

Lab 3: Audit Organization's Security for Phishing Attacks

Lab Scenario

Social engineers exploit human behavior (manners, enthusiasm toward work, laziness, innocence, etc.) to gain access to the information resources of the target company. This information is difficult to be guarded against social engineering attacks, as the victim may not be aware that he or she has been deceived. The attacks performed are similar to those used to extract a company's valuable data. To guard against social engineering attacks, a company must evaluate the risk of different types of attacks, estimate the possible losses, and spread awareness among its employees.

As a professional ethical hacker or pen tester, you must perform phishing attacks in the organization to assess the awareness of its employees.

As an administrator or penetration tester, you may have implemented highly sophisticated and expensive technology solutions; however, all these techniques can be bypassed if the employees fall prey to simple social engineering scams. Thus, employees must be educated about the best practices for protecting the organization's systems and information.

In this lab, you will learn how to audit an organization's security for phishing attacks within the organization.

Lab Objectives

- Audit organization's security for phishing attacks using OhPhish

Overview

In phishing attacks, attackers implement social engineering techniques to trick employees into revealing confidential information of their organization. They use social engineering to commit fraud, identity theft, industrial espionage, and so on. To guard against social engineering attacks, organizations must develop effective policies and procedures; however, merely developing them is not enough.

To be truly effective in combating social engineering attacks, an organization should do the following:

- Disseminate policies among its employees and provide proper education and training.
- Provide specialized training benefits to employees who are at a high risk of social engineering attacks.
- Obtain signatures of employees on a statement acknowledging that they understand the policies.
- Define the consequences of policy violations.

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

OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides an organization with a platform to launch phishing simulation campaigns on its employees. The platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.

Here, we will audit the organization's security infrastructure for phishing attacks using OhPhish.

1. ☐ Before starting this task, you must activate your **OhPhish** account.
2. ☐ Open any web browser (here, **Mozilla Firefox**). Log in to your **ASPEN** account and navigate to **Certified Ethical Hacker v11** in the **My Courses** section.

If you do not have an ASPEN account or access to CEHv12 program on ASPEN, please write to **support@eccouncil.org** for an OhPhish account. Once your account is setup, you will receive an email from **aware@eccouncil.org** with an account activation link. Upon activation, continue from **STEP 12**.

3. ☐ Click on **Click here** hyperlink in the **OhPhish** notification above **My Courses** section.

The screenshot shows the ASPEN website's 'My Courses' section. At the top, there's a navigation bar with the ASPEN logo and links for Home, My Courses (highlighted), Training, Training Partner, Instructor, CISOMAG, CodeRed, and About. Below the navigation bar, a yellow notification banner with a red border contains a warning icon and the text: 'You have access to OhPhish Freemium Account(EC-Council's phishing simulation service worth \$2500) for FREE [Click here](#) to activate your subscription.' Below the banner, the 'My Courses' title is on the left, and a blue button labeled 'SUBMIT SUBSCRIPTION/DASHBOARD CODE' is on the right. Underneath, the course 'Certified Ethical Hacker v12' is listed with a green progress bar. Below the course title, there are five cards representing different stages of the course: 'In Process' (Training), 'Pending' (Evaluation), 'Pending' (Exam), 'Pending' (Certificate), and 'N/A' (ECE Status). Each card has a corresponding icon and a blue button with the stage name.


Stage	Status	Action
Training	In Process	TRAINING
Evaluation	Pending	EVALUATION
Exam	Pending	EXAM
Certificate	Pending	CERTIFICATE
ECE STATUS	N/A	ECE STATUS

4. ☐ You will be redirected to the OhPhish **Sign Up** page. Enter the remaining personal details, check **I'm not a robot** checkbox and click **Complete Signup** button.

Dashboard | OhPhish

https://portal.ohphish.com/ceh-register

SHIELD ALLIANCE
An EC-Council Company
OhPhish - Complete Cyber Security Awareness Training Solutions



Sign Up

Hi, [redacted] we need some more information before you start using OhPhish.

[redacted]

[redacted]


[redacted]@gmail.com

[redacted]

[redacted].org

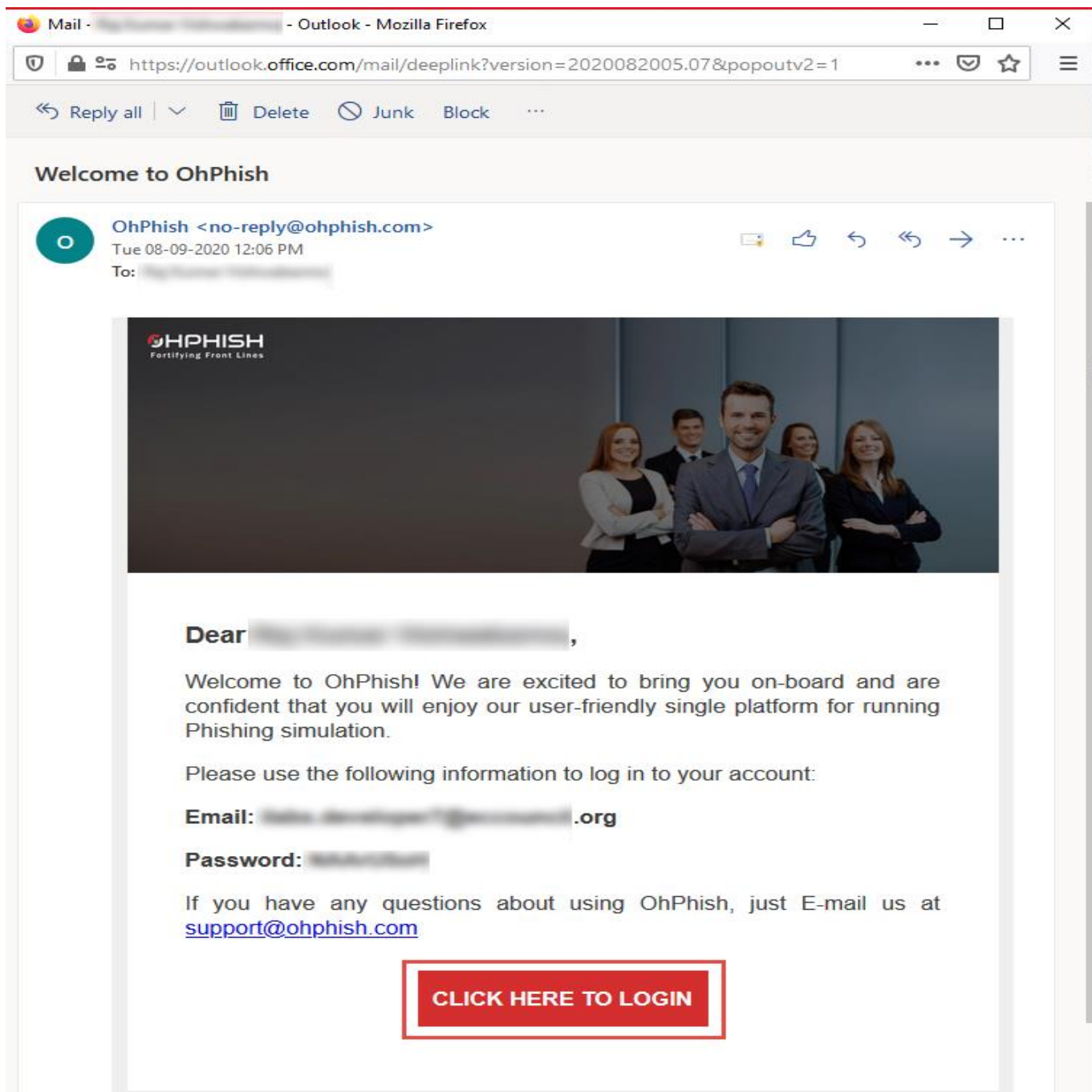
[redacted]

500 - 1000

☒ I'm not a robot 
reCAPTCHA
Privacy - Terms

Complete Signup

5. ☐ Account creation **Alert!** appears, click **OK**.
6. ☐ Now, open your email account given during registration process. Open an email from **OhPhish** and in the email, click **CLICK HERE TO LOGIN** button.



7. ☐ **EC-Council Aware** page appears, in the **Username** field enter your email address and click **Next**. In the next page, enter your password in the **Password** field and click **Sign In**.

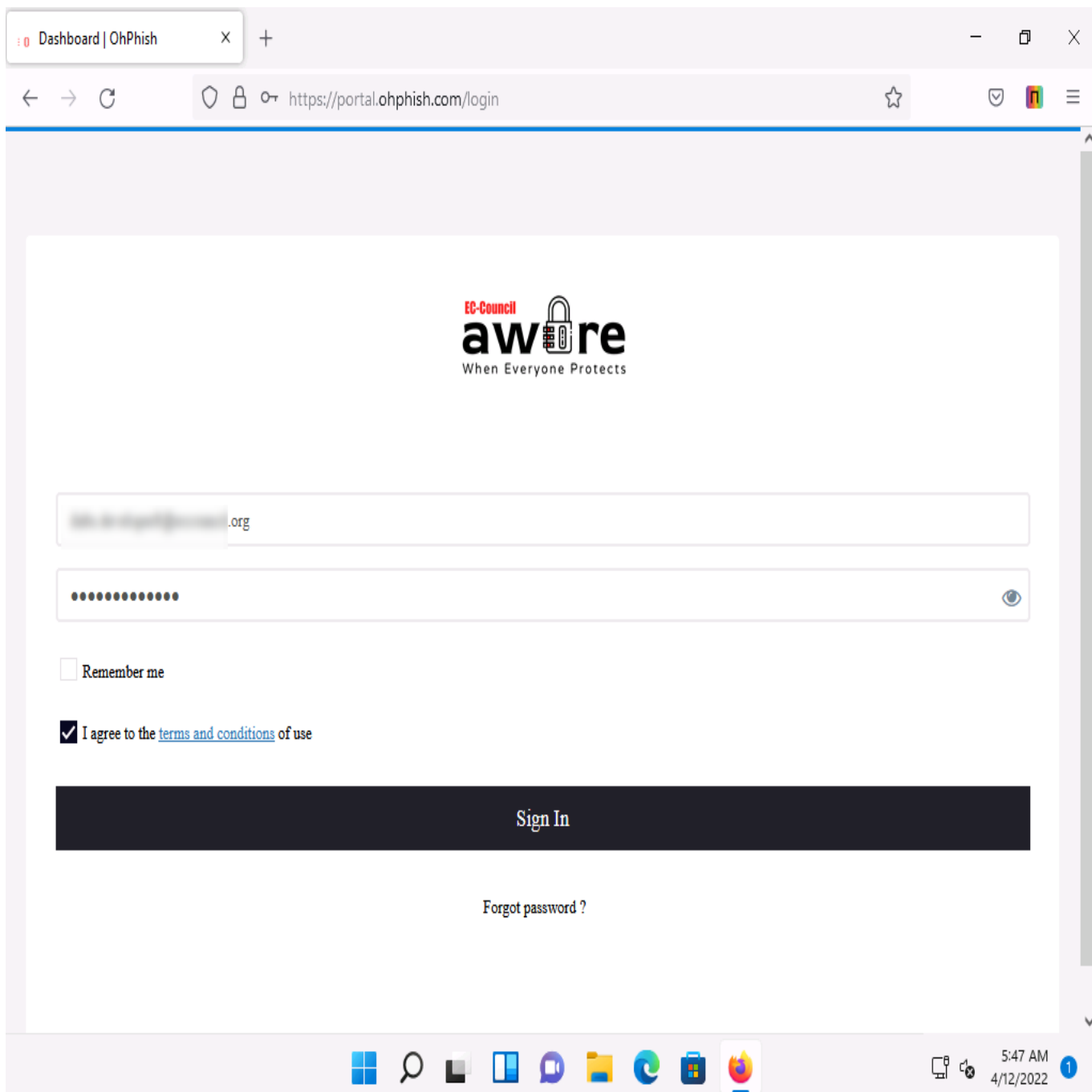
If **Save login for ohphish.com?** notification appears, click **Don't Save**.

