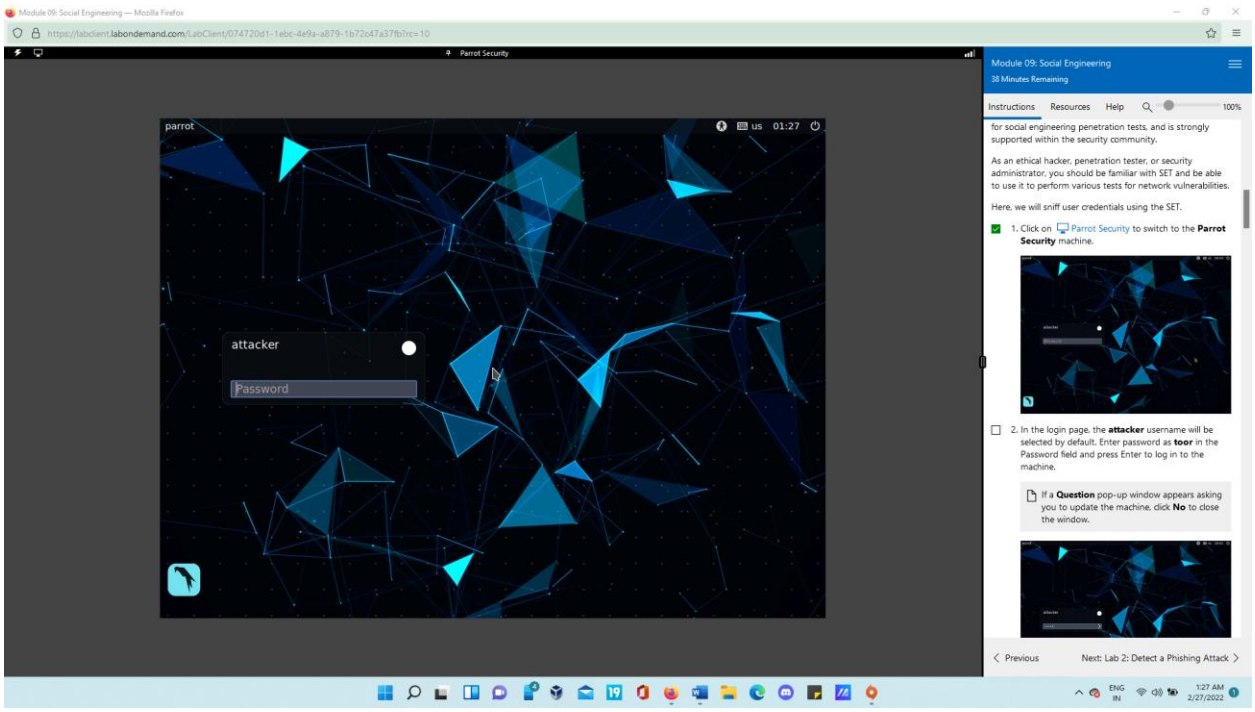
Module: Social Engineering

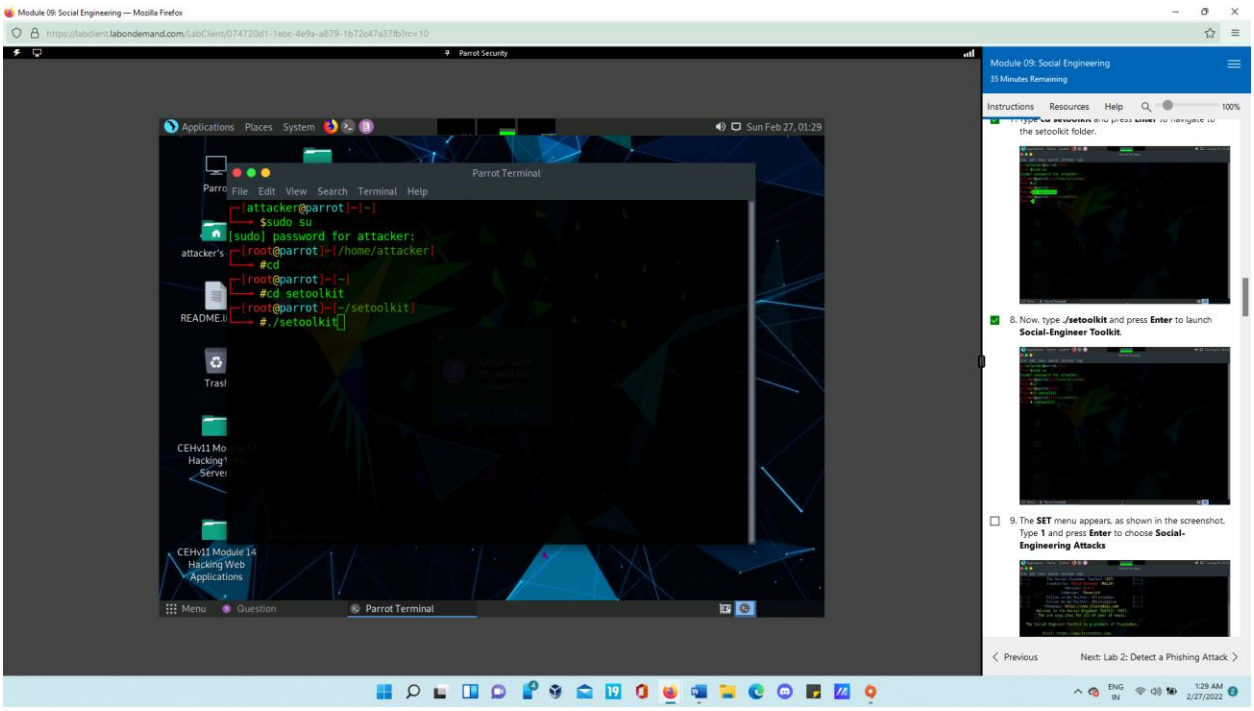
Lab 1: Perform Social Engineering using Various Techniques

Task 1: Sniff Credentials using the Social-Engineer Toolkit (SET)

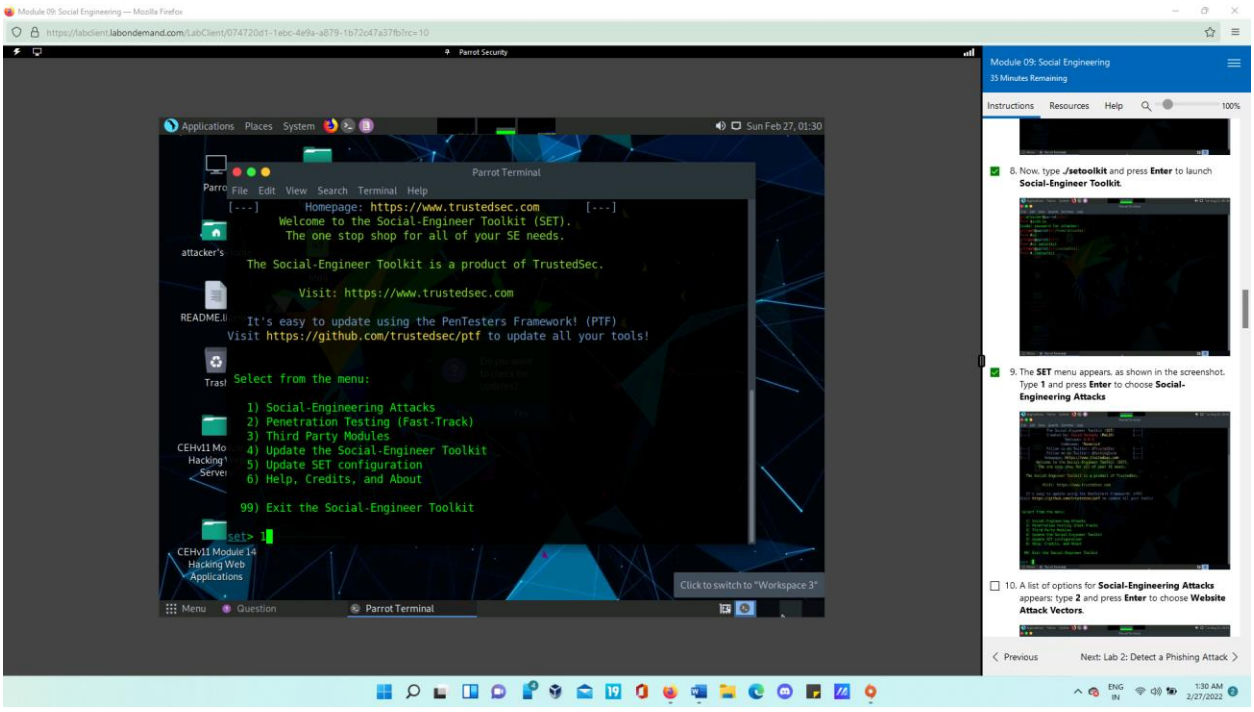
- Open ParrotOS.



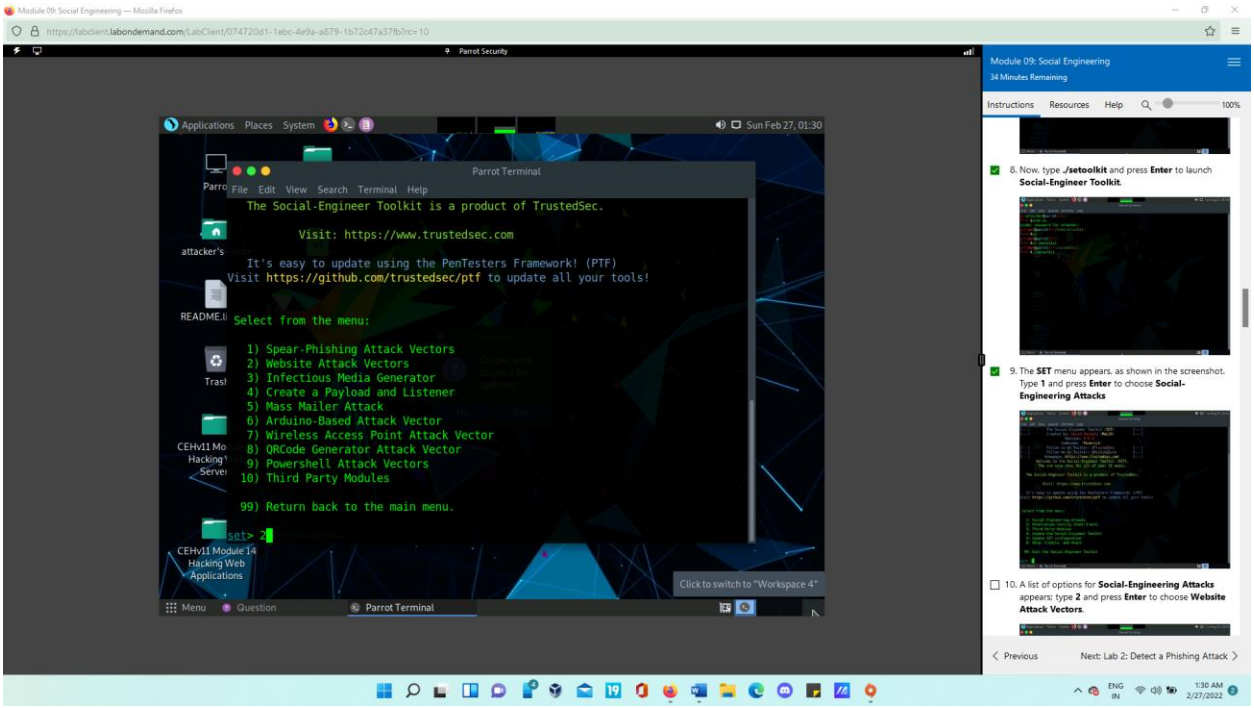
- Open terminal, escalate privileges to root > navigate to root directory > type ./setoolkit. This wil launch social engineering toolkit.



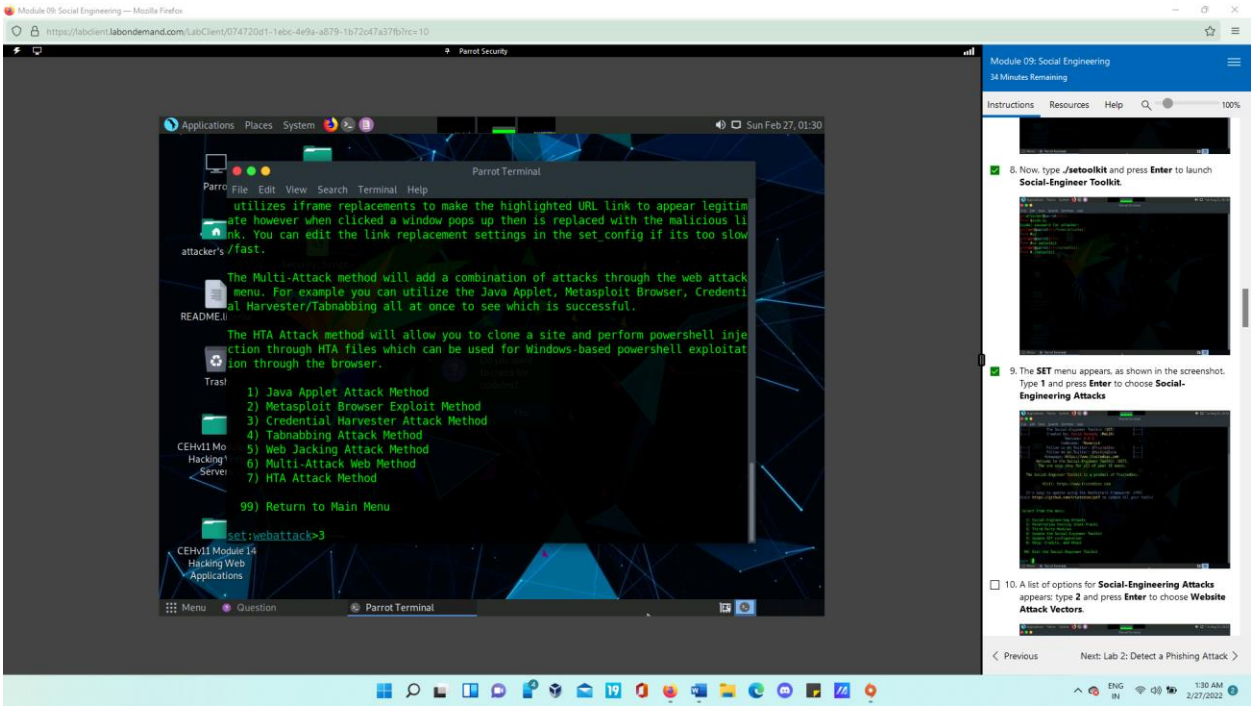
- To choose Social Engineering attacks, type 1 and press enter**.**

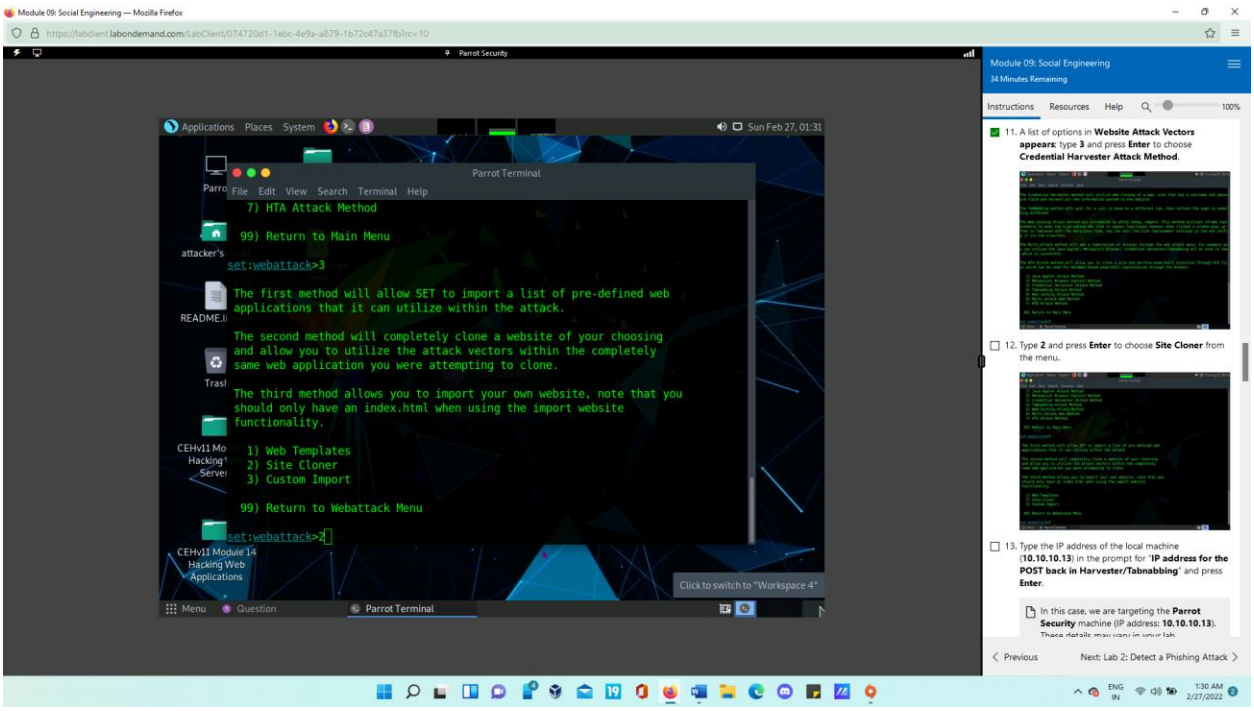


- To choose Website Attack Vectors, type 2 and press enter.

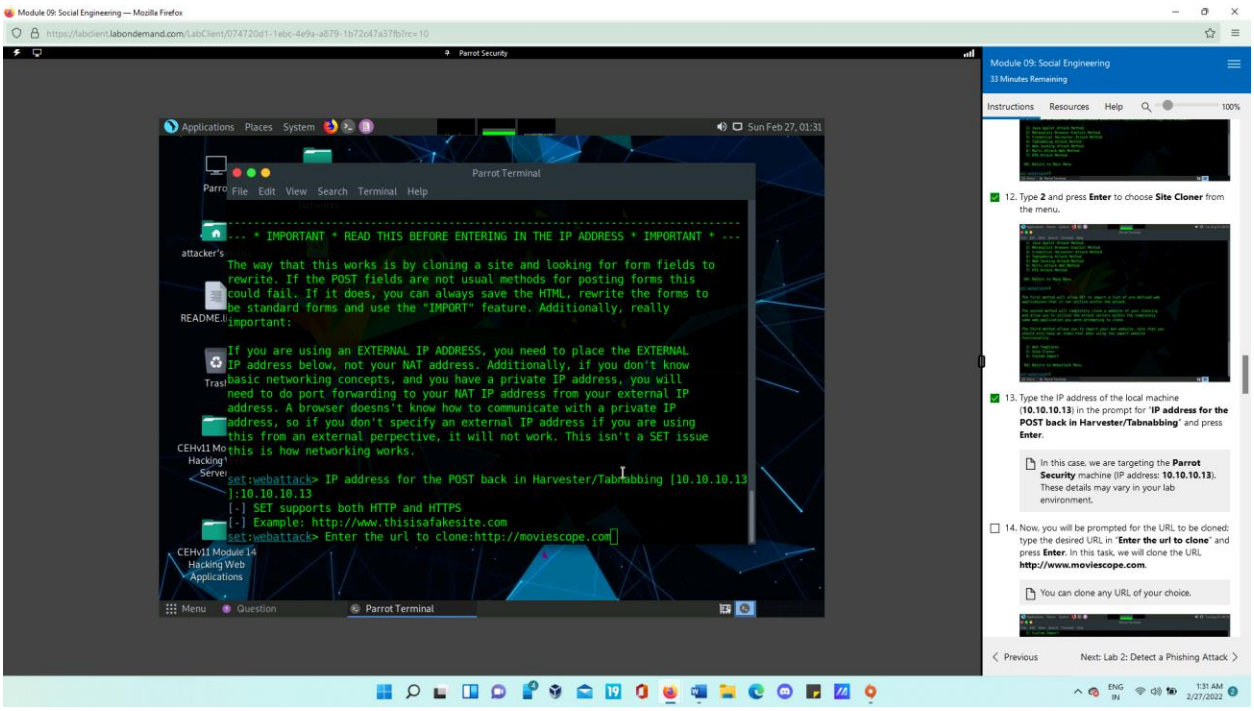


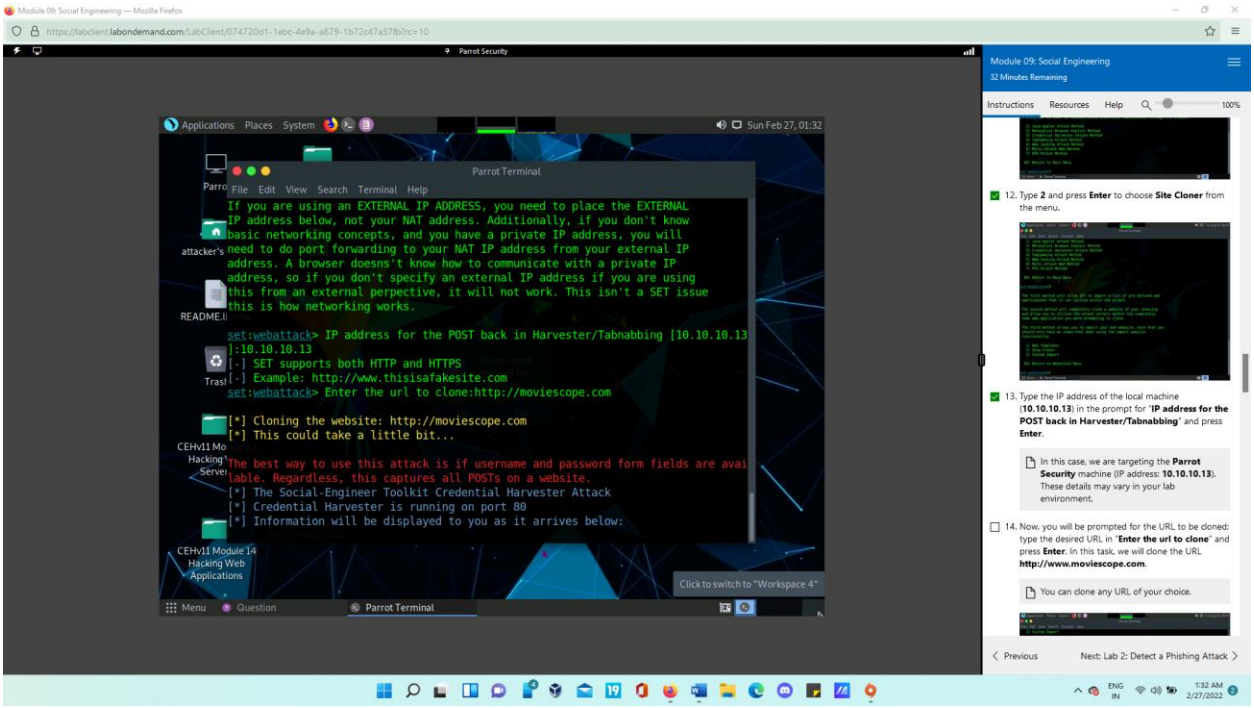
- Type 3 to choose Credential Harvester Attack Method and press enter. Then Choose Site Cloner, type 2 and press enter.



