CYBER FORENSICS

NAME: ARAVINDHAN.K

ROLLNO: CH.EN.U4CYS22001

Experiment 5

Phishing Email analysis with www.tryhackme.com

Introduction

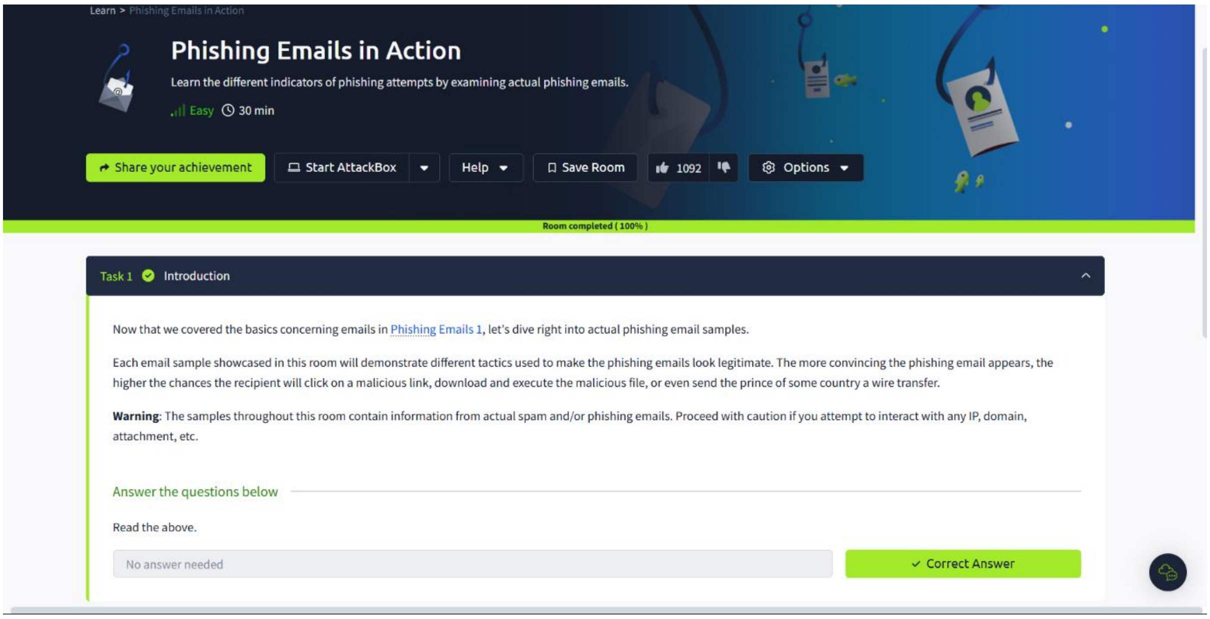
Phishing is a prevalent cyber threat where attackers use fraudulent emails to deceive recipients into revealing sensitive information or installing malicious software. Analyzing phishing emails is a critical skill in email forensics, enabling cybersecurity professionals to detect, investigate, and prevent phishing attacks. This experiment focuses on using the TryHackMe platform to analyze phishing emails, identify indicators of compromise (IOCs), and gain insights into the methods attackers employ.

Aim:

To perform email forensics. (https://tryhackme.com/r/room/phishingemails2rytmuv)

Screenshot:

Question 1:



Phishing Emails in Action

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

Easy 30 min

Task 1 ✓ Introduction

Now that we covered the basics concerning emails in Phishing Emails 1, let's dive right into actual phishing email samples.

