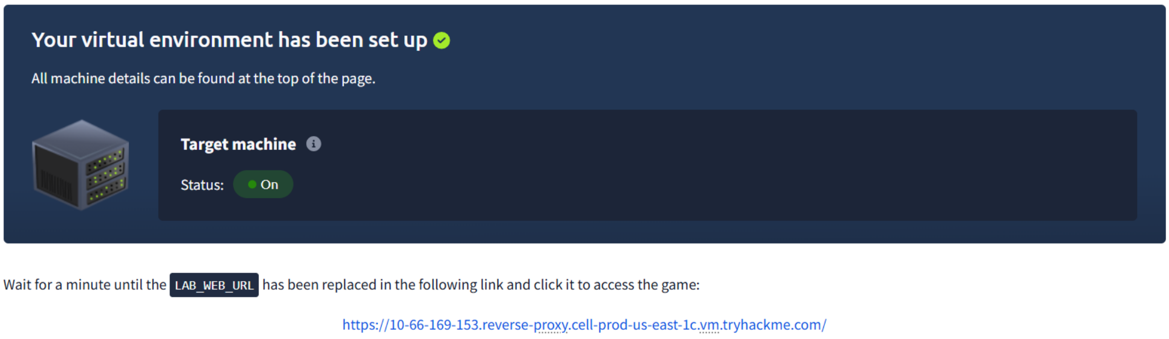
Social engineering task

Name: Muhammad A’beed bin Firdaus (52215124303)

Exercise 1 (The Phishing Pond)

Go to tryhackme The Phishing Pond and start the VM, then click the link below.



Your virtual environment has been set up ✓

All machine details can be found at the top of the page.

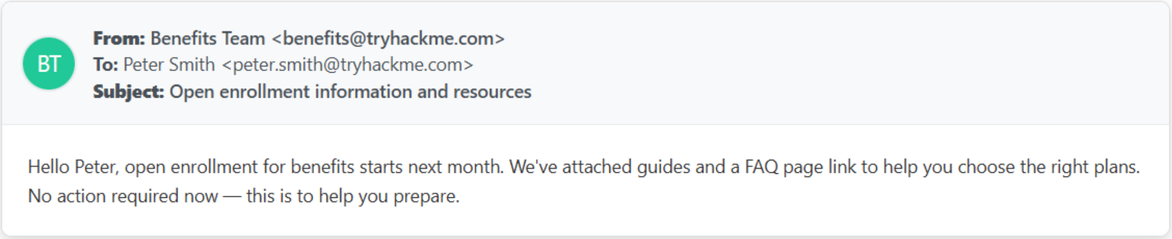
Target machine ℹ

Status: ● On

Wait for a minute until the `LAB_WEB_URL` has been replaced in the following link and click it to access the game:

https://10-66-169-153.reverse-proxy.cell-prod-us-east-1c.vm.tryhackme.com/

Start answering the questions whether the emails are legit or phishing.

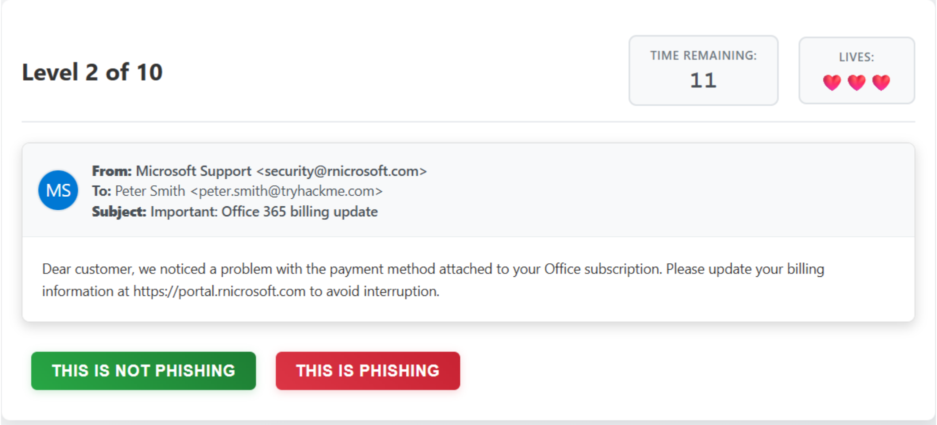


BT

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.