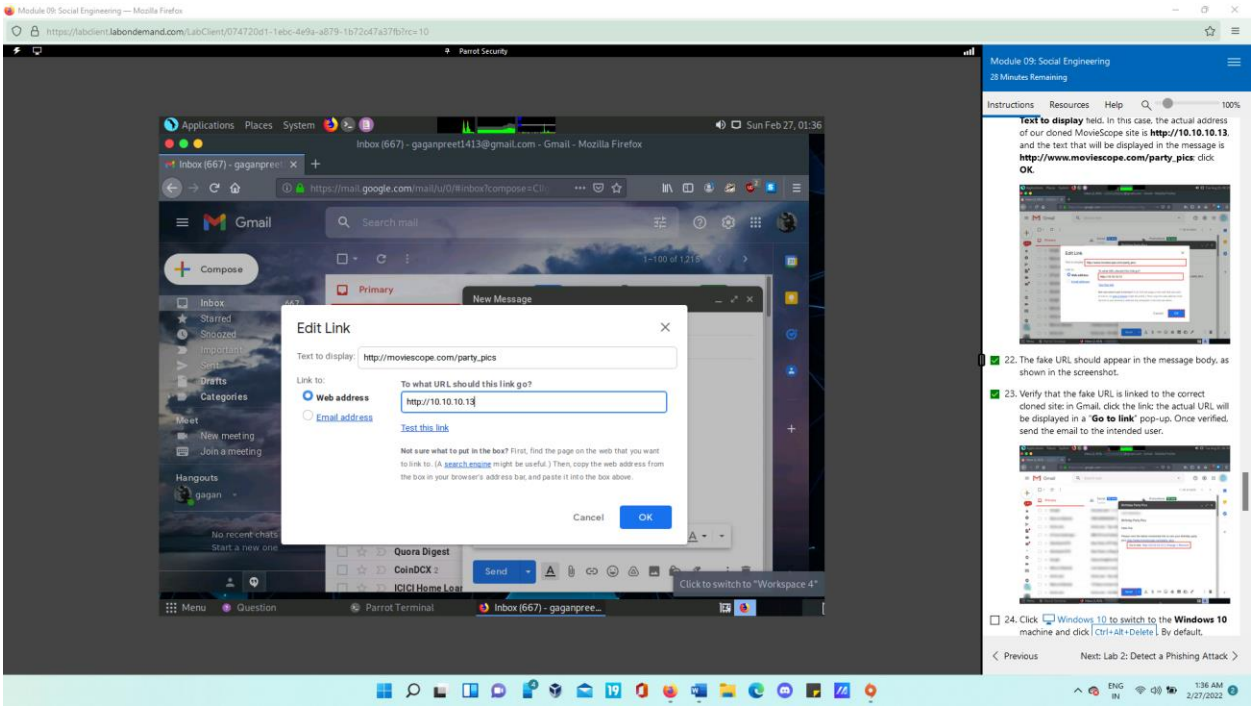


- Type 10.10.10.13 in the IP address for the POST back in Harvester/Tabnagging option and press enter. Then, use the URL http://www.moviescope.com in the option “type URL to clone” option

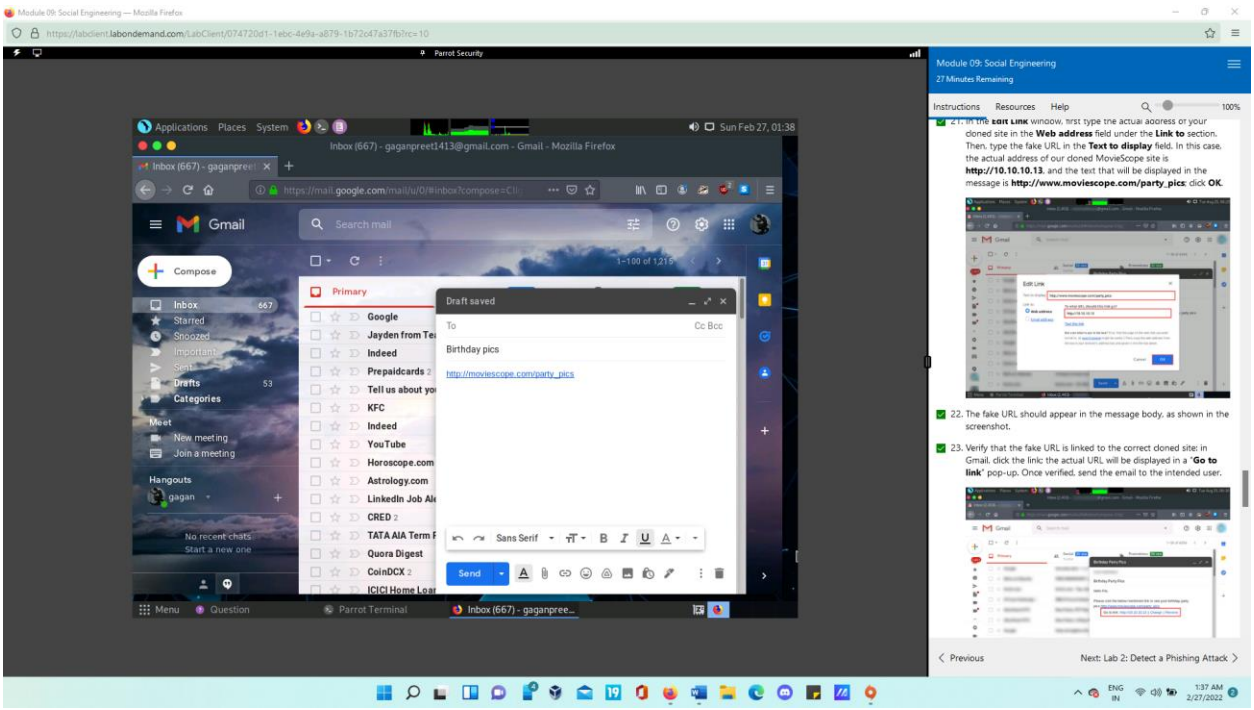

Module 09: Social Engineering — Mozilla Firefox
Parrot Security
Applications Places System
Sun Feb 27, 01:31
Parrot Terminal
File Edit View Search Terminal Help
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---
The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perpective, it will not work. This isn't a SET issue this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.10.13]:10.10.10.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://moviescope.com
attacker's
README.l
Trasl
CEHv11 Mo Hacking Server
CEHv11 Module 14 Hacking Web Applications
Menu
Question
Parrot Terminal
Module 09: Social Engineering
33 Minutes Remaining
Instructions
Resources
Help
100%
12. Type 2 and press Enter to choose Site Cloner from the menu.
13. Type the IP address of the local machine (10.10.10.13) in the prompt for 'IP address for the POST back in Harvester/Tabnabbing' and press Enter.
In this case, we are targeting the Parrot Security machine (IP address: 10.10.10.13). These details may vary in your lab environment.
14. Now, you will be prompted for the URL to be cloned: type the desired URL in 'Enter the url to clone' and press Enter. In this task, we will clone the URL http://www.moviescope.com.
You can clone any URL of your choice.
Previous
Next: Lab 2: Detect a Phishing Attack
ENG IN
1:31 AM 2/27/2022


Module 09: Social Engineering — Mozilla Firefox
Parrot Security
Applications Places System
Sun Feb 27, 01:32
Parrot Terminal
File Edit View Search Terminal Help
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perpective, it will not work. This isn't a SET issue this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.10.13]:10.10.10.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://moviescope.com
[*] Cloning the website: http://moviescope.com
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
Click to switch to "Workspace 4"
attacker's
README.l
Trasl
CEHv11 Mo Hacking Server
CEHv11 Module 14 Hacking Web Applications
Menu
Question
Parrot Terminal
Module 09: Social Engineering
32 Minutes Remaining
Instructions
Resources
Help
100%
12. Type 2 and press Enter to choose Site Cloner from the menu.
13. Type the IP address of the local machine (10.10.10.13) in the prompt for 'IP address for the POST back in Harvester/Tabnabbing' and press Enter.
In this case, we are targeting the Parrot Security machine (IP address: 10.10.10.13). These details may vary in your lab environment.
14. Now, you will be prompted for the URL to be cloned: type the desired URL in 'Enter the url to clone' and press Enter. In this task, we will clone the URL http://www.moviescope.com.
You can clone any URL of your choice.
Previous
Next: Lab 2: Detect a Phishing Attack
ENG IN
1:32 AM 2/27/2022

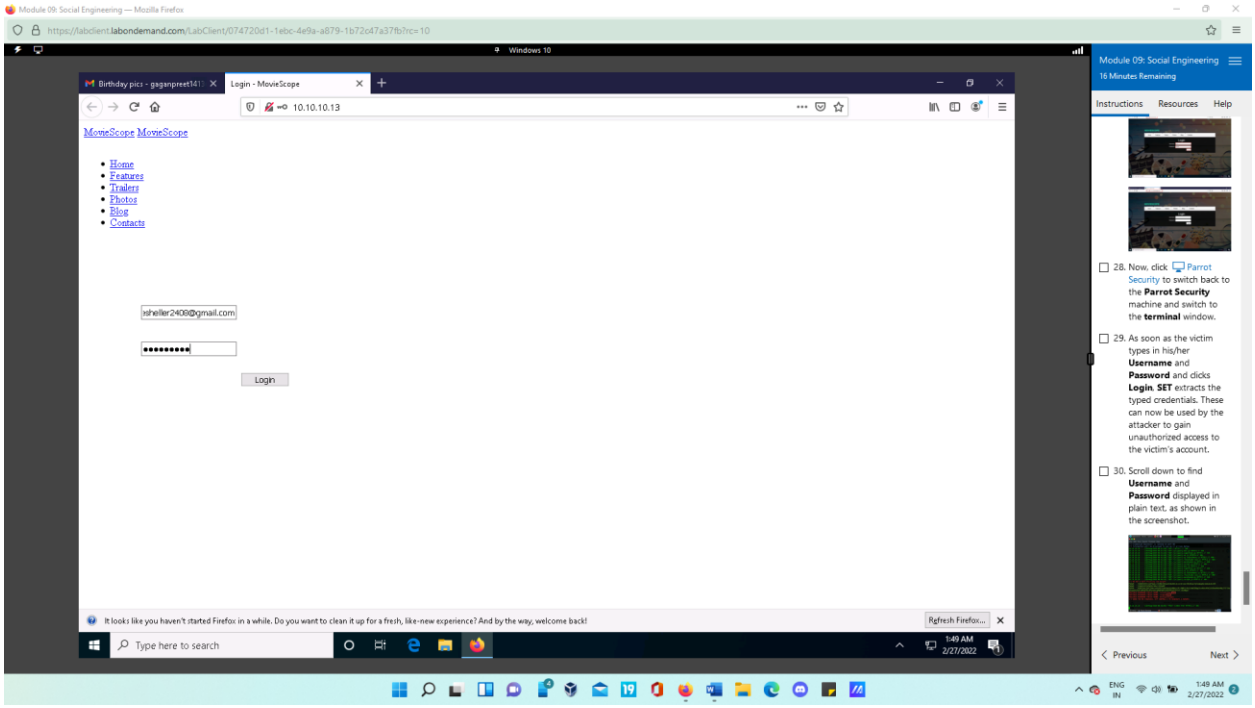
- After cloning a website, we need to send this link to a victim using email. We need to draft such email so that victim should not be suspicious in opening the link.



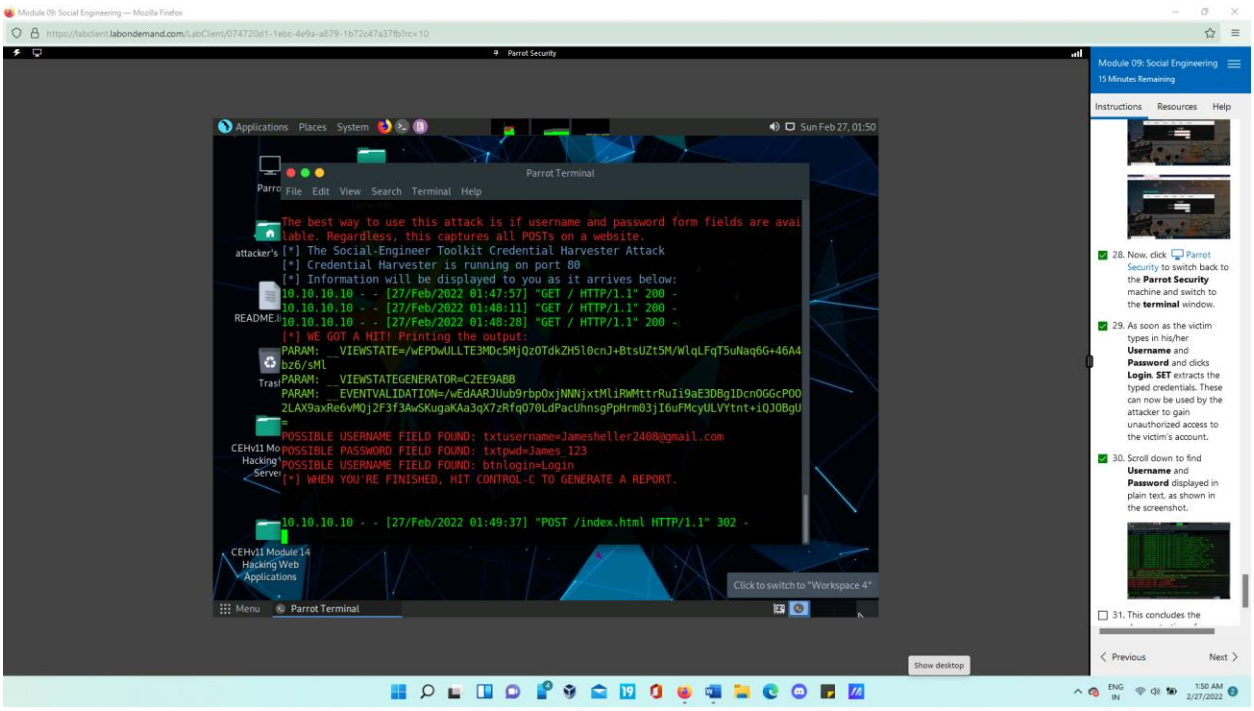
- Now send the email to the victim.



- Now open the victim's account (In this case, you) and open the URL which was sent.
- The victim will be asked to enter his or her username and password into form fields that look exactly like those on the legitimate website. The victim will be led to the real MovieScope login page after entering the Username and Password and clicking Login. The cloned and real sites have different URLs in the browser address bar.



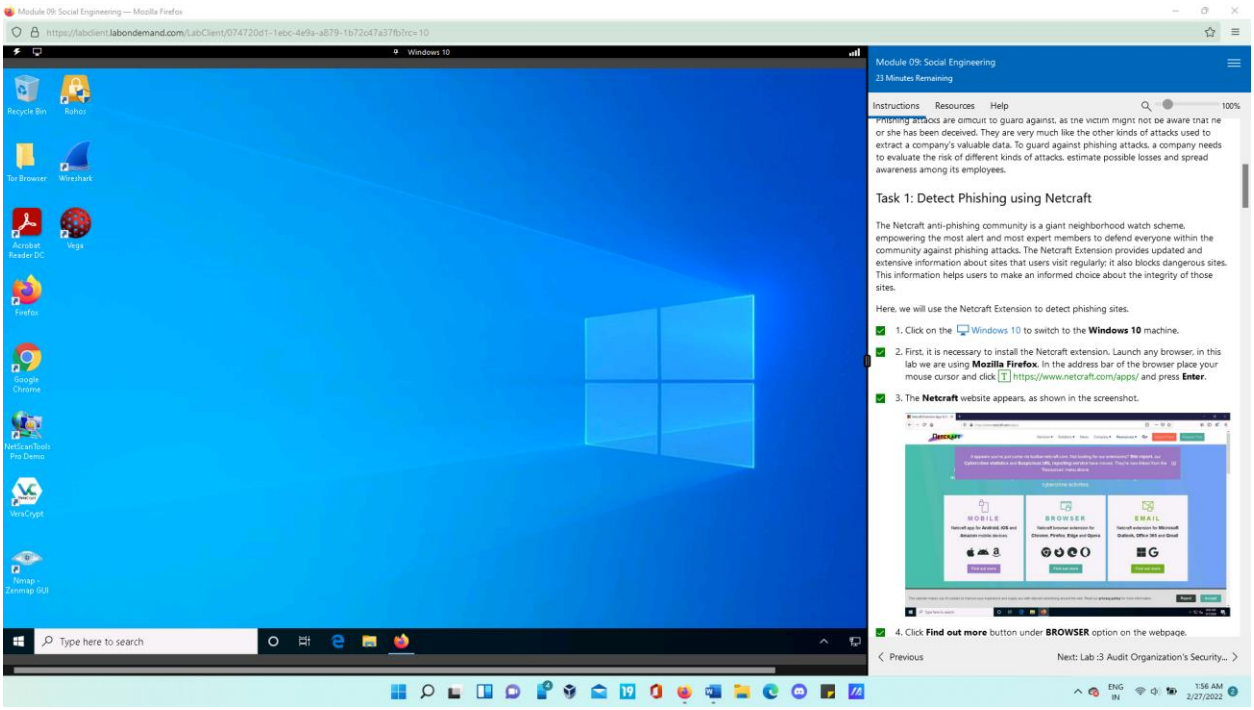
- Now open Terminal window in ParrotOS. SET extracts the exact credentials as soon as the victim types in the username and password. These can be used by the attacker for unauthorized use of victim's account.

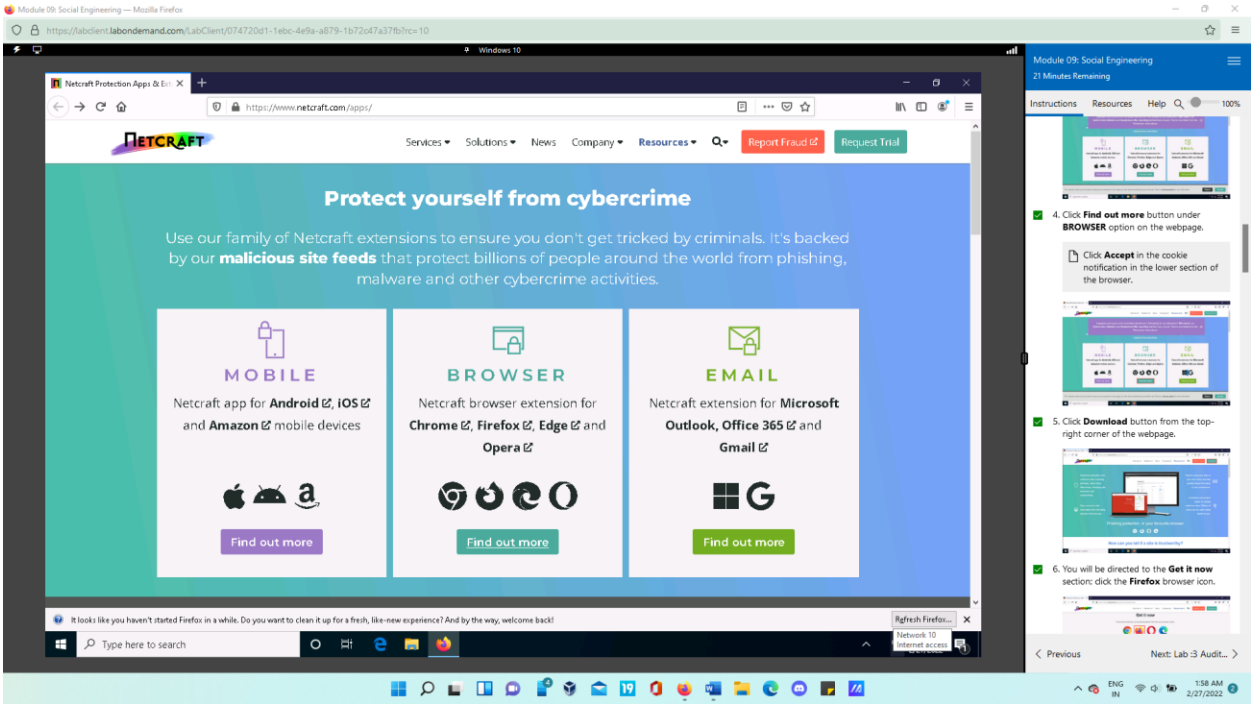


Lab 2: Detect a Phishing Attack

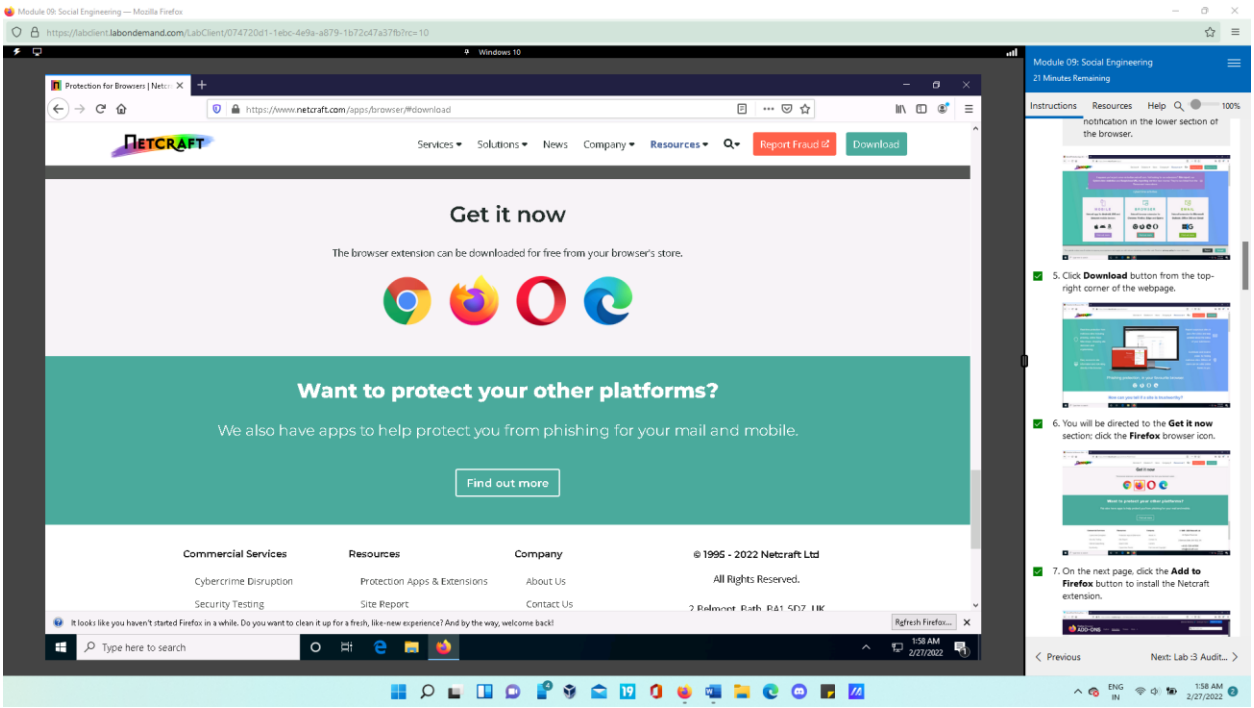
Task 1: Detect Phishing using Netcraft

- Open web browser in Windows10 machine. In this we will install Netcraft browser extension. Type in https://www.netcraft.com/apps/ in URL section and press enter.

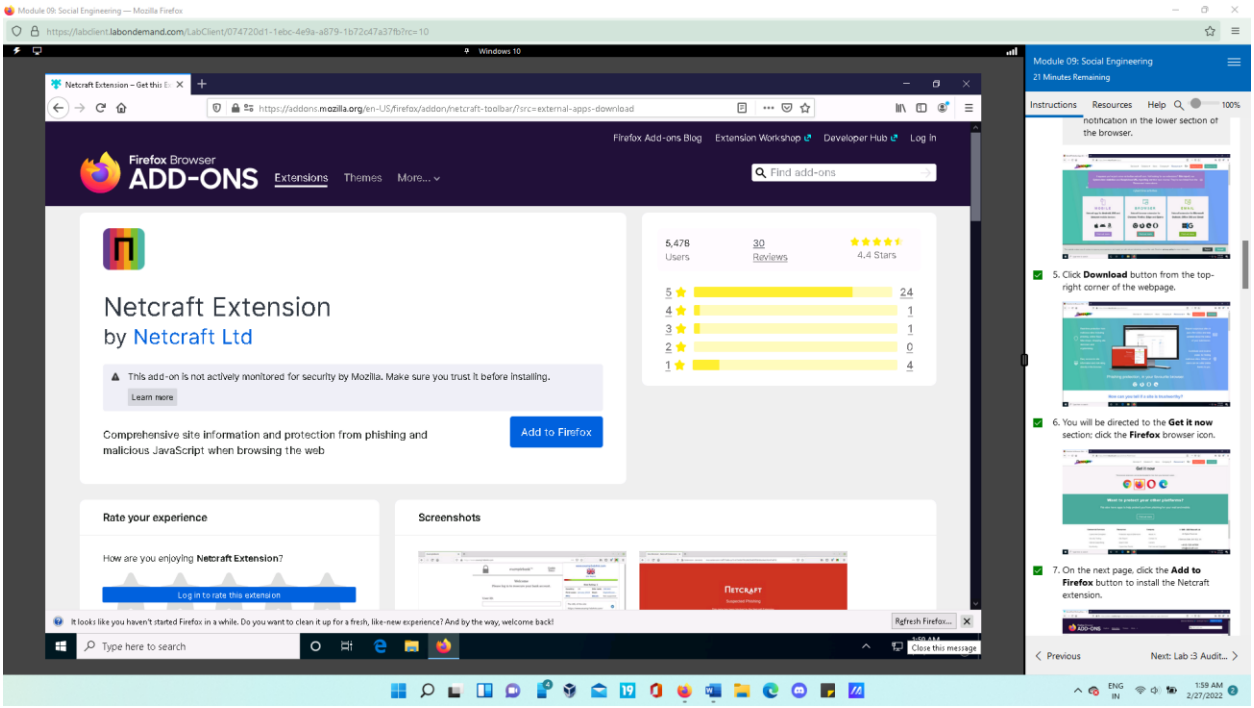




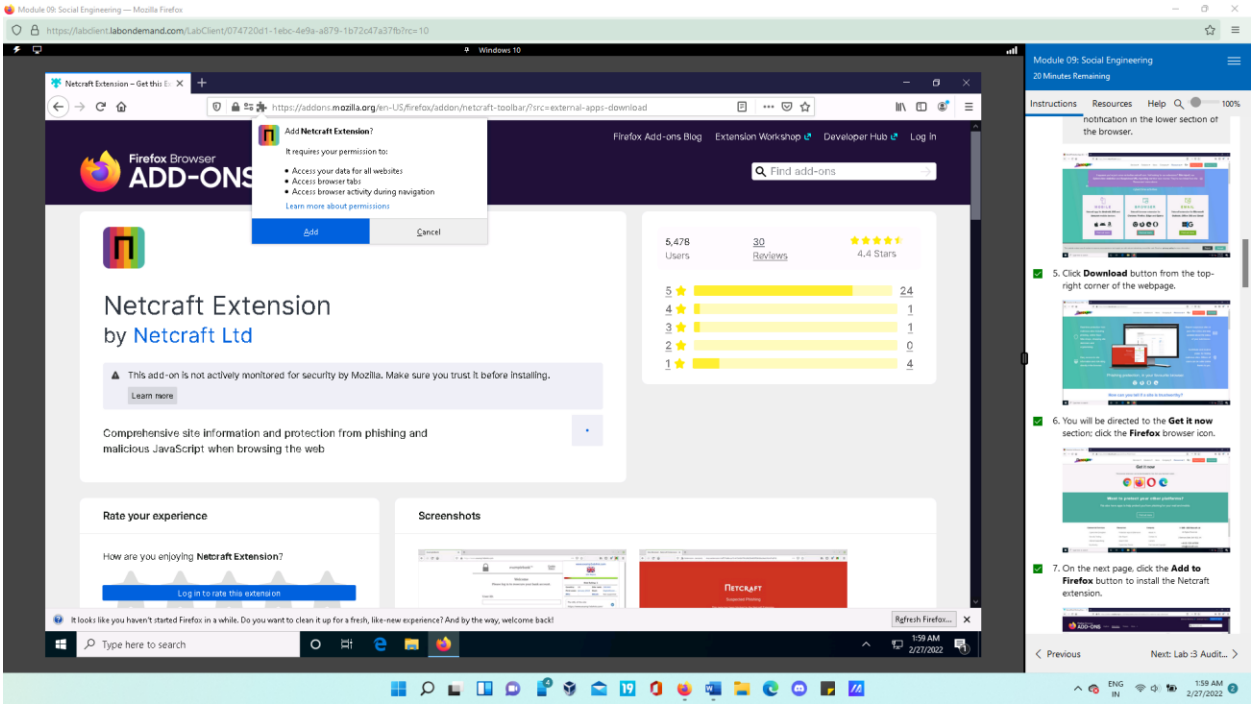
- Press Download button and choose Firefox browser.