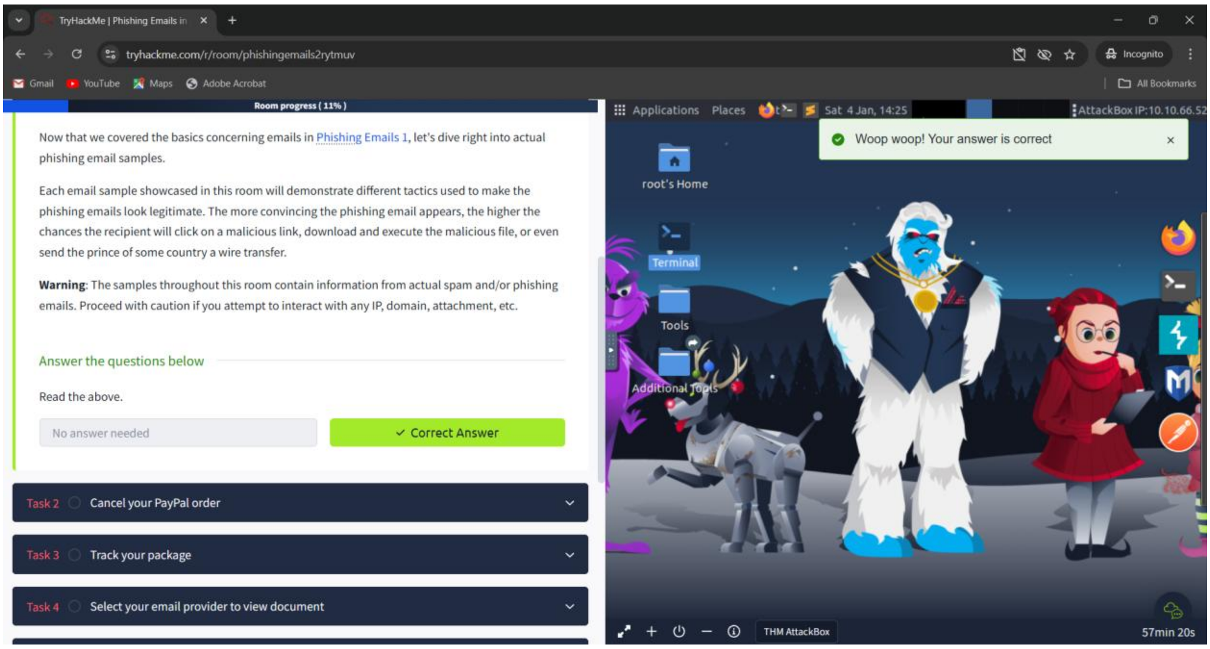
Each email sample showcased in this room will demonstrate different tactics used to make the phishing emails look legitimate. The more convincing the phishing email appears, the higher the chances the recipient will click on a malicious link, download and execute the malicious file, or even send the prince of some country a wire transfer.

Warning: The samples throughout this room contain information from actual spam and/or phishing emails. Proceed with caution if you attempt to interact with any IP, domain, attachment, etc.

Answer the questions below

Read the above.

No answer needed ✓ Correct Answer



Now that we covered the basics concerning emails in Phishing Emails 1, let's dive right into actual phishing email samples.

Each email sample showcased in this room will demonstrate different tactics used to make the phishing emails look legitimate. The more convincing the phishing email appears, the higher the chances the recipient will click on a malicious link, download and execute the malicious file, or even send the prince of some country a wire transfer.

Warning: The samples throughout this room contain information from actual spam and/or phishing emails. Proceed with caution if you attempt to interact with any IP, domain, attachment, etc.

Answer the questions below

Read the above.

No answer needed

✓ Correct Answer

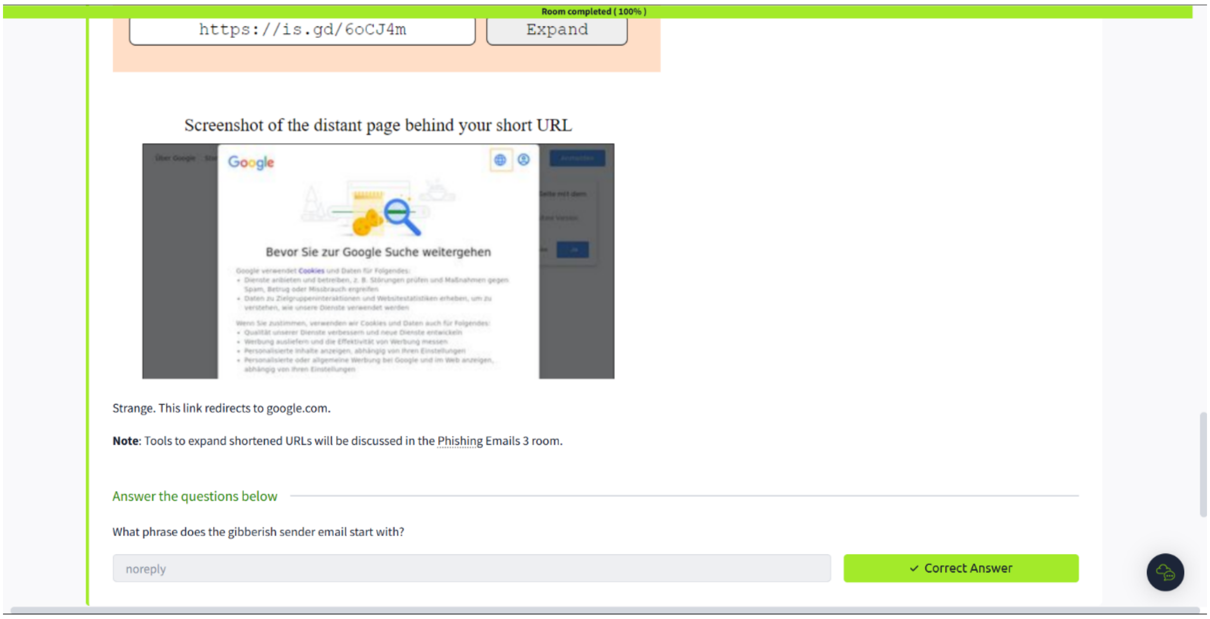
Woop woop! Your answer is correct

Task 2 ○ Cancel your PayPal order

Task 3 ○ Track your package

Task 4 ○ Select your email provider to view document

Question 2:



https://is.gd/6oCJ4m

Expand

Screenshot of the distant page behind your short URL

Bevor Sie zur Google Suche weitergehen

Google verwendet Cookies und Daten für Folgendes:

