Module 09: Social Engineering

Scenario

Organizations fall victim to social engineering tactics despite having strong security policies and solutions in place. This is because social engineering exploits the most vulnerable link in information system security—employees. Cybercriminals are increasingly using social engineering techniques to target people's weaknesses or play on their good natures.

Social engineering can take many forms, including phishing emails, fake sites, and impersonation. If the features of these techniques make them an art, the psychological insights that inform them make them a science.

While non-existent or inadequate defense mechanisms in an organization can encourage attackers to use various social engineering techniques to target its employees, the bottom line is that there is no technological defense against social engineering. Organizations must educate employees on how to recognize and respond to these attacks, but only constant vigilance will minimize attackers' chances of success.

As an expert ethical hacker and penetration tester, you need to assess the preparedness of your organization or the target of evaluation against social engineering attacks. It is important to note, however, that social engineering primarily requires soft skills. The labs in this module therefore demonstrate several techniques that facilitate or automate certain facets of social engineering attacks.

Objective

The objective of the lab is to use social engineering and related techniques to:

- Sniff user/employee credentials such as employee IDs, names, and email addresses
- Obtain employees' basic personal details and organizational information
- Obtain usernames and passwords
- Perform phishing
- Detect phishing

Overview of Social Engineering

Social engineering is the art of manipulating people to divulge sensitive information that will be used to perform some kind of malicious action. Because social engineering targets human weakness, even organizations with strong security policies are vulnerable to being compromised by attackers. The impact of social engineering attacks on organizations can include economic losses, damage to goodwill, loss of privacy, risk of terrorism, lawsuits and arbitration, and temporary or permanent closure.

There are many ways in which companies may be vulnerable to social engineering attacks. These include:

- Insufficient security training
- Unregulated access to information
- An organizational structure consisting of several units
- Non-existent or lacking security policies

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform social engineering tests. The recommended labs that will assist you in learning various social engineering techniques are:

1. Perform social engineering using various techniques
    - Sniff credentials using the Social-Engineer Toolkit (SET)
2. Detect a phishing attack
    - Detect phishing using Netcraft
    - Detect phishing using PhishTank
3. Audit organization's security for phishing attacks
    - Audit organization's security for phishing attacks using OhPhish

---

Lab 1: Perform Social Engineering using Various Techniques

Lab Scenario

As a professional ethical hacker or penetration tester, you should use various social engineering techniques to examine the security of an organization and the awareness of employees.

In a social engineering test, you should try to trick the user into disclosing personal information such as credit card numbers, bank account details, telephone numbers, or confidential information about their organization or computer system. In the real world, attackers would use these details either to commit fraud or to launch further attacks on the target system

Lab Objectives

- Sniff credentials using the Social-Engineer Toolkit (SET)

Overview of Social Engineering Techniques

There are three types of social engineering attacks: human-, computer-, and mobile-based.

- **Human-based social engineering** uses interaction to gather sensitive information, employing techniques such as impersonation, vishing, and eavesdropping
- **Computer-based social engineering** uses computers to extract sensitive information, employing techniques such as phishing, spamming, and instant messaging
- **Mobile-based social engineering** uses mobile applications to obtain information, employing techniques such as publishing malicious apps, repackaging legitimate apps, using fake security applications, and SMiShing (SMS Phishing)

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

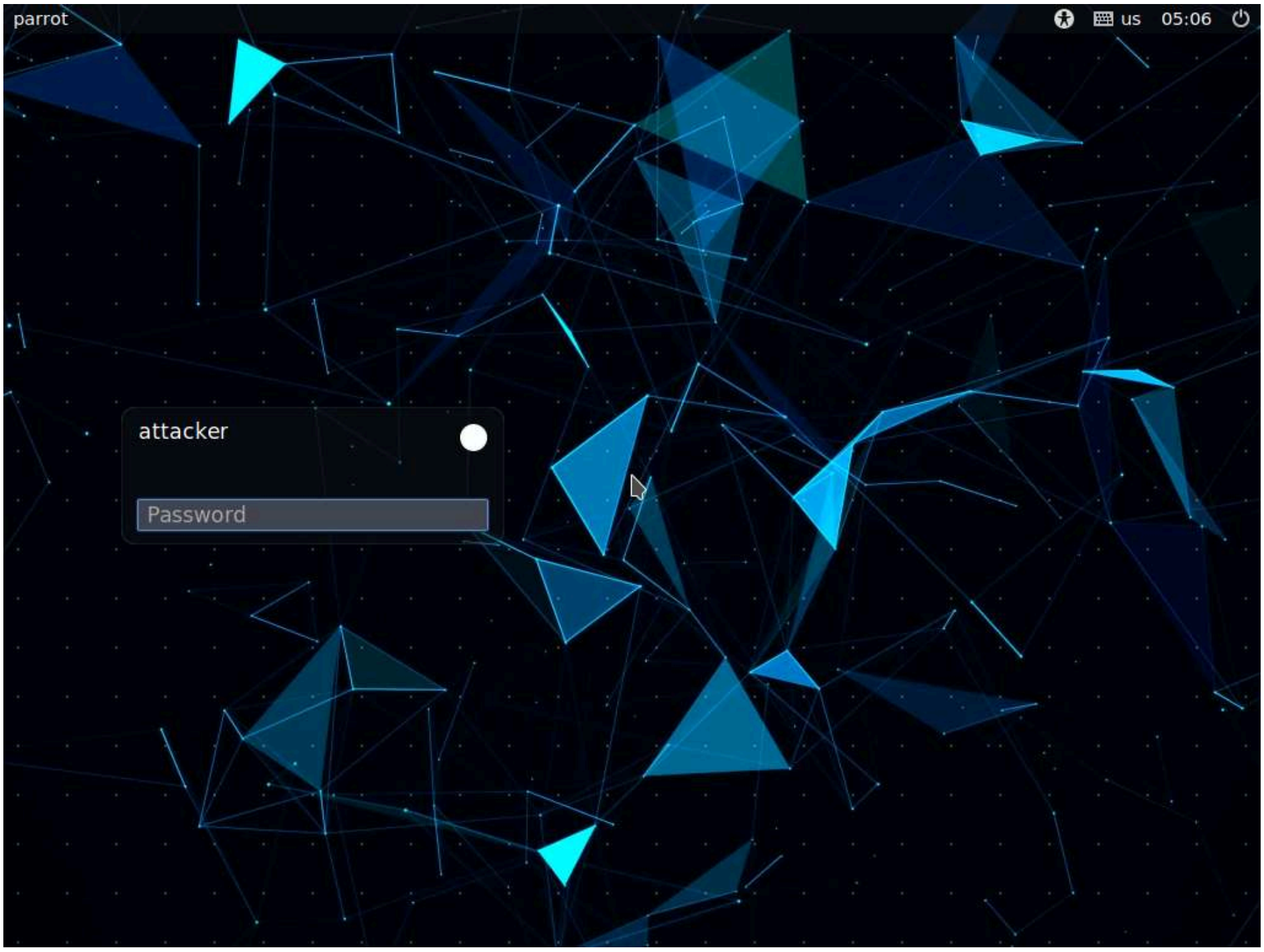
The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. SET is particularly useful to attackers, because it is freely available and can be used to carry out a range of attacks. For example, it allows attackers to draft email messages, attach malicious files, and send them to a large number of people using spear phishing. Moreover, SET's multi-attack method allows Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing to be used simultaneously. SET categorizes attacks according to the attack vector used such as email, web, and USB.