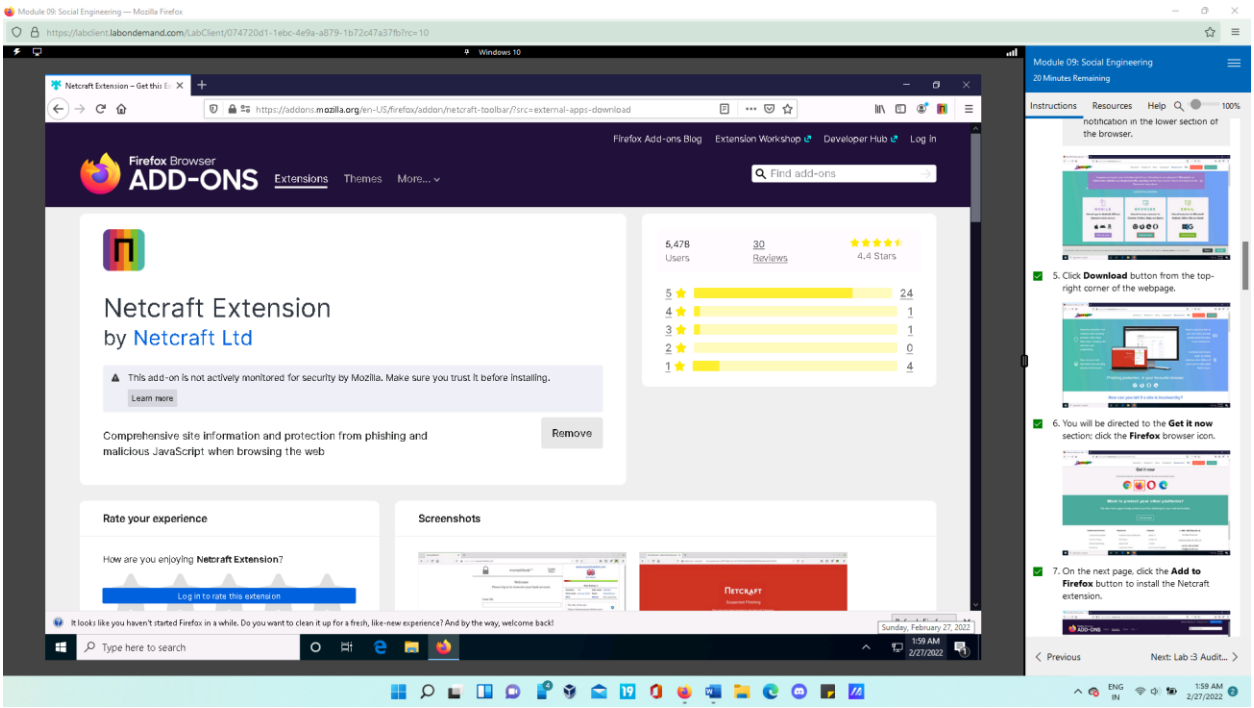
- In the next page, press Add to Firefox to begin installation.



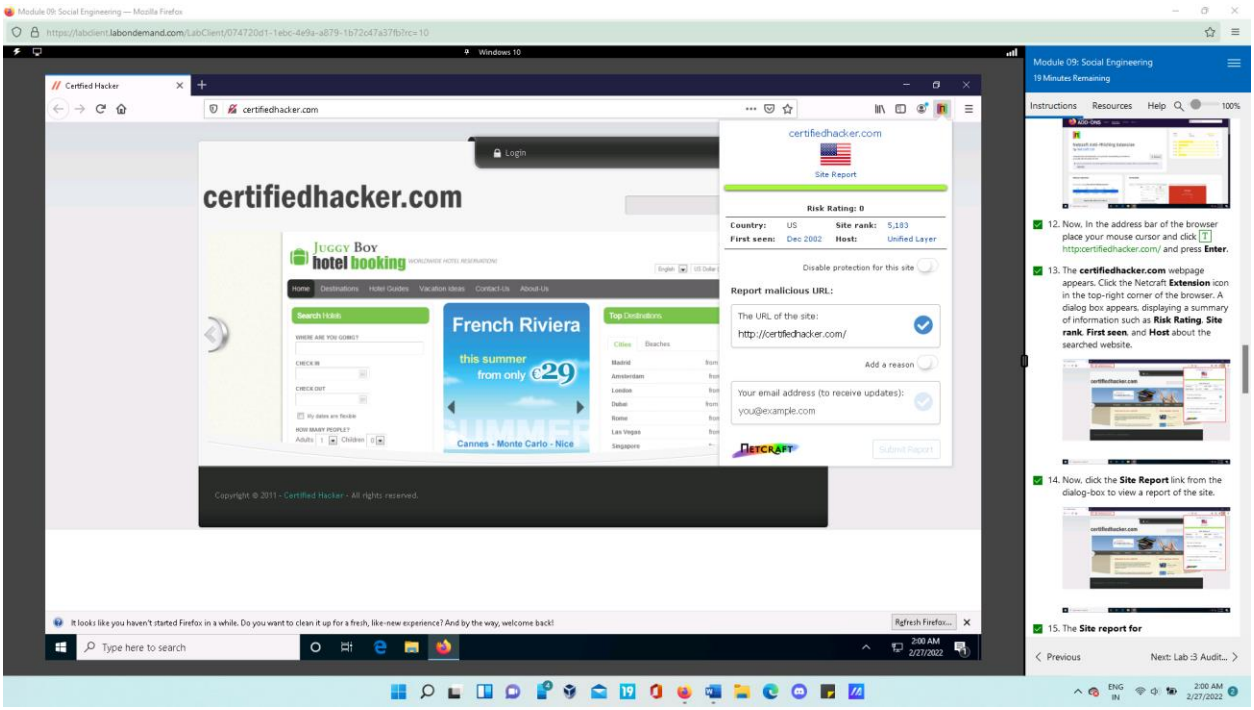
- Click Add and restart the browser.



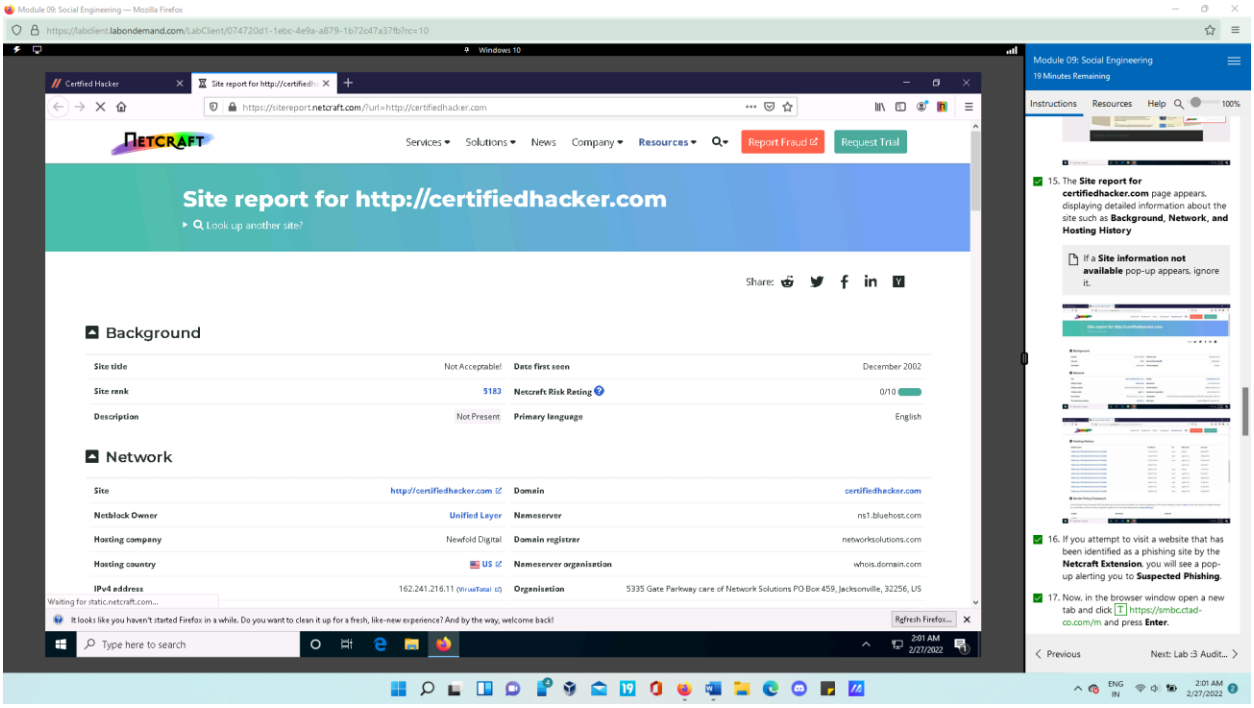
- Netcraft browser extension has been successfully installed as seen in the top-right corner.

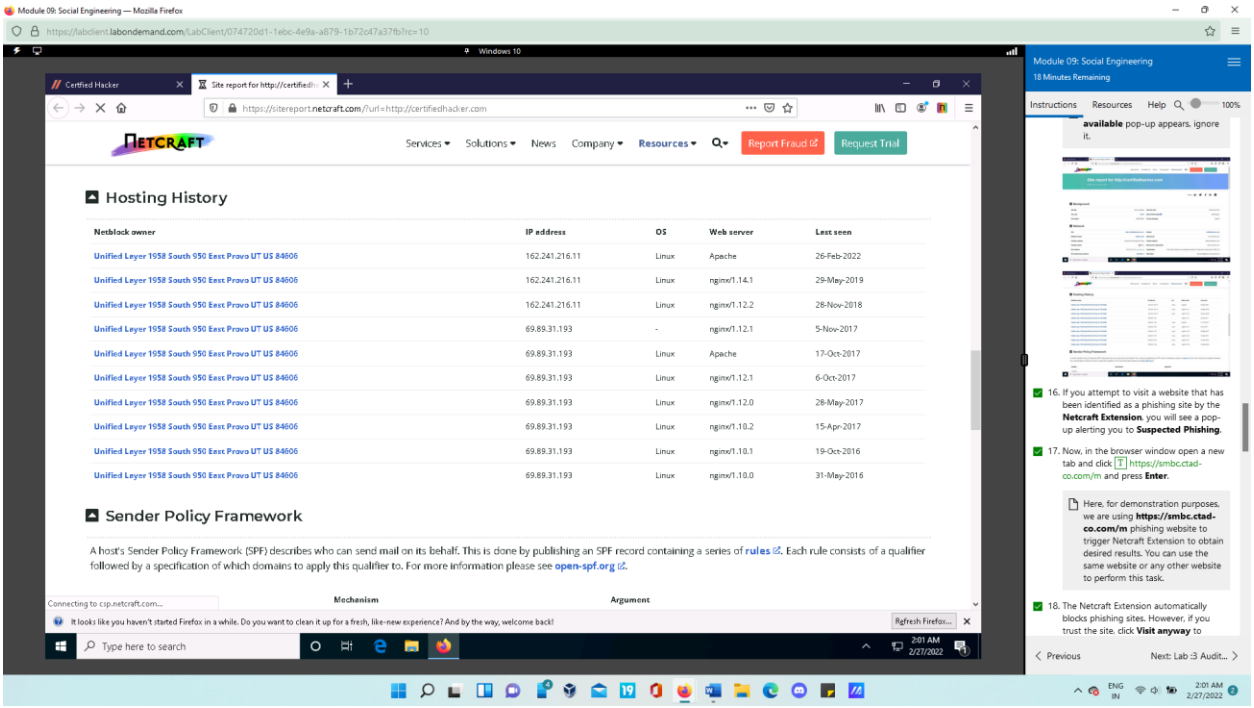


- Navigate to the URL http:certifiedhacker.com/ and click Netcraft extension icon. A dialog box with summary of information like Risk Rating, Site rank, First seen and Host will be displayed about the URL used.

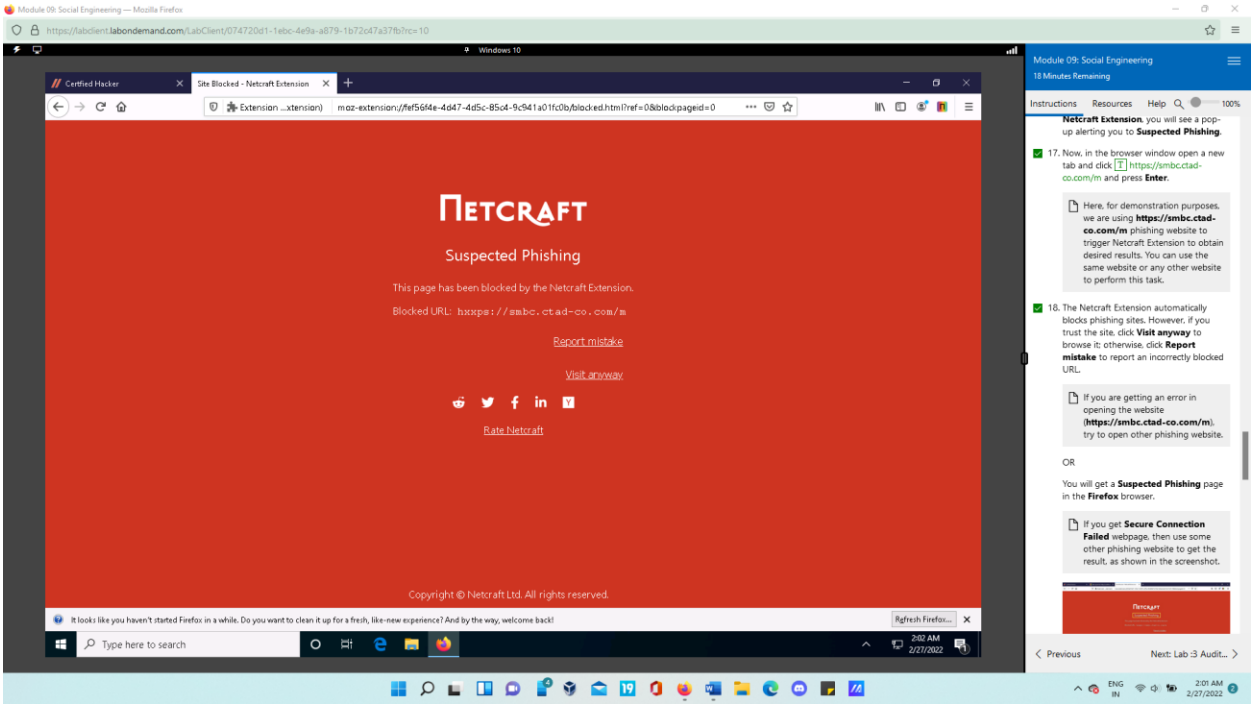


- Now, click the **Site Report** link from the dialog-box to view a report of the site. The **Site report for certifiedhacker.com** page appears, displaying detailed information about the site such as **Background, Network, and Hosting History** If you attempt to visit a website that has been identified as a phishing site by the **Netcraft Extension**, you will see a pop-up alerting you to **Suspected Phishing**.





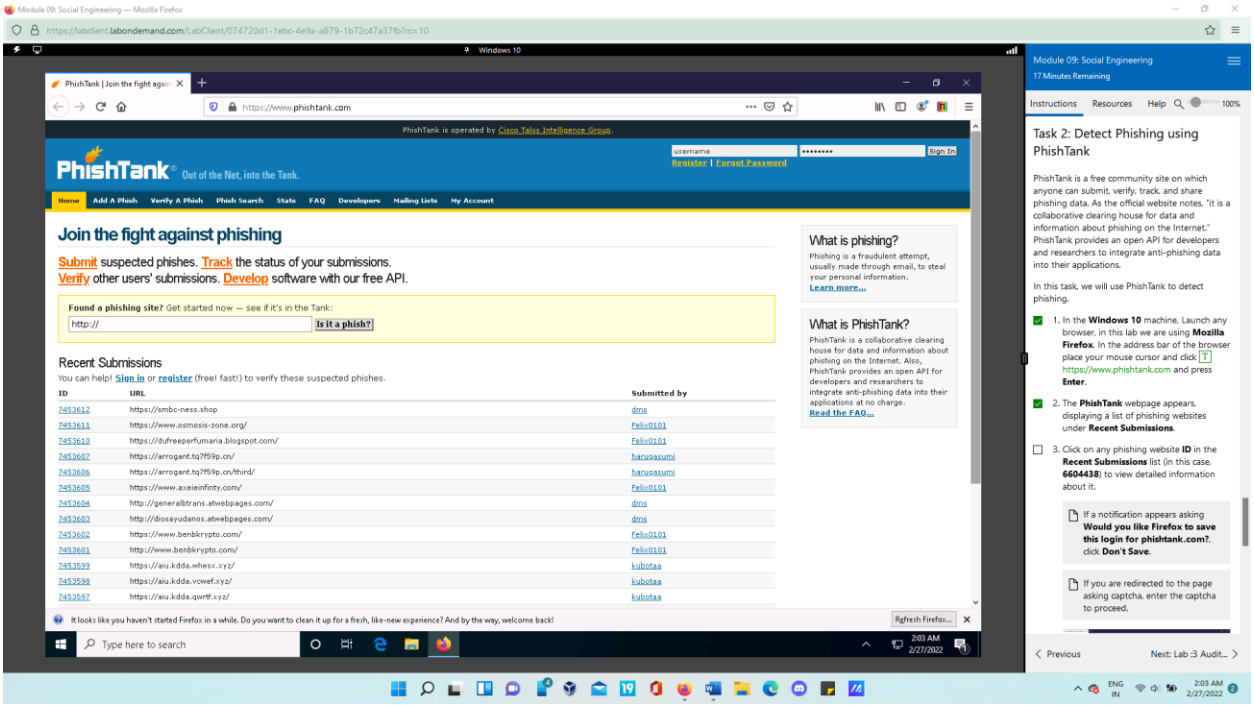
- In a new tab browse to https://smbc.ctad-co.com/m



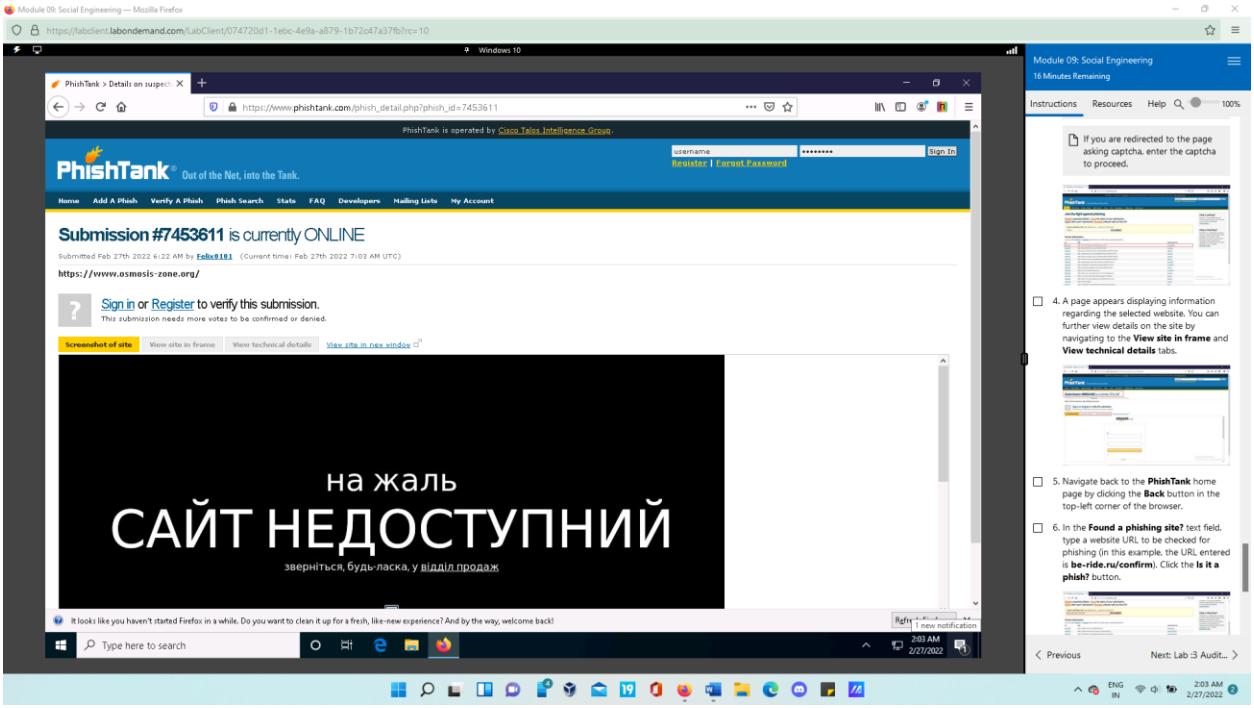
The Netcraft Extension detects phishing sites and disables them automatically. If you trust the site, you can visit it anyhow; otherwise, you can report a wrongly blocked URL by clicking Report error.

Task 2: Detect Phishing using PhishTank

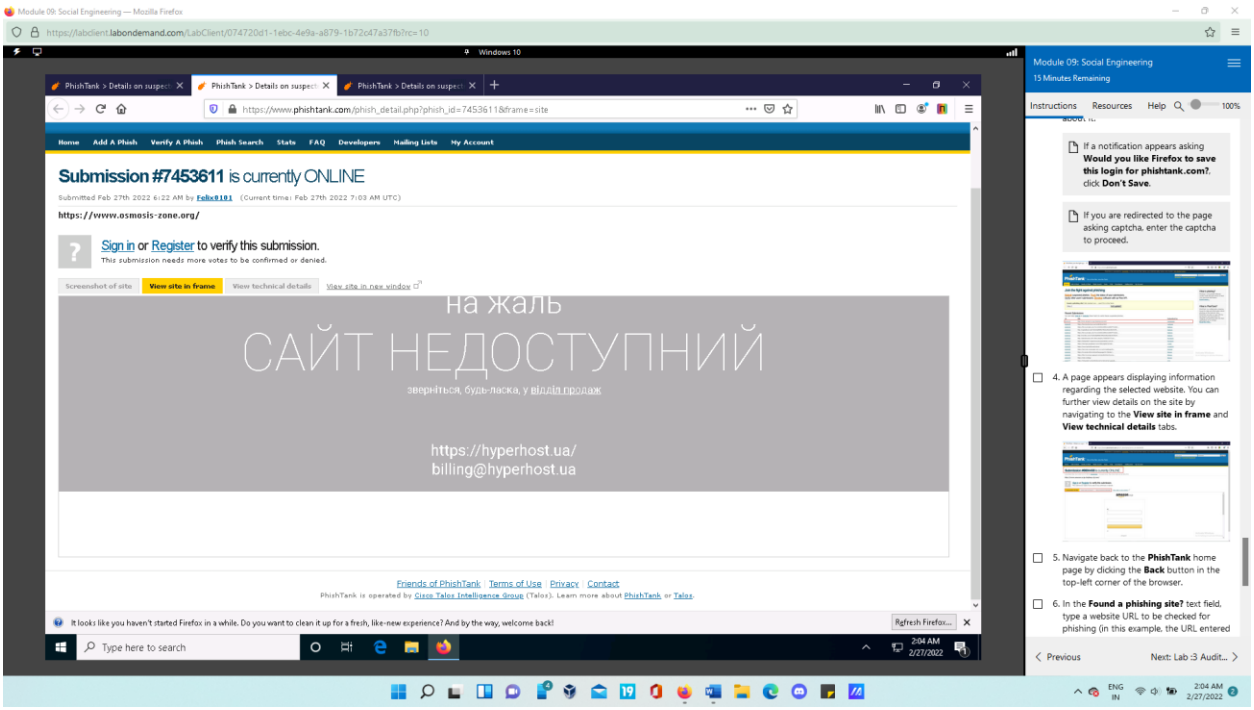
- Launch Web browser in Windows10 and navigate to https://www.phishtank.com. Under Recent Submissions, the PhishTank portal displays, providing a list of phishing websites.

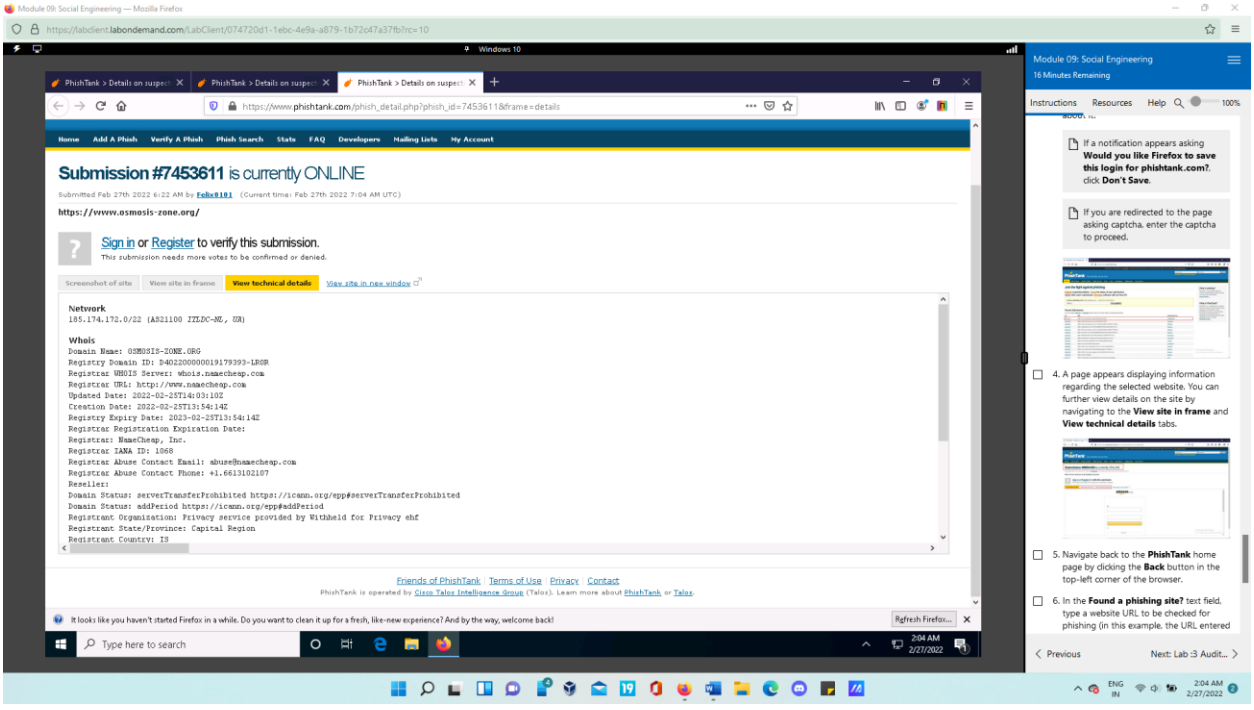


- To access full information on any phishing website ID in the Recent Submissions list, click on
it.