Legit email, no wrong grammar or weird links



Level 2 of 10

TIME REMAINING: 11

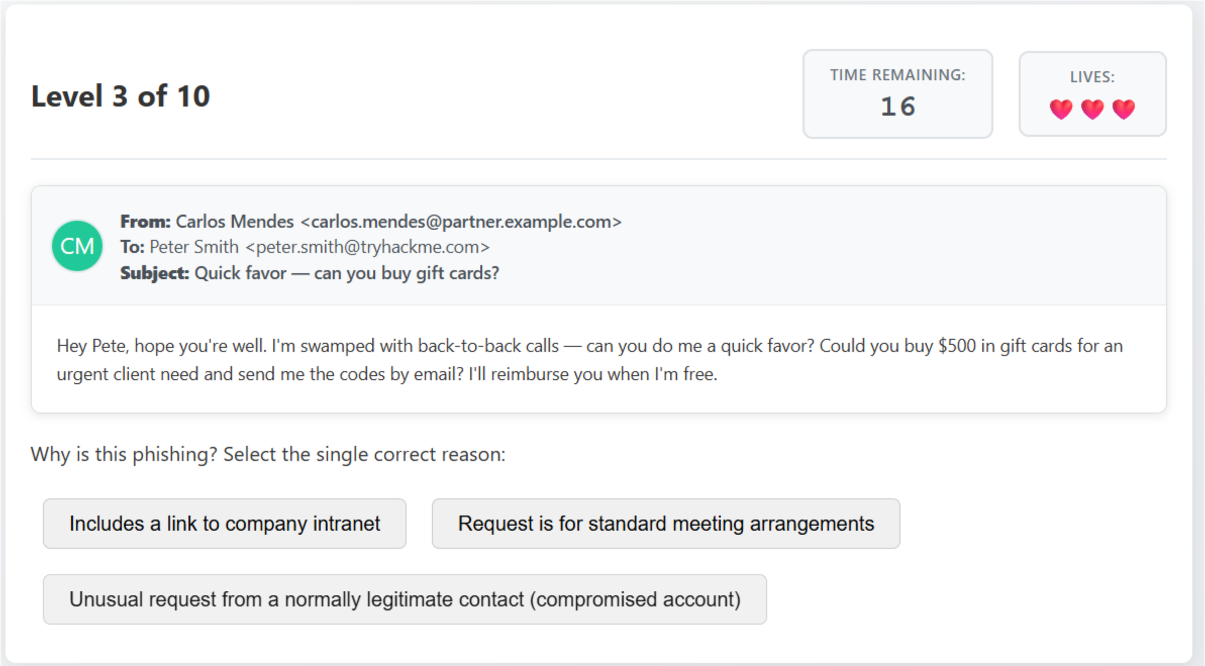
LIVES: ♥ ♥ ♥

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.

Link is fake, r nicrosoft, masked to look like Microsoft.



Level 3 of 10

TIME REMAINING: 16

LIVES: ♥ ♥ ♥

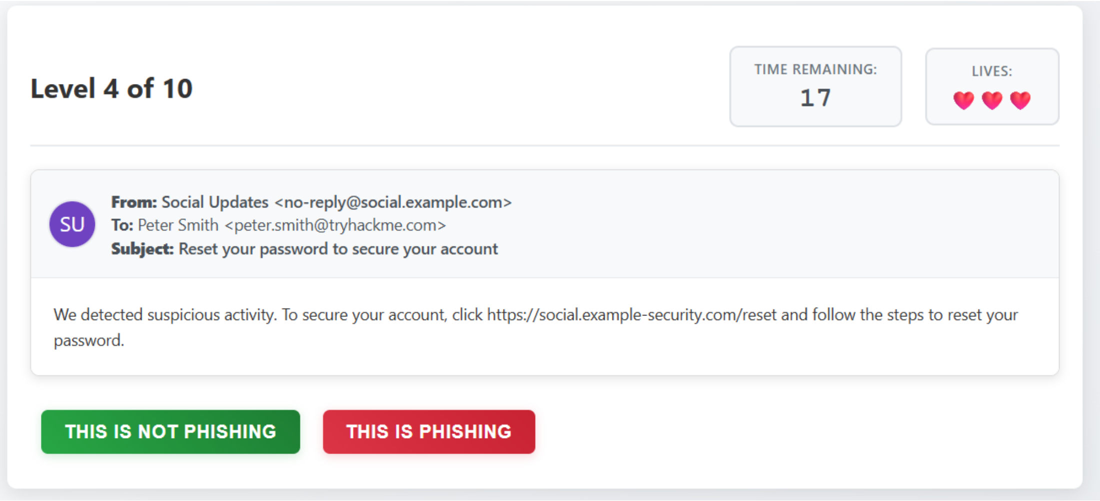
From: Carlos Mendes <carlos.mendes@partner.example.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Quick favor — can you buy gift cards?

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:

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

Phishing, unusual request from contact.