Although many kinds of attacks can be carried out using SET, it is also a must-have tool for penetration testers to check for vulnerabilities. For this reason, SET is the standard for social engineering penetration tests, and is strongly supported within the security community.

As an ethical hacker, penetration tester, or security administrator, you should be familiar with SET and be able to use it to perform various tests for network vulnerabilities.

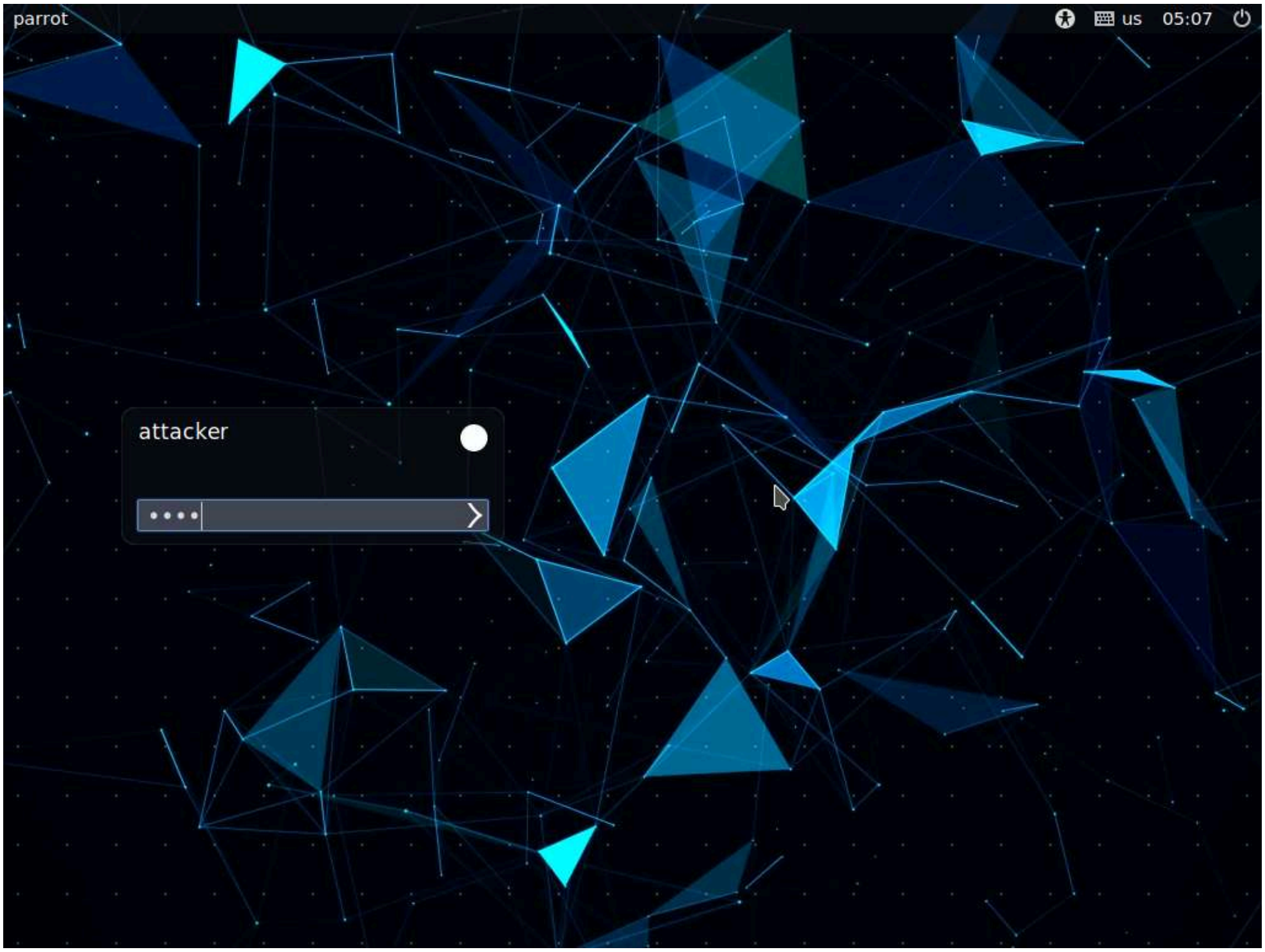
Here, we will sniff user credentials using the SET.