- Dienste anbieten und betreiben, z. B. Störungen prüfen und Maßnahmen gegen Spam, Betrug oder Missbrauch ergreifen
- Daten zu Zielgruppeninteraktionen und Websitestatistiken erheben, um zu verstehen, wie unsere Dienste verwendet werden

Wenn Sie zustimmen, verwenden wir Cookies und Daten auch für Folgendes:

- Qualität unserer Dienste verbessern und neue Dienste entwickeln
- Werbung ausliefern und die Effektivität von Werbung messen
- Personalisierte Inhalte anzeigen, abhängig von Ihren Einstellungen
- Personalisierte oder allgemeine Werbung bei Google und im Web anzeigen, abhängig von Ihren Einstellungen

Strange. This link redirects to google.com.

Note: Tools to expand shortened URLs will be discussed in the Phishing Emails 3 room.

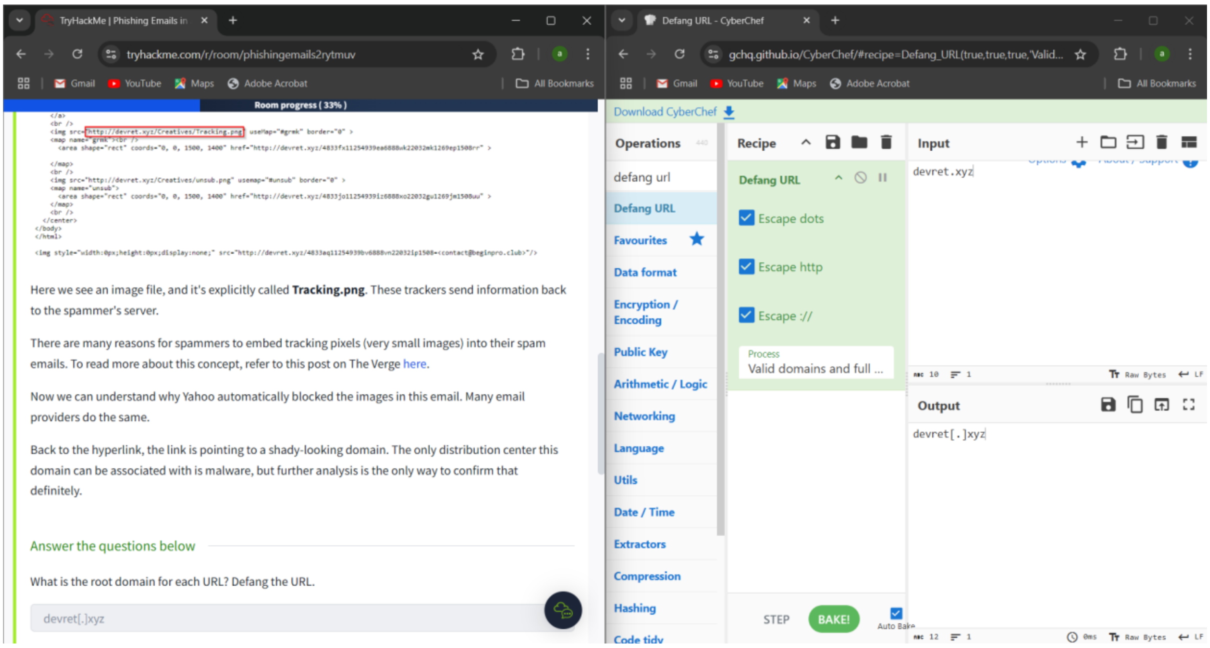
Answer the questions below

What phrase does the gibberish sender email start with?

noreply

✓ Correct Answer

Question 3:


TryHackMe | Phishing Emails in
tryhackme.com/r/room/phishingemails2rytmuv
Gmail
YouTube
Maps
Adobe Acrobat
All Bookmarks
Room progress (33%)

```
    </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>"/>
```

Here we see an image file, and it's explicitly called **Tracking.png**. These trackers send information back to the spammer's server.

There are many reasons for spammers to embed tracking pixels (very small images) into their spam emails. To read more about this concept, refer to this post on The Verge here.

Now we can understand why Yahoo automatically blocked the images in this email. Many email providers do the same.