Level 4 of 10

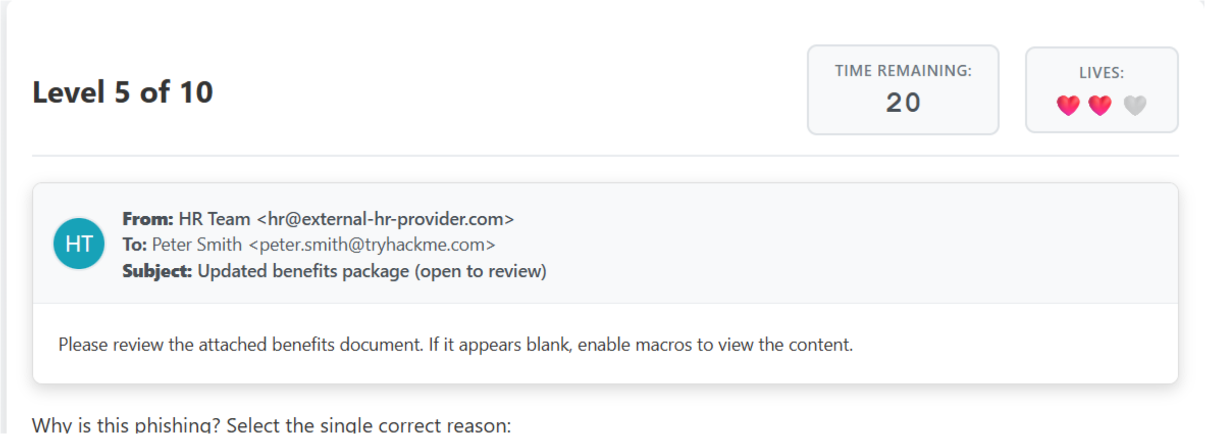
TIME REMAINING: 17

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.

Phishing, fake url link.



Level 5 of 10

TIME REMAINING: 20

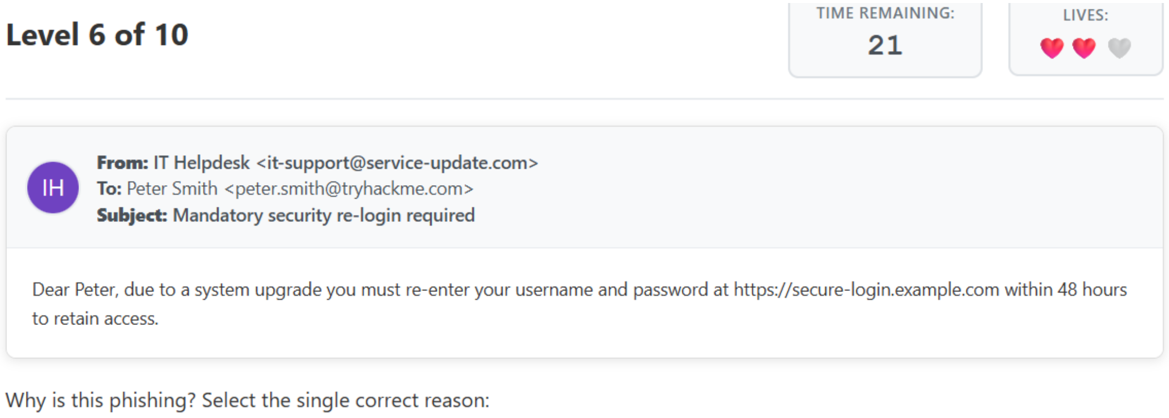
LIVES: ♥ ♥ ♡

From: HR Team <hr@external-hr-provider.com>
To: Peter Smith <peter.smith@tryhackme.com>
Subject: Updated benefits package (open to review)

Please review the attached benefits document. If it appears blank, enable macros to view the content.

Why is this phishing? Select the single correct reason:

Phishing, it asked to enable macros



Level 6 of 10

TIME REMAINING: 21

LIVES: ♥ ♥ ♡

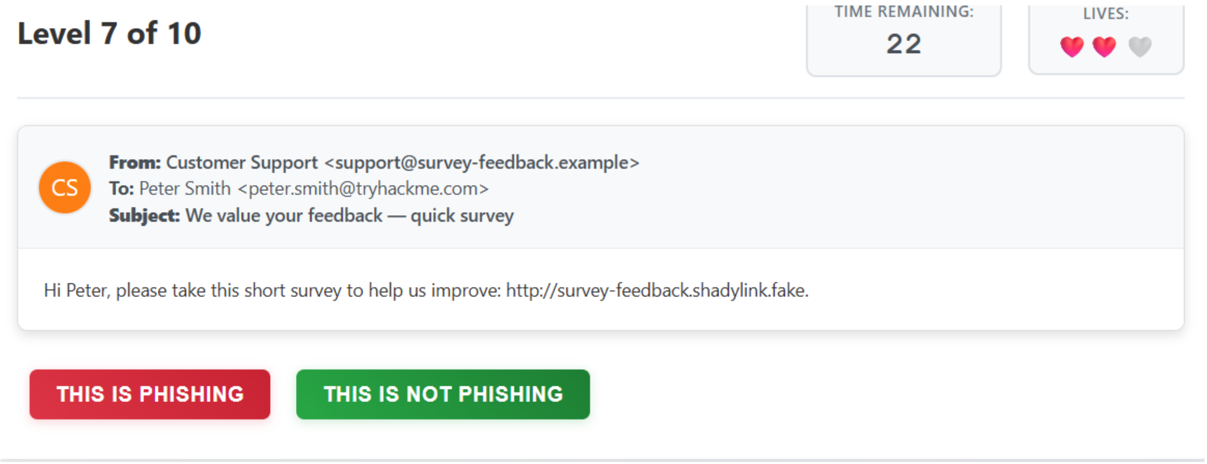
IH

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:

Phishing, link is malicious and will store credentials.



Level 7 of 10

TIME REMAINING: 22

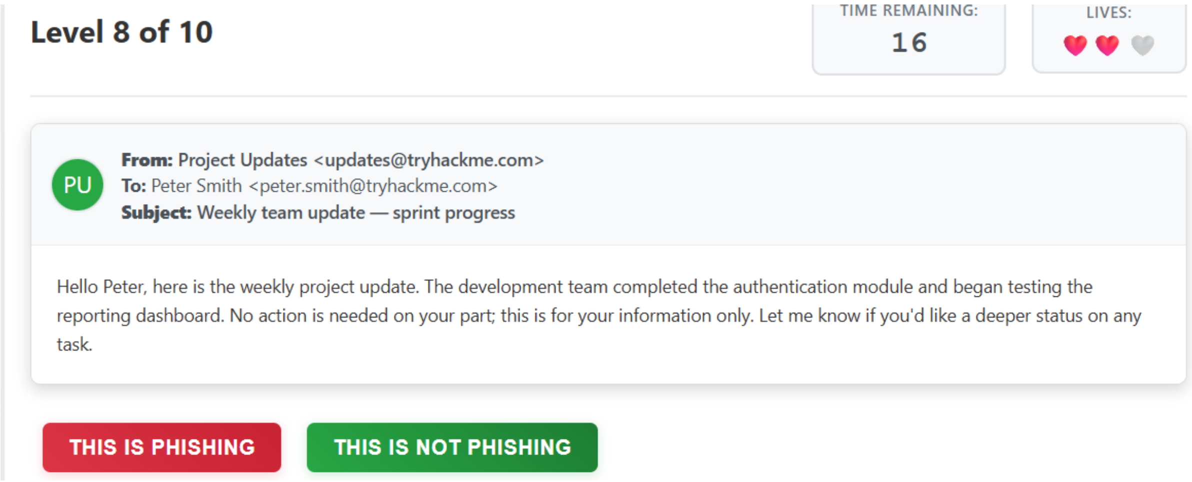
LIVES: ♥ ♥ ♡

CS

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.

Phishing, fake link.



Level 8 of 10

TIME REMAINING: 16

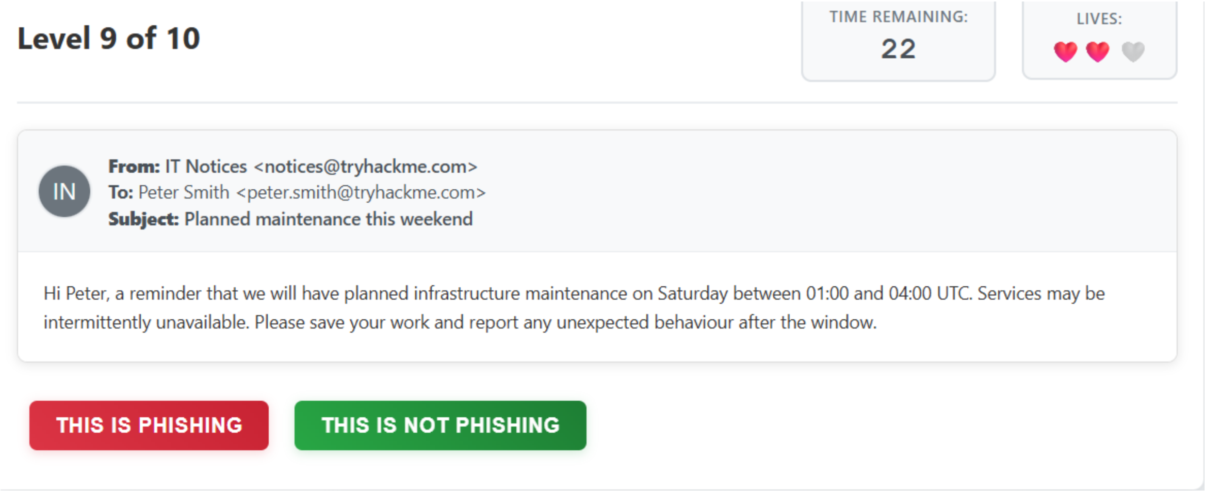
LIVES: ♥ ♥ ♡

PU

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.