1. By default the **Parrot Security** machine is selected.

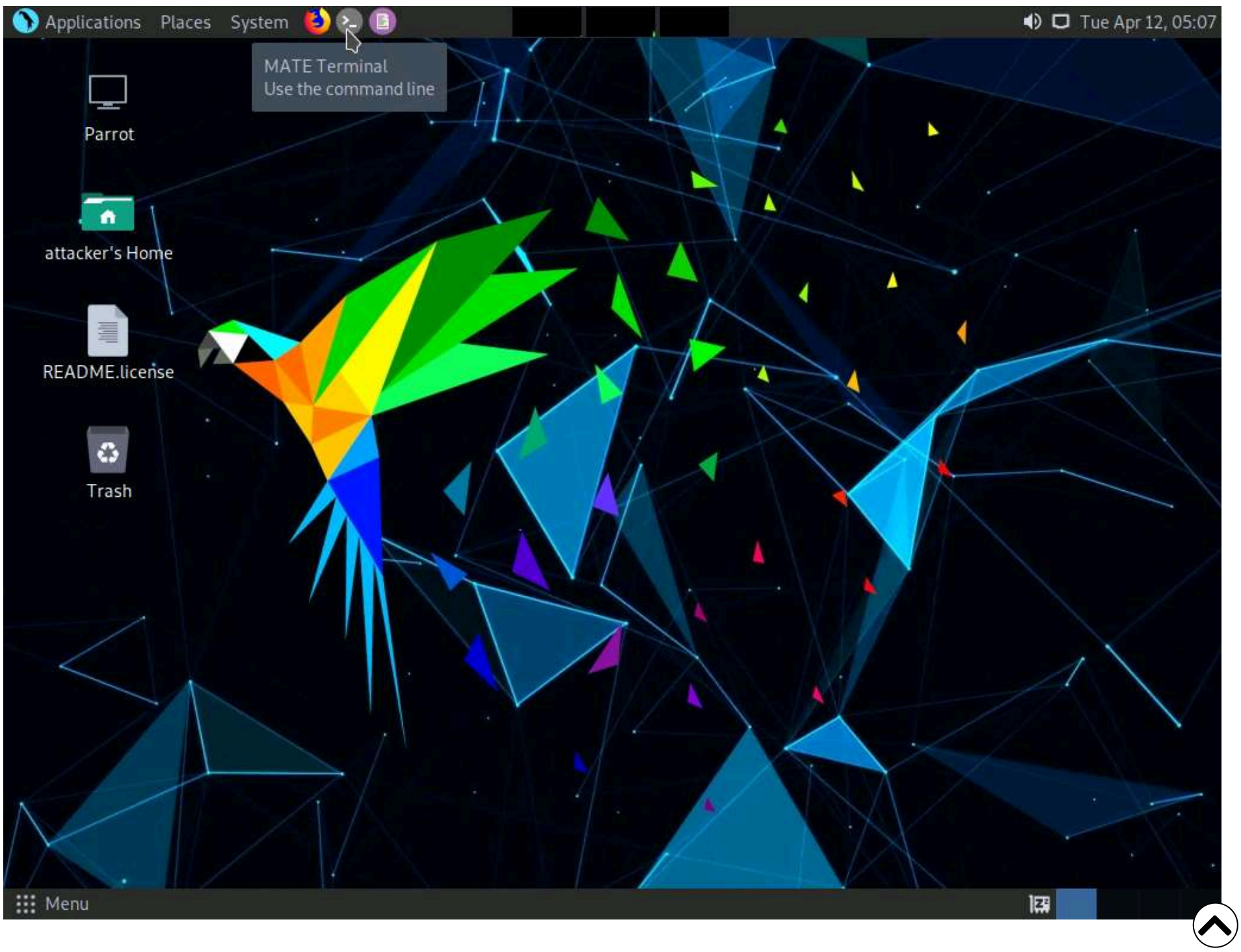


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the Password field and press Enter to log in to the machine.

Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

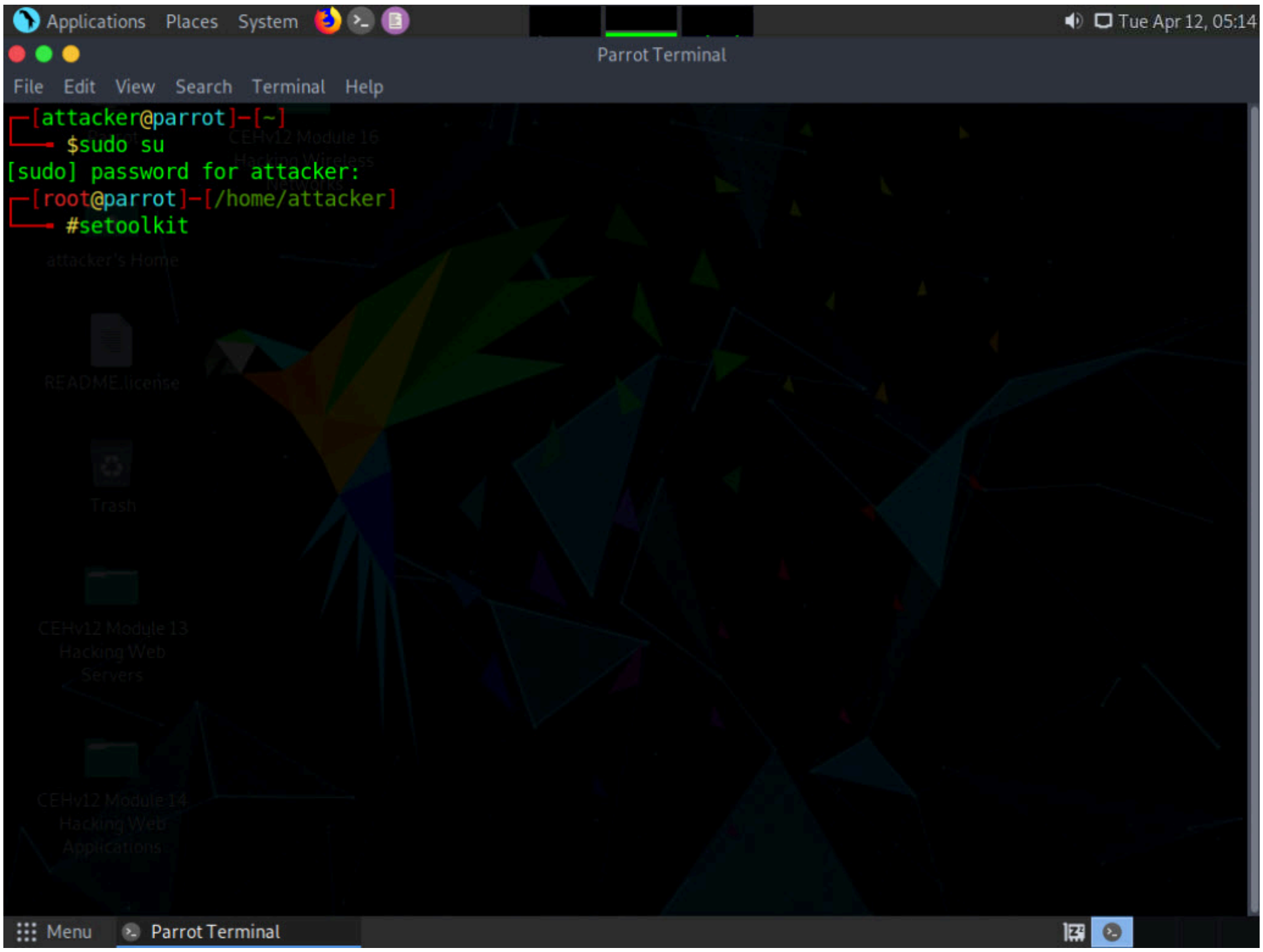


4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

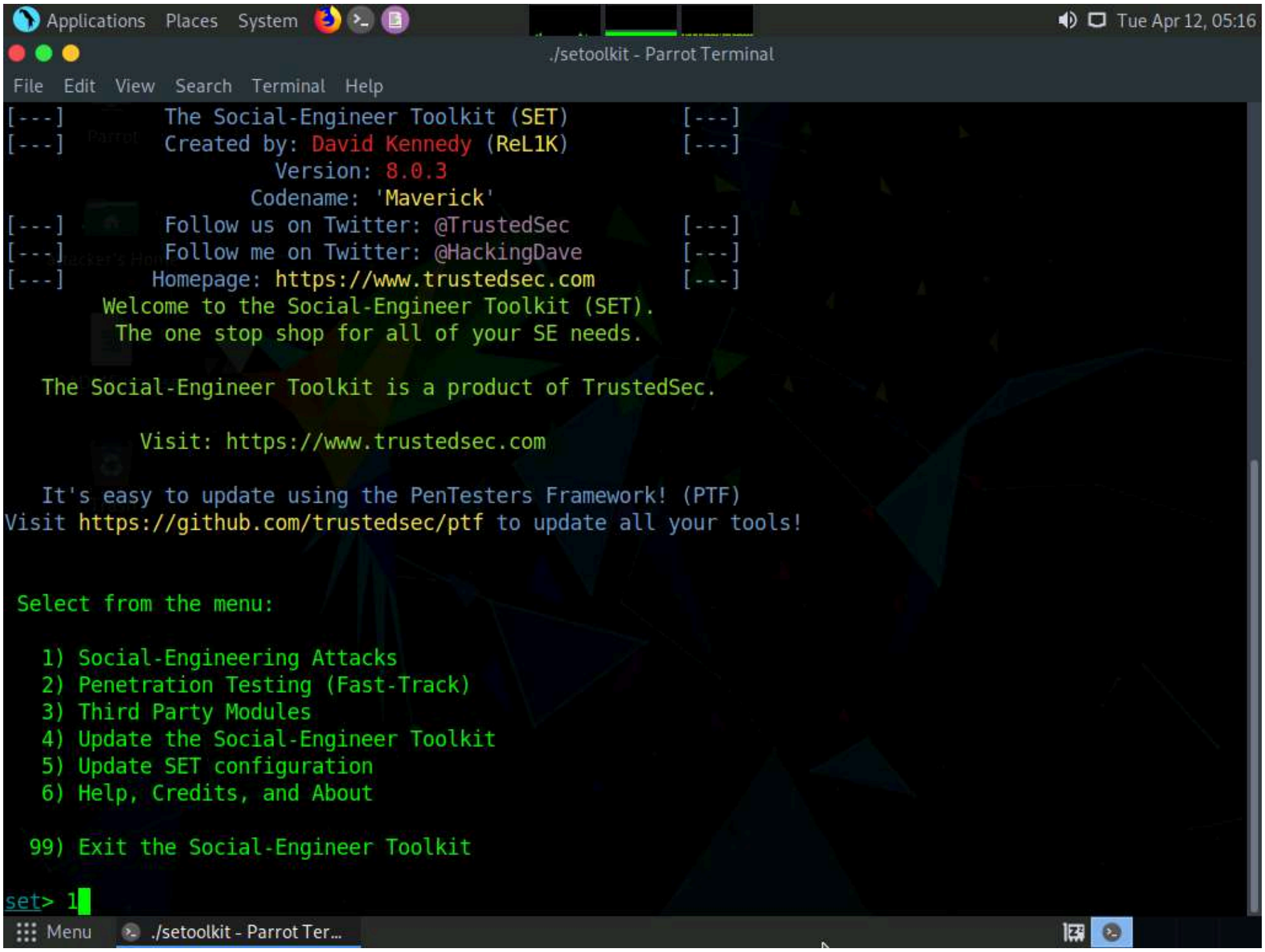
Note: The password that you type will not be visible.