Back to the hyperlink, the link is pointing to a shady-looking domain. The only distribution center this domain can be associated with is malware, but further analysis is the only way to confirm that definitely.

Answer the questions below

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

devret[.]xyz

Defang URL

☑ Escape dots

☑ Escape http

☑ Escape ://

Process: Valid domains and full ...

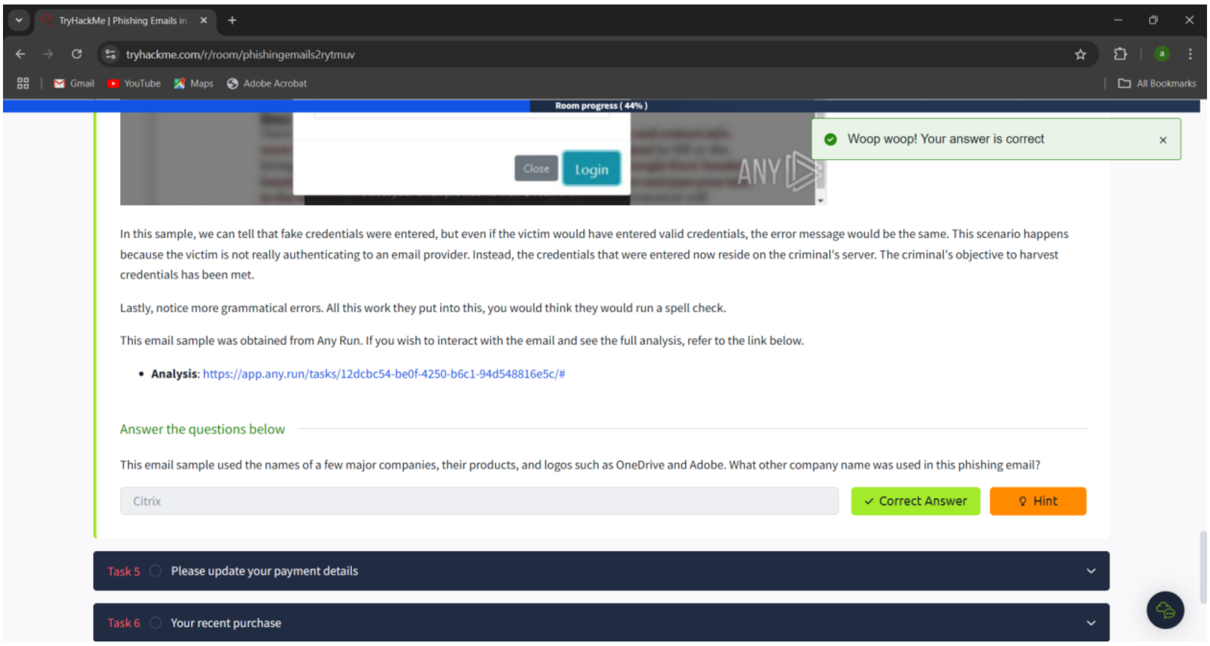
Input

```
devret.xyz
```

Output

```
devret[.]xyz
```

Question 4:



Woop woop! Your answer is correct

In this sample, we can tell that fake credentials were entered, but even if the victim would have entered valid credentials, the error message would be the same. This scenario happens because the victim is not really authenticating to an email provider. Instead, the credentials that were entered now reside on the criminal's server. The criminal's objective to harvest credentials has been met.

Lastly, notice more grammatical errors. All this work they put into this, you would think they would run a spell check.

This email sample was obtained from Any Run. If you wish to interact with the email and see the full analysis, refer to the link below.