Legit, no links or malicious urls.

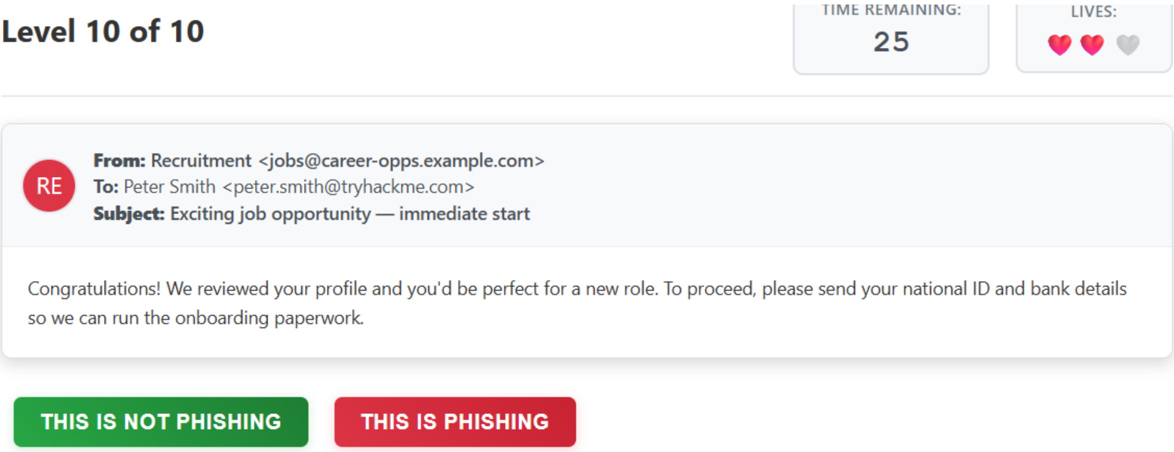

Level 9 of 10

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.

Legit, no malicious urls.

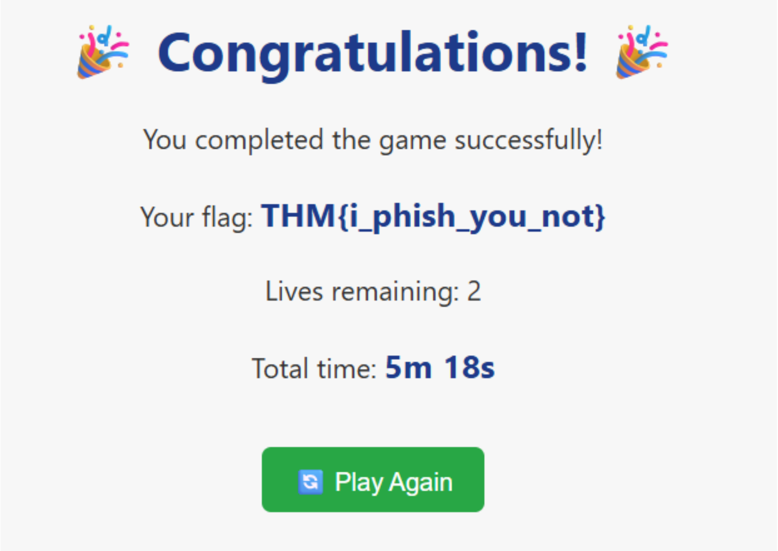

Level 10 of 10

RE

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.

Phishing, asking for national ID and bank.


🎉 Congratulations! 🎉

You completed the game successfully!

Your flag: **THM{i_phish_you_not}**

Lives remaining: 2

Total time: **5m 18s**

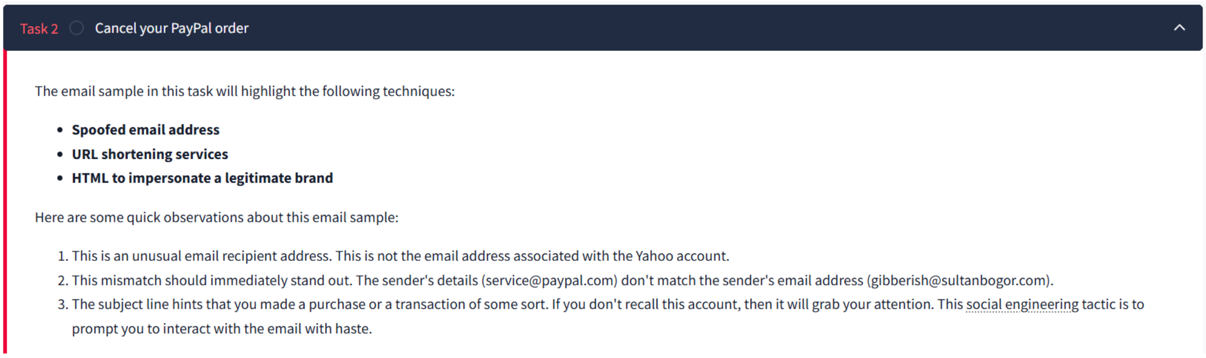
Done, get the flag and complete the exercise.