6. Type **setoolkit** and press **Enter** to launch Social-Engineer Toolkit (SET).

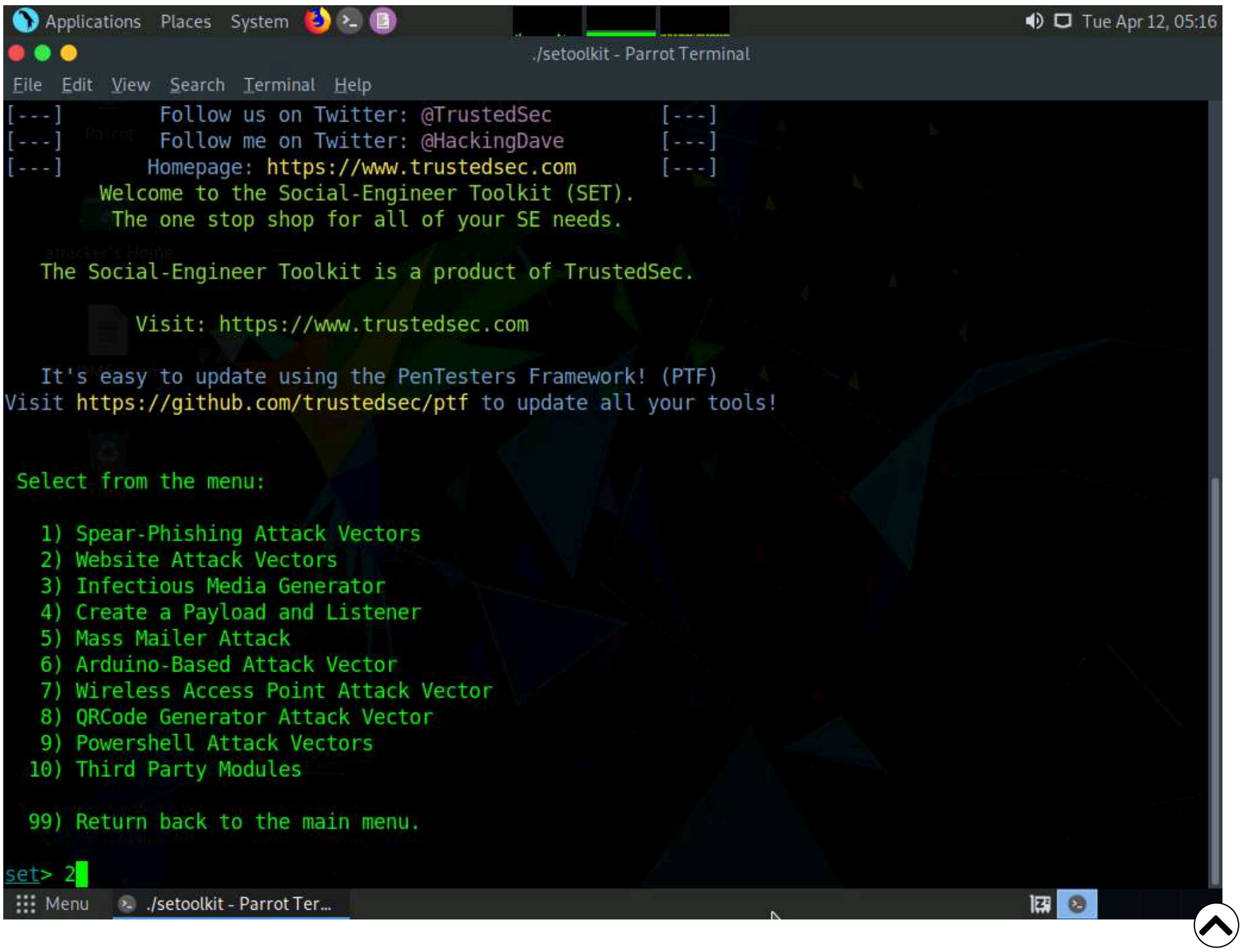


7. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **Social-Engineering Attacks**