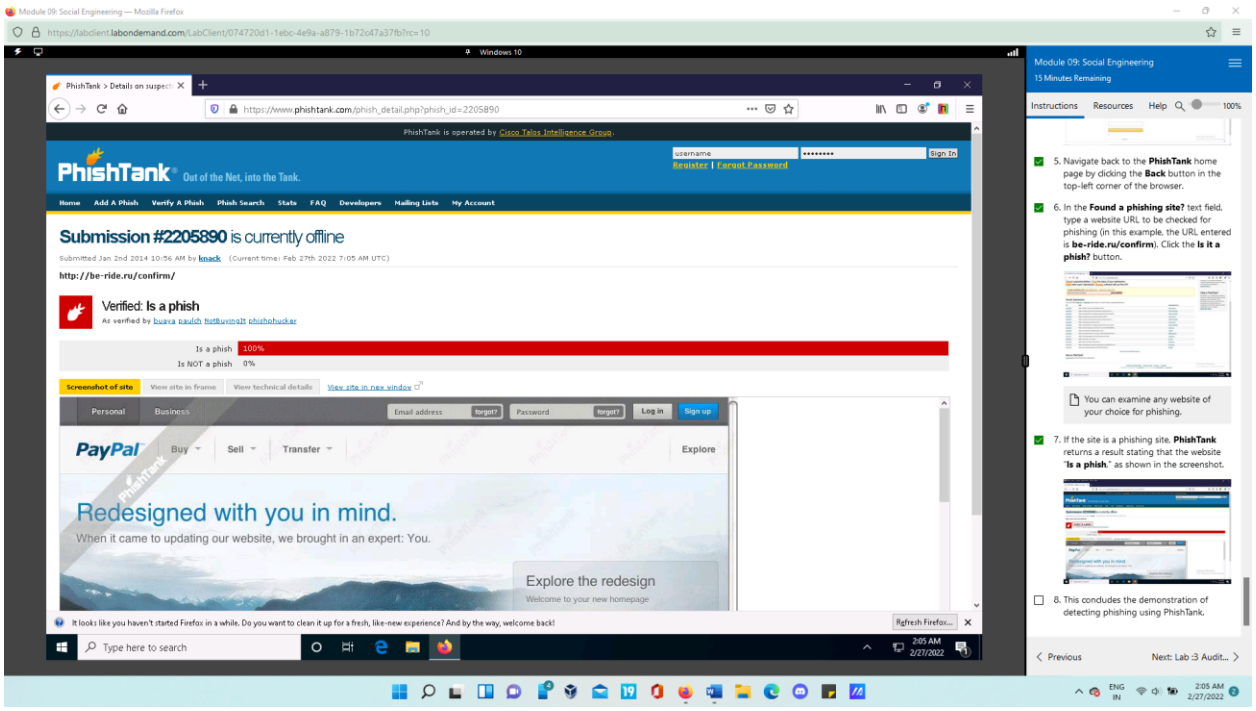


- A page with information about the selected website appears. Navigate to the View site in frame and view technical details tabs to see more information about the site. Click the Back button in the top-left corner of the browser to return to the PhishTank home page.





- Type a website URL to be tested for phishing in the Found a phishing site? text field. To find out if it's a phish, click the Is it a phish? button. If the site is a phishing site, PhishTank will provide a result that says, "Is a phish."

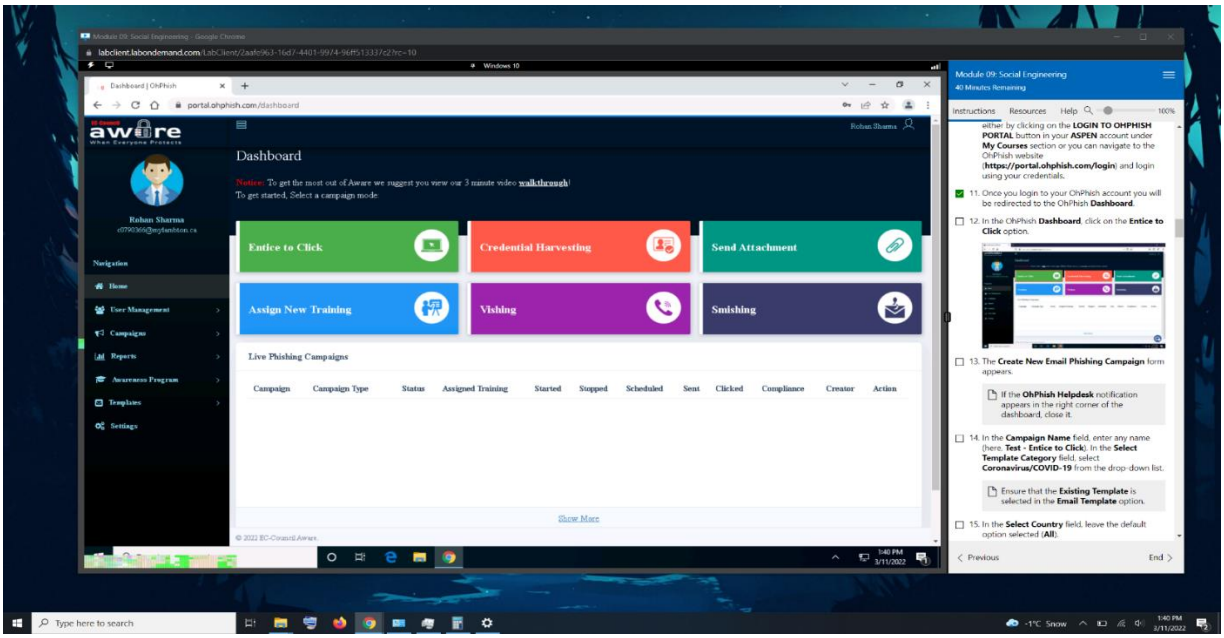


Lab 3: Audit Organization’s Security for Phishing attack

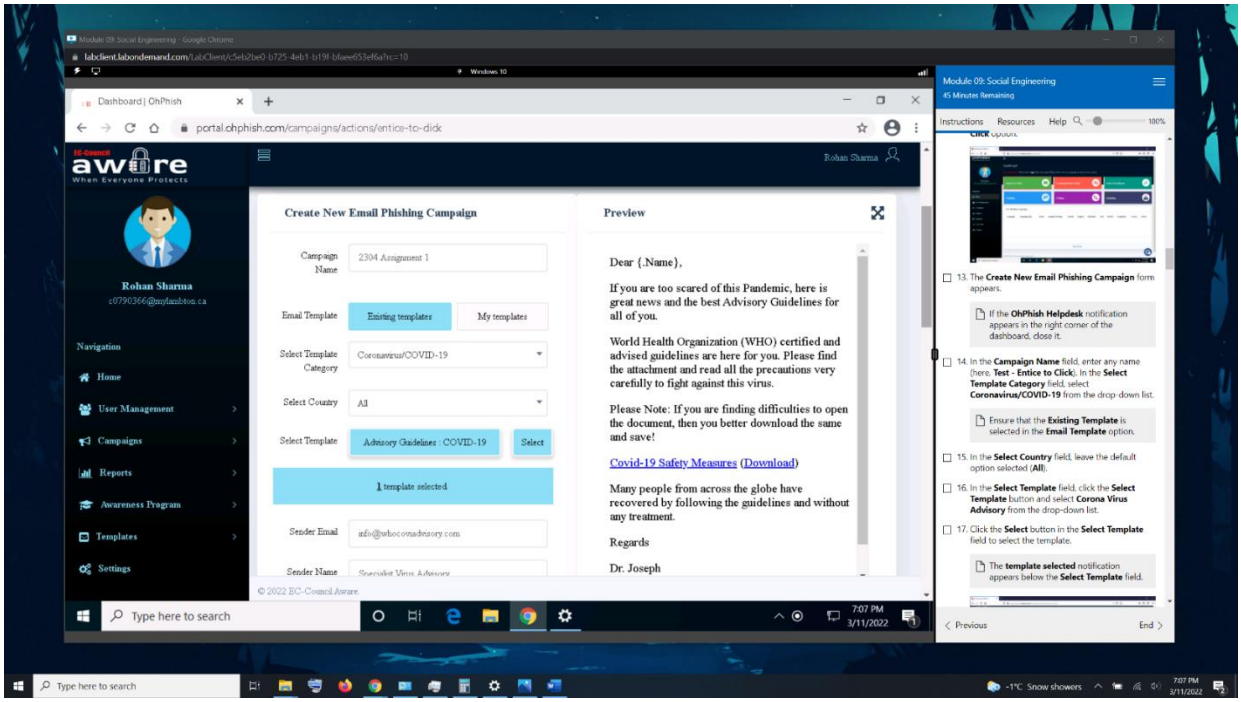
Task 1: Audit Organization's Security for Phishing Attacks using OhPhish

In this task we’ll be using OhPhish to test an organization’s defense against phishing attacks.

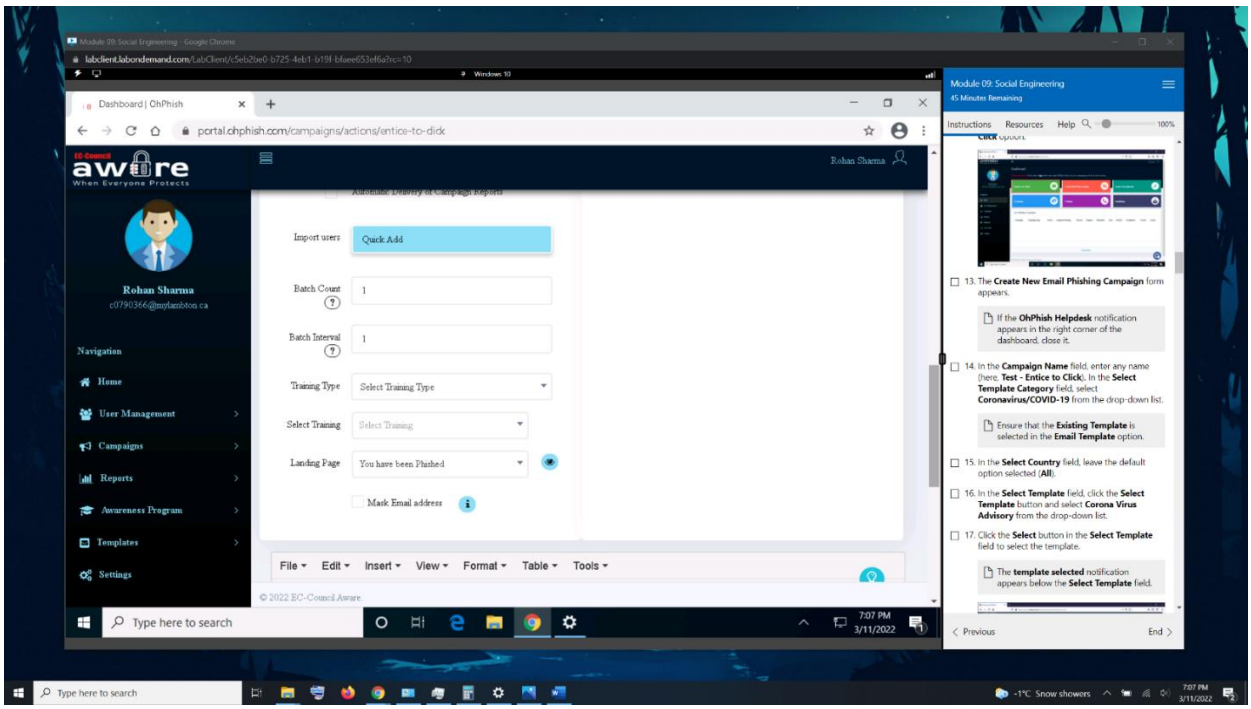
- Launch Web browser in Windows10 and login to the OhPhish portal which leads to the dashboard. We’ll proceed to Entice to Click option from there.

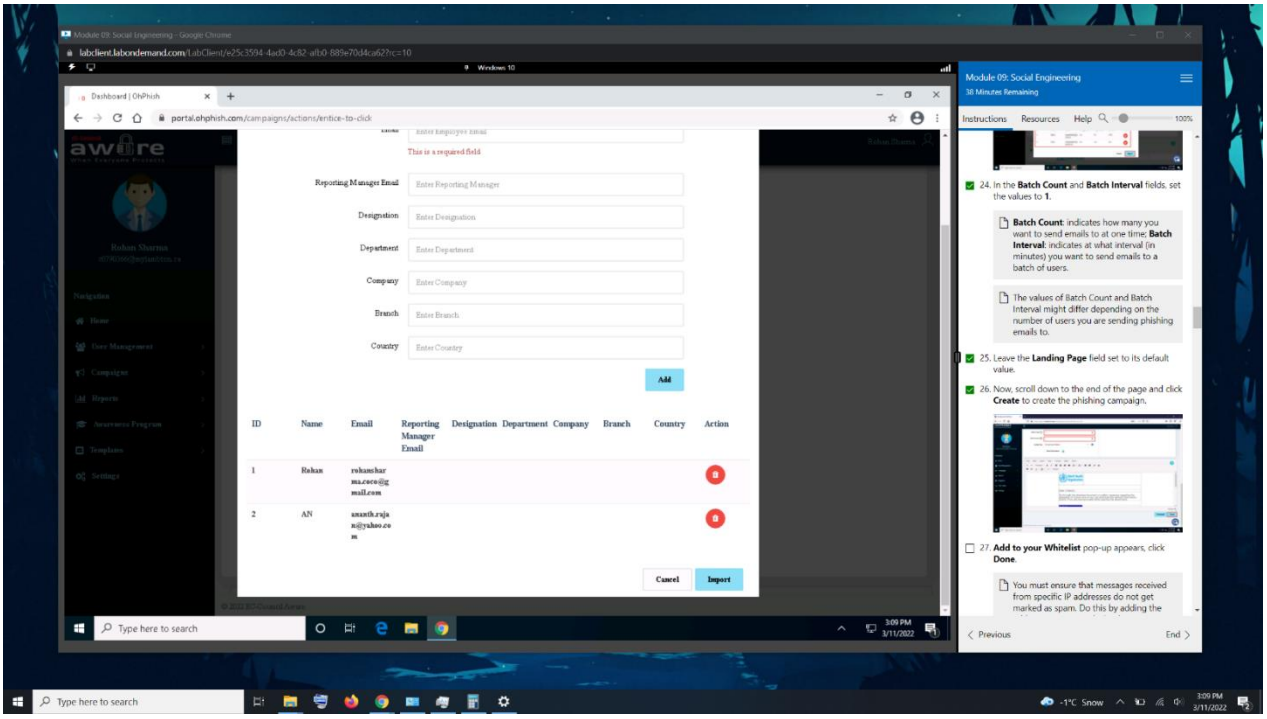


- Next, we’ll create a new phishing campaign with the name 2304 Assignment-1 which will be based on Covid-19, where the used will be tricked to click on link disguised as a link for new covid guidelines.

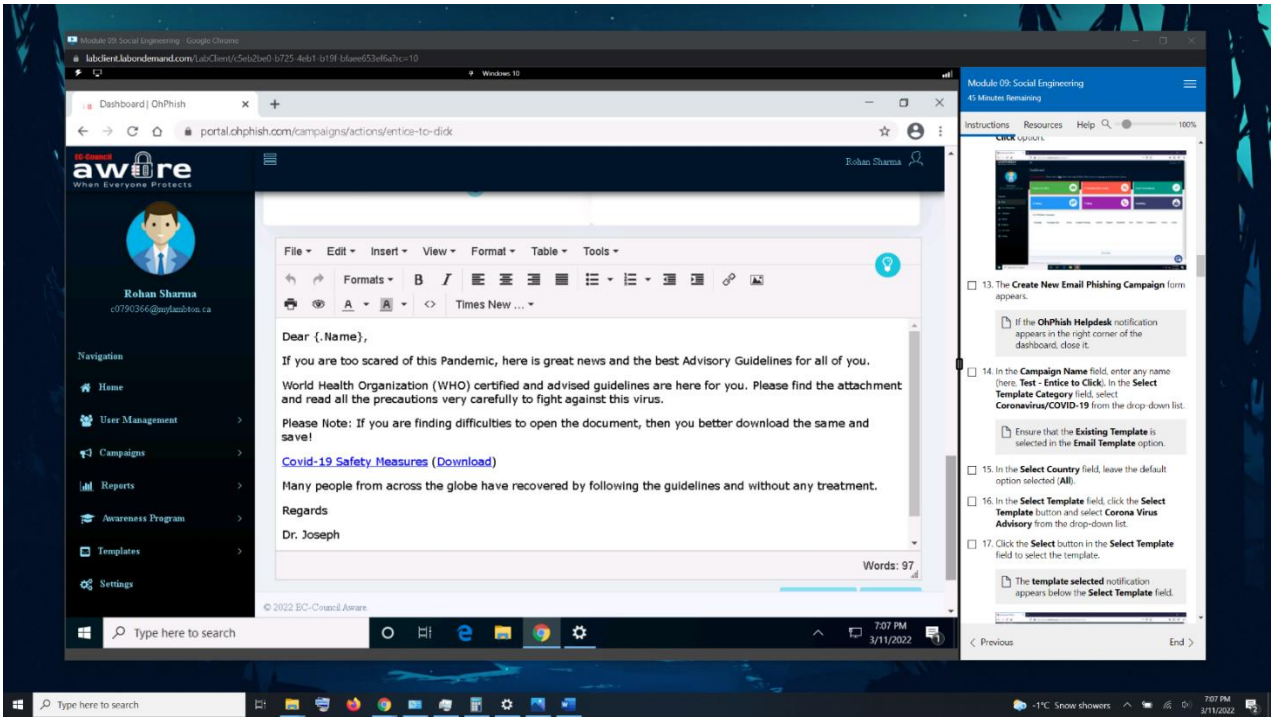

Module 09: Social Engineering - Google Chrome
labclient.labondemand.com/LabClient/c5eb2be0-b725-4eb1-b19f-b6aee653ef6a?rc=10
Windows 10
Dashboard | OhPhish
portal.chphish.com/campaigns/actions/entice-to-click
aware
When Everyone Protects
Rohan Sharma
Rohan Sharma
c0790366@mylambton.ca
Navigation
Home
User Management
Campaigns
Reports
Awareness Program
Templates
Settings
Create New Email Phishing Campaign
Campaign Name
2304 Assignment 1
Email Template
Existing templates
My templates
Select Template Category
Coronavirus/COVID-19
Select Country
All
Select Template
Advisory Guidelines : COVID-19
Select
1 template selected
Sender Email
info@whocovadvisory.com
Sender Name
Specialist Virus Advisory
© 2022 EC-Council Aware.
Preview
Dear {.Name},
If you are too scared of this Pandemic, here is great news and the best Advisory Guidelines for all of you.
World Health Organization (WHO) certified and advised guidelines are here for you. Please find the attachment and read all the precautions very carefully to fight against this virus.
Please Note: If you are finding difficulties to open the document, then you better download the same and save!
Covid-19 Safety Measures (Download)
Many people from across the globe have recovered by following the guidelines and without any treatment.
Regards
Dr. Joseph
Type here to search
7:07 PM
3/11/2022
Module 09: Social Engineering
45 Minutes Remaining
Instructions
Resources
Help
100%
13. The Create New Email Phishing Campaign form appears.
If the OhPhish Helpdesk notification appears in the right corner of the dashboard, close it.
14. In the Campaign Name field, enter any name (here, Test - Entice to Click). In the Select Template Category field, select Coronavirus/COVID-19 from the drop-down list.
Ensure that the Existing Template is selected in the Email Template option.
15. In the Select Country field, leave the default option selected (All).
16. In the Select Template field, click the Select Template button and select Corona Virus Advisory from the drop-down list.
17. Click the Select button in the Select Template field to select the template.
The template selected notification appears below the Select Template field.
Previous
End
Type here to search
-1°C Snow showers
7:07 PM
3/11/2022

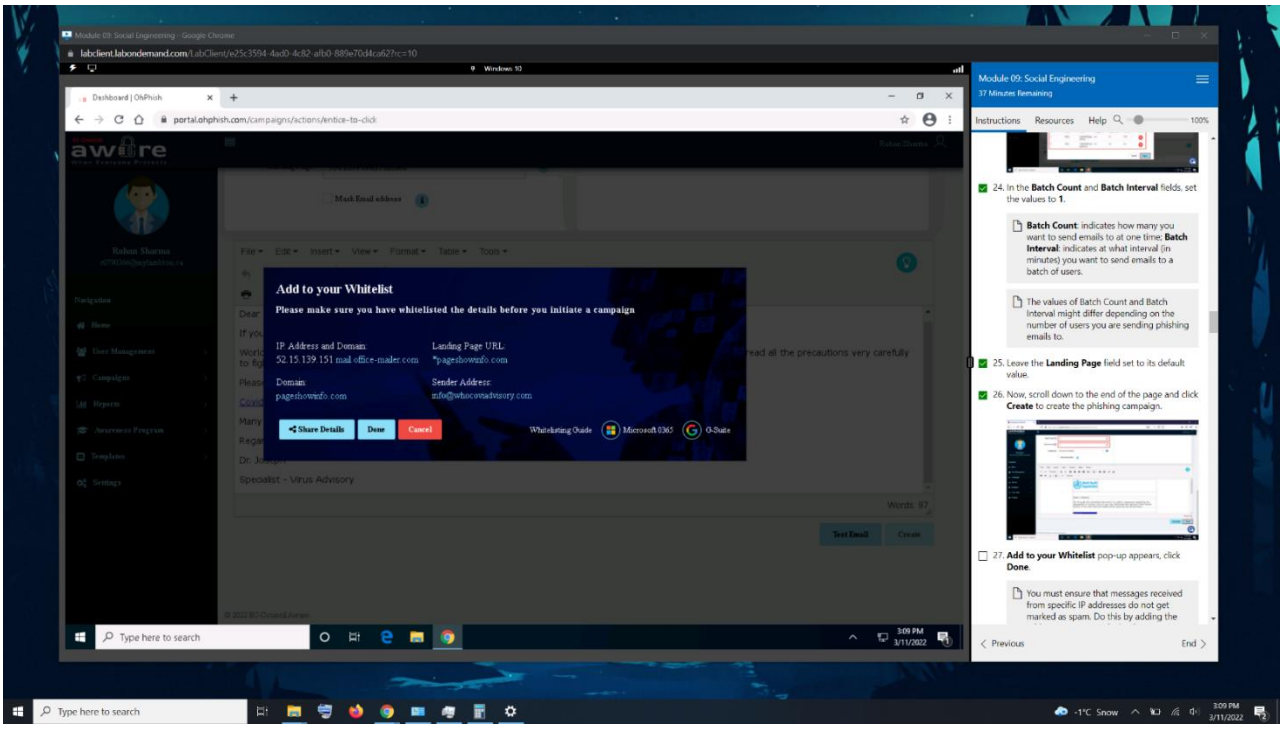
- We'll add the target users, for which we require at least their name and email. After adding the required details for 2 targets we'll click on import.

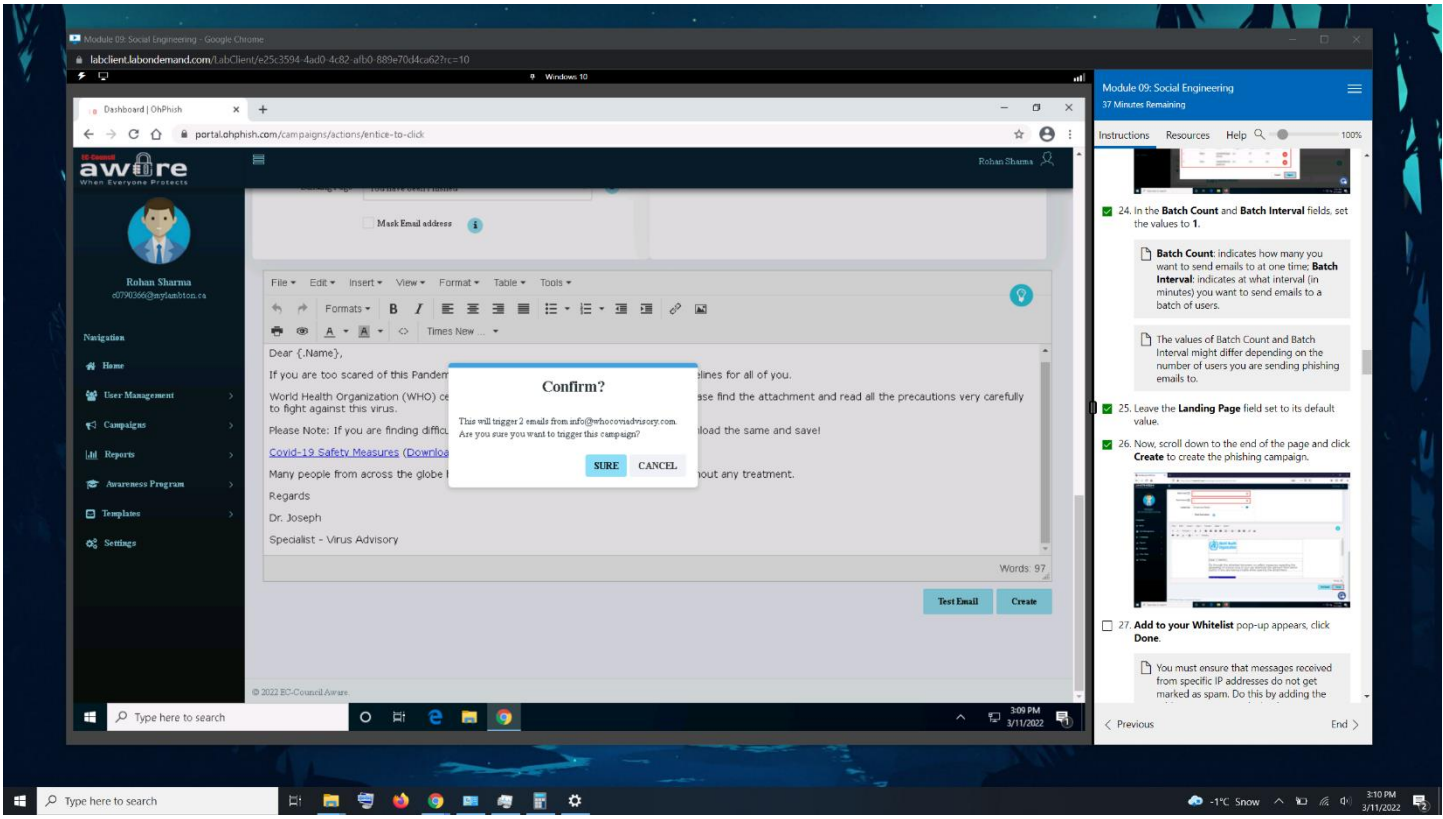




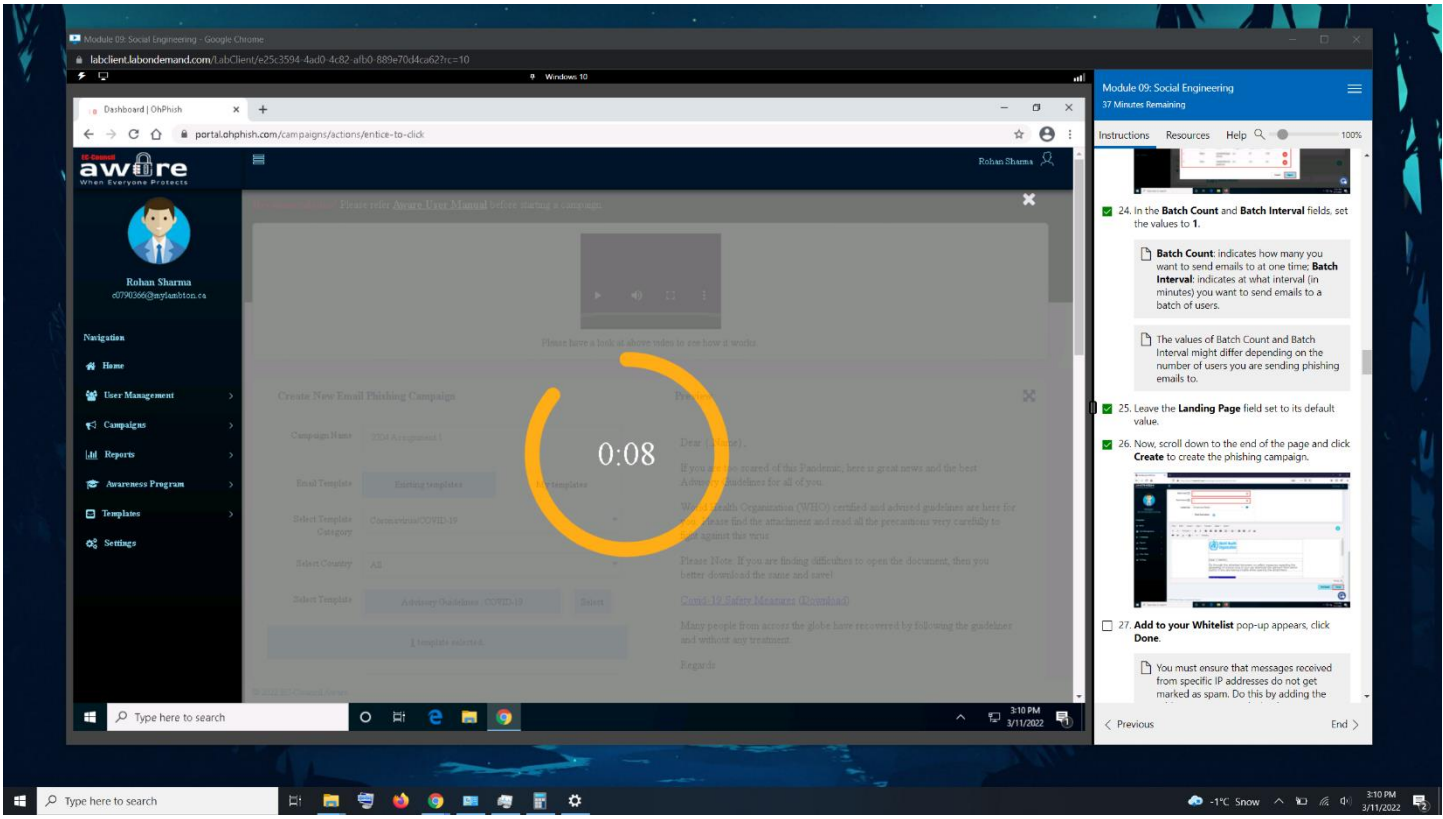
- After confirming the sample email we'll create the campaign, note the domain to whitelist and then proceed through the confirmation prompts as displayed.