Exercise 2 (Phishing emails in action)

Phishing Emails in Action

Learn the different indicators of phishing attempts by examining actual phishing emails.

Complete all the task to finish the exercise.



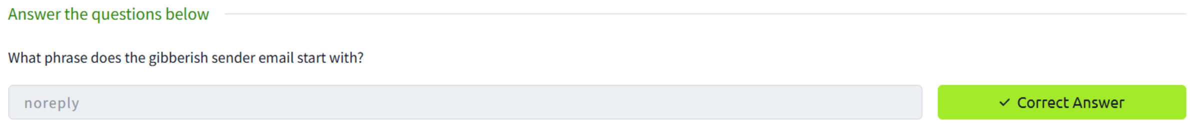
The email sample in this task will highlight the following techniques:

- **Spoofed email address**
- **URL shortening services**
- **HTML to impersonate a legitimate brand**

Here are some quick observations about this email sample:

1. This is an unusual email recipient address. This is not the email address associated with the Yahoo account.
2. This mismatch should immediately stand out. The sender's details (service@paypal.com) don't match the sender's email address (gibberish@sultanbogor.com).
3. The subject line hints that you made a purchase or a transaction of some sort. If you don't recall this account, then it will grab your attention. This social engineering tactic is to prompt you to interact with the email with haste.

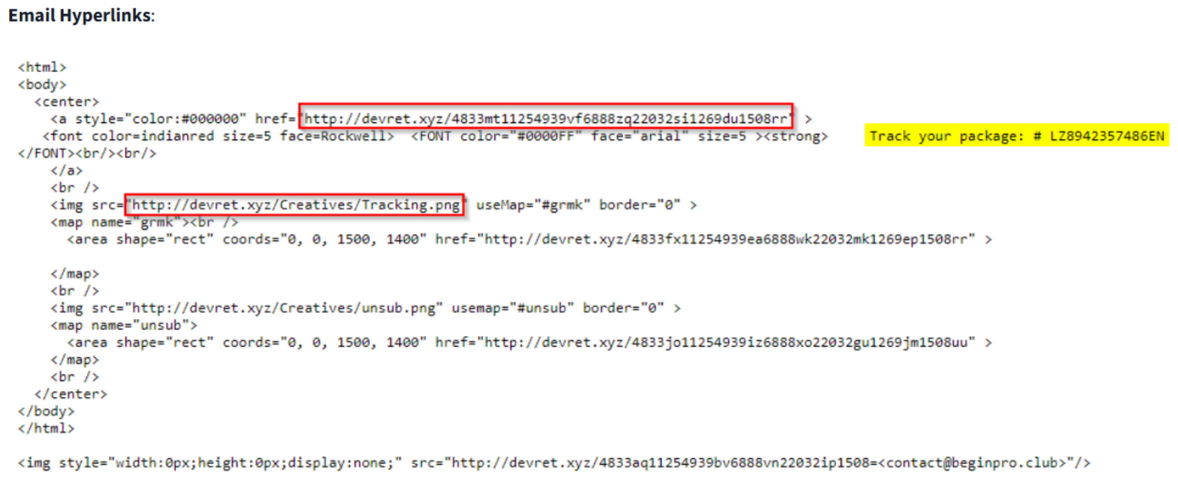
The sender's email started with noreply.



Answer the questions below

What phrase does the gibberish sender email start with?