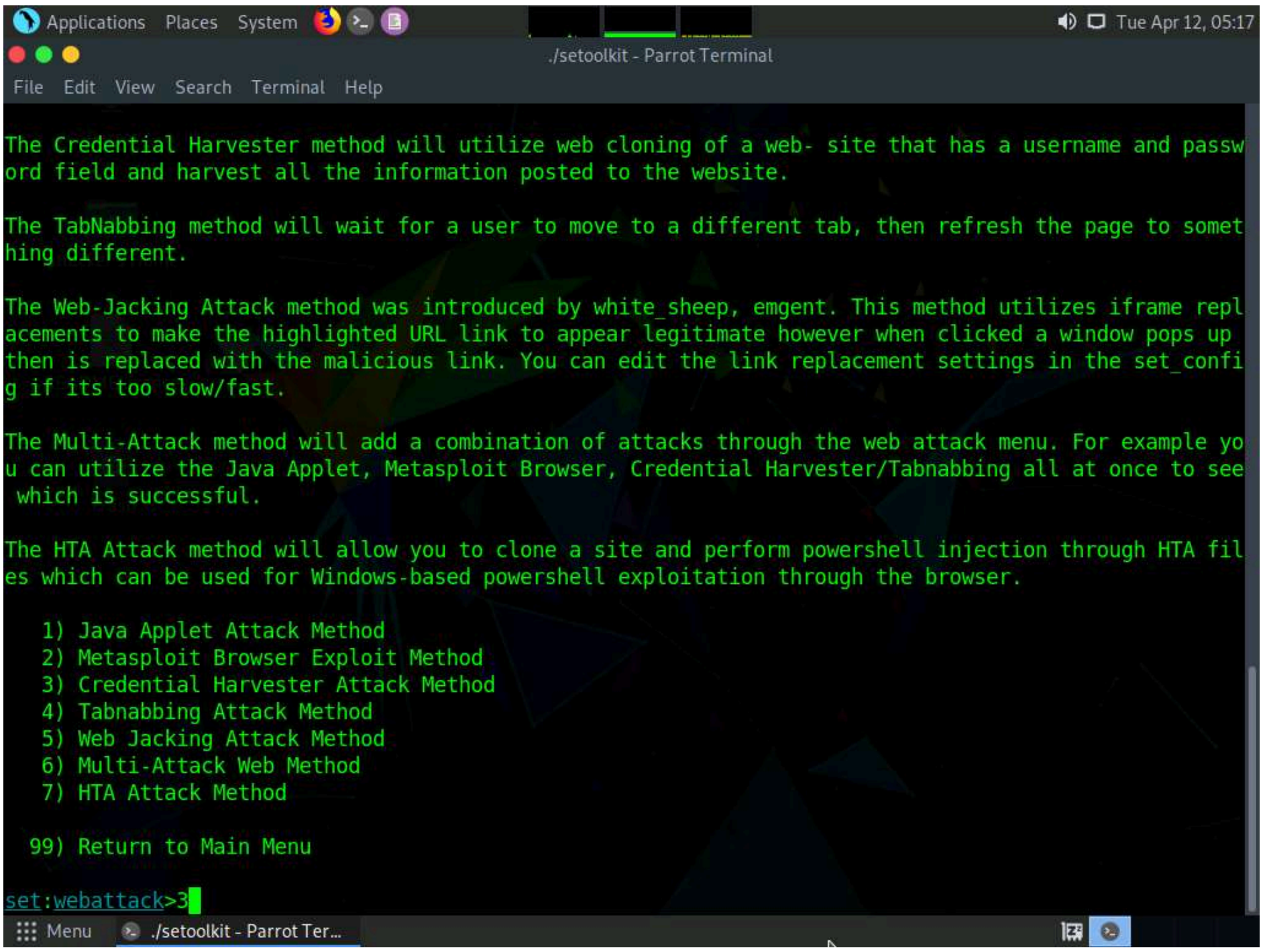
Note: If a **Do you agree to the terms of service [y/n]** question appears, enter **y** and press **Enter**.