☐ Remember me☒ I agree to the [terms and conditions](#) of use

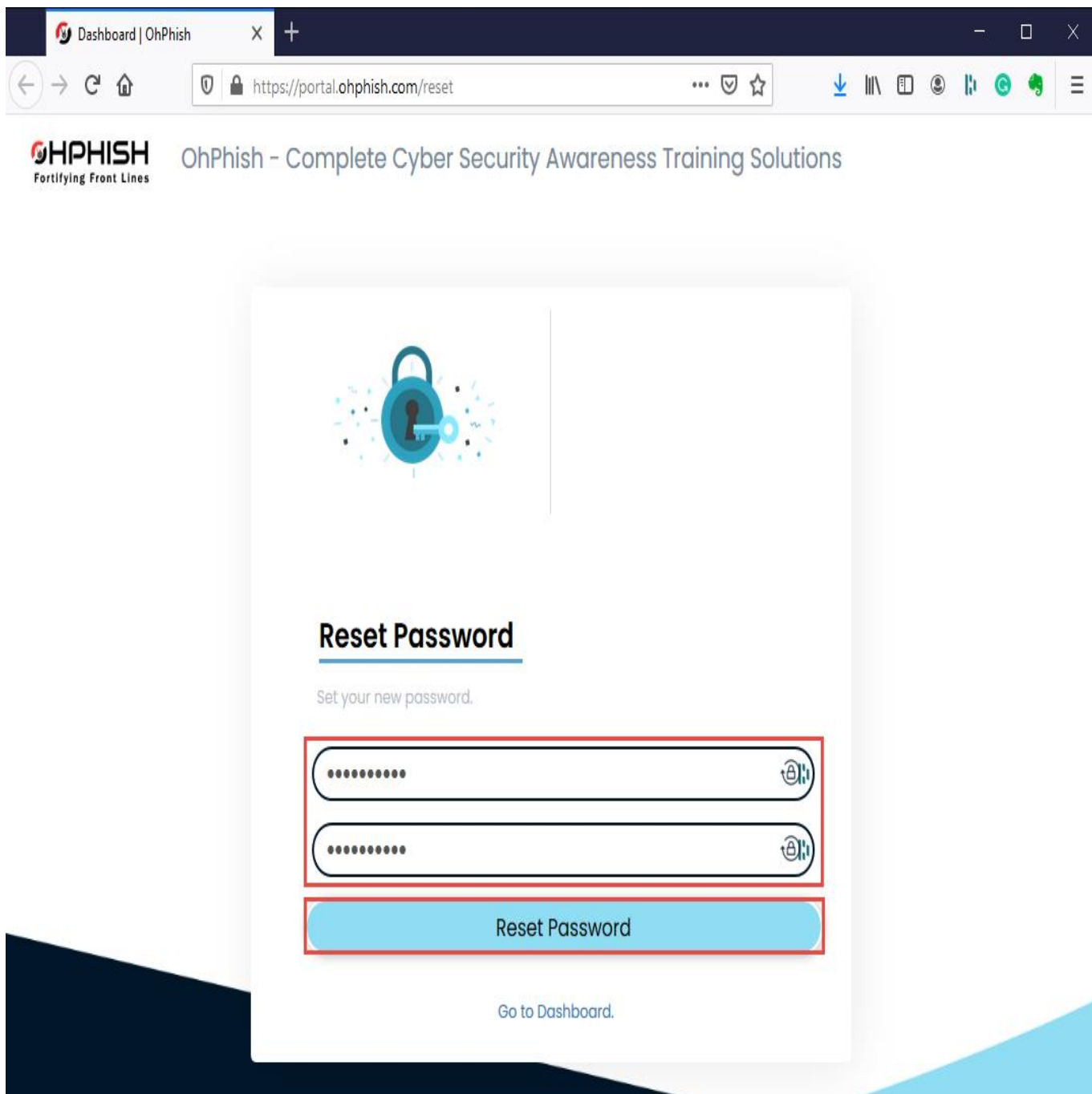
Next

[Forgot password ?](#)

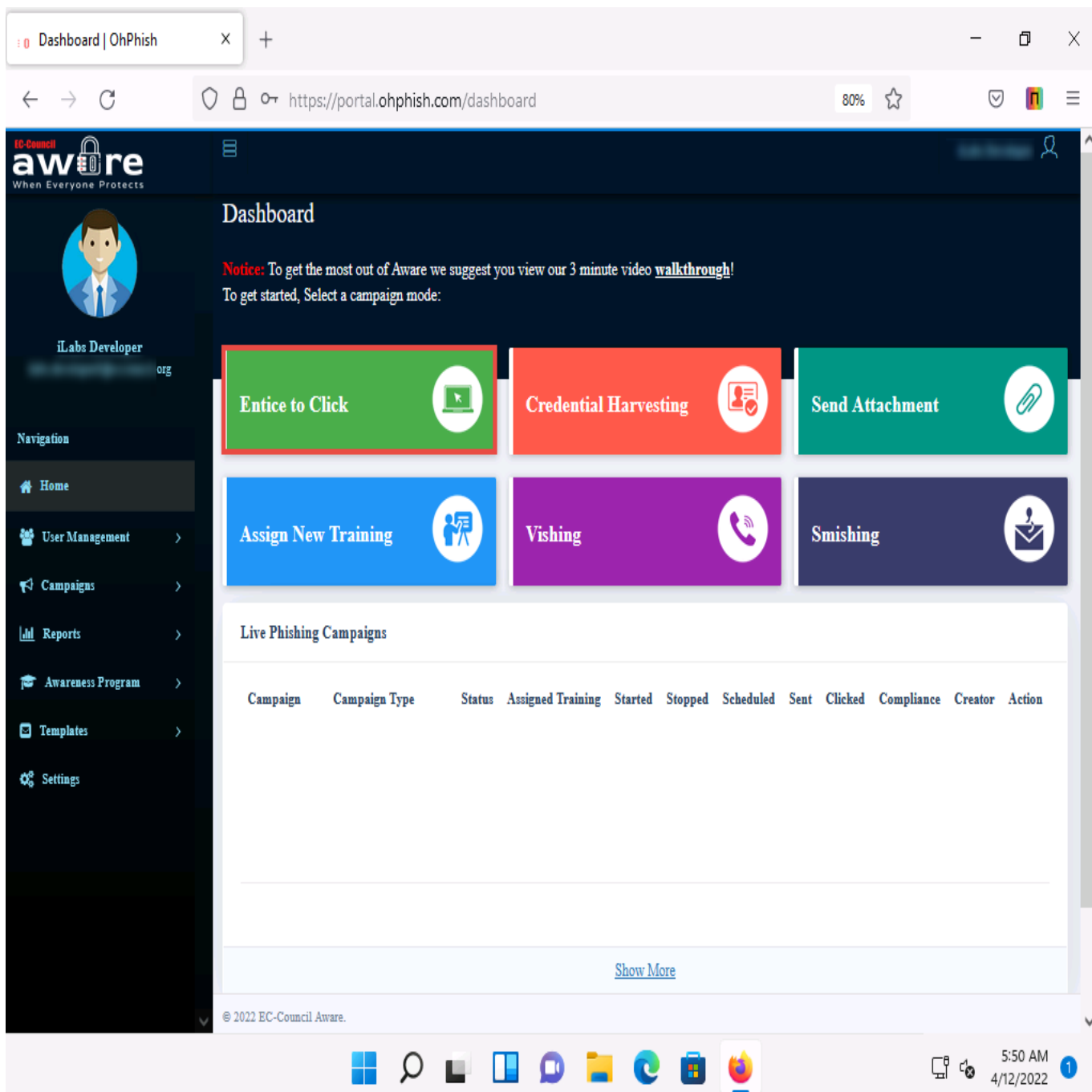




8. ☐ You will be redirected to **Reset Password** page, enter the new password in both the fields and click **Reset Password** button to reset the password.



9. ☐ Your account password is changed successfully.
10. ☐ Now, you can login to your OhPhish account either by clicking on the **LOGIN TO OHPHISH PORTAL** button in your **ASPEN** account under **My Courses** section or you can navigate to the OhPhish website (<https://portal.ohphish.com/login>) and login using your credentials.
11. ☐ Once you login to your OhPhish account you will be redirected to the OhPhish **Dashboard**.
12. ☐ In the OhPhish **Dashboard**, click on the **Entice to Click** option.



13. ☐ The **Create New Email Phishing Campaign** form appears.

If the **OhPhish Helpdesk** notification appears in the right corner of the dashboard, close it.

Almost Done pop-up appears, click **DISCARD CHANGES**.

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 **Work From Home: COVID-19** 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.

Dashboard | OhPhish

https://portal.ohphish.com/campaigns/actions/entice-to-click

80%

EC-Council **aware**
When Everyone Protects

iLabs Developer
[Profile Picture]

Navigation

- Home
- User Management
- Campaigns
- Reports
- Awareness Program
- Templates
- Settings

Create New Email Phishing Campaign

Campaign Name:

Email Template:

Select Template Category:

Select Country:

Select Template:

1 template selected.

Sender Email:

Sender Name:

Subject:

Select Time Zone:

Expiry Date:

Preview

Hi {Name},

This pandemic situation is seeing all the workforce going worse around the world. Taking safety measures and precautions in this situation have become mandatory. The rapid outbreak has led all the organizations to take safety measures under the Communicable Disease Management Policy.

According to the act under this policy is part of the awareness among the organizations and all the employees should adhere to the same and read the policy along with an acknowledgment e-mail by today EOD.

[WFH - Policy.pdf](#)

For any doubts and queries, it is suggested that you contact the Human Resource team for better clarity.

Regards,

Team Human Resource

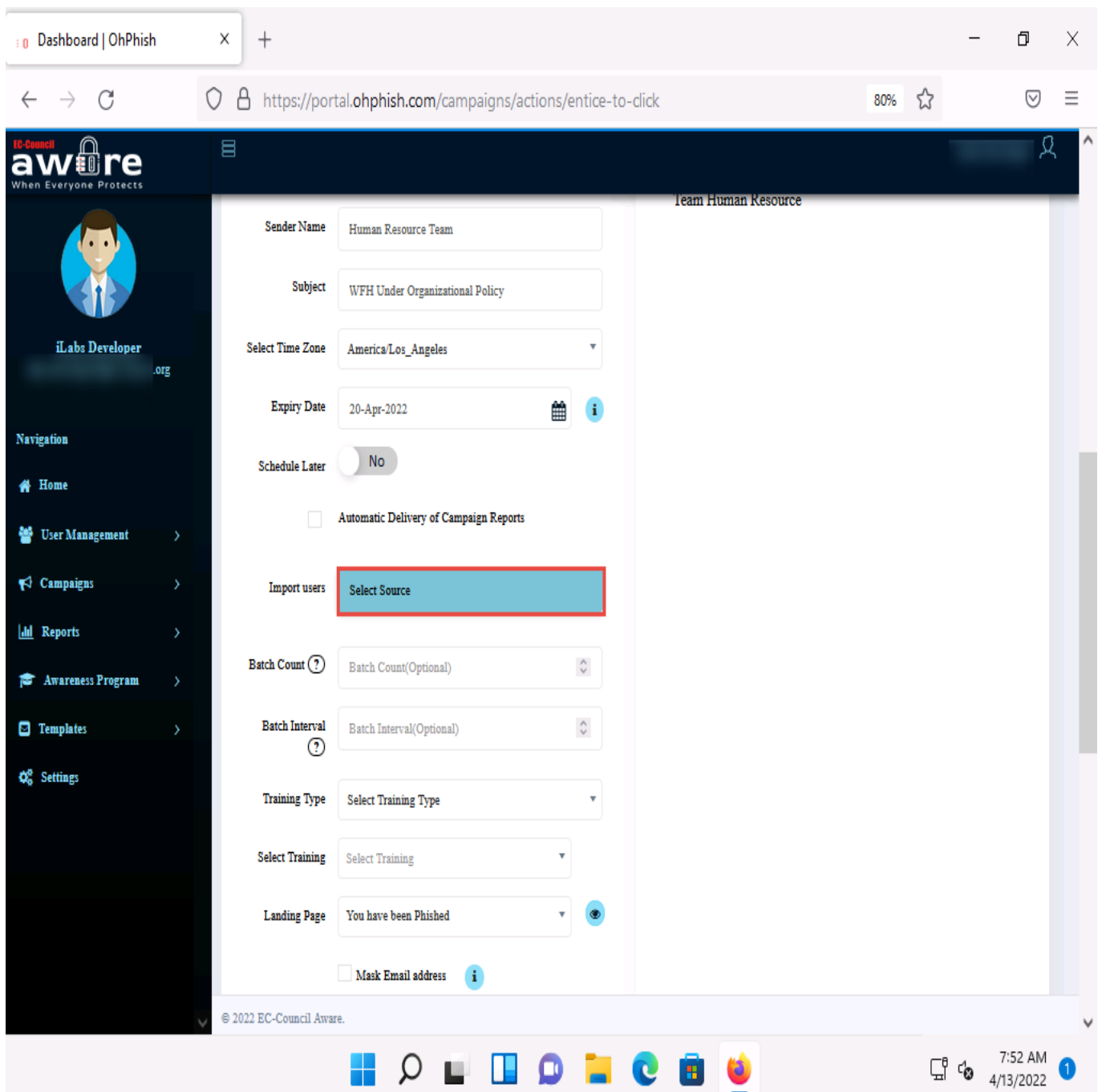
© 2022 EC-Council Aware.