- **Analysis**: https://app.any.run/tasks/12dcbc54-be0f-4250-b6c1-94d548816e5c/#

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

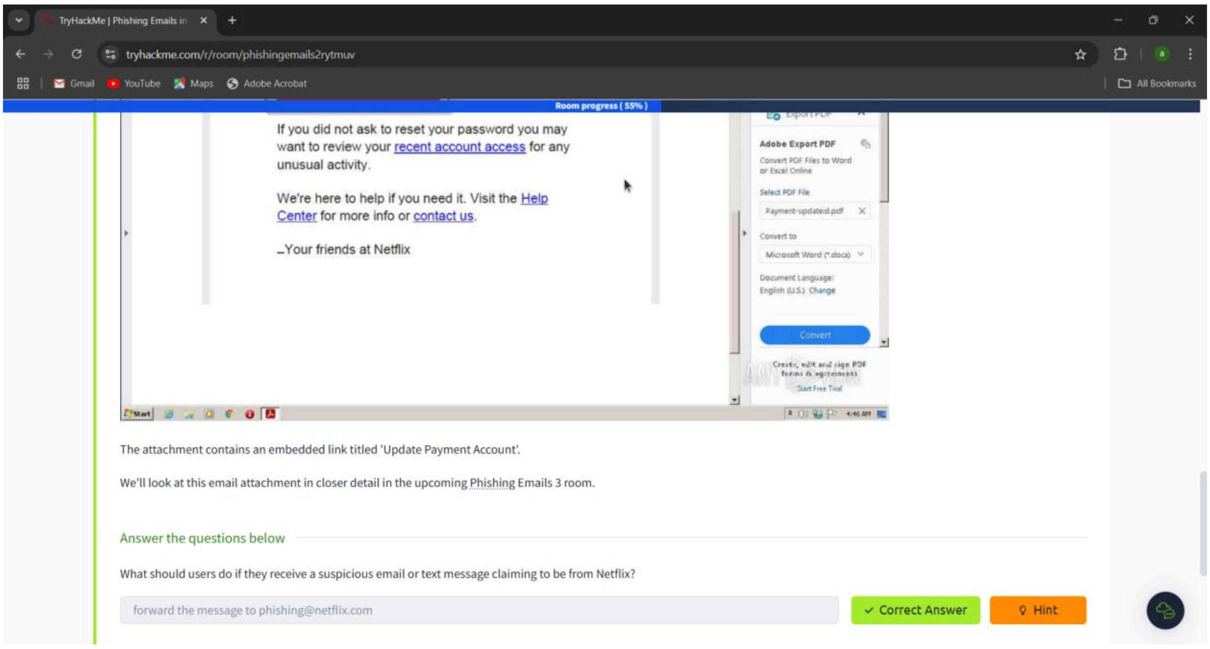
✓ Correct Answer

Hint

Task 5 ○ Please update your payment details

Task 6 ○ Your recent purchase

Question 5:



If you did not ask to reset your password you may want to review your recent account access for any unusual activity.

We're here to help if you need it. Visit the Help Center for more info or contact us.

–Your friends at Netflix

The attachment contains an embedded link titled 'Update Payment Account'.

We'll look at this email attachment in closer detail in the upcoming Phishing Emails 3 room.

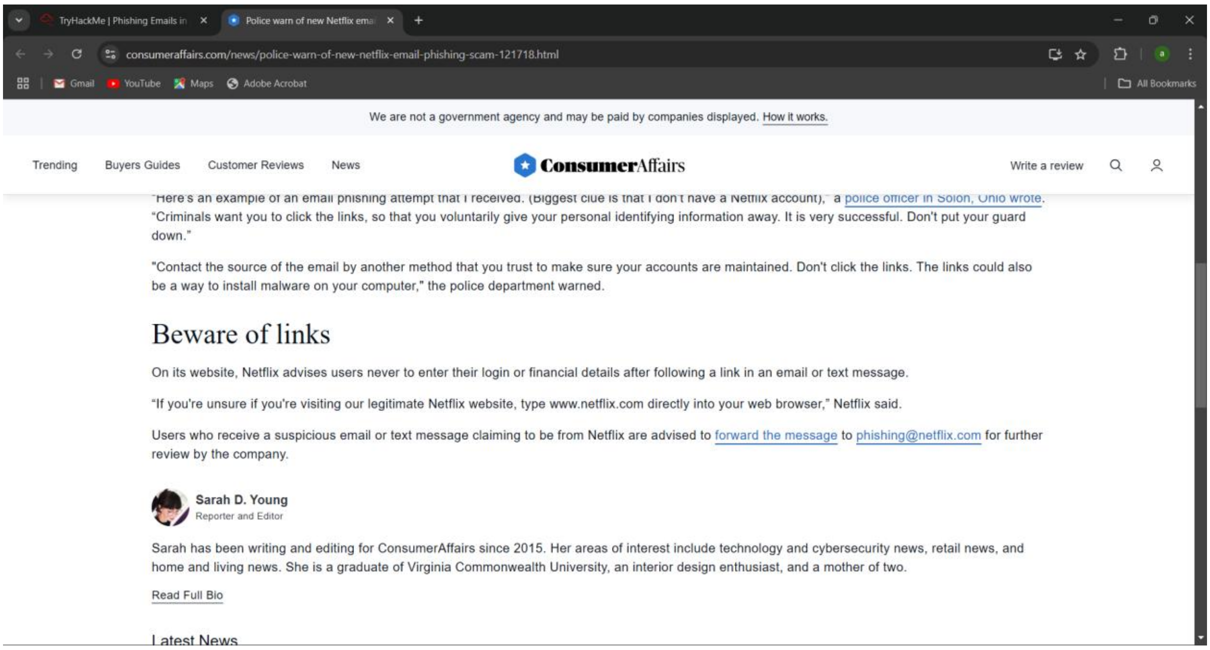
Answer the questions below

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

✓ Correct Answer

Hint


TryHackMe | Phishing Emails in
Police warn of new Netflix emai
consumeraffairs.com/news/police-warn-of-new-netflix-email-phishing-scam-121718.html
Gmail
YouTube
Maps
Adobe Acrobat
All Bookmarks
Trending
Buyers Guides
Customer Reviews
News
ConsumerAffairs
Write a review

We are not a government agency and may be paid by companies displayed. How it works.