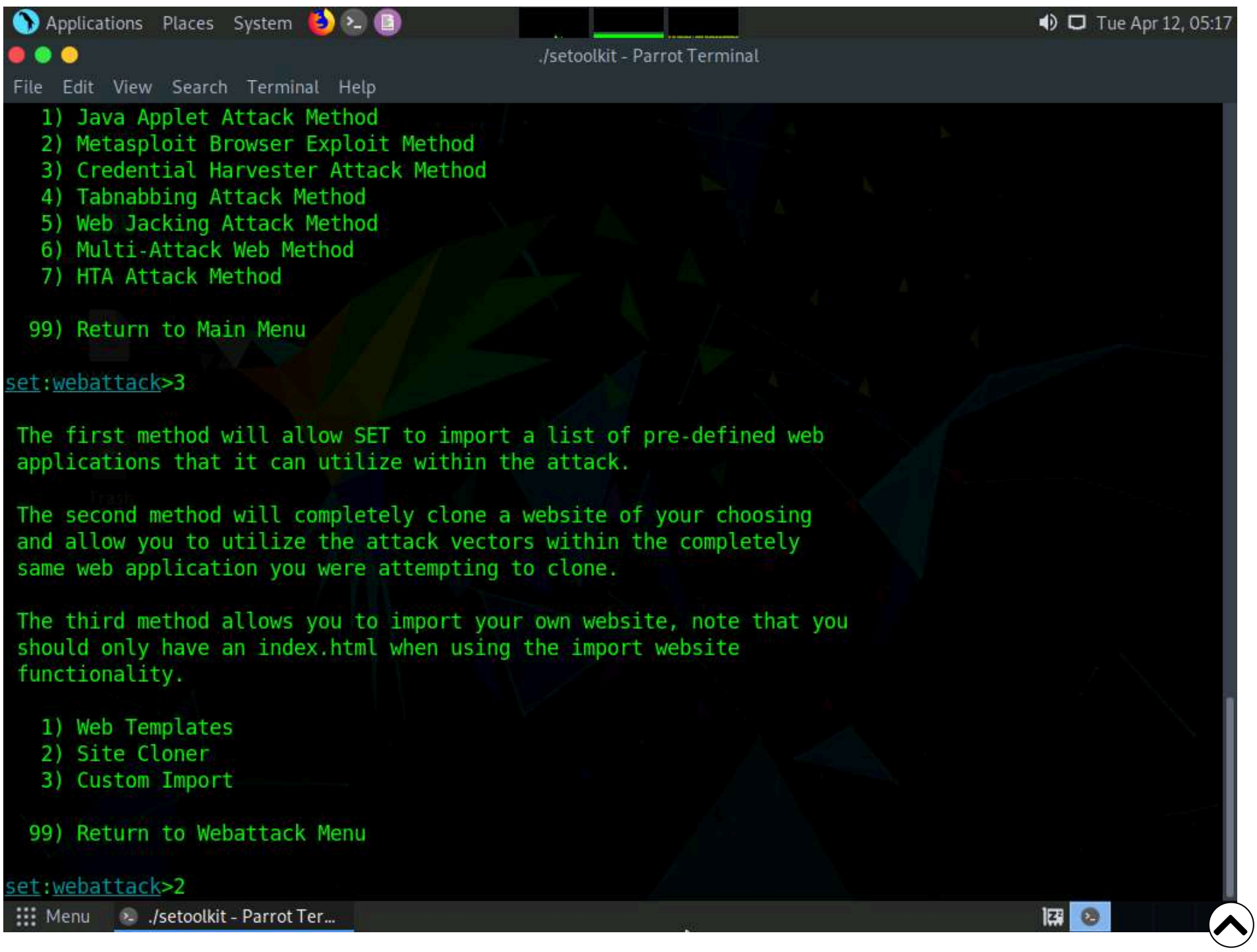
8. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors**.



9. A list of options in **Website Attack Vectors appears**; type **3** and press **Enter** to choose **Credential Harvester Attack Method**.