7:50 AM 4/13/2022

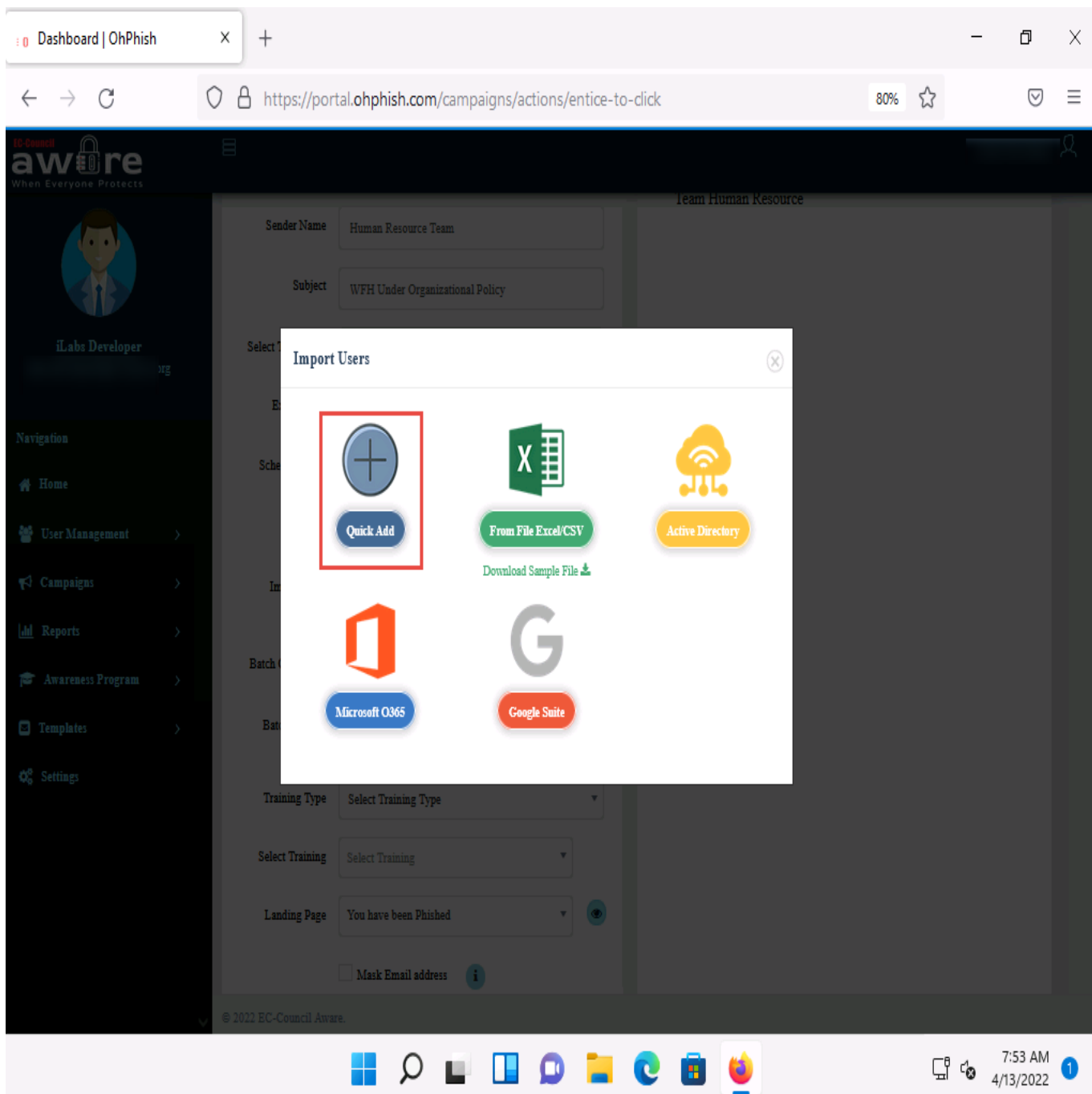
18. ☐ Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.


You can change the above-mentioned options if you want to.

19. ☐ In the **Import users** field, click **Select Source**.



20. ☐ **Import Users** pop-up appears, click to select **Quick Add** option from the list of options.



21.  The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.

Dashboard | OhPhish

https://portal.ohphish.com/campaigns/actions/entice-to-click

80%

Import Users Info

Name

Email

Reporting Manager Email

Designation

Department

Company

Branch

Country

Add

ID	Name	Email	Reporting Manager Email	Designation	Department	Company	Branch	Country	Action
----	------	-------	-------------------------	-------------	------------	---------	--------	---------	--------

Cancel Import

© 2022 EC-Council Aware.

22. ☐ Similarly, you can add the details of multiple users. Here, we added two users.
23. ☐ After adding the users' details, click **Import**.

Dashboard | OhPhish

https://portal.ohphish.com/campaigns/actions/entice-to-click

10-Council aware When Everyone Protects

iLabs Developer

Navigation

- Home
- User Management
- Campaigns
- Reports
- Awareness Program
- Templates
- Settings

Enter Employee Email

This is a required field

Reporting Manager Email

Designation

Department

Company

Branch

Country

Add

ID	Name	Email	Reporting Manager Email	Designation	Department	Company	Branch	Country	Action
1		@gmail.com	h@gmail.com						
2		@gmail.com	h@gmail.com						

Cancel Import

© 2022 EC-Council Aware.

7:57 AM 4/13/2022

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.

Dashboard | OhPhish

https://portal.ohphish.com/campaigns/actions/entice-to-click

80%

IC-Council
aware
When Everyone Protects

iLabs Developer
@ilabsdeveloper.org

Navigation

- Home
- User Management
- Campaigns
- Reports
- Awareness Program
- Templates
- Settings

Schedule Later ☐ No

☐ Automatic Delivery of Campaign Reports

Import users [Quick Add](#)

Batch Count (?) 1

Batch Interval (?) 1

Training Type Select Training Type

Select Training Select Training

Landing Page You have been Phished

☐ Mask Email address

File Edit Insert View Format Table Tools

Formats B I [Text Alignment Icons] [List Icons] [Link Icon] [Image Icon]

A A serif

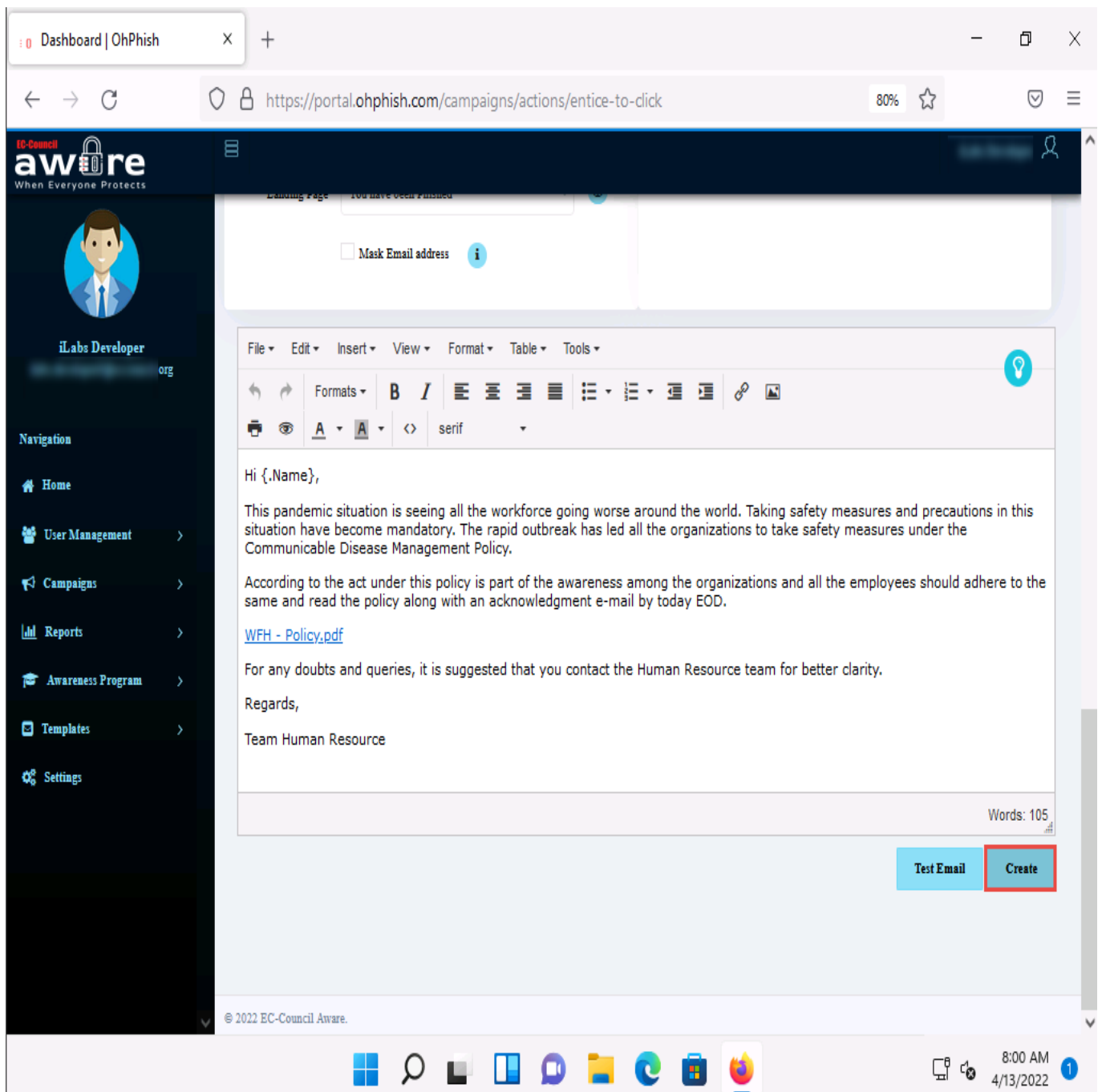
Hi {Name},

This pandemic situation is seeing all the workforce going worse around the world. Taking safety measures and precautions in this

© 2022 EC-Council Aware.

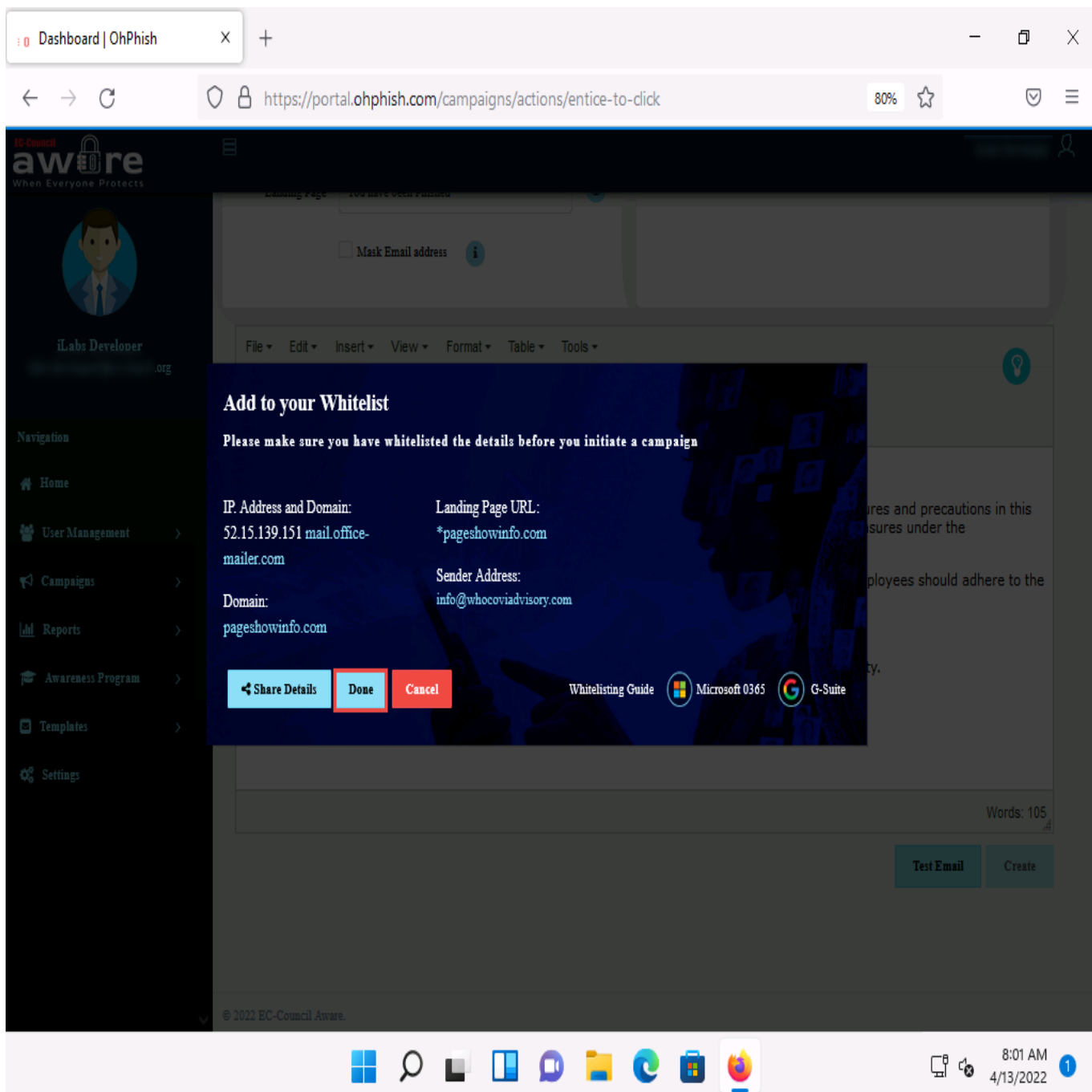
7:59 AM
4/13/2022

26. ☐ Now, scroll down to the end of the page and click **Create** to create the phishing campaign.