noreply



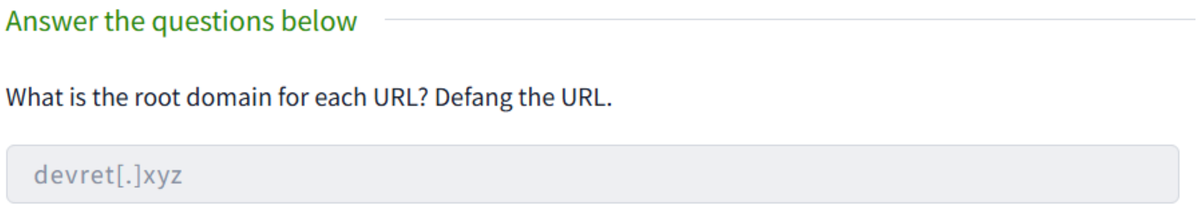
Email Hyperlinks:

```
<html>
<body>
  <center>
    <a style="color:#000000" href="http://devret.xyz/4833mt11254939vf6888zq22032si1269du1508rr" >
   <font color=indianred size=5 face=Rockwell>  <FONT color="#0000FF" face="arial" size=5 ><strong>     Track your package: # LZ8942357486EN
</FONT><br/><br/>
    </a>
    <br />
    <img src="http://devret.xyz/Creatives/Tracking.png" useMap="#grmk" border="0" >
    <map name="grmk"><br />
      <area shape="rect" coords="0, 0, 1500, 1400" href="http://devret.xyz/4833fx11254939ea6888wk22032mk1269ep1508rr" >

    </map>
    <br />
    <img src="http://devret.xyz/Creatives/unsub.png" usemap="#unsub" border="0" >
    <map name="unsub">
      <area shape="rect" coords="0, 0, 1500, 1400" href="http://devret.xyz/4833jo11254939iz6888xo22032gu1269jm1508uu" >
    </map>
    <br />
  </center>
</body>
</html>

<img style="width:0px;height:0px;display:none;" src="http://devret.xyz/4833aq11254939bv6888vn22032ip1508=<contact@beginpro.club>"/>
```

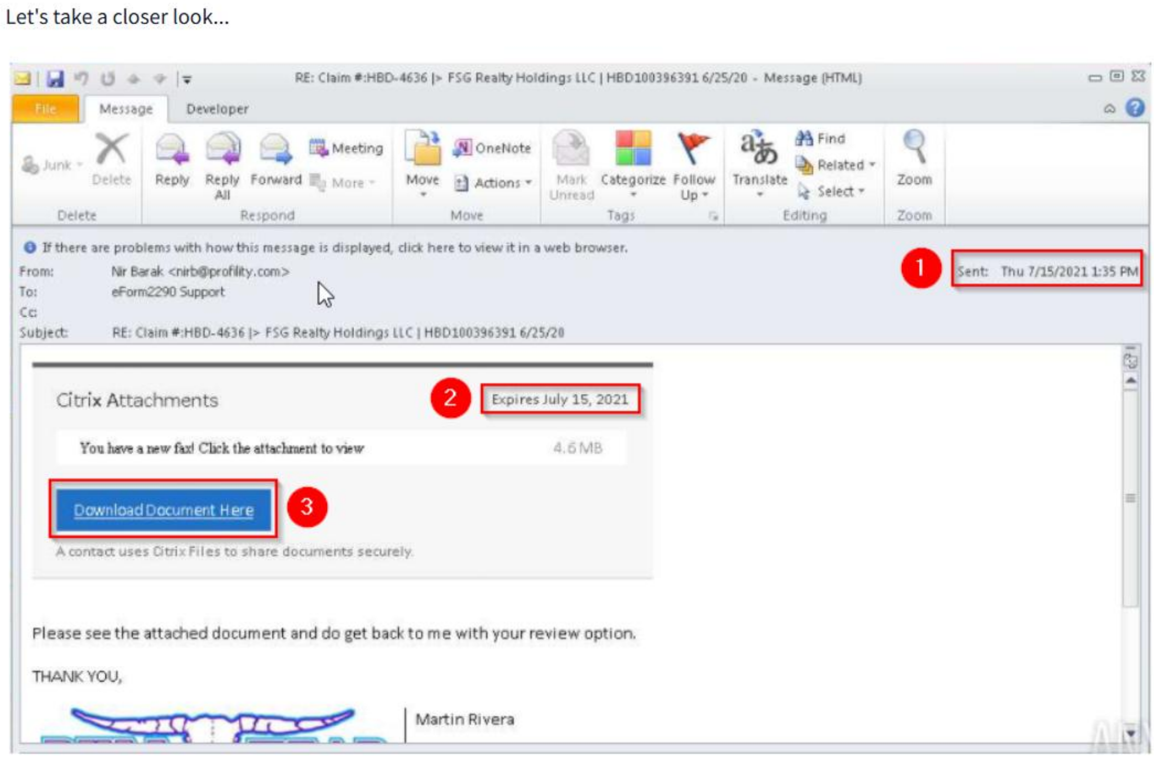
To defang the URL, insert [] between “. “ . So, from devret.xyz -> devret[.]xyz.



Answer the questions below

What is the root domain for each URL? Defang the URL.

devret[.]xyz



Let's take a closer look...

RE: Claim #:HBD-4636 |> FSG Realty Holdings LLC | HBD100396391 6/25/20 - Message (HTML)

If there are problems with how this message is displayed, click here to view it in a web browser.