"Here's an example of an email phishing attempt that I received. (Biggest clue is that I don't have a Netflix account)," a police officer in Solon, Ohio wrote. "Criminals want you to click the links, so that you voluntarily give your personal identifying information away. It is very successful. Don't put your guard down."

"Contact the source of the email by another method that you trust to make sure your accounts are maintained. Don't click the links. The links could also be a way to install malware on your computer," the police department warned.

Beware of links

On its website, Netflix advises users never to enter their login or financial details after following a link in an email or text message.

"If you're unsure if you're visiting our legitimate Netflix website, type www.netflix.com directly into your web browser," Netflix said.

Users who receive a suspicious email or text message claiming to be from Netflix are advised to forward the message to phishing@netflix.com for further review by the company.

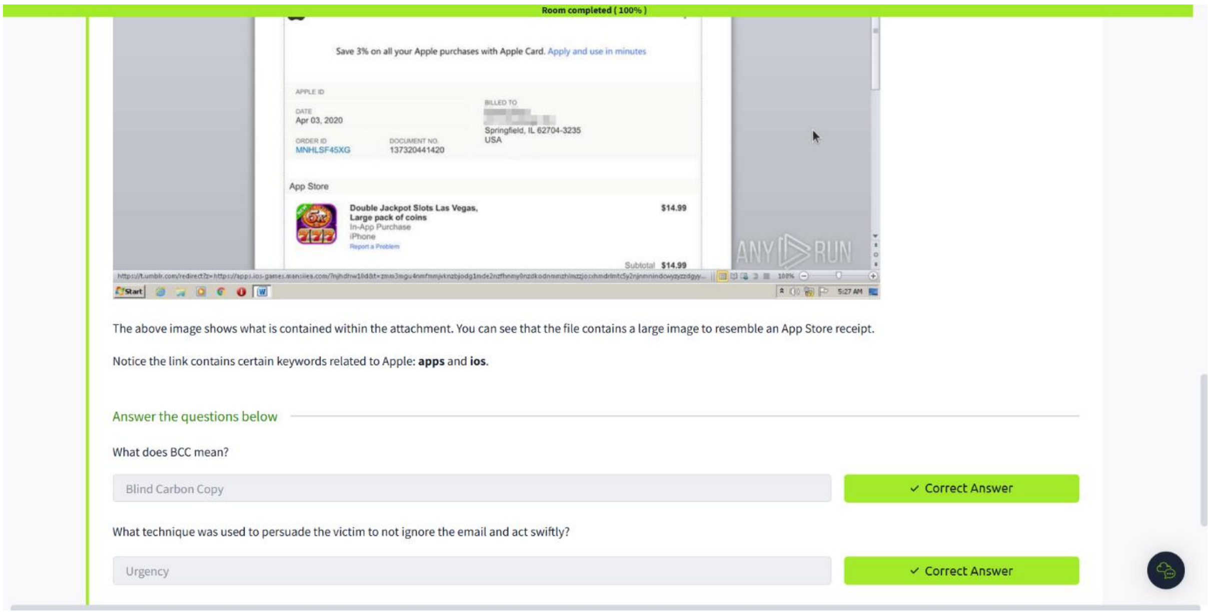
Sarah D. Young
Reporter and Editor

Sarah has been writing and editing for ConsumerAffairs since 2015. Her areas of interest include technology and cybersecurity news, retail news, and home and living news. She is a graduate of Virginia Commonwealth University, an interior design enthusiast, and a mother of two.

Read Full Bio

Latest News

Question 6:



Room completed (100%)

Save 3% on all your Apple purchases with Apple Card. Apply and use in minutes

APPLE ID

DATE
Apr 03, 2020

ORDER ID
MNHLSF45XG

DOCUMENT NO.
137320441420

BILLED TO
[redacted]
Springfield, IL 62704-3235
USA

App Store

Double Jackpot Slots Las Vegas,
Large pack of coins
In-App Purchase
iPhone
Report a Problem

$14.99

Subtotal $14.99

https://t.umblr.com/redirect?z=https://apps.ios-games.mansiies.com/?njhdhw18d&t=zmm3mgu4nmfmmjvknzbjodg1mde2nzfhnmy0nzdkodnmmzhlmzzjosxhmdrlmtc5y2njnmnindcwyzyzdgyy...

5:27 AM

The above image shows what is contained within the attachment. You can see that the file contains a large image to resemble an App Store receipt.

Notice the link contains certain keywords related to Apple: **apps** and **ios**.