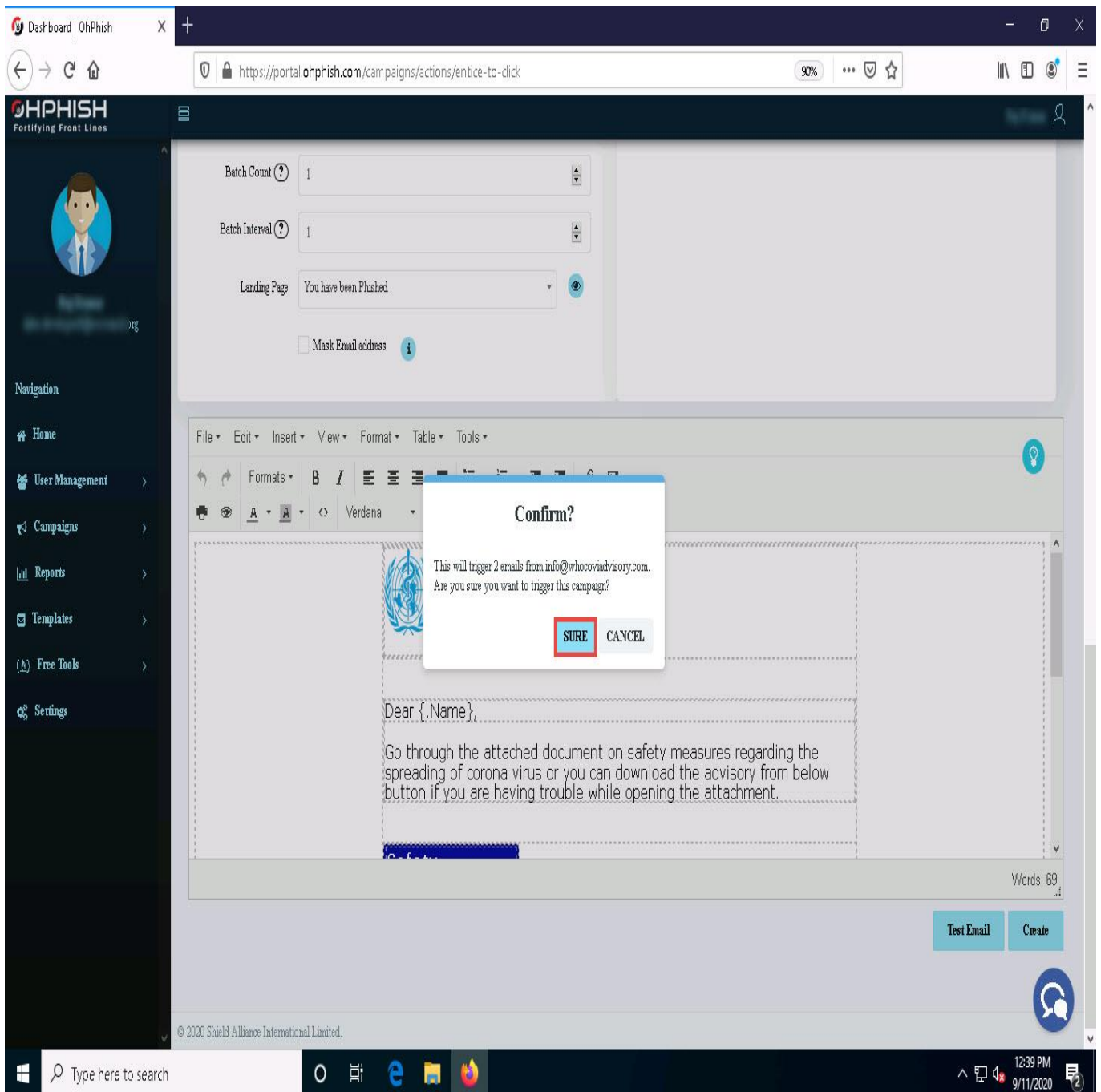


27. ☐ **Add to your Whitelist** pop-up appears, click **Done**.

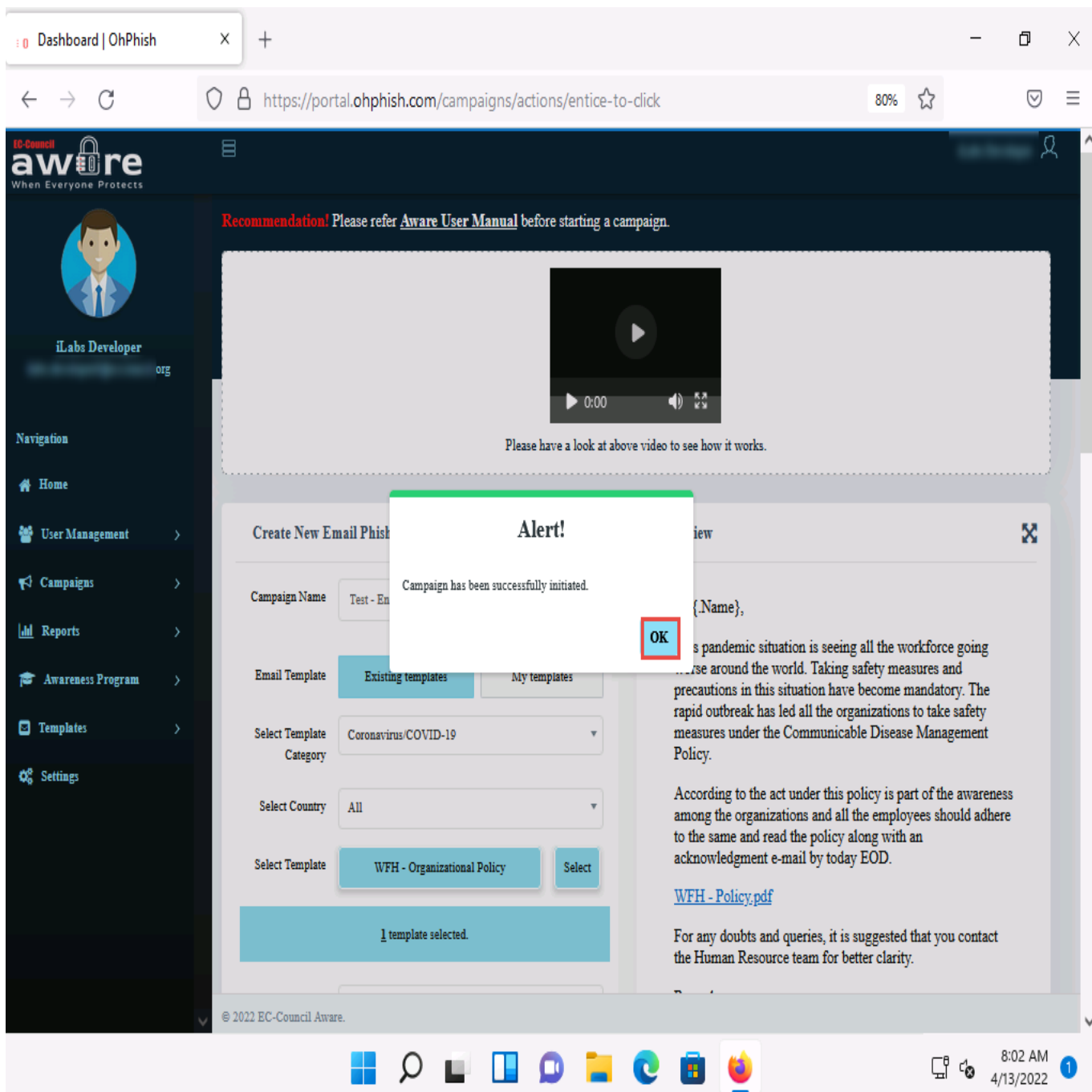
You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.



28. ☐ The **Confirm?** pop-up appears; click **SURE**.



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**.

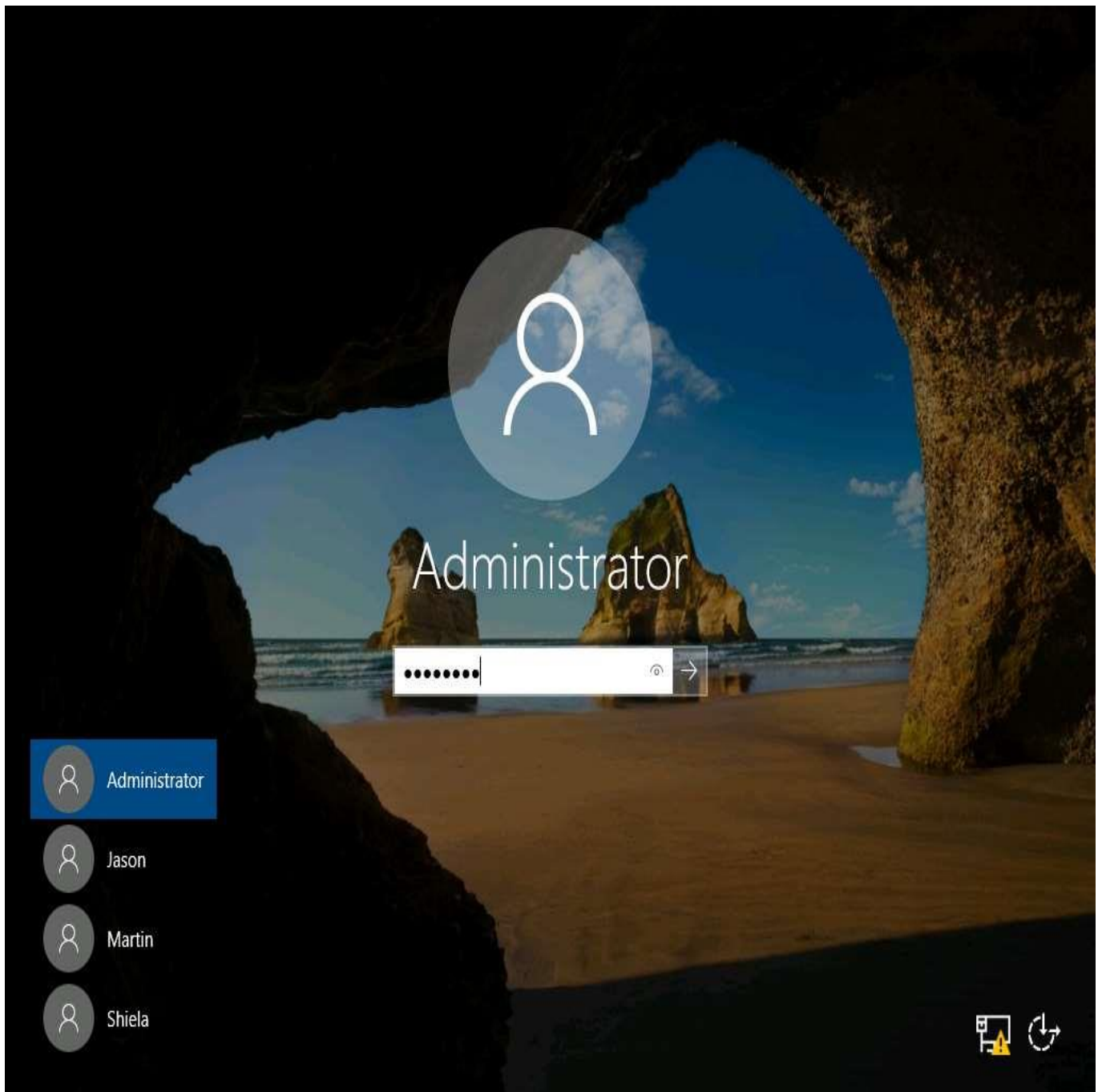


31. ☐ Now, we must open the phishing email as a victim (here, an employee of the organization). To do so, click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine.



32. ☐ Click on [Ctrl+Alt+Delete](#) to activate it, by default, **Administrator** profile is selected click **Pa\$\$w0rd** to enter password in to the machine and press **Enter** to login.

Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

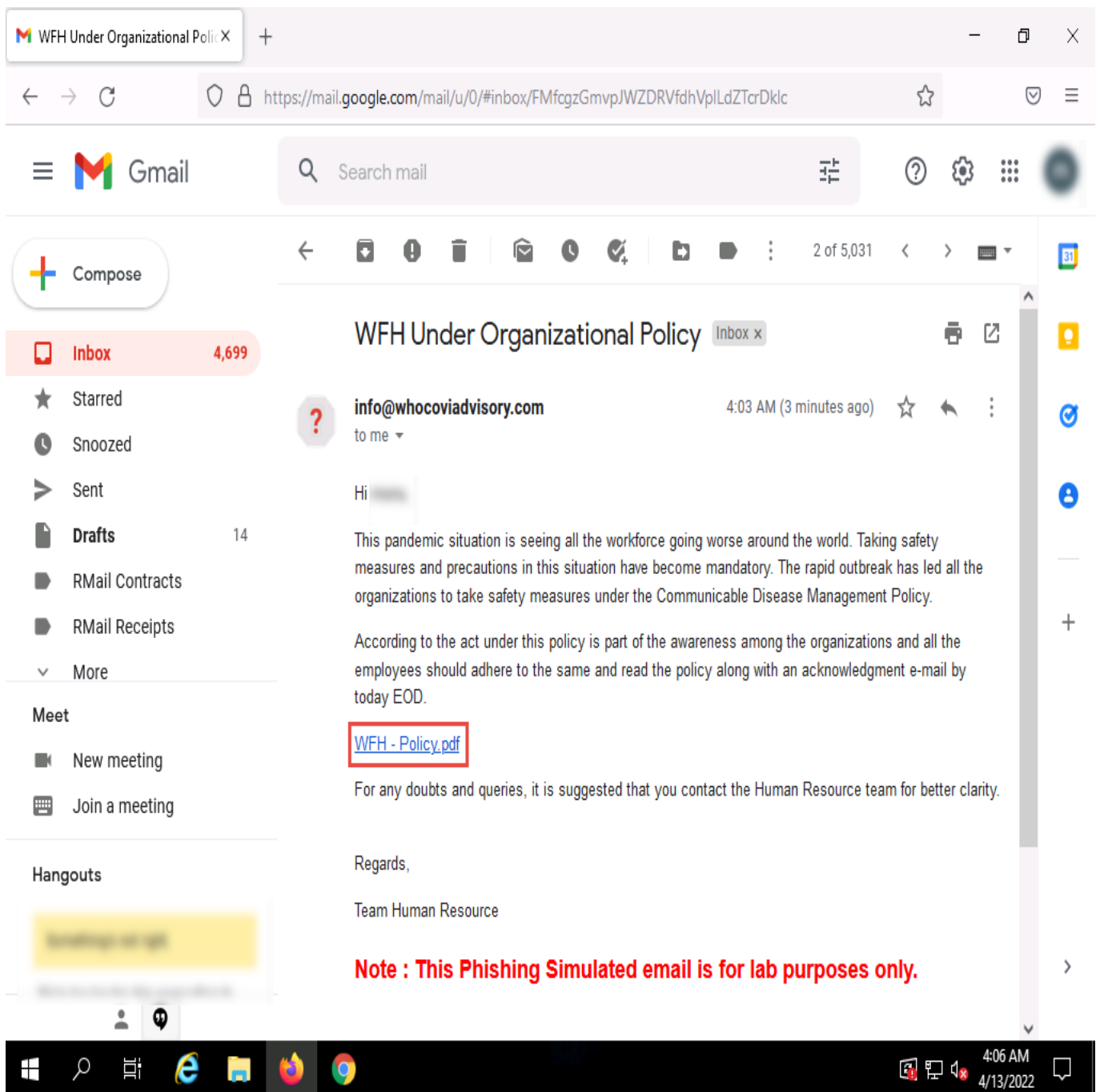


33. ☐ Open any web browser (here, **Mozilla Firefox**) and then open the email client provided while creating the phishing campaign (here, **Gmail**).
34. ☐ After you login to your **Gmail** account, search for an email with the subject **WFH Under Organizational Policy** in the **Inbox**.

Depending on the security implementations of your organization, for example, if proper spam filters are enabled, this phishing email will end up in the **Spam** folder.

If the email is not present in the **Inbox** folder, then check your **Spam** folder.

35. ☐ Click on the **WFH - Policy.pdf** link in the email.



36. ☐ A **Warning - phishing suspected** page appears, as shown in the screenshot.
37. ☐ You can further click report an incorrect warning link to whitelist the link.




Warning — phishing (web forgery) suspected

The site you are trying to visit has been identified as a forgery, intended to trick you into disclosing financial, personal or other sensitive information.

You can continue to <https://who.pageshowinfo.com/api/campaign?e=0981da8523786a74394cc40affe21597fd4c8bb9&c=6256adc845da4d0c3da7d9aa> at your own risk.

If you believe that this site is not actually a phishing site, you can [report an incorrect warning](#).

Advisory provided by 



38. ☐ Close the current tab.
39. ☐ Now, click [Windows 11](#) to switch back to the **Windows 11** machine.
40. ☐ Click on the **Test – Entice to Click** campaign present on the **OhPhish Dashboard**. You can observe that one person has clicked the link.

Refresh the Ohphish dashboard page, if the clicked value is still 0.

The screenshot shows the OhPhish Aware dashboard. The top navigation bar includes the 'aware' logo and a user profile. The main content area is titled 'Dashboard' and features a notice about a 3-minute video walkthrough. Below the notice are six campaign mode buttons: 'Entice to Click', 'Credential Harvesting', 'Send Attachment', 'Assign New Training', 'Vishing', and 'Smishing'. A section titled 'Live Phishing Campaigns' contains a table with the following data:

Campaign	Campaign Type	Status	Assigned Training	Started	Stopped	Scheduled	Sent	Clicked	Compliance	Creator	Action
Test - Entice to Click	Email	In Progress	No Training Assigned	April 13, 2022 4:02 AM	Apr 20, 2022 America/Los_Angeles	NA	2	1	50.00%		

The bottom of the dashboard shows the copyright notice '© 2022 EC-Council Aware.' and a Windows taskbar with the time '8:12 AM 4/13/2022'.

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).

Dashboard | OhPhish

https://portal.ohphish.com/campaigns/6256adc845da4d0c3da7d9aa

80%

IC-Council
aware
When Everyone Protects

iLabs Developer
[Profile Picture]
[Email Address].org

Navigation

- Home
- User Management
- Campaigns
- Reports
- Awareness Program
- Templates
- Settings

Test - Entice to Click/April 20, 2022

Download Excel

Campaign Details

Campaign Name	Date Initiated
Test - Entice to Click	Wednesday, April 13th 2022
Expiry Date	Domain
Wednesday, April 20th 2022	https://www.eccouncil.org/
Template Name	Template Category
WFH - Organizational Policy	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.

8:15 AM
4/13/2022

43. ☐ Now, click **Home** in the left pane to navigate back to the OhPhish **Dashboard**.
44. ☐ In the OhPhish **Dashboard**, click on the **Send Attachment** option.

The screenshot shows the OhPhish dashboard interface. At the top, there's a navigation bar with the OhPhish logo and a user profile. Below this, a sidebar on the left contains navigation links: Home, User Management, Campaigns, Reports, Awareness Program, Templates, and Settings. The main content area is titled 'Dashboard' and includes a notice about viewing a 3-minute video walkthrough. Below the notice, there are six large, colorful buttons representing different phishing campaign types: Entice to Click (green), Credential Harvesting (red), Send Attachment (teal), Assign New Training (blue), Vishing (purple), and Smishing (dark blue). The 'Send Attachment' button is highlighted with a red border. Below these buttons, there's a section titled 'Live Phishing Campaigns' which contains a table of active campaigns.

Campaign	Campaign Type	Status	Assigned Training	Started	Stopped	Scheduled	Sent	Clicked	Compliance	Creator	Action
Test - Entice to Click	Email	In Progress	No Training Assigned	April 13, 2022 4:02 AM	Apr 20, 2022 America/Los_Angeles	NA	2	1	50.00%		

45. ☐ The **Create New Email Phishing Campaign** form appears.

Almost Done pop-up appears, click **DISCARD CHANGES**.

46. ☐ In the **Campaign Name** field, enter any name (here, **Test – Send to Attachment**). In the **Select Template Category** field, select **Office Mailers** from the drop-down list.

Ensure that the **Existing templates** button is selected in the **Email Template** field.

47. ☐ In the **Select Country** field, leave the default option selected (**All**).
48. ☐ In the **Select Template** field, select the **PF Amount Credited** option from the drop-down list and then click the **Select** button.
49. ☐ Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

You can change the above-mentioned options if you want to.

50. ☐ In the **Attachment** field, enter any name (here, **PFinfo**).

The screenshot shows the 'Send Attachment' campaign configuration page in the OhPhish portal. The page is titled 'Dashboard | OhPhish' and the URL is 'https://portal.ohphish.com/campaigns/actions/send-attachment'. The sidebar on the left includes a user profile for 'iLabs Developer' and a navigation menu with links to Home, User Management, Campaigns, Reports, Awareness Program, Templates, and Settings. The main form contains the following fields:

- Campaign Name:** Test - Send to Attachment
- Email Template:** Existing templates (selected), My templates
- Select Template Category:** Office Mailers
- Select Country:** All
- Select Template:** PF Amount Credited (selected), Select
- 1 template selected.**
- Sender Email:** hr@yourorgname.com
- Sender Name:** HR - ABP News
- Subject:** PF amount has been credited
- Select Time Zone:** America/Los_Angeles
- Expiry Date:** 20-Apr-2022
- Schedule Later:** No
- Attachment:** PFinfo (selected), doc

The preview on the right shows the email content:

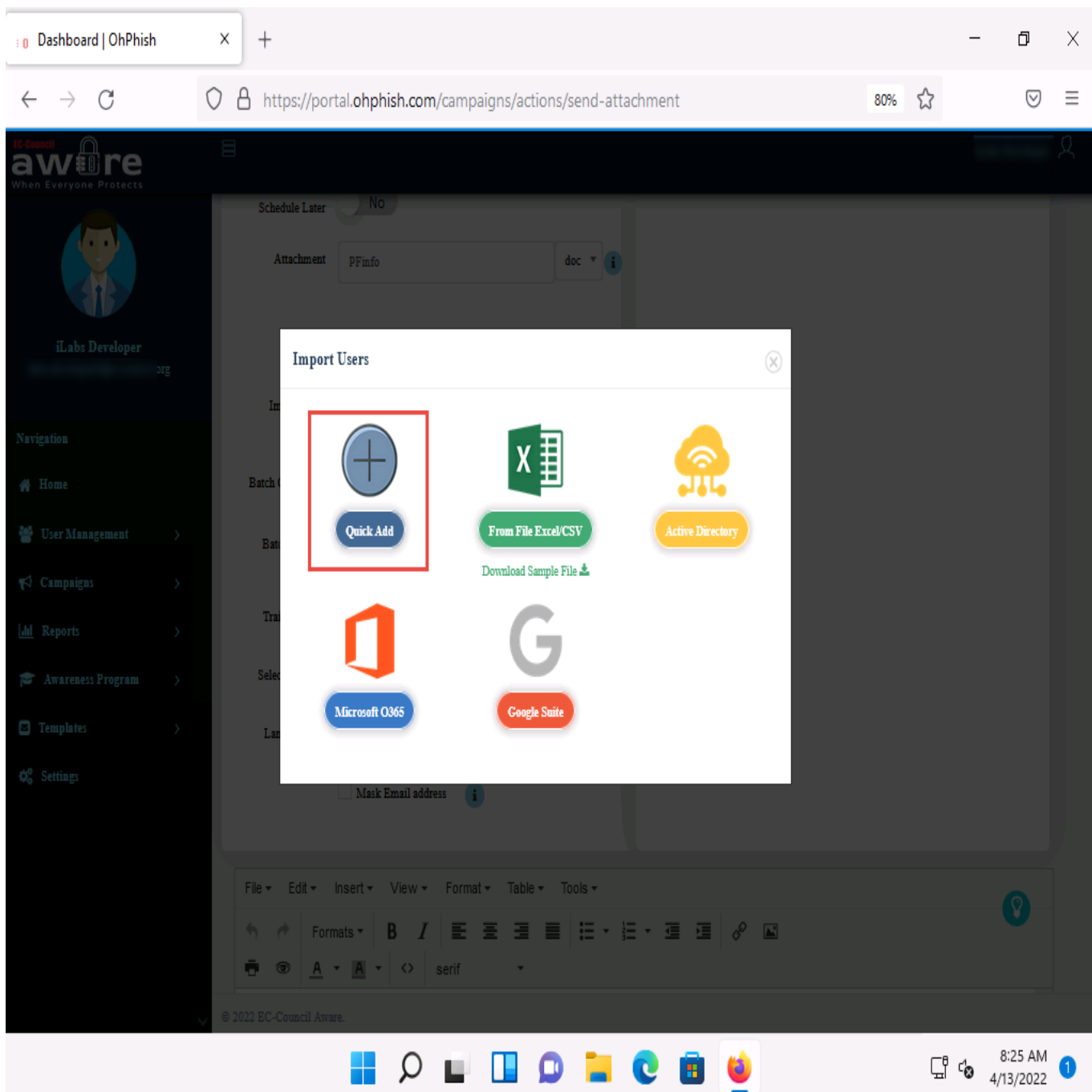
Dear {Name},

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](#).