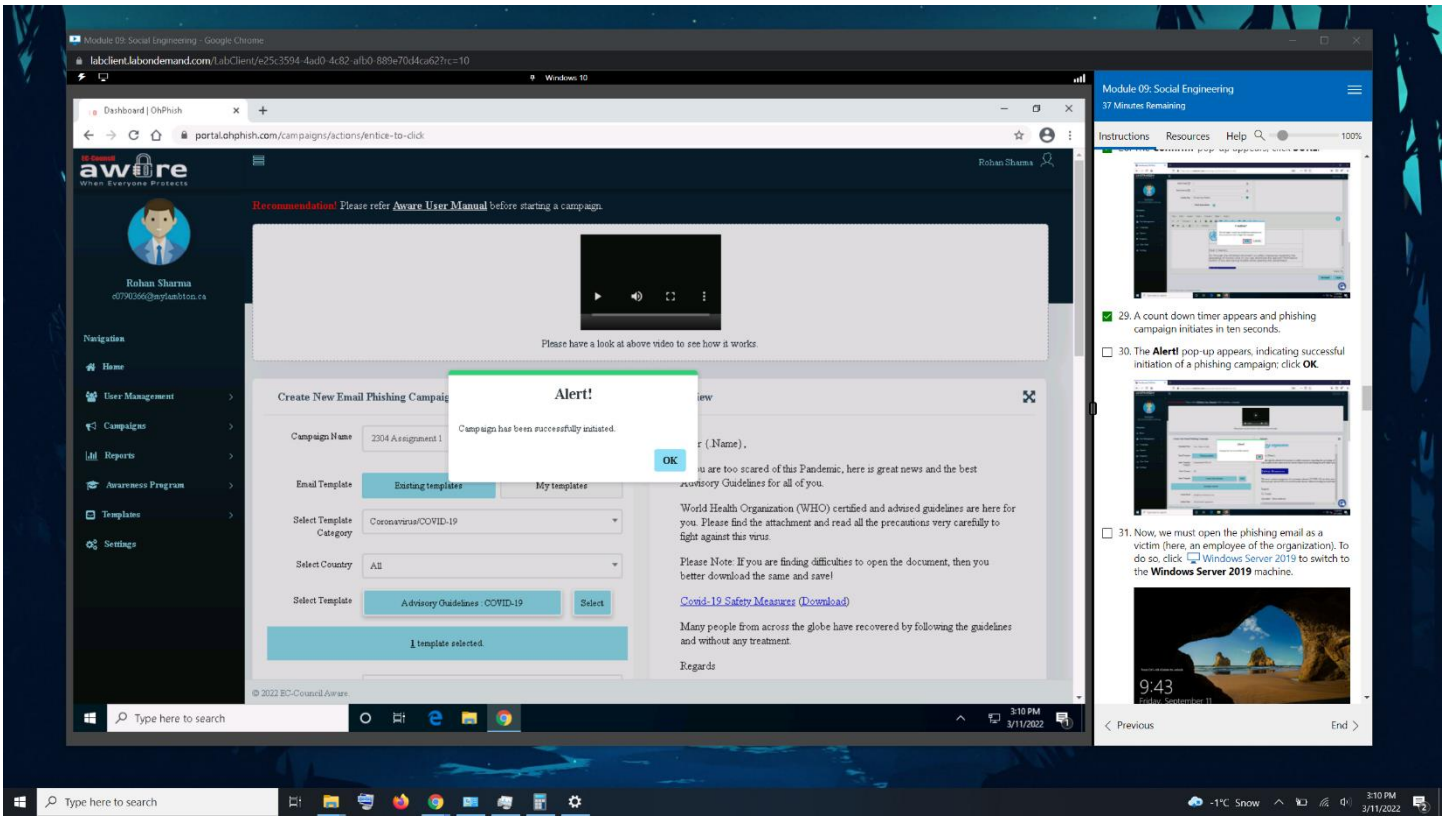




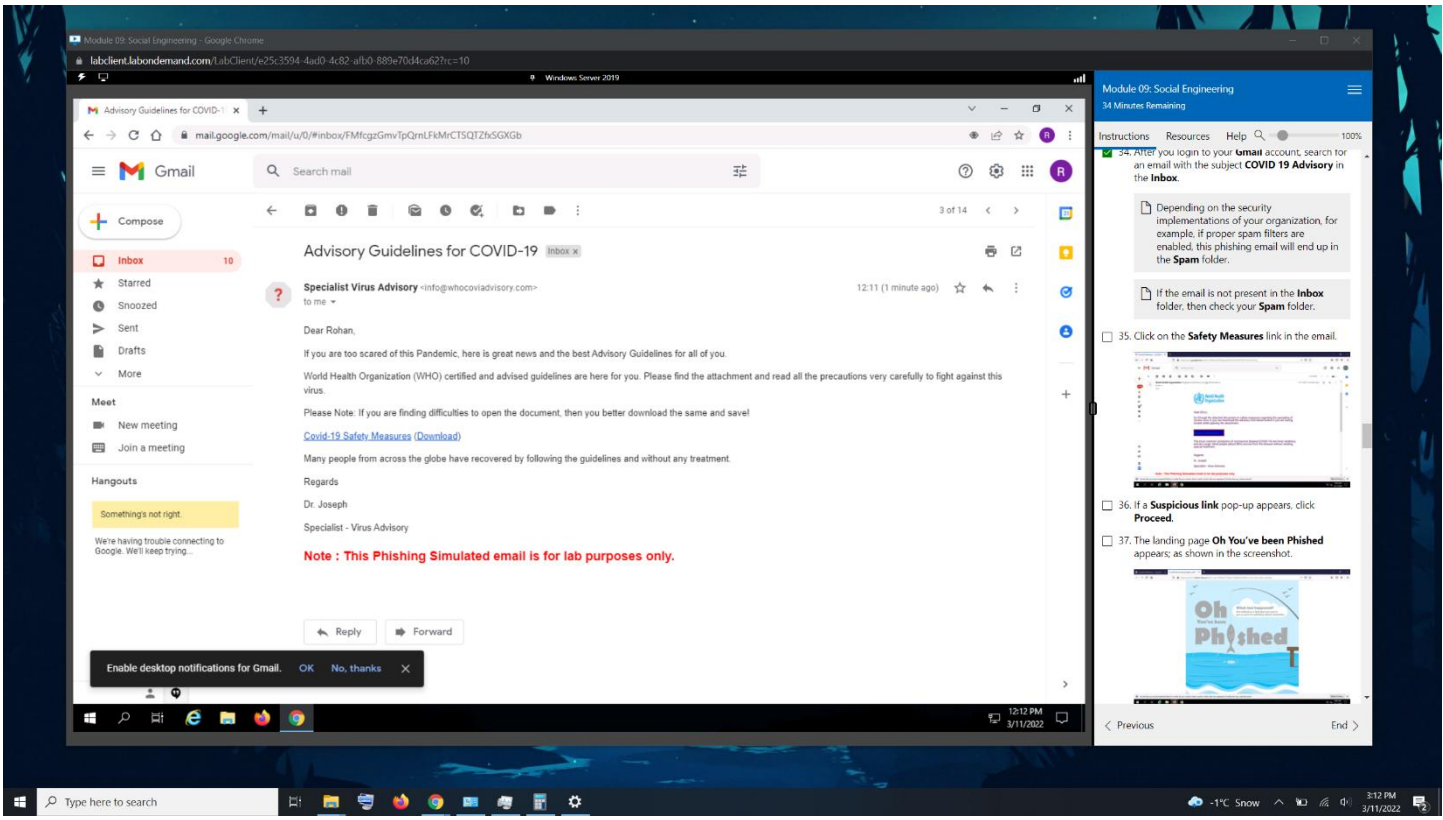


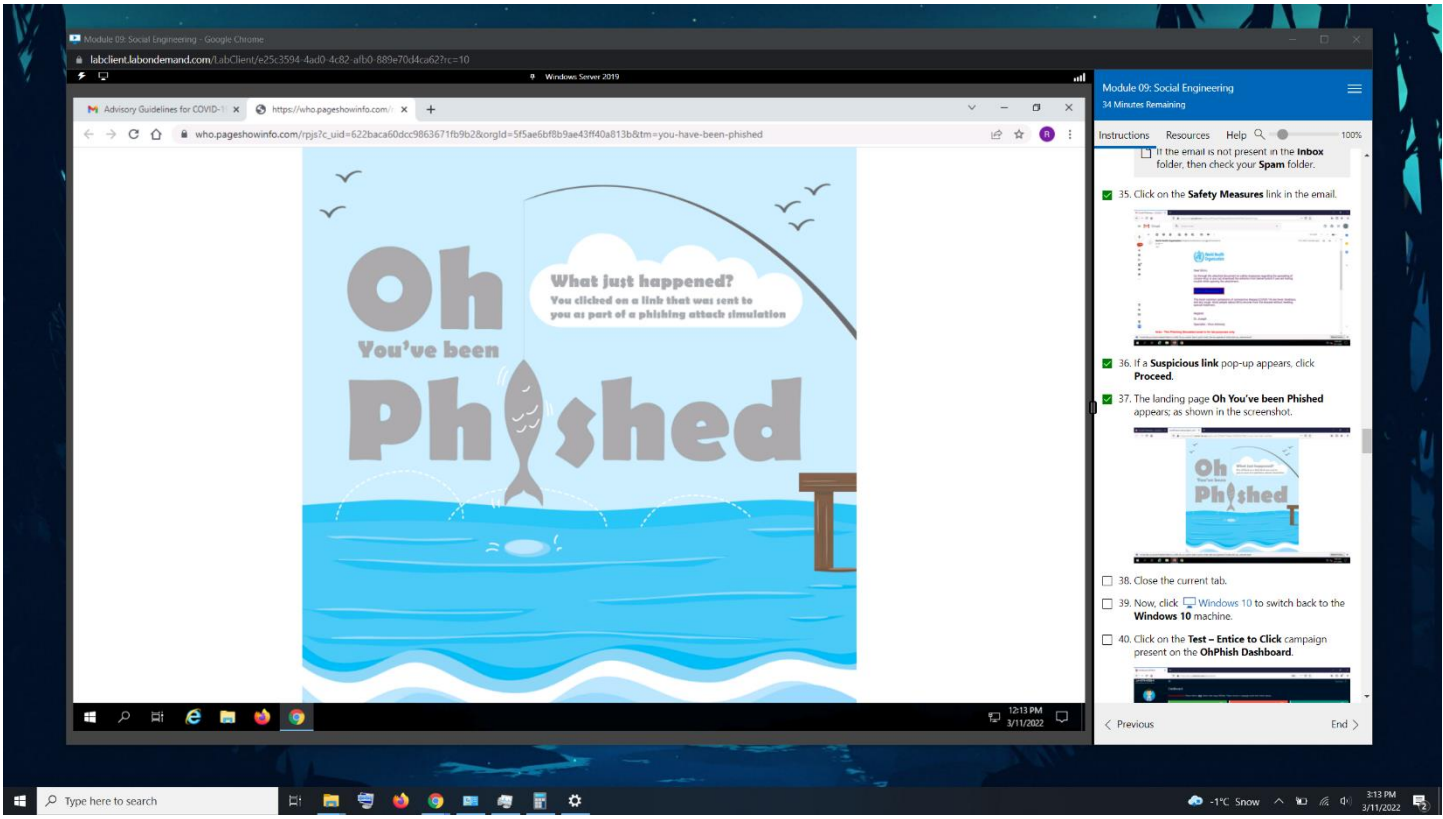
- A countdown is initiated to start the phishing campaign, after which a campaign initiation confirmation appears


Module 09: Social Engineering - Google Chrome
labclient.labondemand.com/LabClient/e25c3594-4ad0-4c82-afb0-889e70d4ca62?rc=10
Windows 10
Dashboard | OhPhish
portal.ohphish.com/campaigns/actions/entice-to-click
aware
When Everyone Protects
Rohan Sharma
Rohan Sharma
c0790366@mylambton.ca
Navigation
Home
User Management
Campaigns
Reports
Awareness Program
Templates
Settings
Please refer Aware User Manual before starting a campaign.
Please have a look at above video to see how it works.
Create New Email Phishing Campaign
0:08
Module 09: Social Engineering
37 Minutes Remaining
Instructions
Resources
Help
100%
24. In the Batch Count and Batch Interval fields, set the values to 1.
Batch Count: indicates how many you want to send emails to at one time; Batch Interval: indicates at what interval (in minutes) you want to send emails to a batch of users.
The values of Batch Count and Batch Interval might differ depending on the number of users you are sending phishing emails to.
25. Leave the Landing Page field set to its default value.
26. Now, scroll down to the end of the page and click Create to create the phishing campaign.
27. Add to your Whitelist pop-up appears, click Done.
You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the
Previous
End
Type here to search
3:10 PM
3/11/2022
-1°C Snow

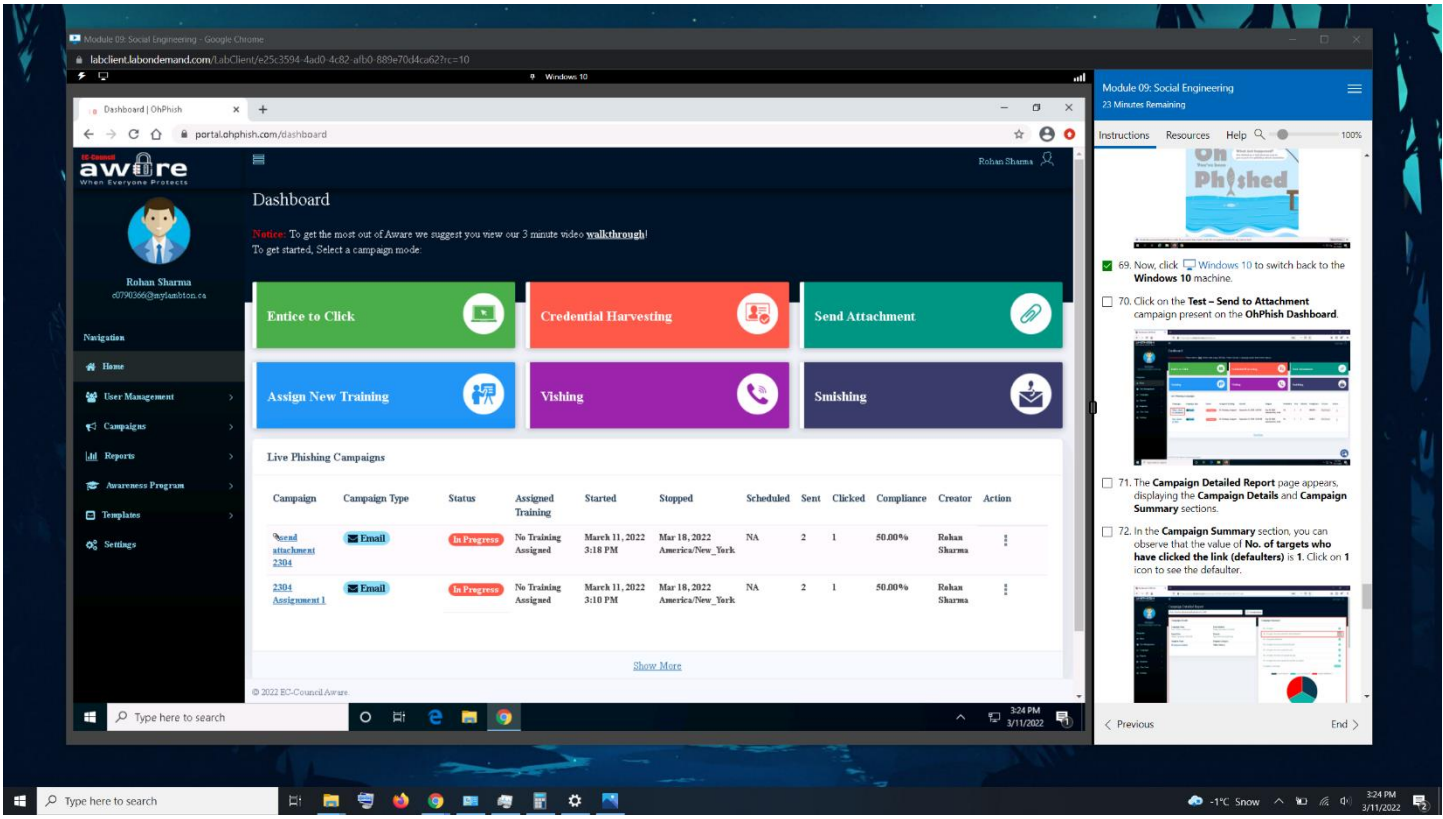

Module 09: Social Engineering - Google Chrome
labclient.labondemand.com/LabClient/e25c3594-4ad0-4c82-afb0-889e70d4ca62?rc=10
Windows 10
Dashboard | OhPhish
portal.ohphish.com/campaigns/actions/entice-to-click
aware
When Everyone Protects
Rohan Sharma
Rohan Sharma
c0790366@mylambton.ca
Navigation
Home
User Management
Campaigns
Reports
Awareness Program
Templates
Settings
Recommendation! Please refer Aware User Manual before starting a campaign.
Please have a look at above video to see how it works.
Create New Email Phishing Campaig
Alert!
Campaign has been successfully initiated.
OK
Campaign Name
2304 Assignment 1
Email Template
Existing templates
My templates
Select Template Category
Coronavirus/COVID-19
Select Country
All
Select Template
Advisory Guidelines : COVID-19
Select
1 template selected.
(Name),
are too scared of this Pandemic, here is great news and the best Advisory Guidelines for all of you.
World Health Organization (WHO) certified and advised guidelines are here for you. Please find the attachment and read all the precautions very carefully to fight against this virus.
Please Note: If you are finding difficulties to open the document, then you better download the same and save!
Covid-19 Safety Measures (Download)
Many people from across the globe have recovered by following the guidelines and without any treatment.
Regards
© 2022 EC-Council Aware.
Module 09: Social Engineering
37 Minutes Remaining
Instructions
Resources
Help
100%
29. A count down timer appears and phishing campaign initiates in ten seconds.
30. The Alert! pop-up appears, indicating successful initiation of a phishing campaign; click OK.
31. Now, we must open the phishing email as a victim (here, an employee of the organization). To do so, click Windows Server 2019 to switch to the Windows Server 2019 machine.
9:43
Friday, September 11
Previous
End
Type here to search
3:10 PM
3/11/2022
-1°C Snow

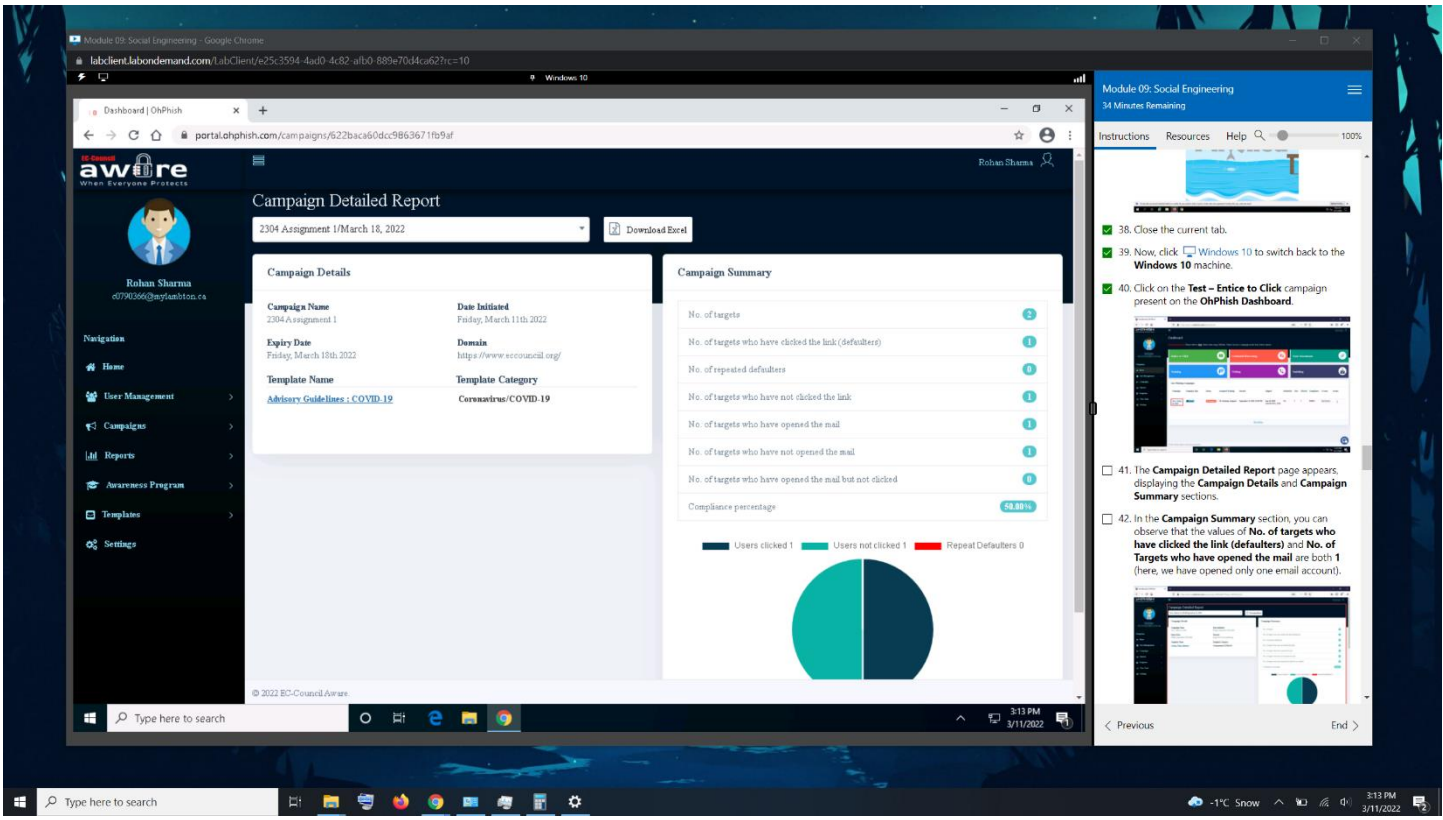
- The victim opens the phishing email and a link for covid guidelines appears, upon clicking the link they are redirected to a webpage stating they have been phished.



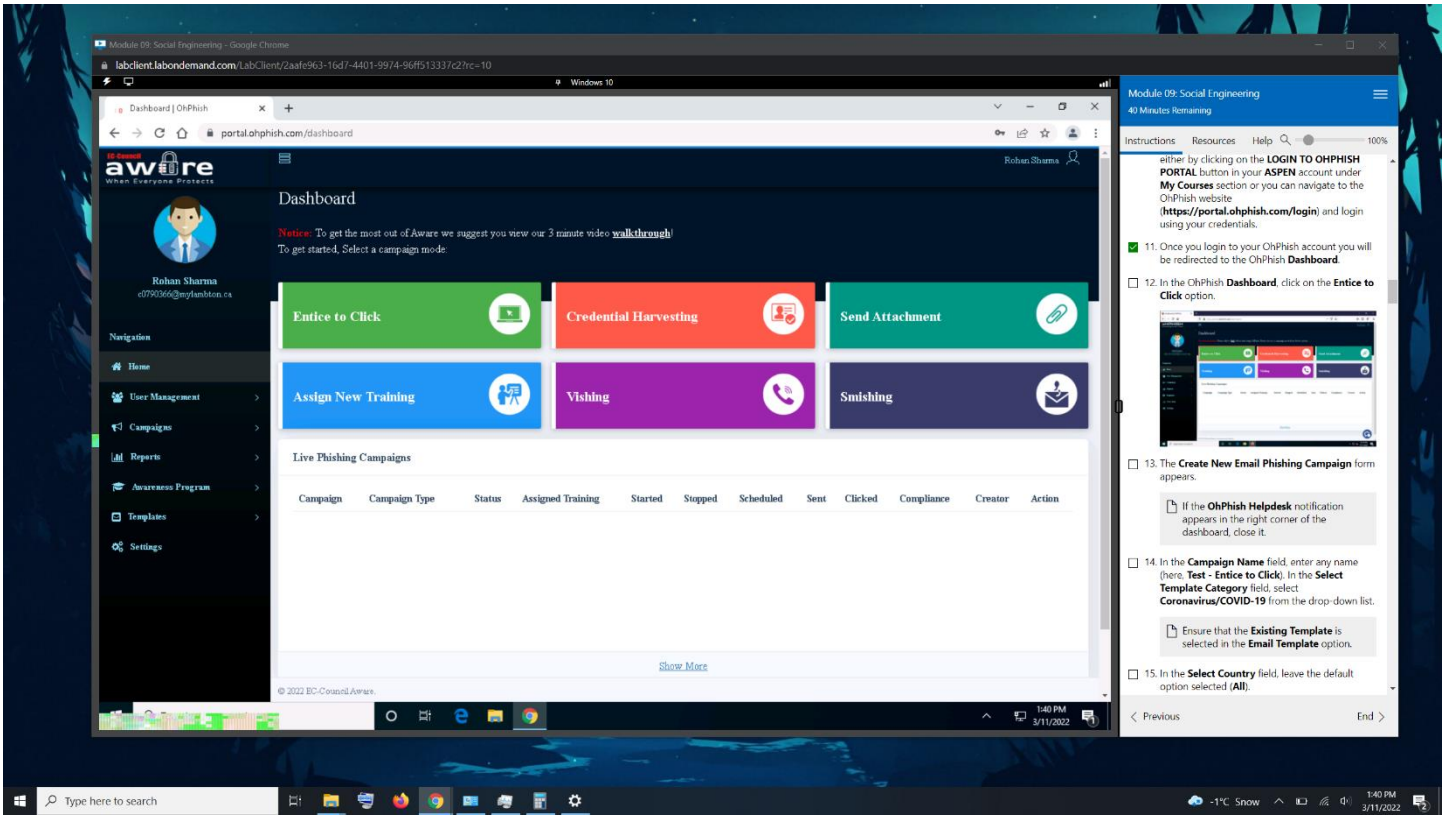


- Back at the dashboard we can click on the campaign name to access its summary, including successfully attacked targets.