Answer the questions below

What does BCC mean?

Blind Carbon Copy

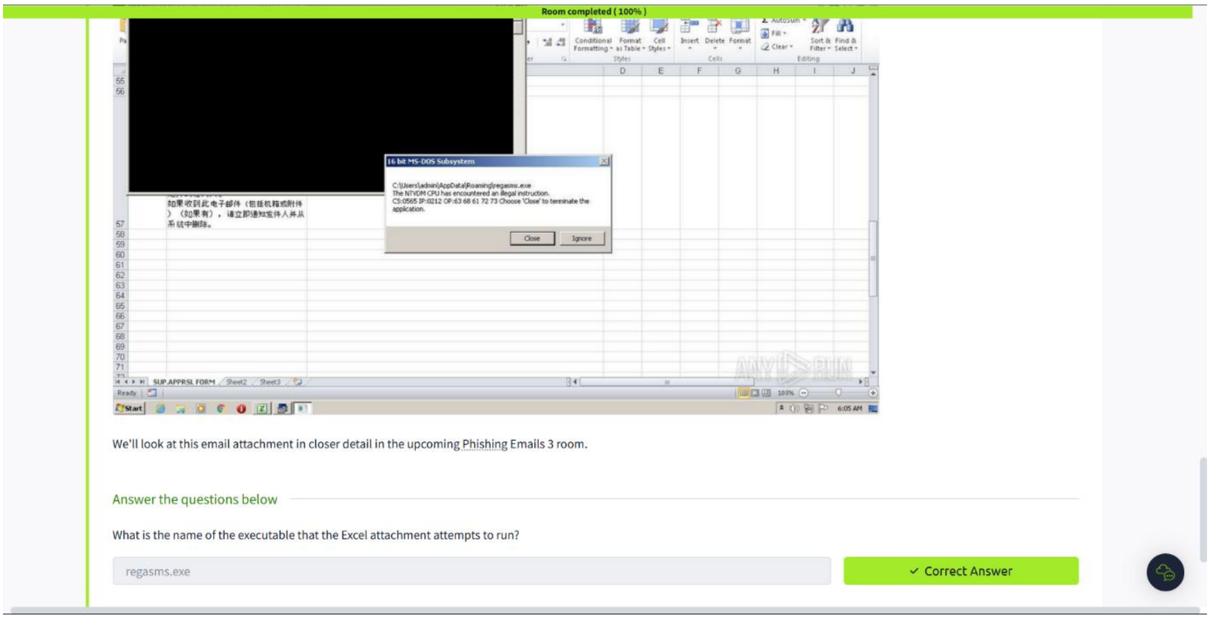
✓ Correct Answer

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

Urgency

✓ Correct Answer

Question 7:



Room completed (100%)

如果收到此电子邮件（包括机箱或附件）（如果有），请立即通知发件人并从系统中删除。

16 bit MS-DOS Subsystem

C:\Users\admin\AppData\Roaming\regasms.exe
The NTVDM CPU has encountered an illegal instruction.
CS:0565 IP:0212 OP:63 68 61 72 73 Choose 'Close' to terminate the application.

We'll look at this email attachment in closer detail in the upcoming Phishing Emails 3 room.