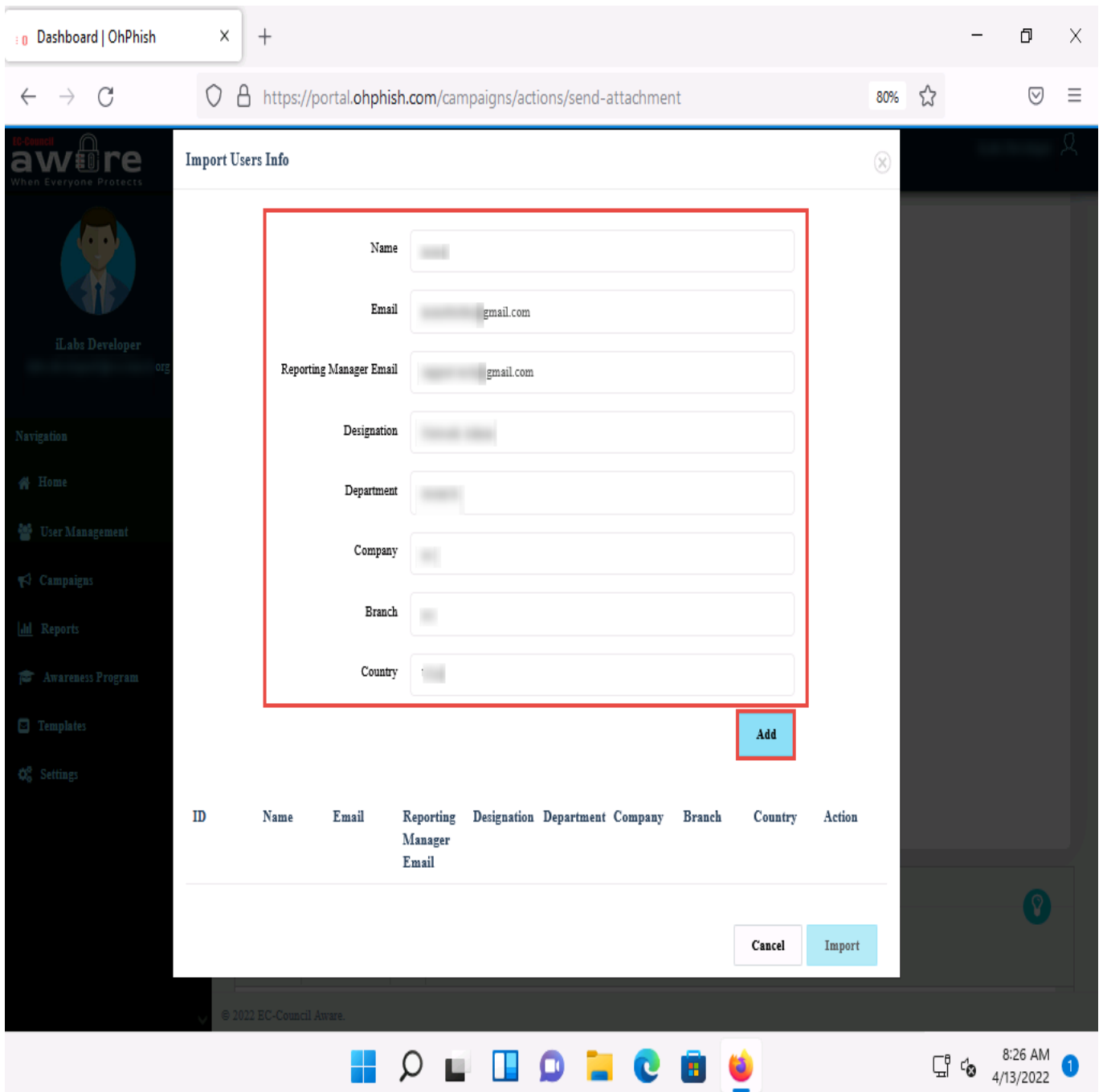
In order to complete this procedure you would need below mentioned information.

- Your full name; as per company records
- Employee ID
- Month and Year of joining the organization;
- Establishment or company Legal name; would be mentioned in your salary slip.

51. ☐ Click **Select Source** button under **Import users** field.
52. ☐ **Import Users** pop-up appears, click to select the **Quick Add** option from the list of options.



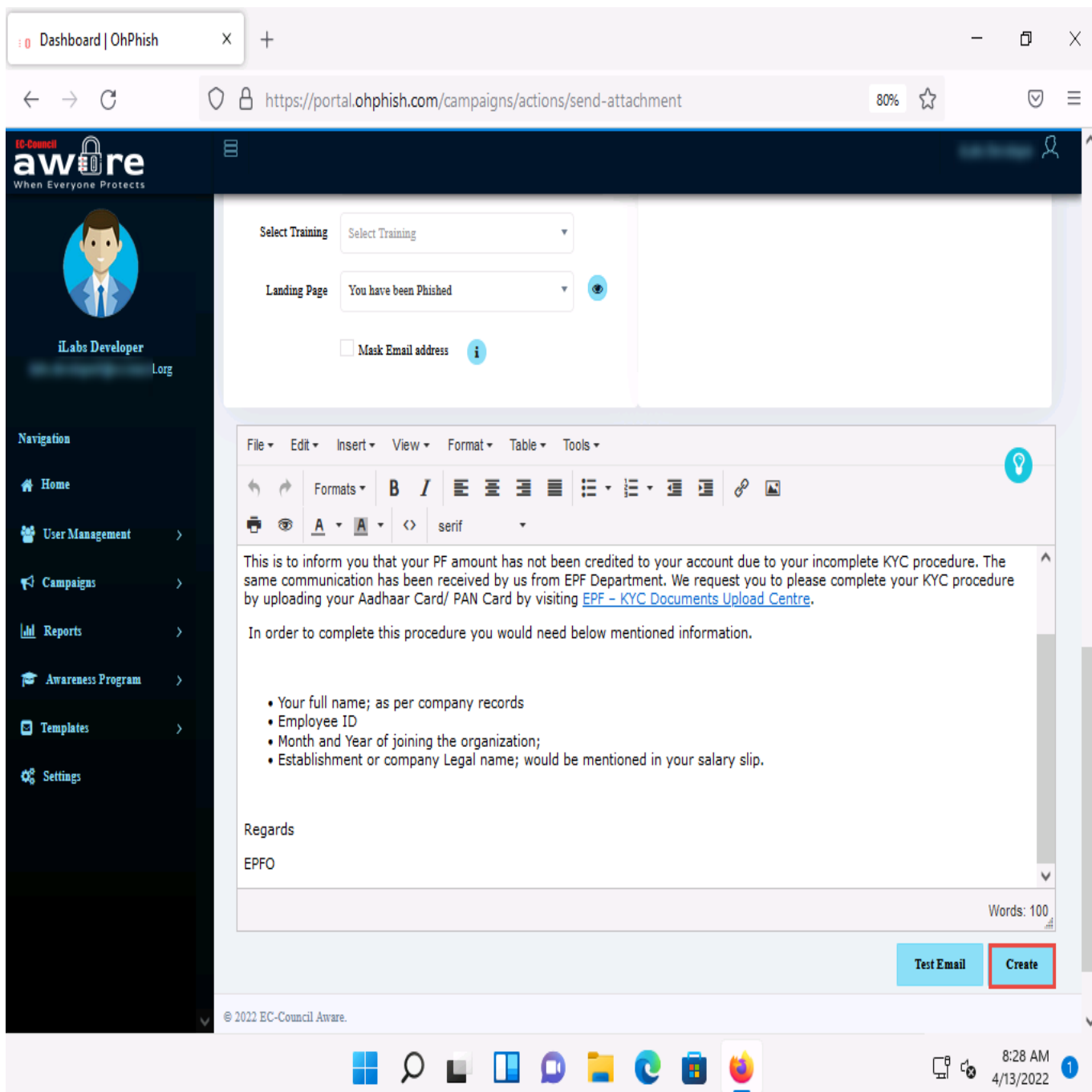
53. ☐ The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.



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.



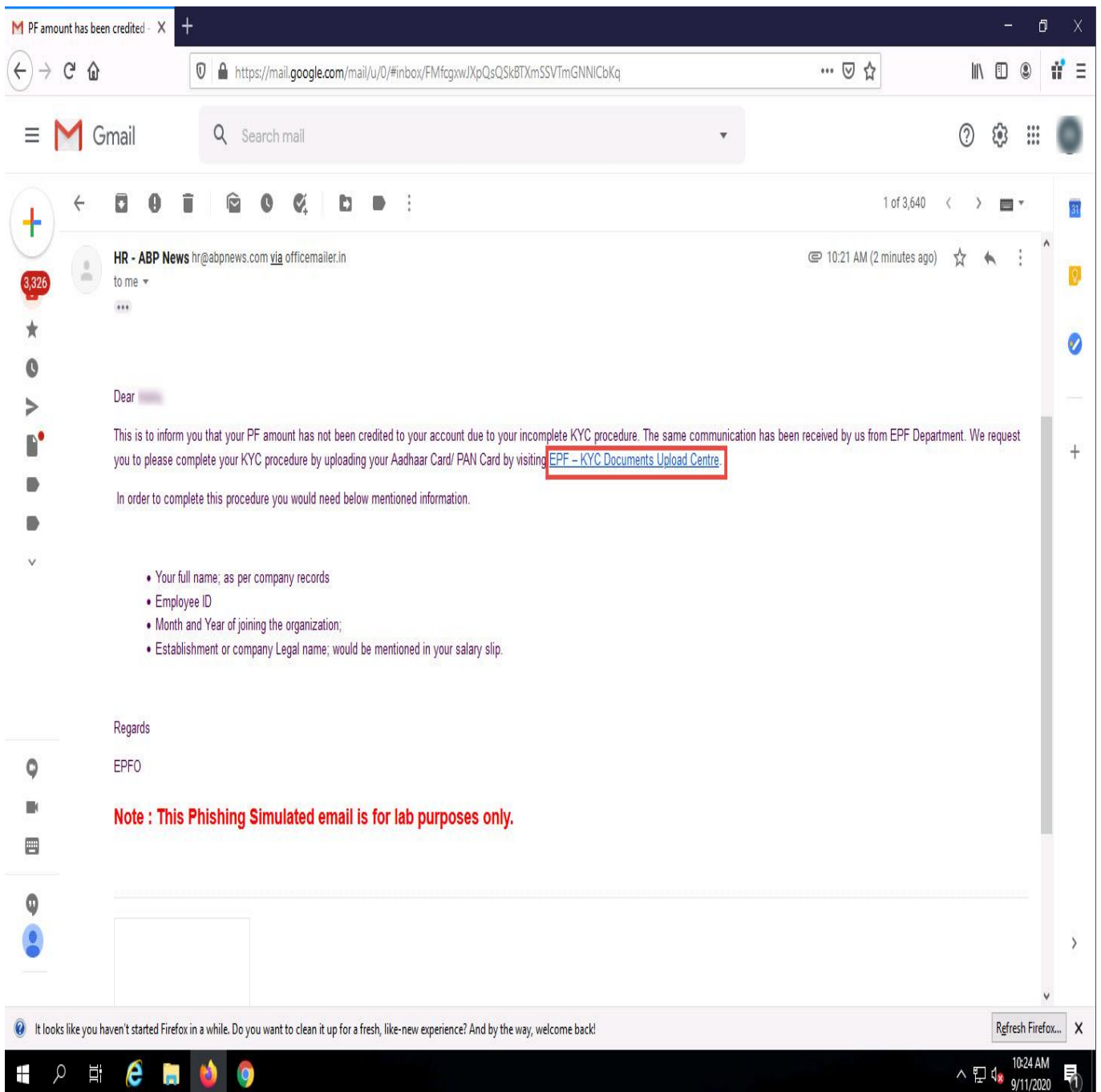
59. ☐ **Add to your Whitelist** pop-up appears, click **Done**.

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.

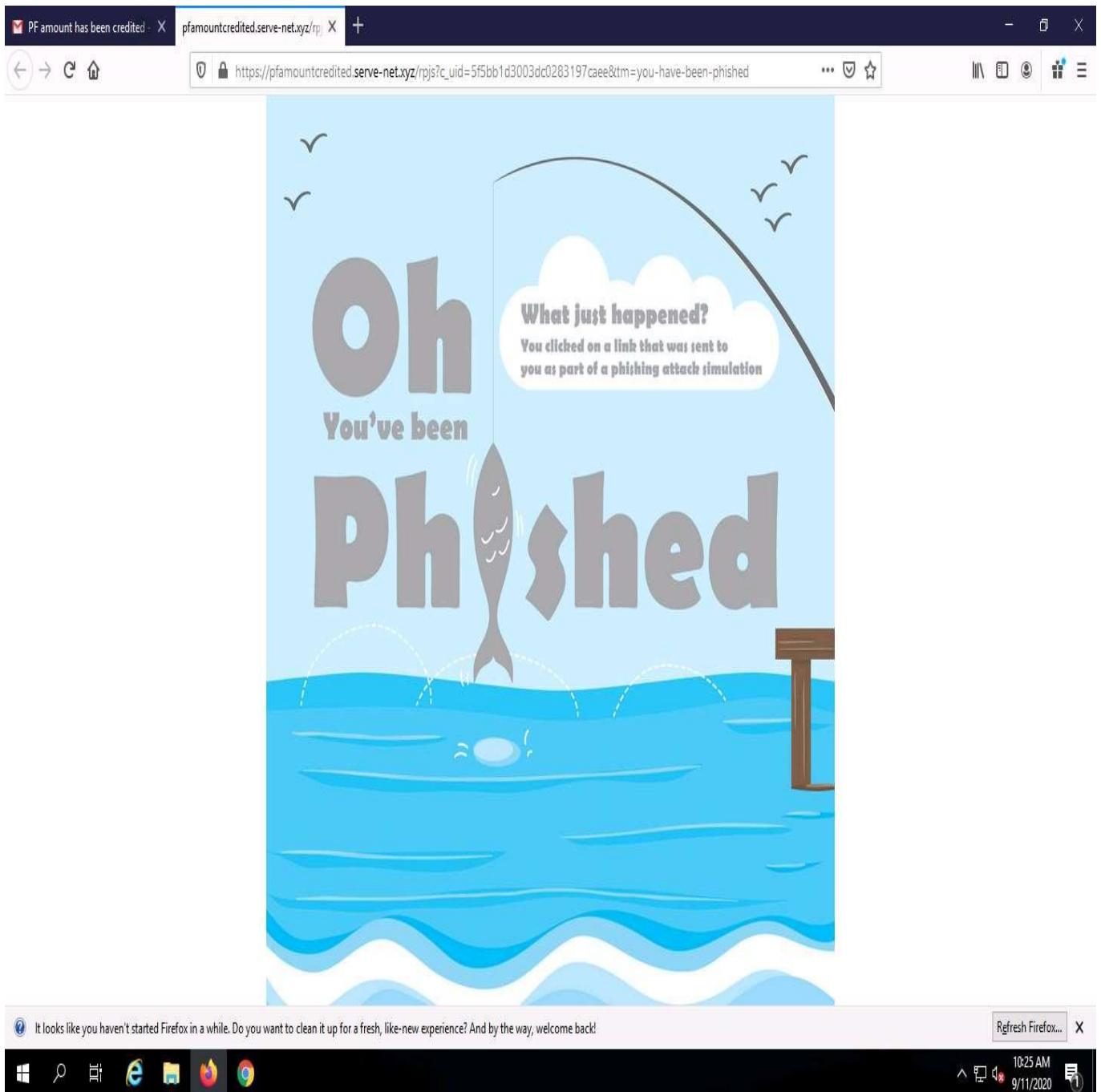
60. ☐ The **Confirm?** pop-up appears; click **SURE**.
61. ☐ A count down timer appears and phishing campaign initiates in ten seconds.
62. ☐ The **Alert!** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.
63. ☐ Now, click [Windows Server 2019](#) to switch to the **Windows Server 2019** machine.