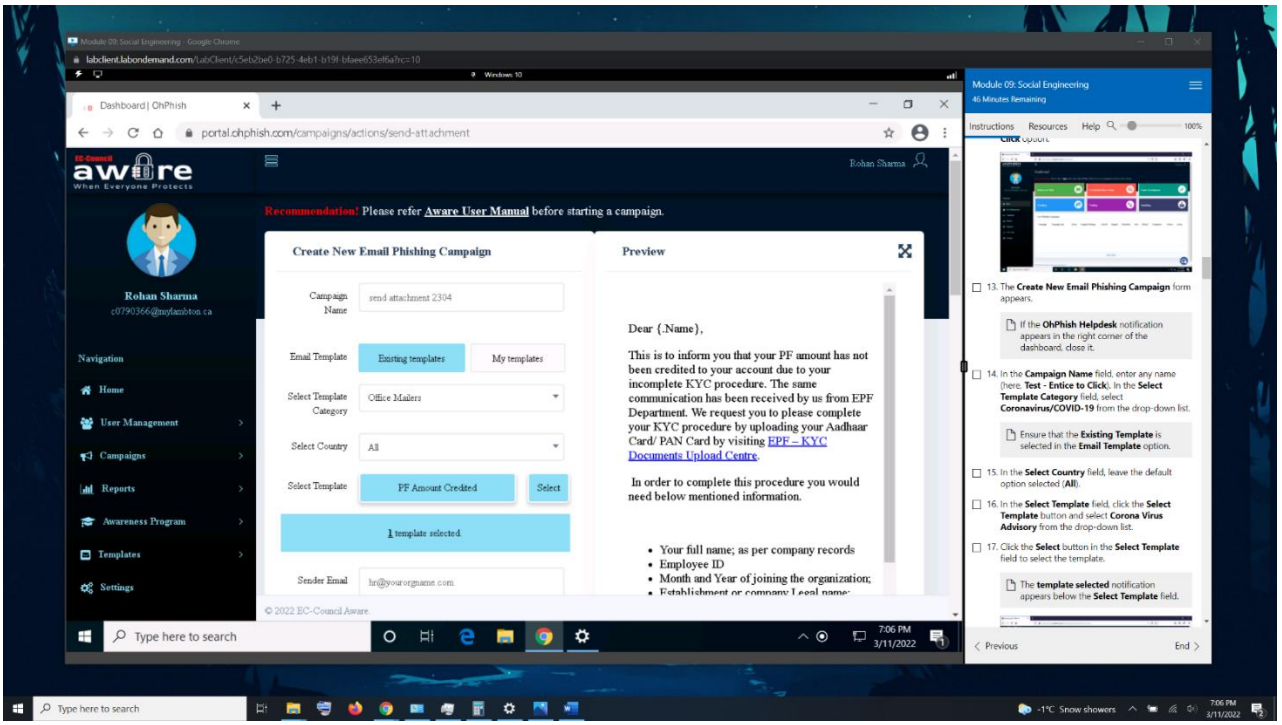

Module 09: Social Engineering - Google Chrome
labclient.labondemand.com/LabClient/e25c3594-4ad0-4c82-afb0-889e70d4ca62?rc=10
Windows 10
Dashboard | OhPhish
portal.ohphish.com/dashboard
aware
When Everyone Protects
Rohan Sharma
Dashboard
Notice: To get the most out of Aware we suggest you view our 3 minute video walkthrough!
To get started, Select a campaign mode:
Entice to Click
Credential Harvesting
Send Attachment
Assign New Training
Vishing
Smishing
Live Phishing Campaigns
Campaign
Campaign Type
Status
Assigned Training
Started
Stopped
Scheduled
Sent
Clicked
Compliance
Creator
Action
Send attachment 2304
Email
In Progress
No Training Assigned
March 11, 2022 3:18 PM
Mar 18, 2022 America/New_York
NA
2
1
50.00%
Rohan Sharma
2304 Assignment 1
Email
In Progress
No Training Assigned
March 11, 2022 3:10 PM
Mar 18, 2022 America/New_York
NA
2
1
50.00%
Rohan Sharma
Show More
© 2022 EC-Council Aware.
Type here to search
3:24 PM
3/11/2022
Module 09: Social Engineering
23 Minutes Remaining
Instructions
Resources
Help
100%
69. Now, click Windows 10 to switch back to the Windows 10 machine.
70. Click on the Test – Send to Attachment campaign present on the OhPhish Dashboard.
71. The Campaign Detailed Report page appears, displaying the Campaign Details and Campaign Summary sections.
72. In the Campaign Summary section, you can observe that the value of No. of targets who have clicked the link (defaulters) is 1. Click on 1 icon to see the defaulter.
Previous
End
Type here to search
-1°C Snow
3:24 PM
3/11/2022

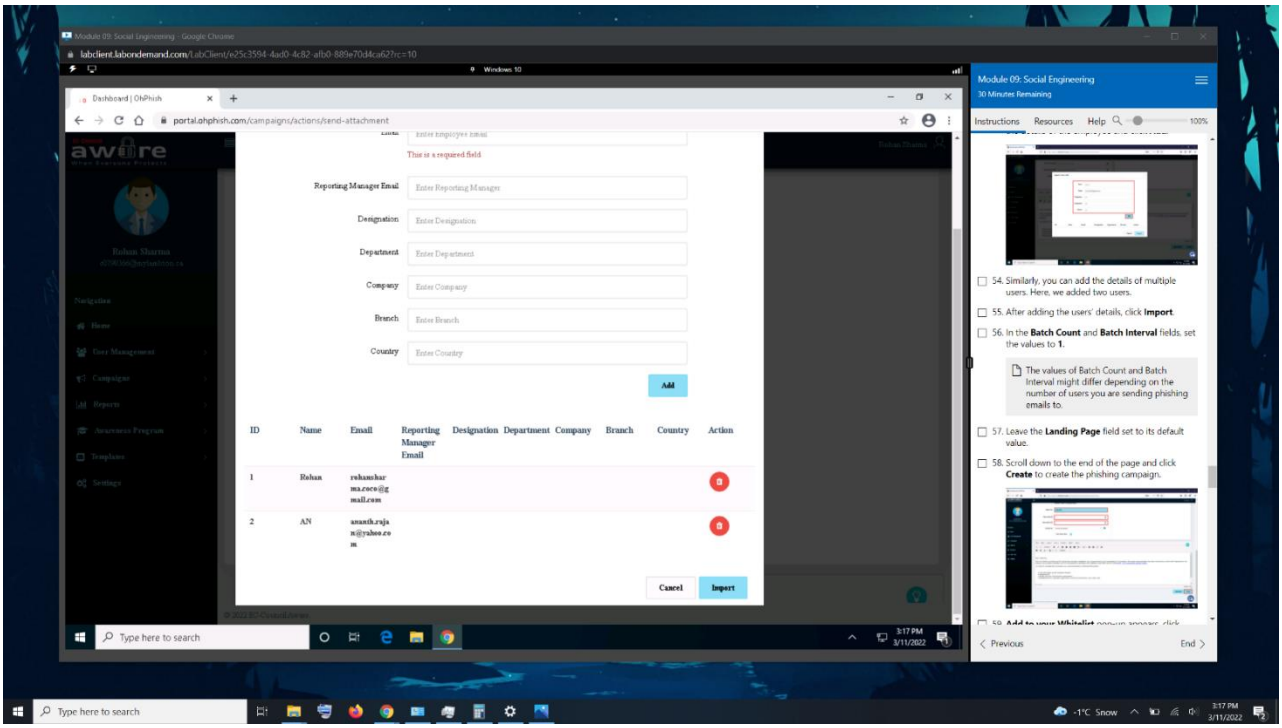

Module 09: Social Engineering - Google Chrome
labclient.labondemand.com/LabClient/e25c3594-4ad0-4c82-afb0-889e70d4ca62?rc=10
Windows 10
Dashboard | OhPhish
portal.ohphish.com/campaigns/622baca60dcc9863671fb9af
aware
When Everyone Protects
Rohan Sharma
Campaign Detailed Report
2304 Assignment 1/March 18, 2022
Download Excel
Campaign Details
Campaign Name
2304 Assignment 1
Date Initiated
Friday, March 11th 2022
Expiry Date
Friday, March 18th 2022
Domain
https://www.eccouncil.org/
Template Name
Advisory Guidelines : COVID-19
Template Category
Coronavirus/COVID-19
Campaign Summary
No. of targets 2
No. of targets who have clicked the link (defaulters) 1
No. of repeated defaulters 0
No. of targets who have not clicked the link 1
No. of targets who have opened the mail 1
No. of targets who have not opened the mail 1
No. of targets who have opened the mail but not clicked 0
Compliance percentage 50.00%
Users clicked 1
Users not clicked 1
Repeat Defaulters 0
© 2022 EC-Council Aware.
Type here to search
3:13 PM
3/11/2022
Module 09: Social Engineering
34 Minutes Remaining
Instructions
Resources
Help
100%
38. Close the current tab.
39. Now, click Windows 10 to switch back to the Windows 10 machine.
40. Click on the Test – Entice to Click campaign present on the OhPhish Dashboard.
41. The Campaign Detailed Report page appears, displaying the Campaign Details and Campaign Summary sections.
42. In the Campaign Summary section, you can observe that the values of No. of targets who have clicked the link (defaulters) and No. of Targets who have opened the mail are both 1 (here, we have opened only one email account).
Previous
End
Type here to search
-1°C Snow
3:13 PM
3/11/2022

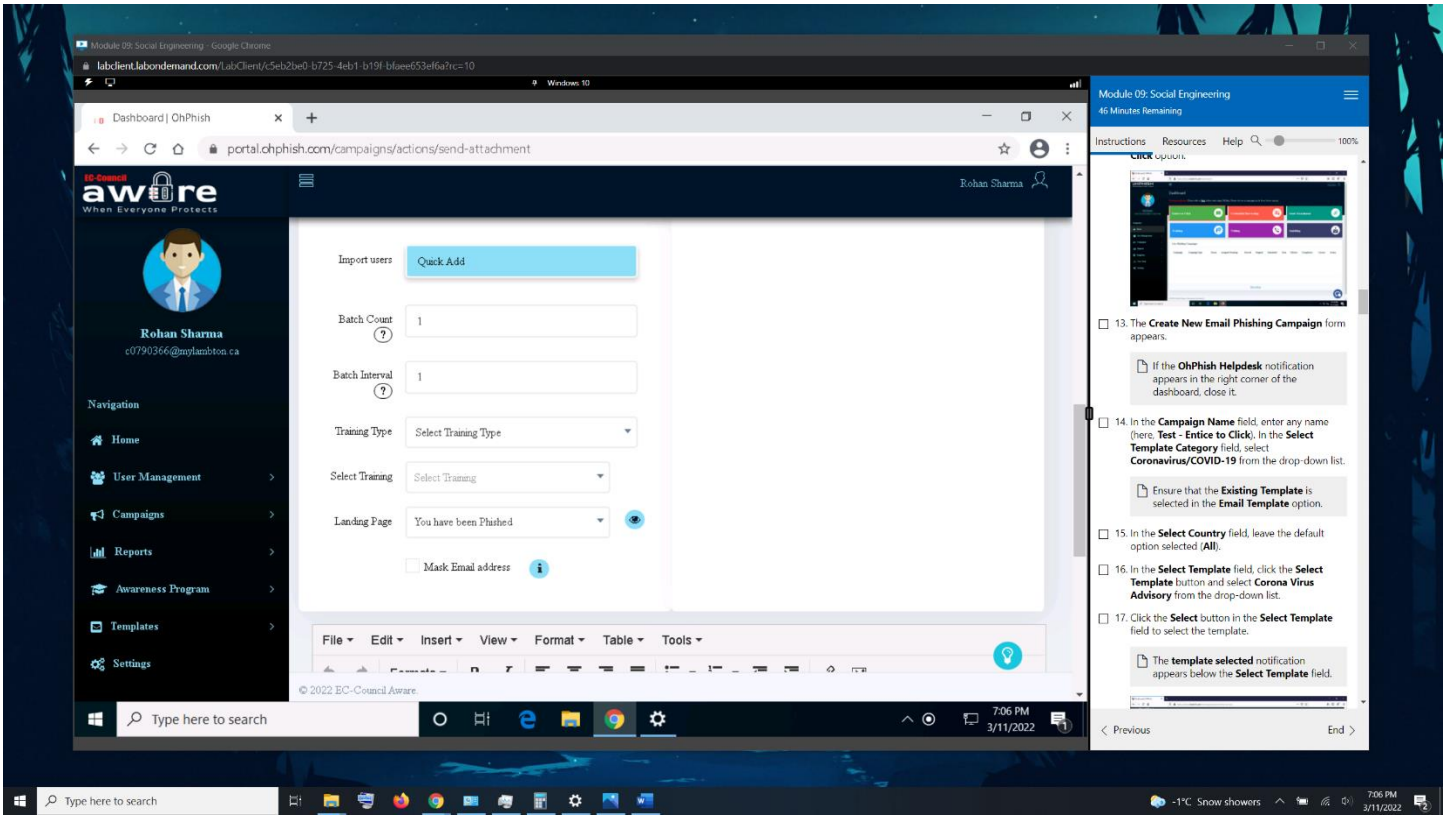
- We’ll start another campaign using the Send Attachment mode.



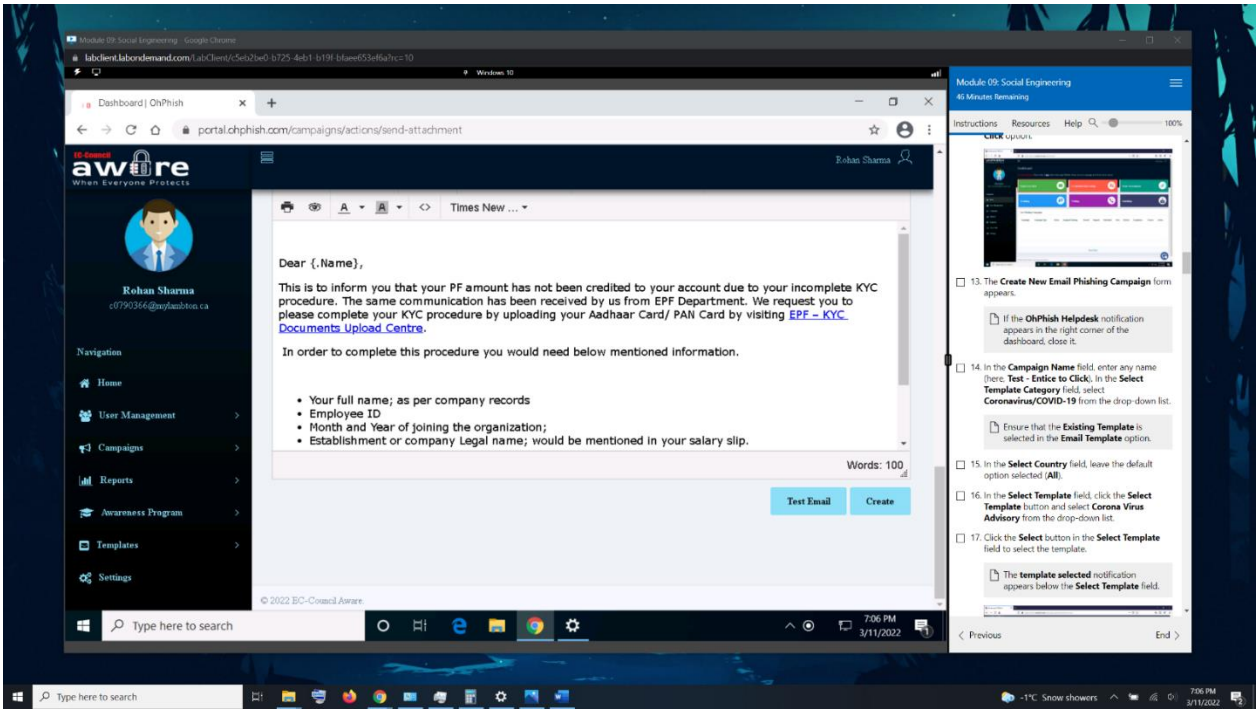
- We’ll use the name send attachment 2304 and Office Mailers (Amount Credited) as the template. Then we’ll add the same targets as used in the previous campaign.

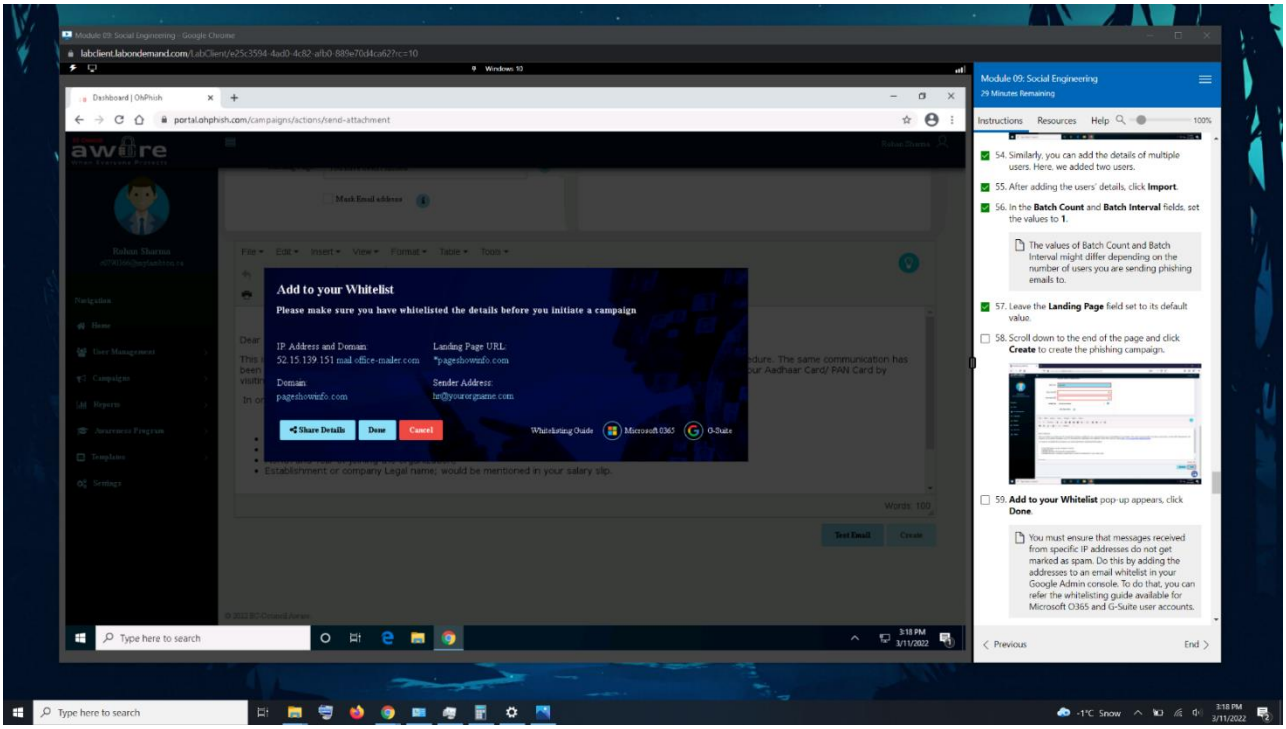

Module 09: Social Engineering - Google Chrome
labclient.labondemand.com/LabClient/c5eb2be0-b725-4eb1-b19f-bfaee653ef6a?rc=10
Windows 10
Dashboard | OhPhish
portal.ohphish.com/campaigns/actions/send-attachment
aware
When Everyone Protects
Rohan Sharma
Recommendation! Please refer Aware User Manual before starting a campaign.
Rohan Sharma
c0790366@mylambton.ca
Navigation
Home
User Management
Campaigns
Reports
Awareness Program
Templates
Settings
Create New Email Phishing Campaign
Campaign Name
send attachment 2304
Email Template
Existing templates
My templates
Select Template Category
Office Mailers
Select Country
All
Select Template
PF Amount Credited
Select
1 template selected
Sender Email
hr@yourorgname.com
Preview
Dear {.Name},
This is to inform you that your PF amount has not been credited to your account due to your incomplete KYC procedure. The same communication has been received by us from EPF Department. We request you to please complete your KYC procedure by uploading your Aadhaar Card/ PAN Card by visiting EPF – KYC Documents Upload Centre.
In order to complete this procedure you would need below mentioned information.
Your full name; as per company records
Employee ID
Month and Year of joining the organization;
© 2022 EC-Council Aware
Type here to search
7:06 PM
3/11/2022
Module 09: Social Engineering
46 Minutes Remaining
Instructions
Resources
Help
100%
13. The Create New Email Phishing Campaign form appears.
If the OhPhish Helpdesk notification appears in the right corner of the dashboard, close it.
14. In the Campaign Name field, enter any name here. Test - Entice to Click. In the Select Template Category field, select Coronavirus/COVID-19 from the drop-down list.
Ensure that the Existing Template is selected in the Email Template option.
15. In the Select Country field, leave the default option selected (All).
16. In the Select Template field, click the Select Template button and select Corona Virus Advisory from the drop-down list.
17. Click the Select button in the Select Template field to select the template.
The template selected notification appears below the Select Template field.
Previous
End
Type here to search
-1°C Snow showers
7:06 PM
3/11/2022


Module 09: Social Engineering - Google Chrome
labclient.labondemand.com/LabClient/e25c3594-4ad0-4c82-afb0-889e70d4ca62?rc=10
Windows 10
Dashboard | OhPhish
portal.ohphish.com/campaigns/actions/send-attachment
This is a required field
Reporting Manager Email
Enter Reporting Manager
Designation
Enter Designation
Department
Enter Department
Company
Enter Company
Branch
Enter Branch
Country
Enter Country
Add
ID
Name
Email
Reporting Manager Email
Designation
Department
Company
Branch
Country
Action
1
Rohan
rohansharma.cscs@gmail.com
2
AN
ananth.rajan@yahoo.com
Cancel
Import
Type here to search
3:17 PM
3/11/2022
Module 09: Social Engineering
30 Minutes Remaining
Instructions
Resources
Help
100%
54. Similarly, you can add the details of multiple users. Here, we added two users.
55. After adding the users' details, click Import.
56. In the Batch Count and Batch Interval fields, set the values to 1.
The values of Batch Count and Batch Interval might differ depending on the number of users you are sending phishing emails to.
57. Leave the Landing Page field set to its default value.
58. Scroll down to the end of the page and click Create to create the phishing campaign.
Previous
End
Type here to search
-1°C Snow
3:17 PM
3/11/2022