From: Nir Barak <nirb@profility.com>

To: eForm2290 Support

Cc:

Subject: RE: Claim #:HBD-4636 |> FSG Realty Holdings LLC | HBD100396391 6/25/20

Sent: Thu 7/15/2021 1:35 PM

Citrix Attachments

Expires July 15, 2021

You have a new fax! Click the attachment to view 4.6 MB

Download Document Here

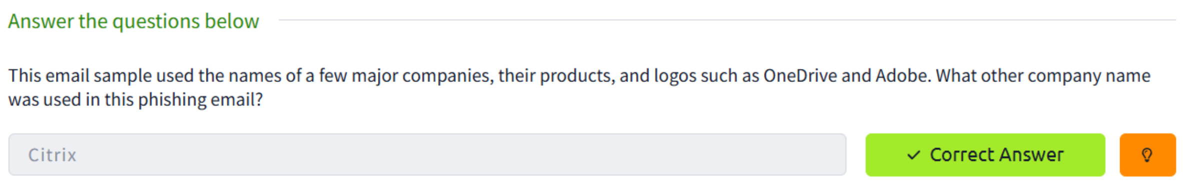
A contact uses Citrix Files to share documents securely.

Please see the attached document and do get back to me with your review option.

THANK YOU,

Martin Rivera

The other company that was used in Citrix.

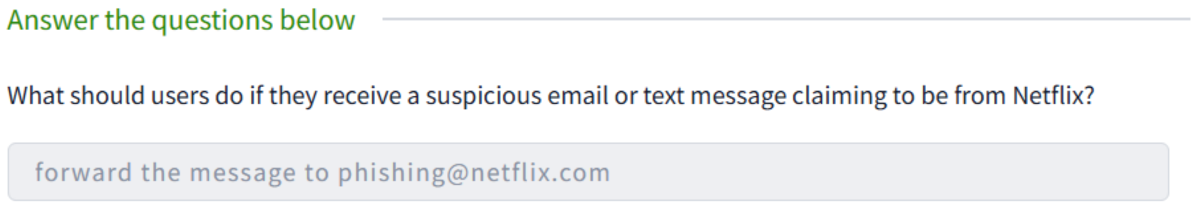


Answer the questions below

This email sample used the names of a few major companies, their products, and logos such as OneDrive and Adobe. What other company name was used in this phishing email?

Citrix

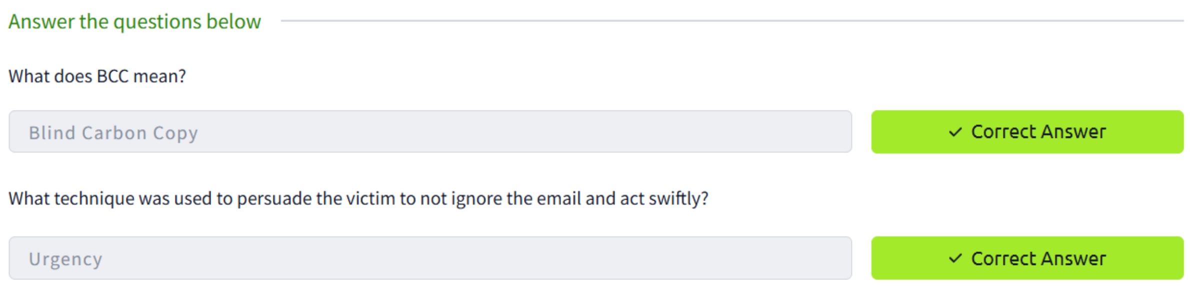
Suspicious emails from Netflix should be immediately reported to the official Netflix phishing site.



Answer the questions below

What should users do if they receive a suspicious email or text message claiming to be from Netflix?

forward the message to phishing@netflix.com



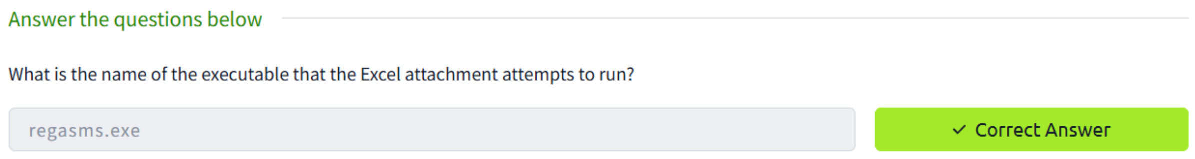
Answer the questions below

What does BCC mean?

Blind Carbon Copy

What technique was used to persuade the victim to not ignore the email and act swiftly?

Urgency



Answer the questions below

What is the name of the executable that the Excel attachment attempts to run?

regasms.exe