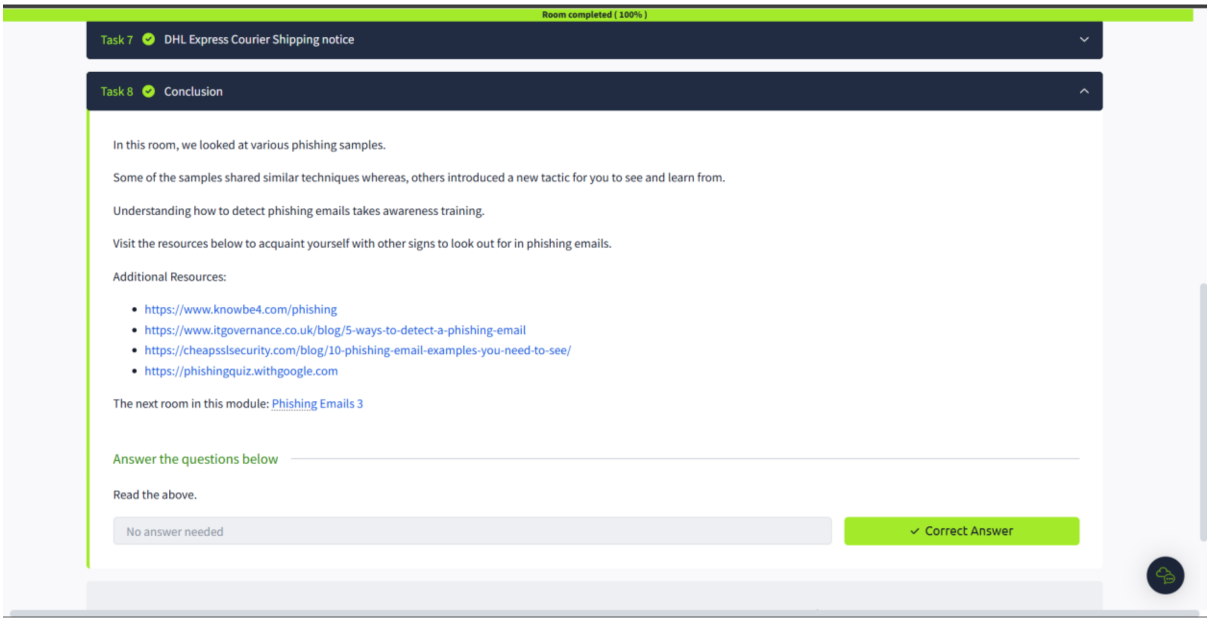
Answer the questions below

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

regasms.exe

✓ Correct Answer

Question 8:



In this room, we looked at various phishing samples.

Some of the samples shared similar techniques whereas, others introduced a new tactic for you to see and learn from.

Understanding how to detect phishing emails takes awareness training.

Visit the resources below to acquaint yourself with other signs to look out for in phishing emails.

Additional Resources:

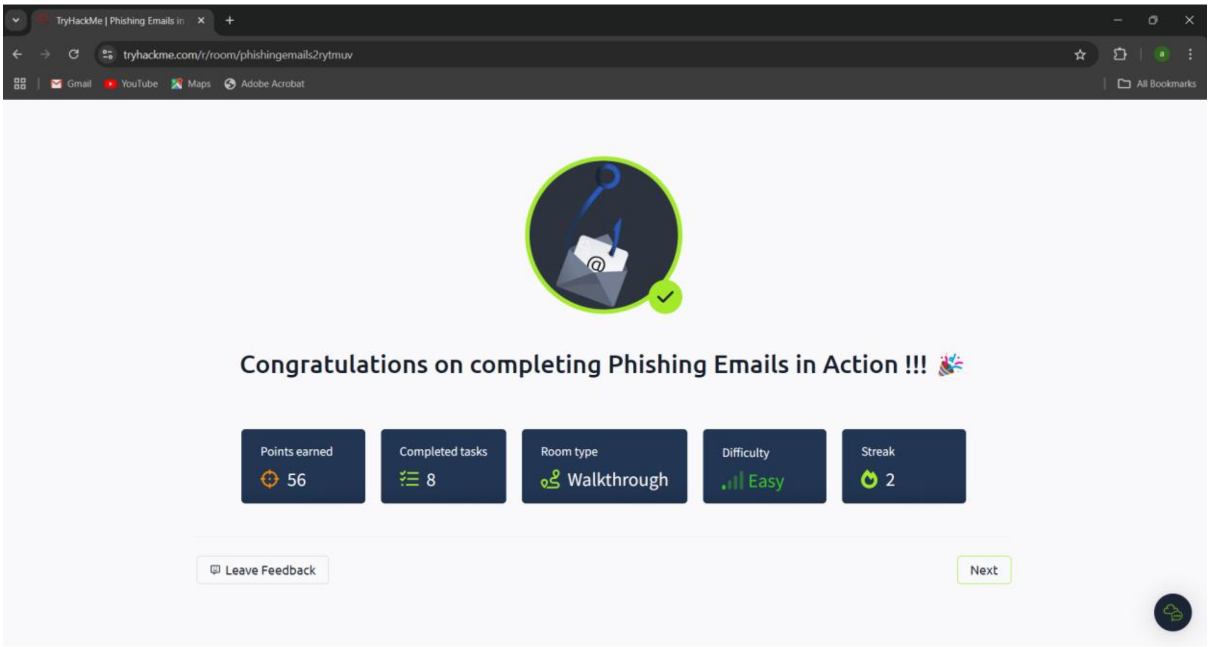
- https://www.knowbe4.com/phishing
- https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email
- https://cheapsslsecurity.com/blog/10-phishing-email-examples-you-need-to-see/
- https://phishingquiz.withgoogle.com

The next room in this module: Phishing Emails 3

Answer the questions below

Read the above.

No answer needed


TryHackMe | Phishing Emails in
tryhackme.com/r/room/phishingemails2rytmuv
Gmail
YouTube
Maps
Adobe Acrobat
All Bookmarks

Congratulations on completing Phishing Emails in Action !!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
56	8	Walkthrough	Easy	2

RESULT:

The experiment successfully demonstrated the process of phishing email analysis. Key findings included identifying malicious attachments, detecting fake sender domains, and analyzing phishing URLs. Completing the TryHackMe tasks enhanced practical skills in email forensics.