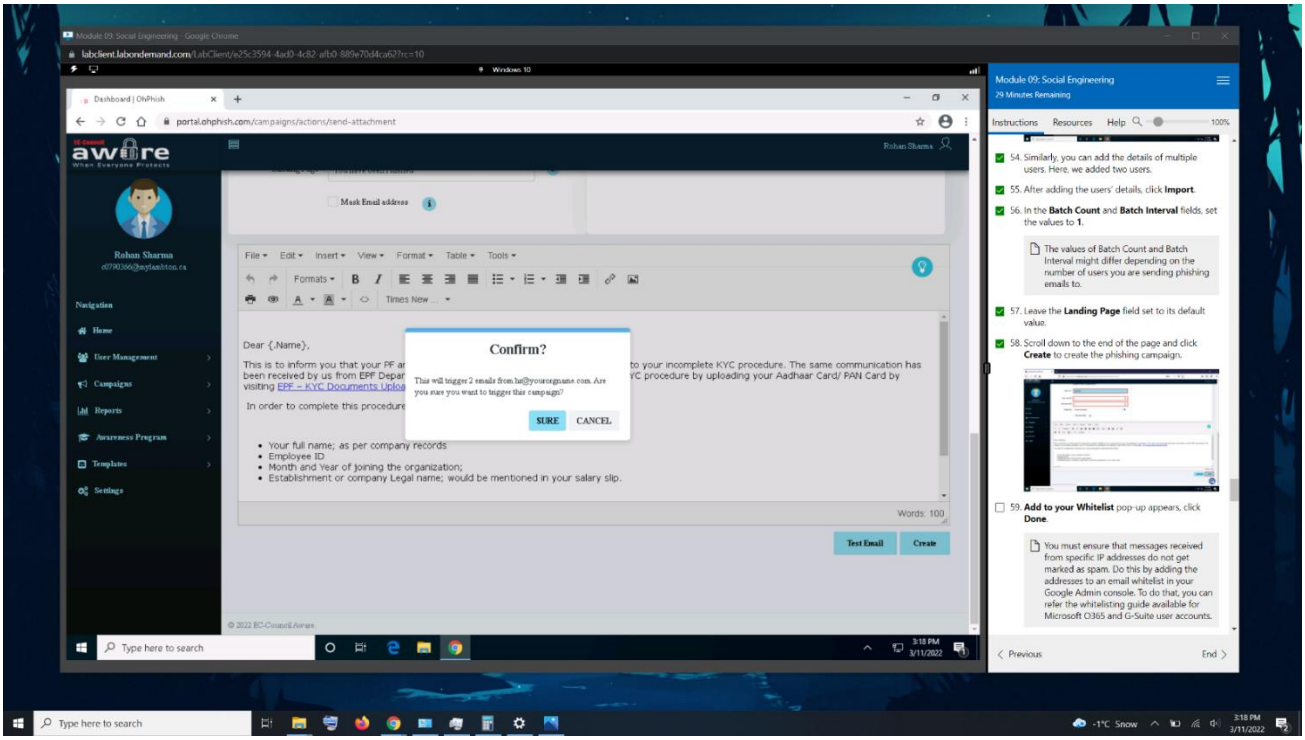


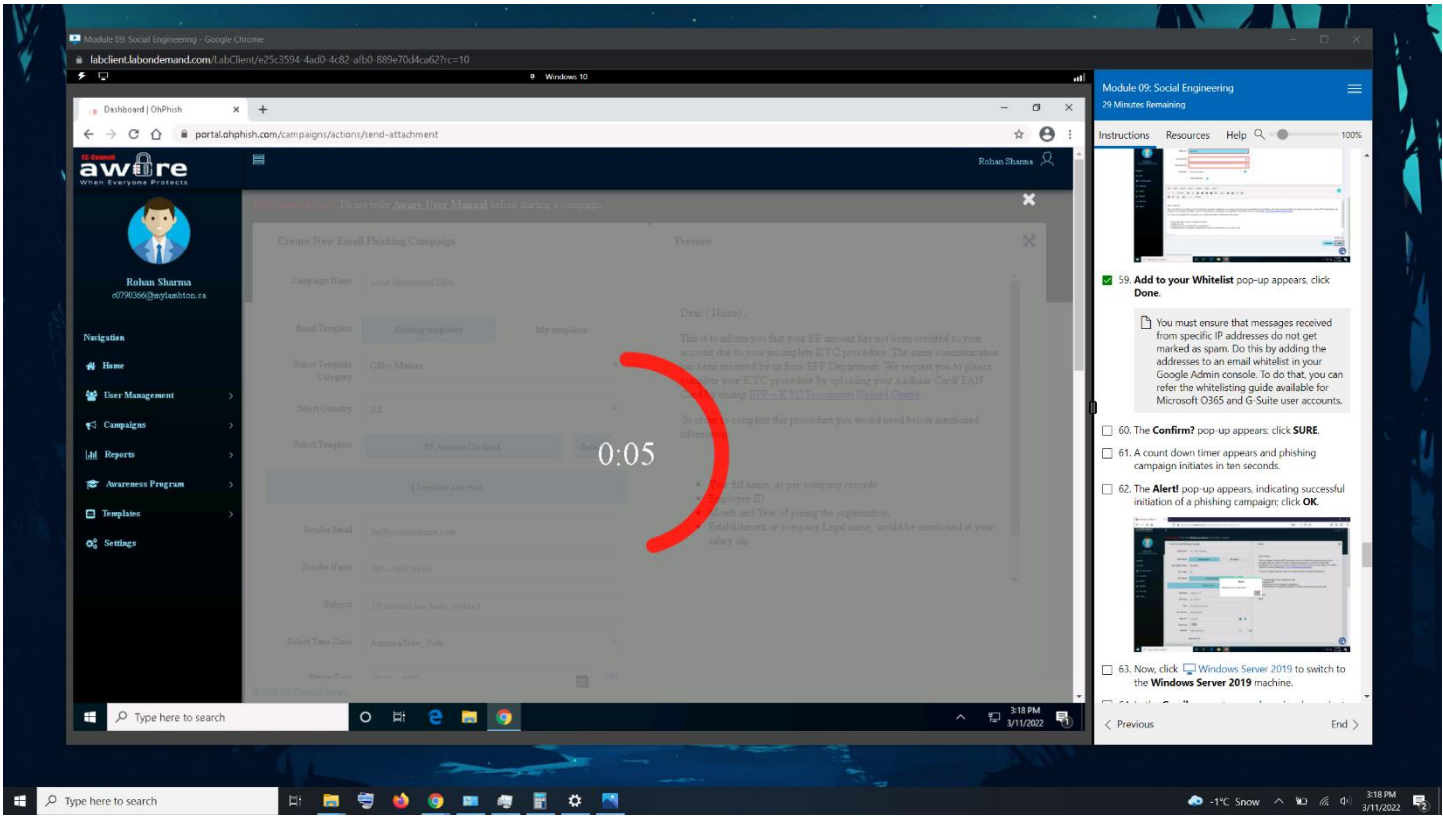
- After checking the test email we'll create the campaign, note the domain to whitelist and then proceed through the confirmation prompts as displayed.

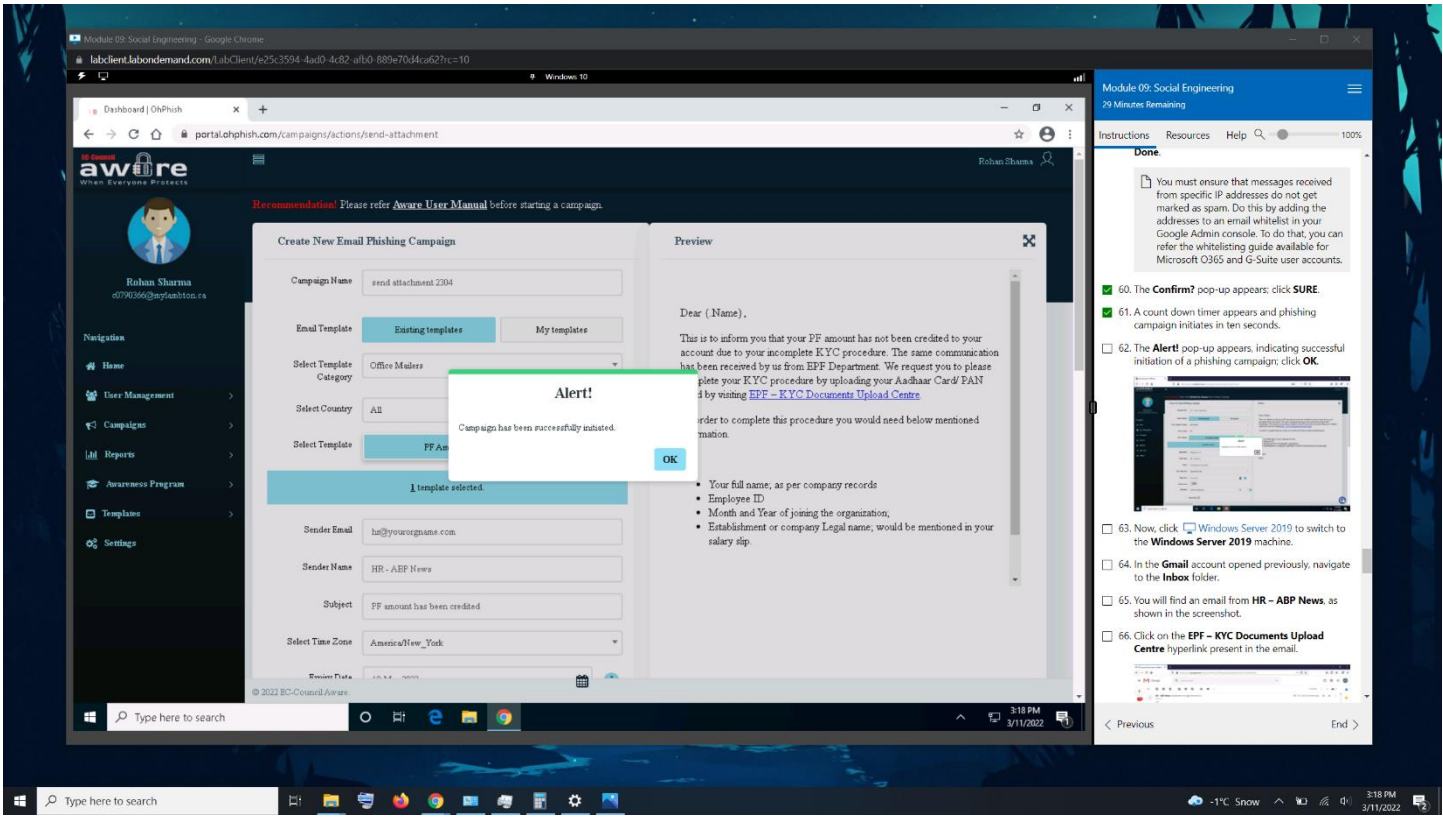




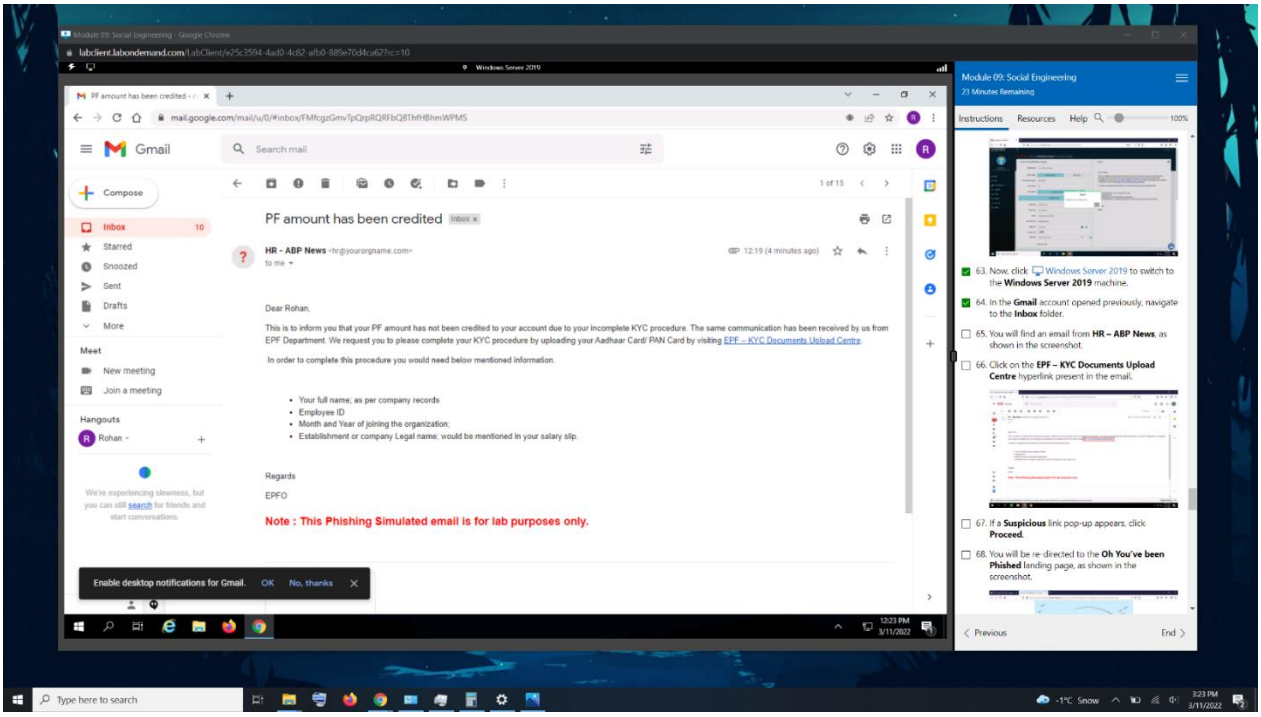
- After final confirmation a countdown is initiated to start the phishing campaign, after which a campaign initiation confirmation appears

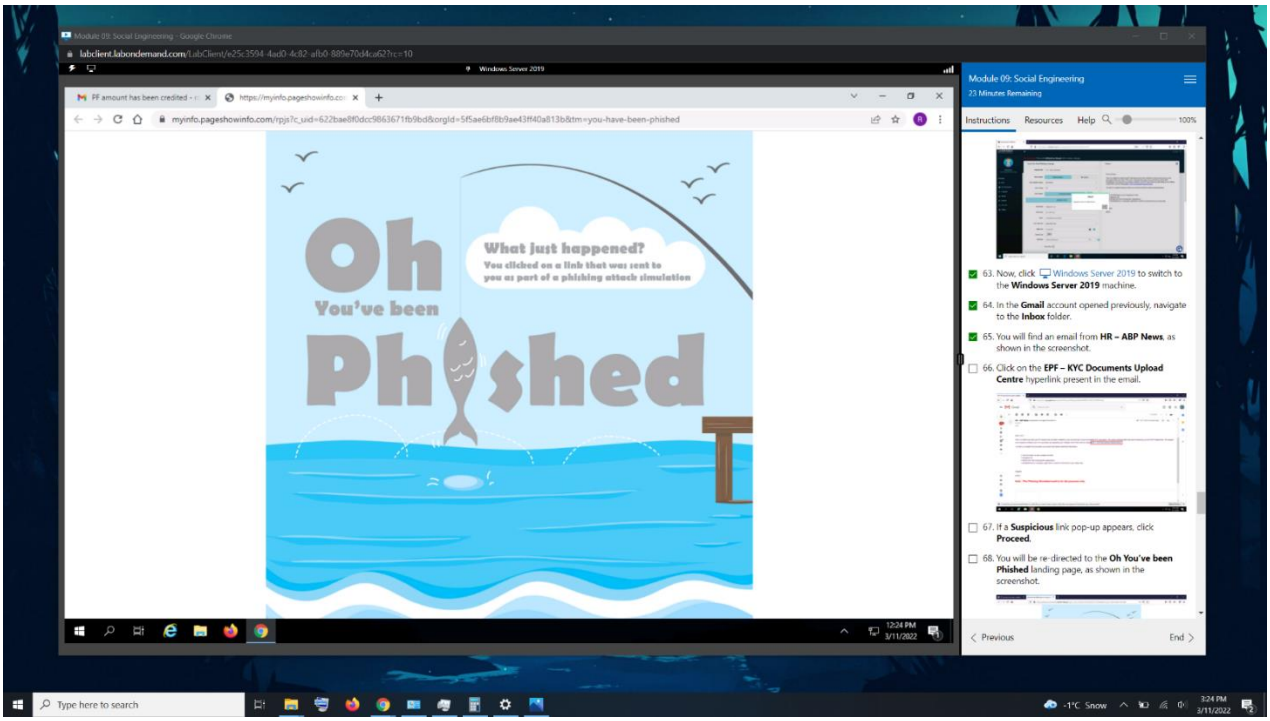

Module 09: Social Engineering - Google Chrome
labclient.labondemand.com/LabClient/e25c3594-4ad0-4c82-afb0-889e70d4ca62?rc=10
Windows 10
Dashboard | OhPhish
portal.ohphish.com/campaigns/actions/send-attachment
aware
When Everyone Protects
Rohan Sharma
Navigation
Home
User Management
Campaigns
Reports
Awareness Program
Templates
Settings
Mask Email address
File Edit Insert View Format Table Tools
Formats
Times New ...
Dear {.Name},
Confirm?
This will trigger 2 emails from hi@yourorgname.com. Are you sure you want to trigger this campaign?
SURE
CANCEL
In order to complete this procedure
Your full name; as per company records
Employee ID
Month and Year of joining the organization;
Establishment or company Legal name; would be mentioned in your salary slip.
Words: 100
Test Email
Create
Module 09: Social Engineering
29 Minutes Remaining
Instructions
Resources
Help
100%
54. Similarly, you can add the details of multiple users. Here, we added two users.
55. After adding the users' details, click Import.
56. In the Batch Count and Batch Interval fields, set the values to 1.
The values of Batch Count and Batch Interval might differ depending on the number of users you are sending phishing emails to.
57. Leave the Landing Page field set to its default value.
58. Scroll down to the end of the page and click Create to create the phishing campaign.
59. Add to your Whitelist pop-up appears, click Done.
You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.
Previous
End
Type here to search
3:18 PM
3/11/2022
-1°C Snow


Module 09: Social Engineering - Google Chrome
labclient.labondemand.com/LabClient/e25c3594-4ad0-4c82-afb0-889e70d4ca62?rc=10
Windows 10
Dashboard | OhPhish
portal.ohphish.com/campaigns/actions/send-attachment
aware
When Everyone Protects
Rohan Sharma
Navigation
Home
User Management
Campaigns
Reports
Awareness Program
Templates
Settings
Please refer Aware User Manual before starting a campaign
Create New Email Phishing Campaign
Preview
0:05
Module 09: Social Engineering
29 Minutes Remaining
Instructions
Resources
Help
100%
59. Add to your Whitelist pop-up appears, click Done.
You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.
60. The Confirm? pop-up appears; click SURE.
61. A count down timer appears and phishing campaign initiates in ten seconds.
62. The Alert! pop-up appears, indicating successful initiation of a phishing campaign; click OK.
63. Now, click Windows Server 2019 to switch to the Windows Server 2019 machine.
Previous
End
Type here to search
3:18 PM
3/11/2022
-1°C Snow

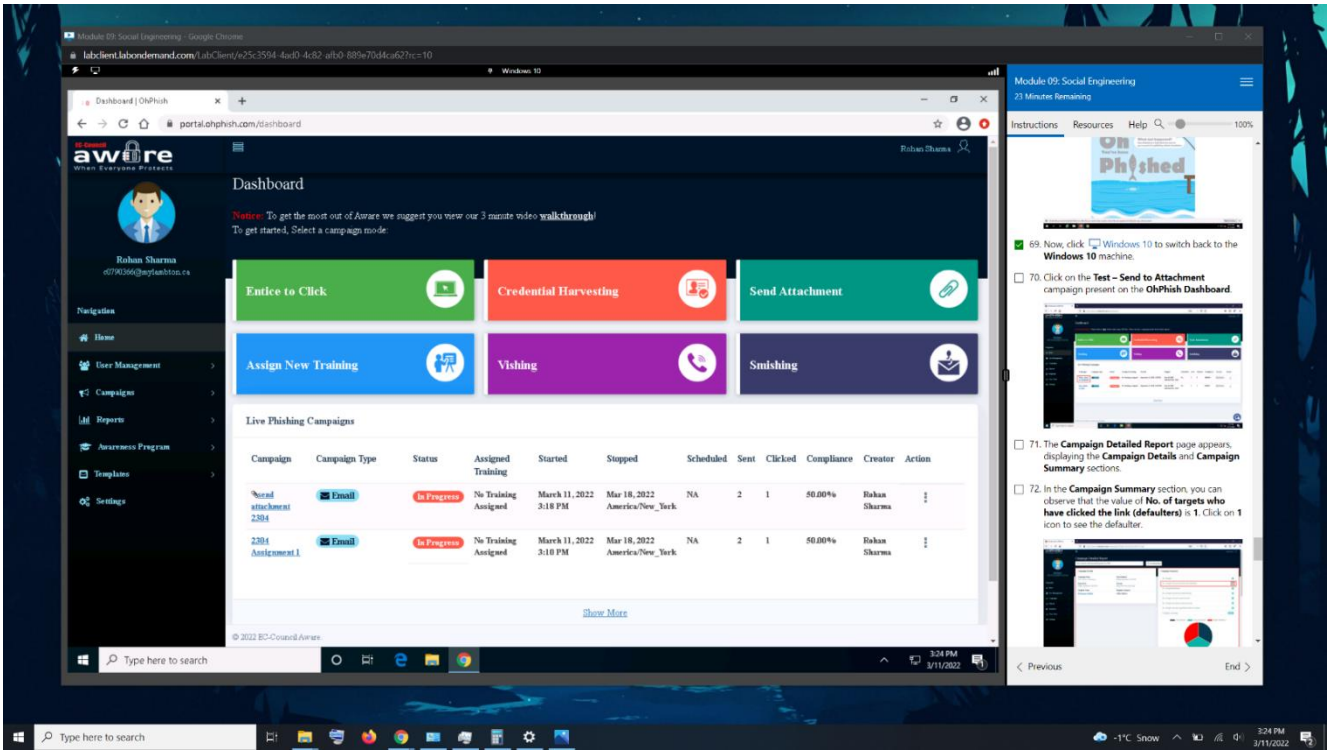


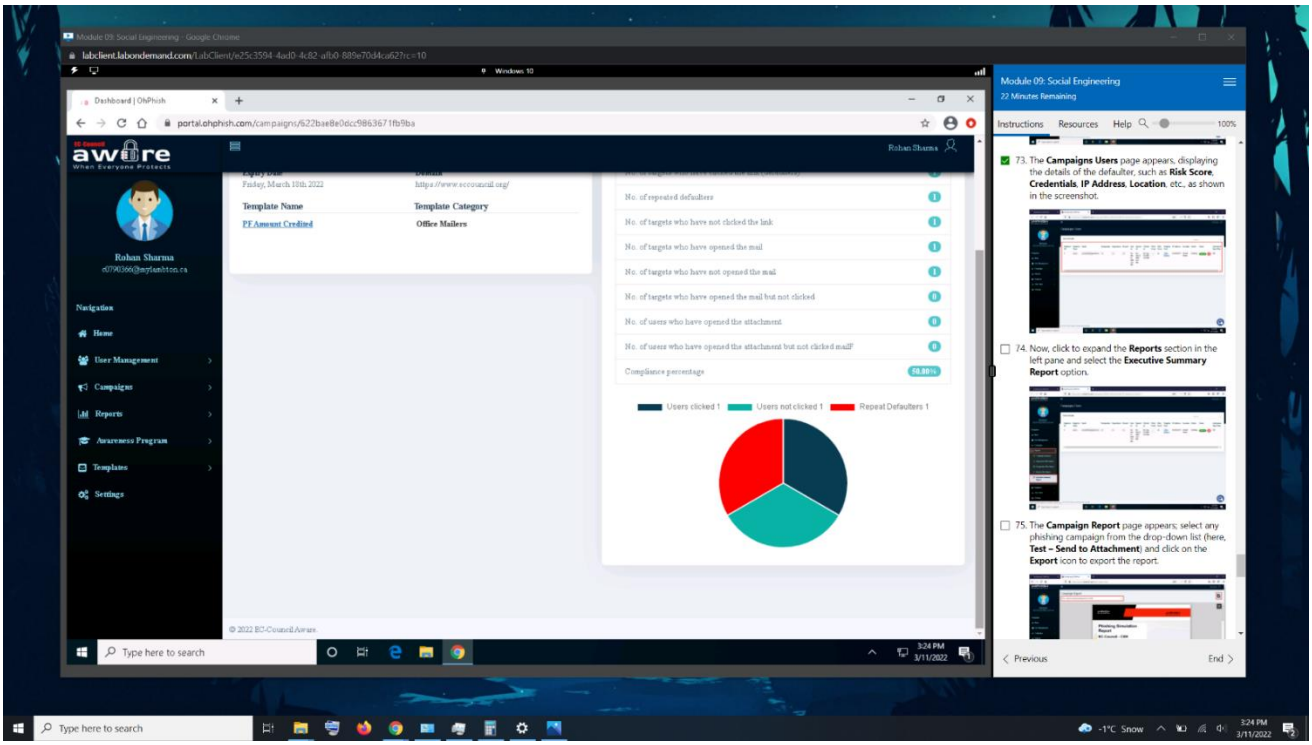
- The victim opens the phishing email and a link for uploading KYC documents appears, upon clicking the link they are redirected to a webpage stating they have been phished


Module 09: Social Engineering
23 Minutes Remaining
Instructions
Resources
Help
100%
63. Now, click Windows Server 2019 to switch to the Windows Server 2019 machine.
64. In the Gmail account opened previously, navigate to the Inbox folder.
65. You will find an email from HR – ABP News, as shown in the screenshot.
66. Click on the EPF – KYC Documents Upload Centre hyperlink present in the email.
67. If a Suspicious link pop-up appears, click Proceed.
68. You will be re-directed to the Oh You've been Phished landing page, as shown in the screenshot.
Previous
End
Gmail
Search mail
Compose
Inbox 10
Starred
Snoozed
Sent
Drafts
More
Meet
New meeting
Join a meeting
Hangouts
Rohan
PF amount has been credited
HR - ABP News
to me
Dear Rohan,
This is to inform you that your PF amount has not been credited to your account due to your incomplete KYC procedure. The same communication has been received by us from EPF Department. We request you to please complete your KYC procedure by uploading your Aadhaar Card/ PAN Card by visiting EPF – KYC Documents Upload Centre
In order to complete this procedure you would need below mentioned information.
Your full name; as per company records
Employee ID
Month and Year of joining the organization;
Establishment or company Legal name; would be mentioned in your salary slip.
Regards
EPFO
Note : This Phishing Simulated email is for lab purposes only.
Enable desktop notifications for Gmail.
OK
No, thanks
Type here to search
-1°C Snow
3:23 PM
3/11/2022

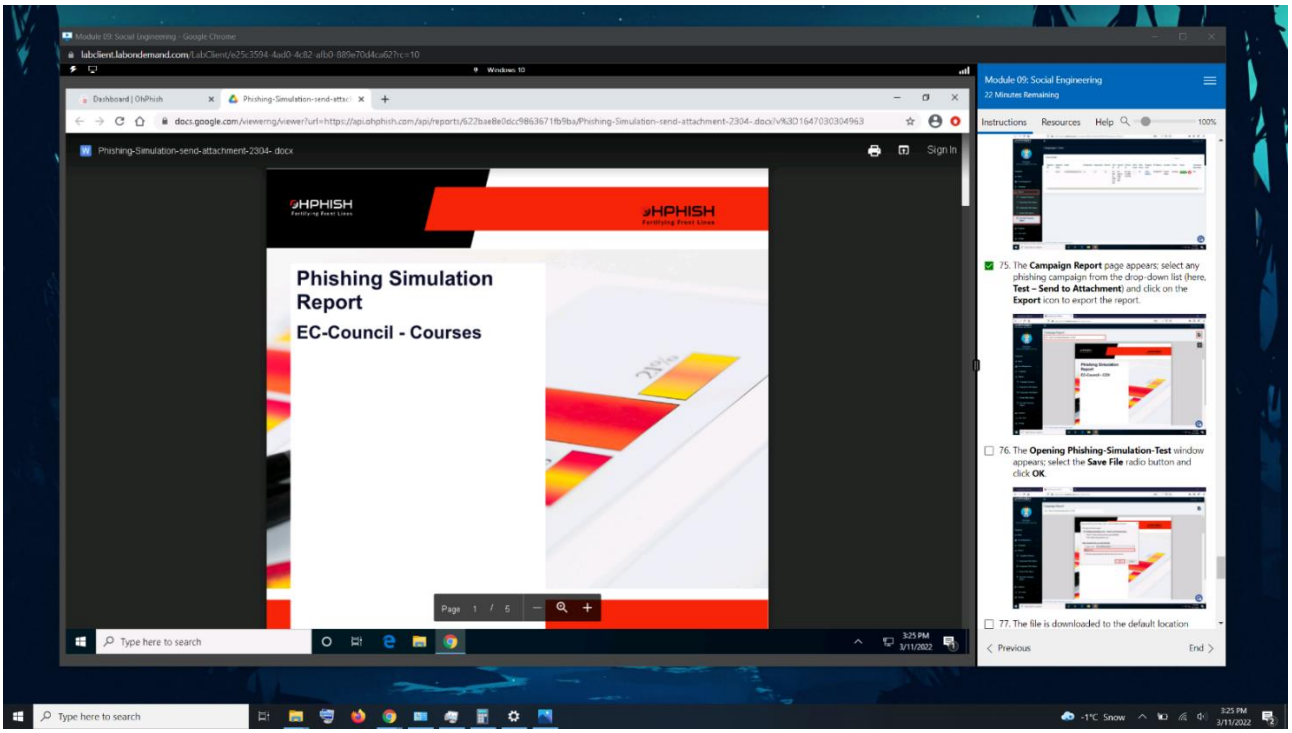

Module 09: Social Engineering
23 Minutes Remaining
Instructions
Resources
Help
100%
63. Now, click Windows Server 2019 to switch to the Windows Server 2019 machine.
64. In the Gmail account opened previously, navigate to the Inbox folder.
65. You will find an email from HR – ABP News, as shown in the screenshot.
66. Click on the EPF – KYC Documents Upload Centre hyperlink present in the email.
67. If a Suspicious link pop-up appears, click Proceed.
68. You will be re-directed to the Oh You've been Phished landing page, as shown in the screenshot.
Previous
End
Oh
You've been
Phished
What just happened?
You clicked on a link that was sent to you as part of a phishing attack simulation
Type here to search
-1°C Snow
3:24 PM
3/11/2022