If you are logged out of the **Windows Server 2019** machine, click [Ctrl+Alt+Delete](#), then login into **Administrator** user profile using **Pa\$\$w0rd** as password.

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.



69. ☐ Now, click [Windows 11](#) to switch back to the **Windows 11** machine.
70. ☐ Click on the **Test – Send to Attachment** campaign present on the **OhPhish Dashboard**.

Dashboard | OhPhish

https://portal.ohphish.com/dashboard

OHPHISH
Fortifying Front Lines

Dashboard

Recommendation! Please refer to [link](#) before start using OhPhish. Please choose a campaign mode from below options.

Entice to Click Credential Harvesting Send Attachment

Training Vishing Smishing

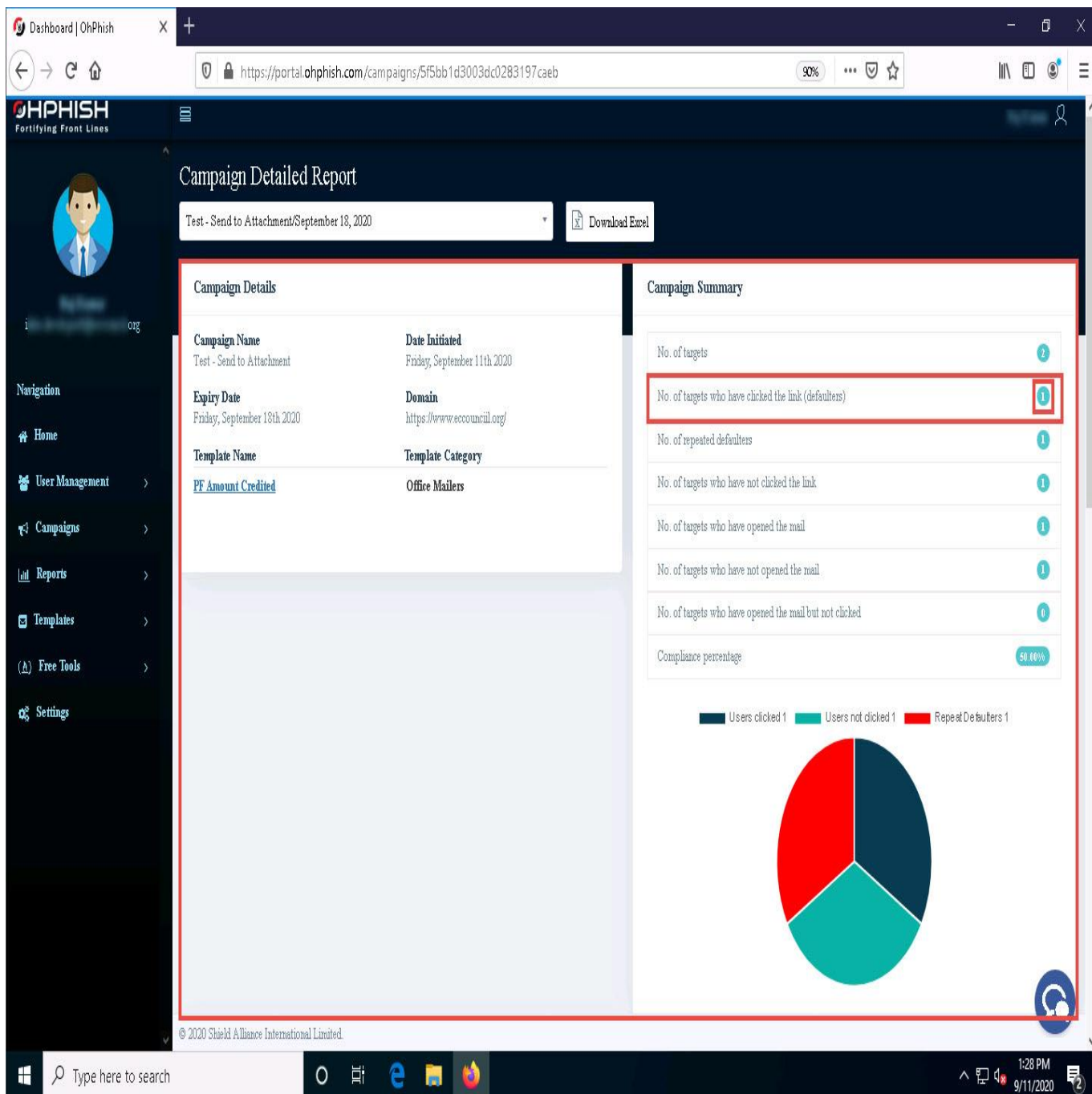
Live Phishing Campaigns

Campaign	Campaign Type	Status	Assigned Training	Started	Stopped	Scheduled	Sent	Clicked	Compliance	Creator	Action
Test - Send to Attachment	Email	In Progress	No Training Assigned	September 11, 2020 1:20 PM	Sep 18, 2020 America/New_York	NA	2	0	100.00%	Not Visible	
Test - Entice to Click	Email	In Progress	No Training Assigned	September 11, 2020 12:40 PM	Sep 18, 2020 America/New_York	NA	2	1	50.00%	Not Visible	

[Show More](#)

© 2020 Shield Alliance International Limited.

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.



73. ☐ The **Campaigns Users** page appears, displaying the details of the defaulter, such as **Risk Score**, **Credentials**, **IP Address**, **Location**, etc., as shown in the screenshot.

OhPHISH
Fortifying Front Lines

Campaigns Users

Users Details

Employee ID	Employee Name	Email	Designation	Department	Branch	Sent At	Opened At	Clicked At	Click Count	Risk Score	Template Used	IP Address	Location	Device	Status	Attachment Open Time
1		@gmail.com				Fri, Sep 11, 2020 1:21 PM	Fri, Sep 11, 2020 1:24 PM	Fri, Sep 11, 2020 1:25 PM	2	30	Office Mailers	66.102.8.217	United States	Desktop	Delivered	Nil

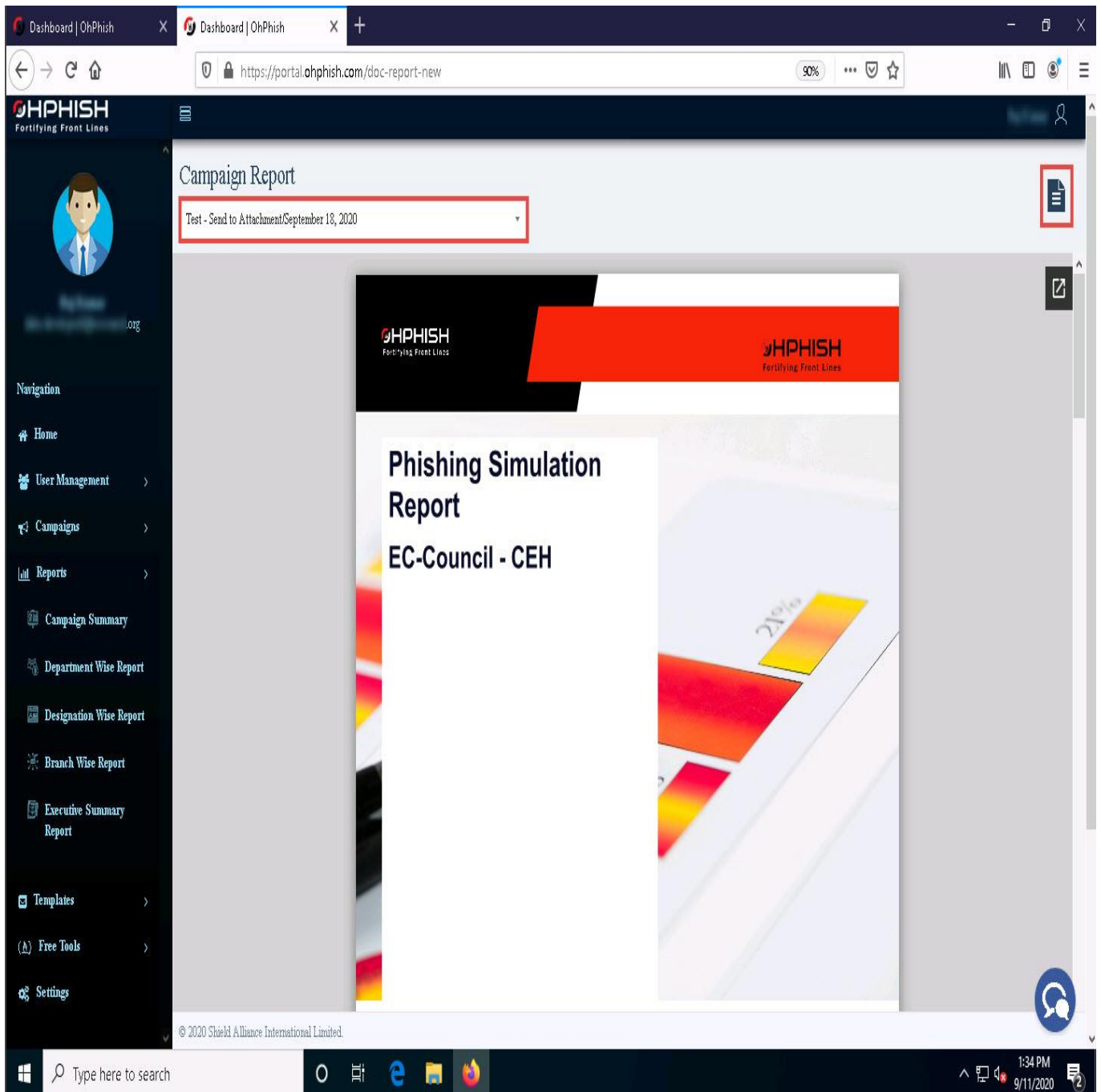
© 2020 Shield Alliance International Limited.

74. ☐ Now, click to expand the **Reports** section in the left pane and select the **Executive Summary Report** option.

