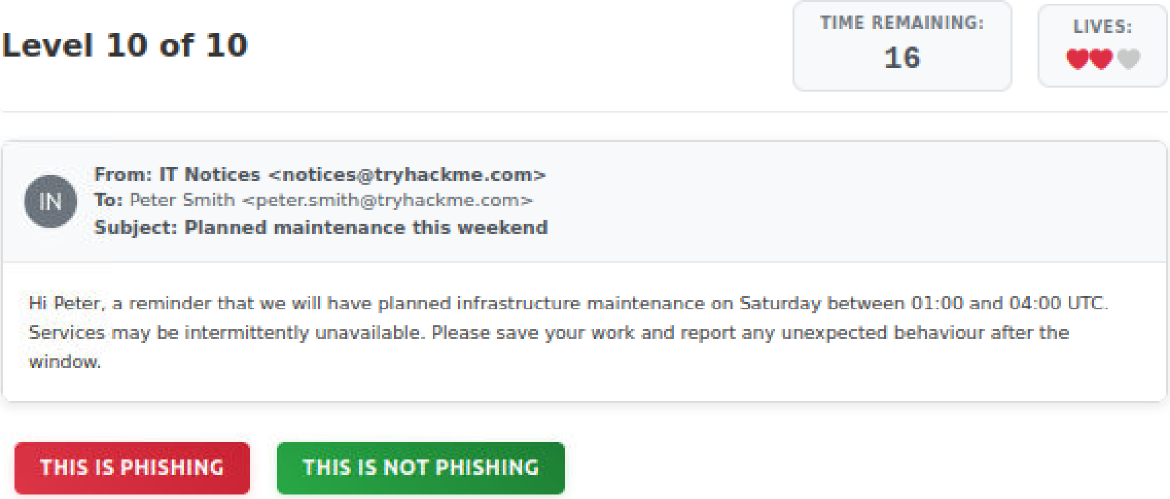
Congratulations! We reviewed your profile and you'd be perfect for a new role. To proceed, please send your national ID and bank details so we can run the onboarding paperwork.

Too Good To Be True: An offer of a job without an interview is a huge red flag.

Data Harvesting: It immediately requests your national ID and banking information, which is a typical identity theft camouflaged as an employment opportunity.

Level 10: IT Maintenance Notice

Answer: THIS IS NOT PHISHING



Level 10 of 10

TIME REMAINING: 16

LIVES: ❤❤♡

IN

From: IT Notices <notices@tryhackme.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Planned maintenance this weekend

Hi Peter, a reminder that we will have planned infrastructure maintenance on Saturday between 01:00 and 04:00 UTC. Services may be intermittently unavailable. Please save your work and report any unexpected behaviour after the window.

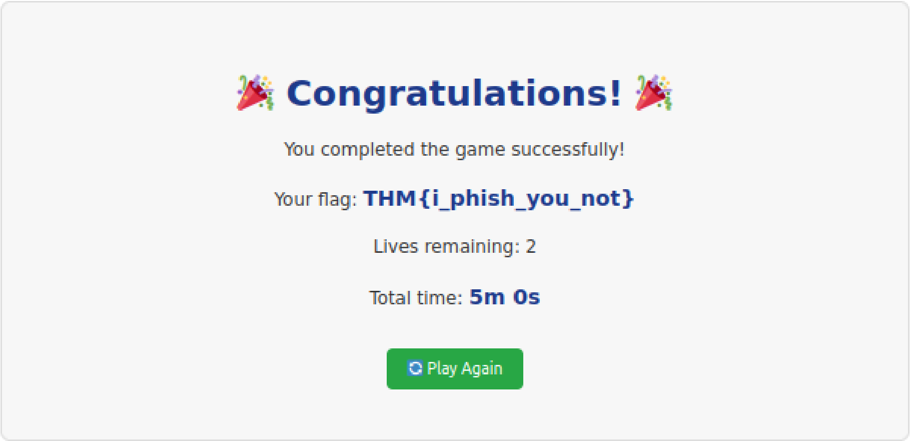
Internal Sender: The email is sent by notices@tryhackme.com which is a legitimate internal address.

Informational Only: It simply provides information to the users of the impending maintenance and to save the work. No requests of passwords or suspicious clicks. (Insert Screenshot: 10.0.png)

Conclusion

I completed the module after being able to identify all 10 scenarios successfully. This drill truly made me understand the importance of checking the domains of the sender, being suspicious of the presence of typos or typosquatting in URLs and being aware of the techniques of social engineering such as artificial urgency or CEO fraud.

Final Flag:



🎉 Congratulations! 🎉

You completed the game successfully!

Your flag: THM{i_phish_you_not}

Lives remaining: 2

Total time: 5m 0s