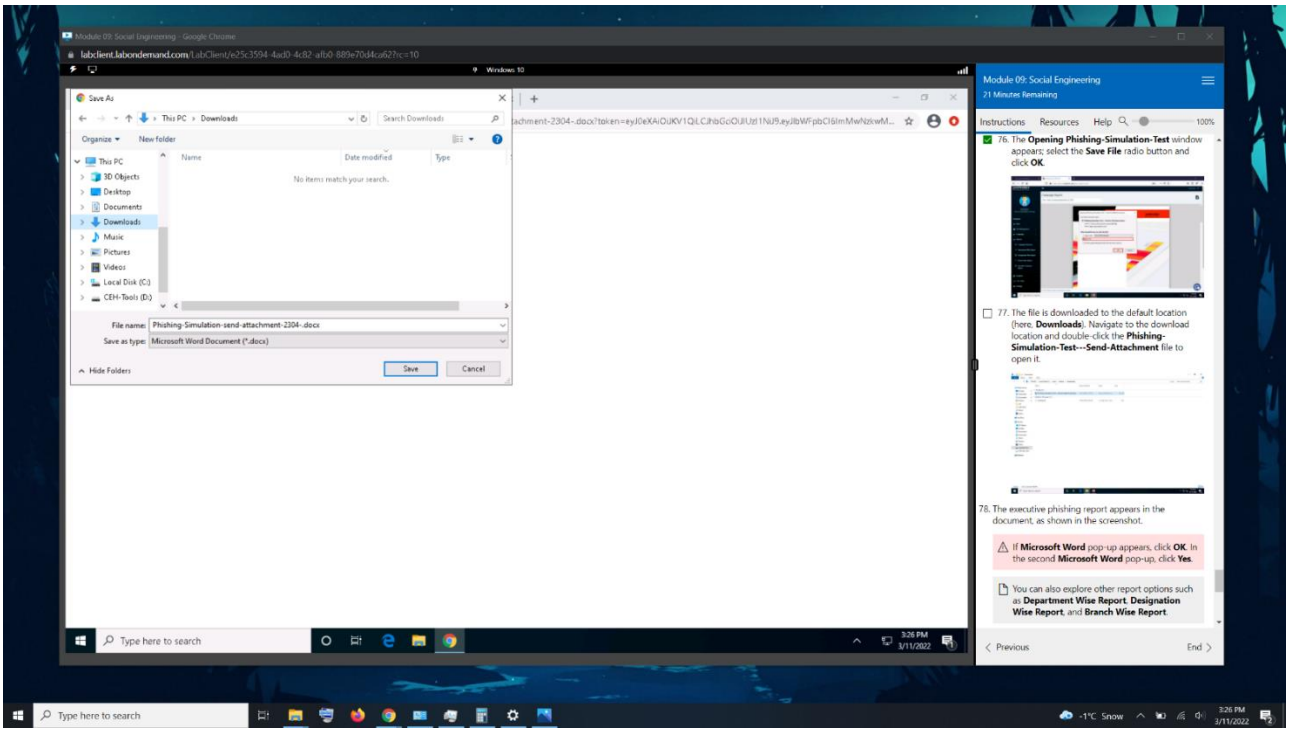
- Back at the dashboard we can click on the campaign name to access its summary, including successfully attacked targets.

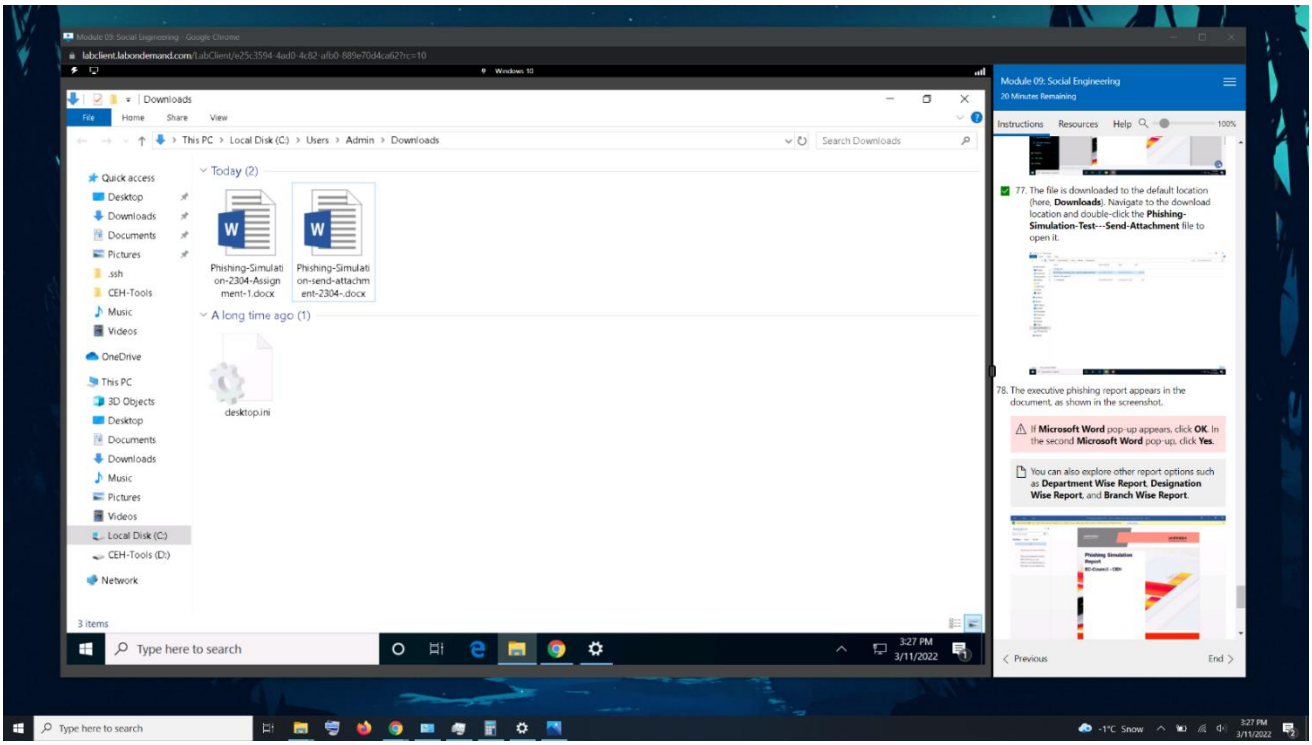


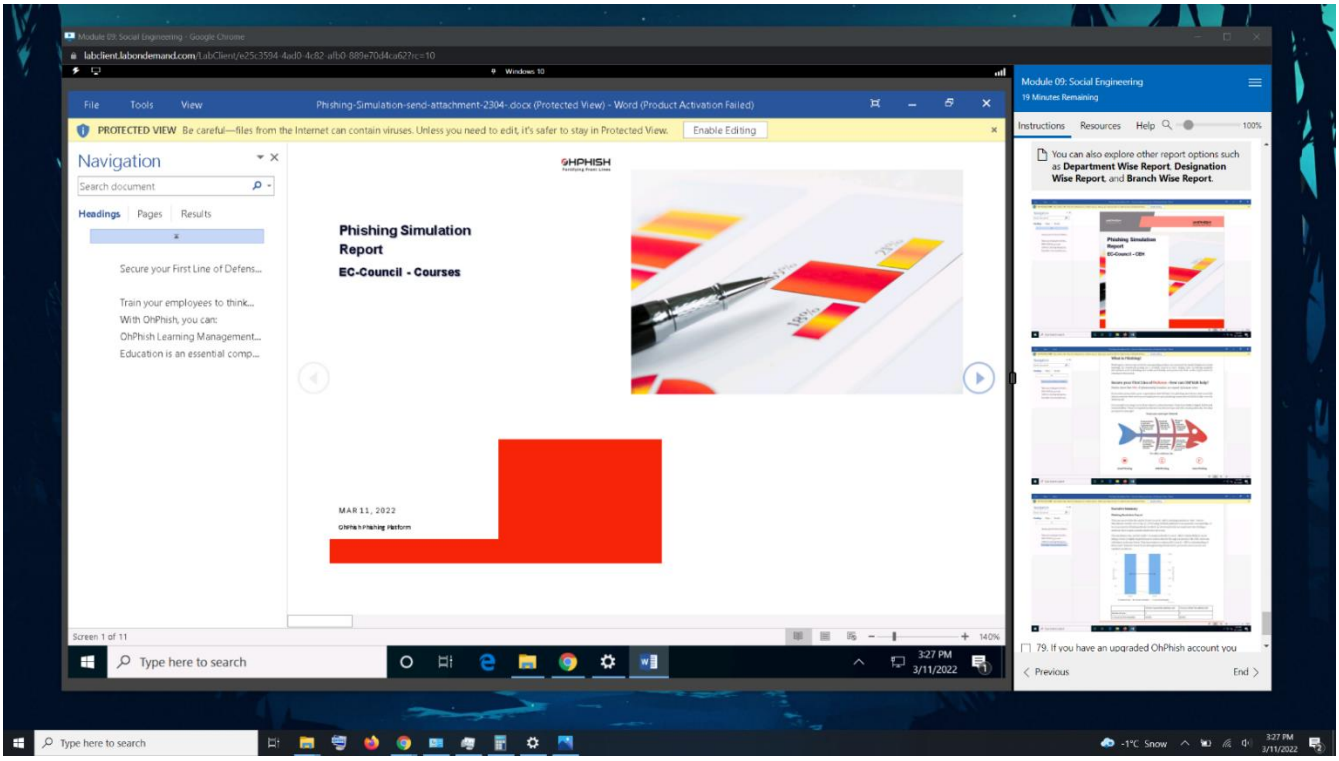


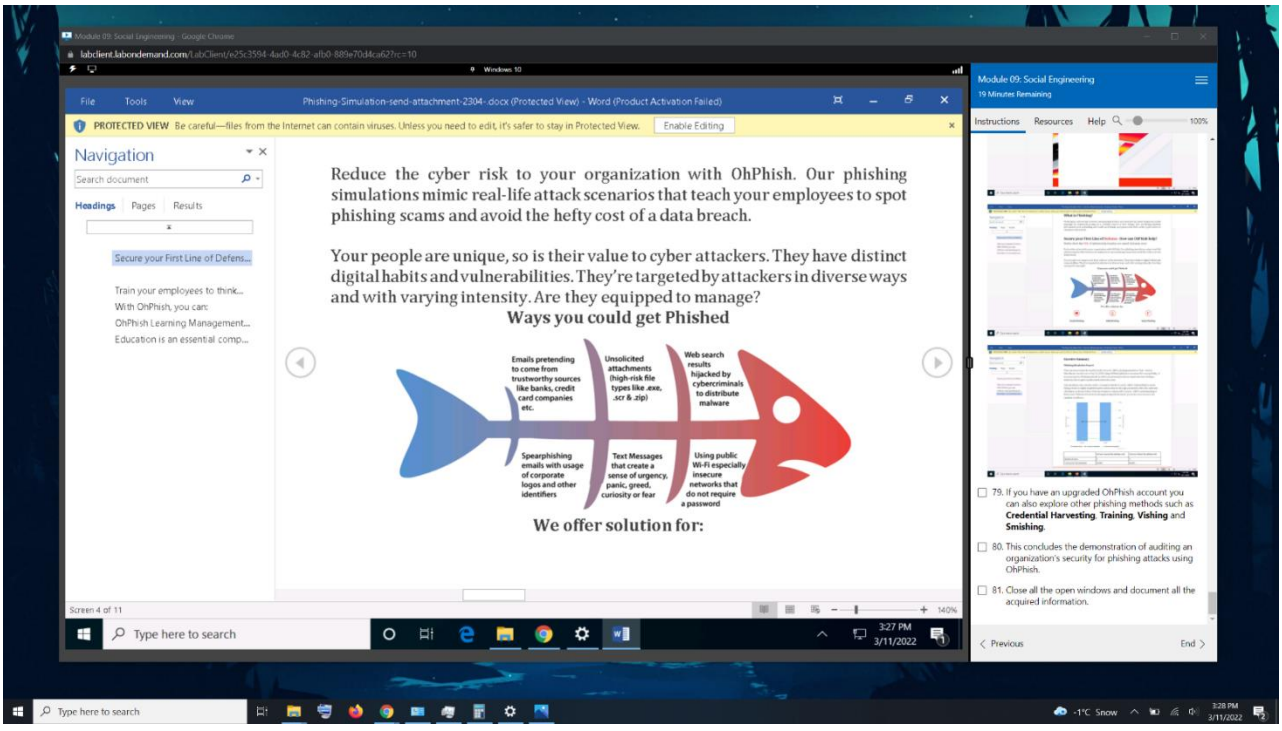
- We can also view/download detailed reports on both the campaigns signifying importance of protection against social engineering attacks.

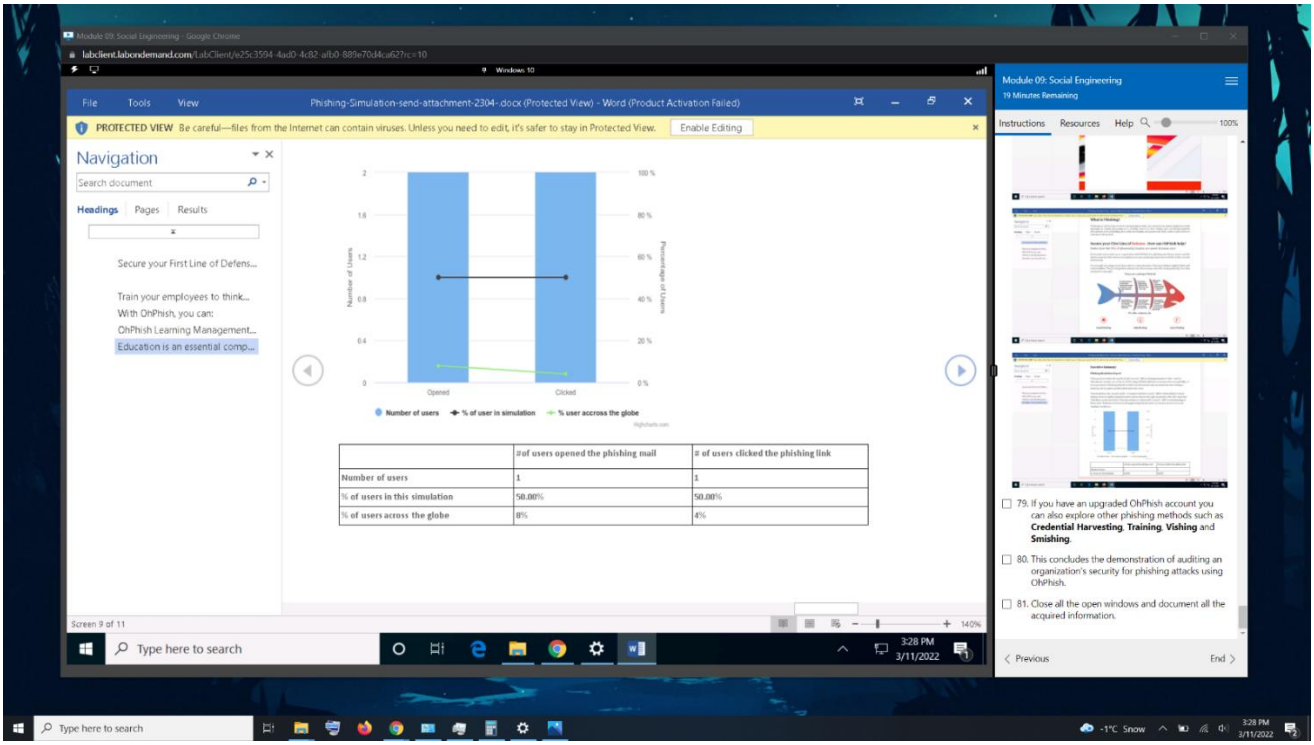


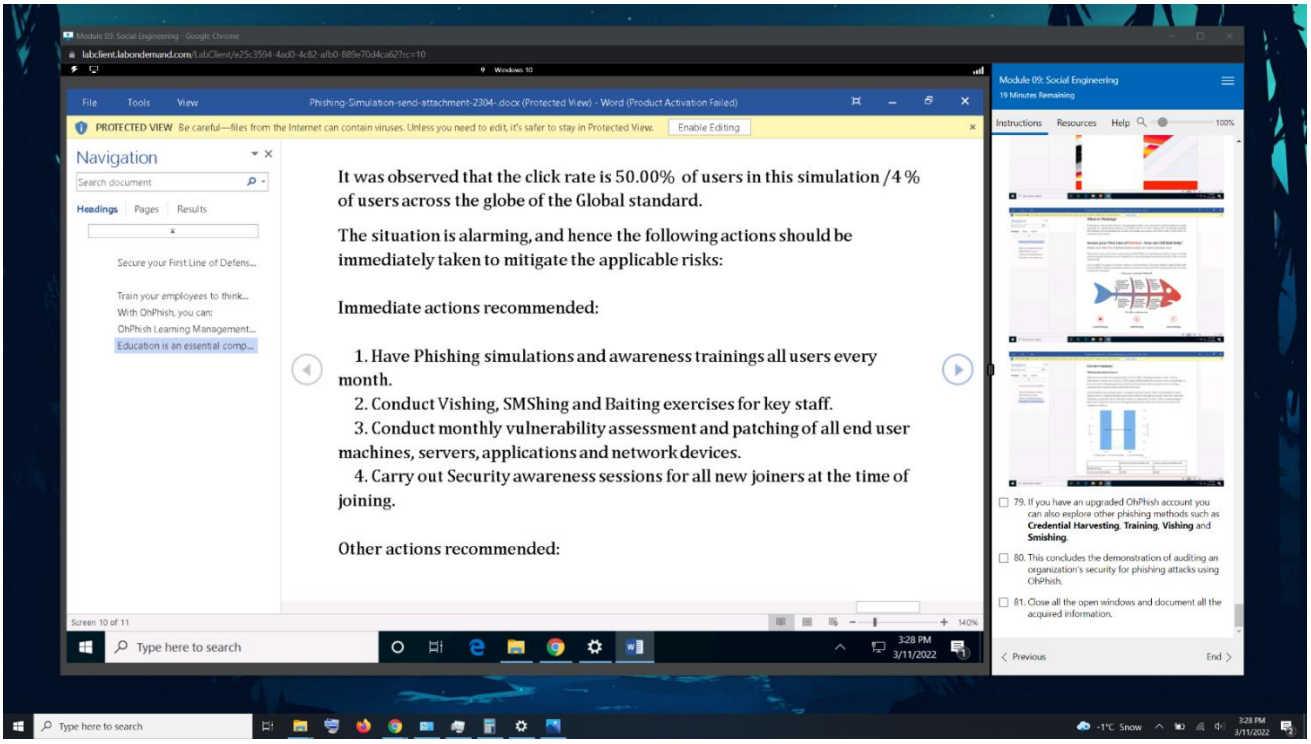

Module 09: Social Engineering
21 Minutes Remaining
Instructions
Resources
Help
100%
76. The Opening Phishing-Simulation-Test window appears; select the Save File radio button and click OK.
77. The file is downloaded to the default location (here, Downloads). Navigate to the download location and double-click the Phishing-Simulation-Test---Send-Attachment file to open it.
78. The executive phishing report appears in the document, as shown in the screenshot.
If Microsoft Word pop-up appears, click OK. In the second Microsoft Word pop-up, click Yes.
You can also explore other report options such as Department Wise Report, Designation Wise Report, and Branch Wise Report.
Previous
End
Save As
Phishing-Simulation-send-attachment-2304-.docx
Save
Cancel
Type here to search
3:26 PM
3/11/2022
-1°C Snow


Module 09: Social Engineering
20 Minutes Remaining
Instructions
Resources
Help
100%
77. The file is downloaded to the default location (here, Downloads). Navigate to the download location and double-click the Phishing-Simulation-Test---Send-Attachment file to open it.
78. The executive phishing report appears in the document, as shown in the screenshot.
If Microsoft Word pop-up appears, click OK. In the second Microsoft Word pop-up, click Yes.
You can also explore other report options such as Department Wise Report, Designation Wise Report, and Branch Wise Report.
Previous
End
Downloads
This PC > Local Disk (C:) > Users > Admin > Downloads
Search Downloads
Today (2)
Phishing-Simulation-2304-Assignment-1.docx
Phishing-Simulation-send-attachment-2304-.docx
A long time ago (1)
desktop.ini
3 items
Type here to search
3:27 PM
3/11/2022
-1°C Snow


Module 09: Social Engineering - Google Chrome
labclient.labondemand.com/LabClient/e25c3594-4ad0-4c82-afb0-889e70d4ca62?rc=10
Windows 10
File Tools View
Phishing-Simulation-send-attachment-2304-.docx (Protected View) - Word (Product Activation Failed)
PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.
Enable Editing
Navigation
Search document
Headings Pages Results
Secure your First Line of Defens...
Train your employees to think...
With OhPhish, you can:
OhPhish Learning Management...
Education is an essential comp...
OHPHISH
Phishing Simulation Report
EC-Council - Courses
MAR 11, 2022
OhPhish Phishing Platform
Screen 1 of 11
140%
Type here to search
3:27 PM
3/11/2022
Module 09: Social Engineering
19 Minutes Remaining
Instructions Resources Help
100%
You can also explore other report options such as Department Wise Report, Designation Wise Report, and Branch Wise Report.
79. If you have an upgraded OhPhish account you
Previous
End
-1°C Snow
3:27 PM
3/11/2022


Module 09: Social Engineering - Google Chrome
labclient.labondemand.com/LabClient/e25c3594-4ad0-4c82-afb0-889e70d4ca62?rc=10
Windows 10
File Tools View
Phishing-Simulation-send-attachment-2304-.docx (Protected View) - Word (Product Activation Failed)
PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.
Enable Editing
Navigation
Search document
Headings Pages Results
Secure your First Line of Defens...
Train your employees to think...
With OhPhish, you can:
OhPhish Learning Management...
Education is an essential comp...
Reduce the cyber risk to your organization with OhPhish. Our phishing simulations mimic real-life attack scenarios that teach your employees to spot phishing scams and avoid the hefty cost of a data breach.
Your people are unique, so is their value to cyber attackers. They have distinct digital habits and vulnerabilities. They're targeted by attackers in diverse ways and with varying intensity. Are they equipped to manage?
Ways you could get Phished
Emails pretending to come from trustworthy sources like banks, credit card companies etc.
Unsolicited attachments (high-risk file types like .exe, .scr & .zip)
Web search results hijacked by cybercriminals to distribute malware
Spearphishing emails with usage of corporate logos and other identifiers
Text Messages that create a sense of urgency, panic, greed, curiosity or fear
Using public Wi-Fi especially insecure networks that do not require a password
We offer solution for:
Screen 4 of 11
140%
Type here to search
3:27 PM
3/11/2022
Module 09: Social Engineering
19 Minutes Remaining
Instructions Resources Help
100%
79. If you have an upgraded OhPhish account you can also explore other phishing methods such as Credential Harvesting, Training, Vishing and Smishing.
80. This concludes the demonstration of auditing an organization's security for phishing attacks using OhPhish.
81. Close all the open windows and document all the acquired information.
Previous
End
-1°C Snow
3:28 PM
3/11/2022


Phishing-Simulation-send-attachment-2304-.docx (Protected View) - Word (Product Activation Failed)
PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.
Enable Editing
Navigation
Search document
Headings
Pages
Results
Secure your First Line of Defens...
Train your employees to think...
With OhPhish, you can:
OhPhish Learning Management...
Education is an essential comp...
Opened
Clicked
Number of users
% of user is simulation
% user accross the globe
#of users opened the phishing mail
# of users clicked the phishing link
Number of users
1
1
% of users in this simulation
50.00%
50.00%
% of users across the globe
0%
4%
Screen 9 of 11
Module 09: Social Engineering
19 Minutes Remaining
Instructions
Resources
Help
79. If you have an upgraded OhPhish account you can also explore other phishing methods such as Credential Harvesting, Training, Vishing and Smishing.
80. This concludes the demonstration of auditing an organization's security for phishing attacks using OhPhish.
81. Close all the open windows and document all the acquired information.
Previous
End
Type here to search
3:28 PM
3/11/2022


Phishing-Simulation-send-attachment-2304-.docx (Protected View) - Word (Product Activation Failed)
PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.
Enable Editing
Navigation
It was observed that the click rate is 50.00% of users in this simulation /4 % of users across the globe of the Global standard.
The situation is alarming, and hence the following actions should be immediately taken to mitigate the applicable risks:
Immediate actions recommended:
1. Have Phishing simulations and awareness trainings all users every month.
2. Conduct Vishing, SMShing and Baiting exercises for key staff.
3. Conduct monthly vulnerability assessment and patching of all end user machines, servers, applications and network devices.
4. Carry out Security awareness sessions for all new joiners at the time of joining.
Other actions recommended:
Screen 10 of 11
Module 09: Social Engineering
19 Minutes Remaining
Instructions
Resources
Help
79. If you have an upgraded OhPhish account you can also explore other phishing methods such as Credential Harvesting, Training, Vishing and Smishing.
80. This concludes the demonstration of auditing an organization's security for phishing attacks using OhPhish.
81. Close all the open windows and document all the acquired information.
Previous
End
Type here to search
3:28 PM
3/11/2022

Conclusion

To conclude, this lab shows how attackers abuse the target's network using sniffing and social engineering to steal the information of victim by phishing attacks. In this lab we performed and detect some phishing attacks. This lab helps to get real time experience to perform packet sniffing and phishing in social engineering for attacks.