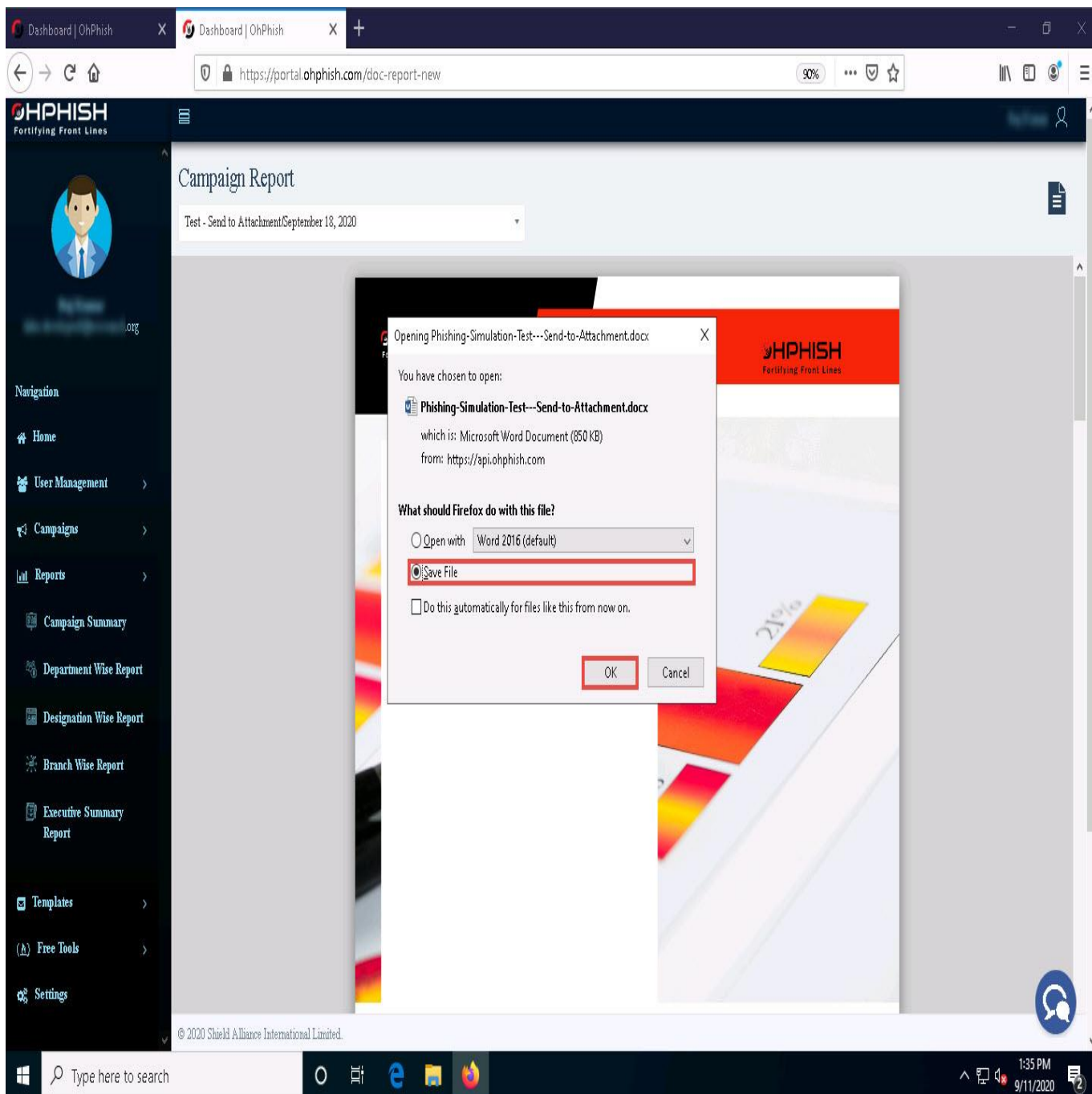
The screenshot shows the OhPhish dashboard interface. The left sidebar contains a navigation menu with the following items: Home, User Management, Campaigns, Reports (highlighted with a red box), Campaign Summary, Department Wise Report, Designation Wise Report, Branch Wise Report, Executive Summary Report (highlighted with a red box), Templates, Free Tools, and Settings. The main content area is titled 'Campaigns Users' and displays a 'Users Details' table. The table has columns for Employee ID, Employee Name, Email, Designation, Department, Branch, Sent At, Opened At, Clicked At, Click Count, Risk Score, Template Used, IP Address, Location, Device, Status, and Attachment Open Time. A single row of data is visible, showing a user with ID 1, Name 'Test', Email 'test@ohphish.com', Designation 'Test', Department 'Test', Branch 'Test', Sent At 'Fri, Sep 11, 2020 1:21 PM', Opened At 'Fri, Sep 11, 2020 1:24 PM', Clicked At 'Fri, Sep 11, 2020 1:25 PM', Click Count '2', Risk Score '30', Template Used 'Office Mailers', IP Address '66.102.8.217', Location 'United States', Device 'Desktop', Status 'Delivered', and Attachment 'Nil'. The bottom of the dashboard shows the URL 'https://portal.ohphish.com/doc-report-new' and the footer text '©2020 Shield Alliance International Limited'.


Employee ID	Employee Name	Email	Designation	Department	Branch	Sent At	Opened At	Clicked At	Click Count	Risk Score	Template Used	IP Address	Location	Device	Status	Attachment Open Time
1	Test	test@ohphish.com	Test	Test	Test	Fri, Sep 11, 2020 1:21 PM	Fri, Sep 11, 2020 1:24 PM	Fri, Sep 11, 2020 1:25 PM	2	30	Office Mailers	66.102.8.217	United States	Desktop	Delivered	Nil

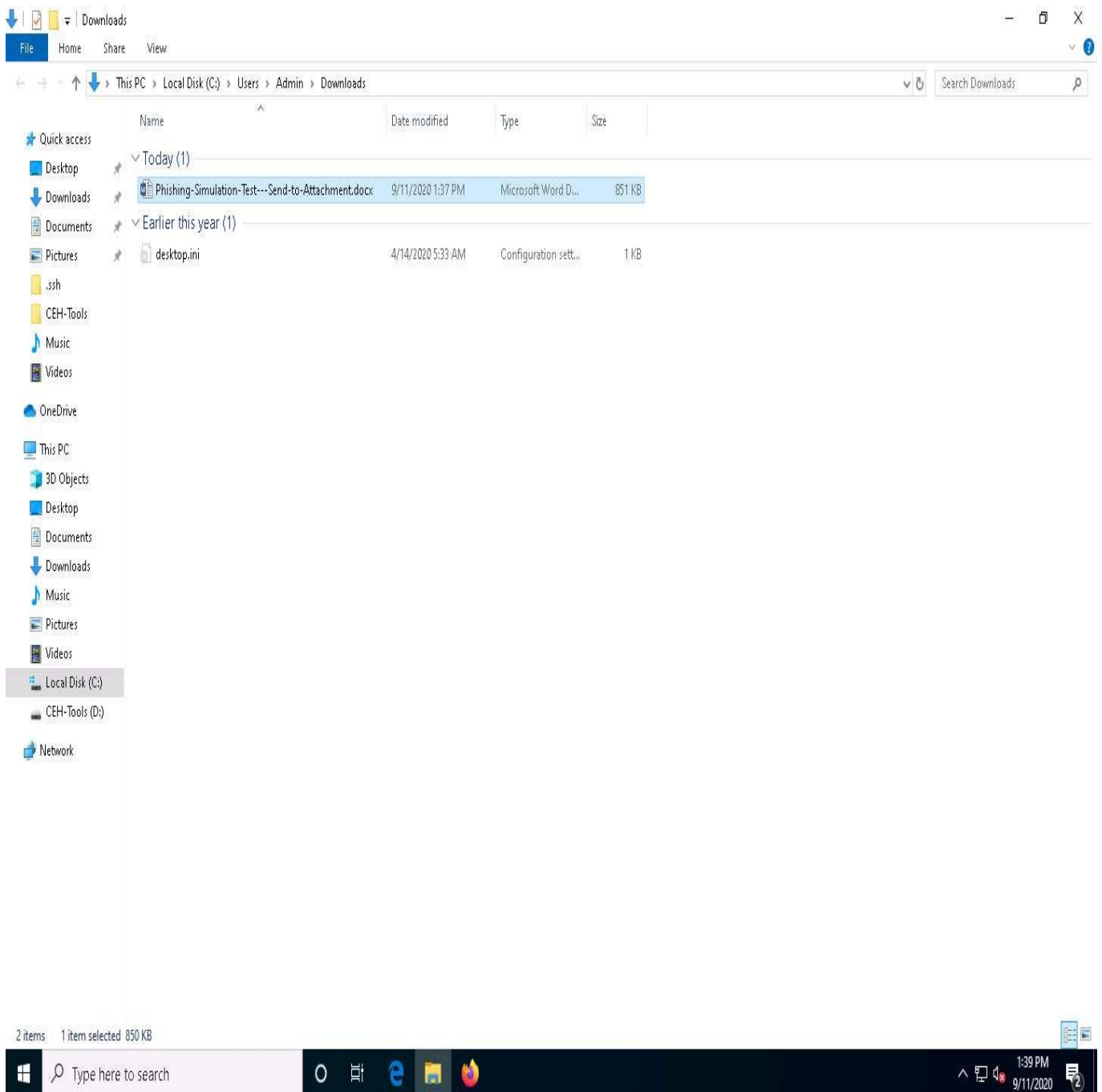
75. ☐ The **Campaign Report** page appears; select any phishing campaign from the drop-down list (here, **Test – Send to Attachment**) and click on the **Export** icon to export the report.



76. ☐ The **Opening Phishing-Simulation-Test** window appears; select the **Save File** radio button and click **OK**.



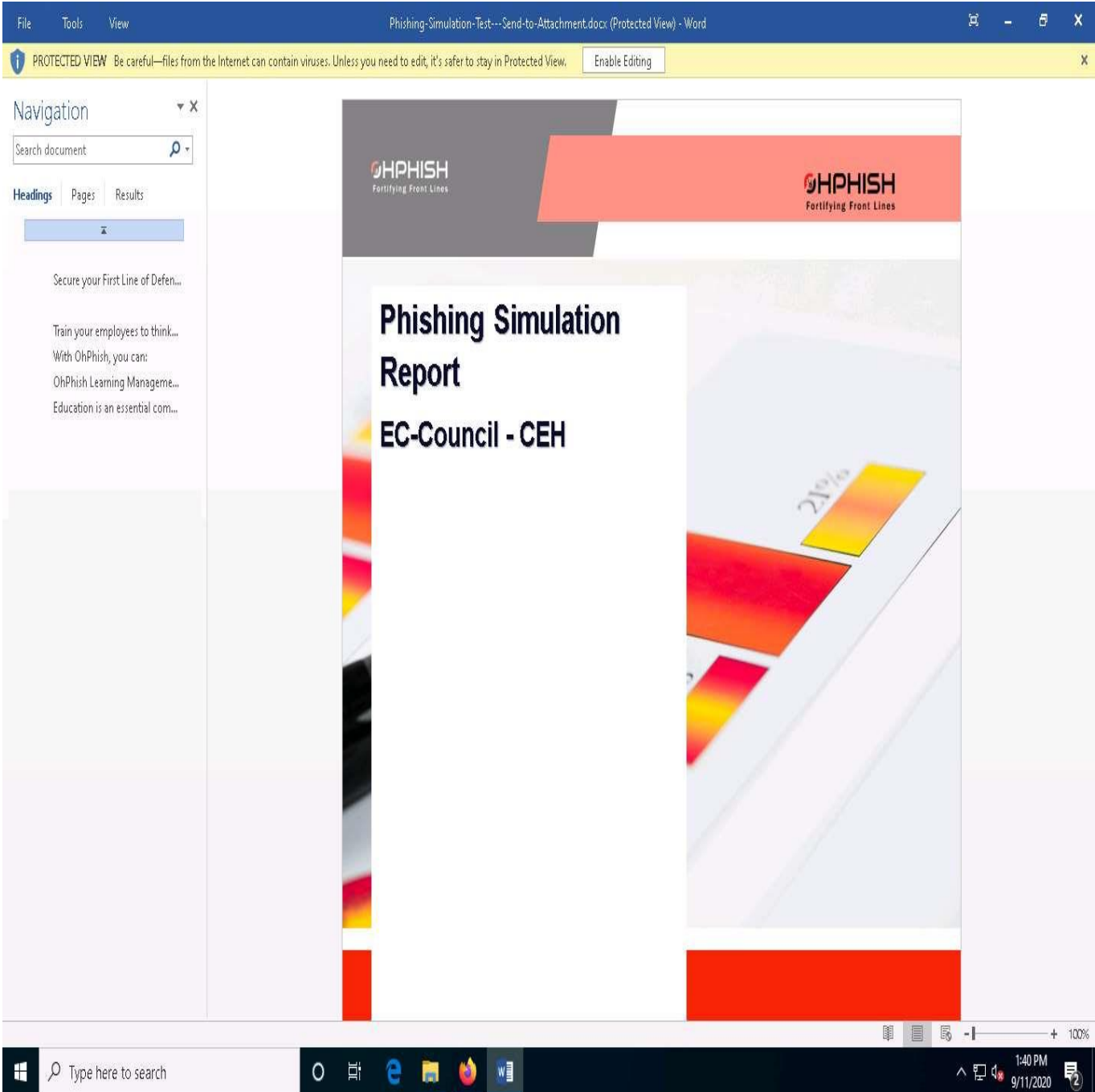
77.  The file is downloaded to the default location (here, **Downloads**). Navigate to the download location and double-click the **Phishing-Simulation-Test---Send-Attachment** file to open it.



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**.



FileToolsView

Phishing-Simulation-Test---Send-to-Attachment.docx (Protected View) - Word

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

HeadingsPagesResults

Secure your First Line of Defen...

Train your employees to think...
With OhPhish, you can:
OhPhish Learning Manageme...
Education is an essential com...

What is Phishing?

Phishing is a cybercrime in which unsuspecting victims are contacted by email, telephone or text message by somebody posing as a credible source to lure victims into providing sensitive information such as banking and credit card details, and passwords. Click on the topics below to read more about each.

Secure your First Line of Defense - How can OhPhish help?

Studies show that **90%** of cybersecurity breaches are caused by human error


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:


Email Phishing


SMS Phishing


Voice Phishing

Type here to search



1:41 PM

9/11/2020

File Tools View Phishing-Simulation-Test---Send-to-Attachment.docx (Protected View) - Word

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 Defen...

Train your employees to think...

With OhPhish, you can:

OhPhish Learning Manageme...

Education is an essential com...

Executive Summary

Phishing Simulation Report

This report provides the results for EC-Council - CEH's phishing simulation Test - Send to Attachment carried out on Sep 11, 2020 using OhPhish platform to measure the susceptibility of in-scope users to Phishing attacks in which an adversary tricks an email user into clicking a malicious link to gain unauthorized network access.

The simulation was carried out for to measure the EC-Council - CEH's vulnerability to users falling victim to highly targeted impersonation attacks through parameters like click rates and click times as shown below. This report aims to enhance EC-Council - CEH's understanding of their users' behavior towards social engineering attacks and to promote a more secure and resilient workforce.

	#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%

OhPhish.com

Windows taskbar: Type here to search, 1:41 PM, 9/11/2020

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.