10. Type **2** and press **Enter** to choose **Site Cloner** from the menu.

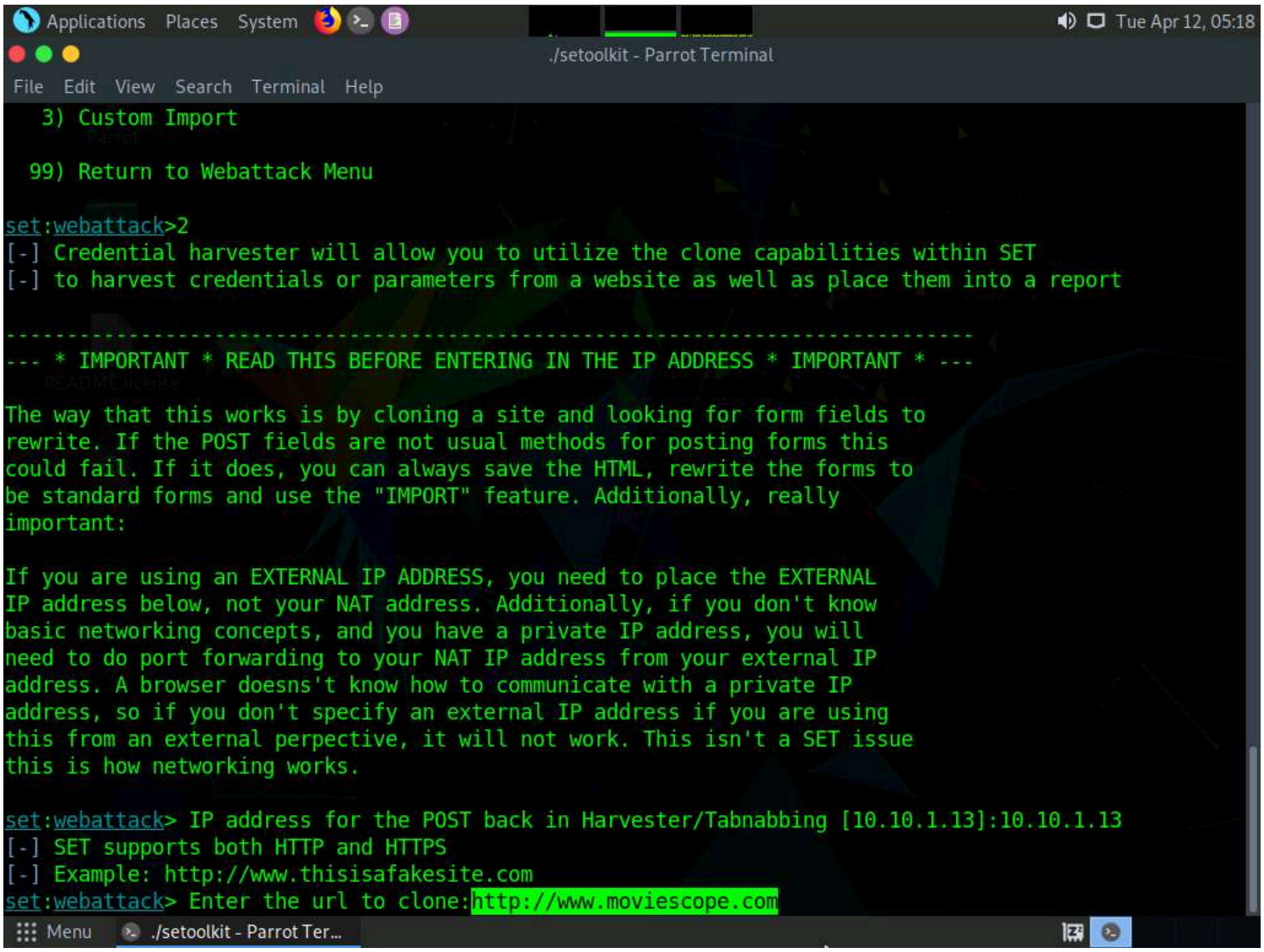


11. Type the IP address of the local machine (**10.10.1.13**) in the prompt for "**IP address for the POST back in Harvester/Tabnabbing**" and press **Enter**.

> Note: In this case, we are targeting the **Parrot Security** machine (IP address: **10.10.1.13**).

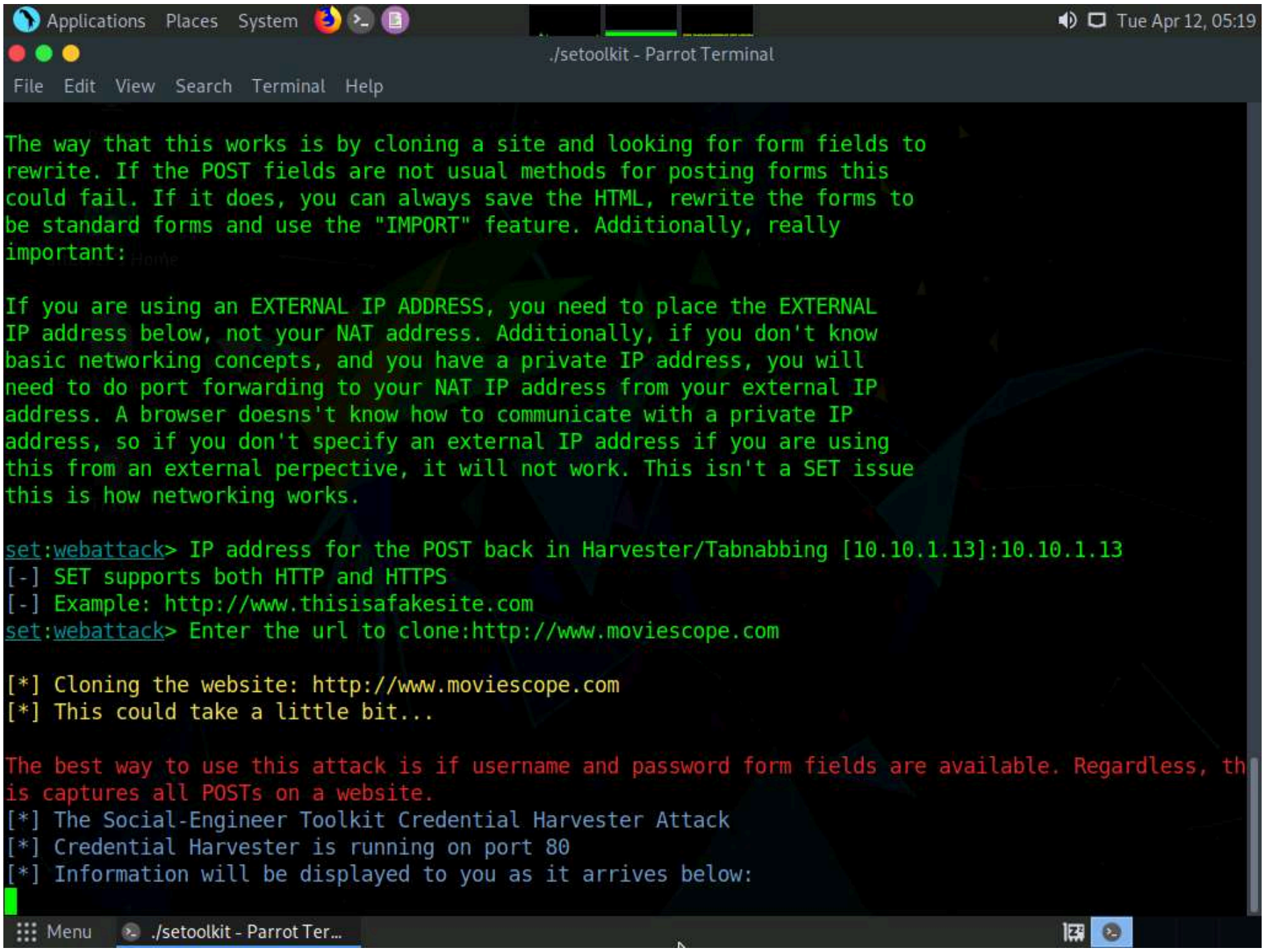
12. Now, you will be prompted for the URL to be cloned; type the desired URL in "**Enter the url to clone**" and press **Enter**. In this task, we will clone the URL **http://www.moviescope.com**.

> Note: You can clone any URL of your choice.



13. If a message appears that reads **Press {return} if you understand what we're saying here**, press **Enter**.

14. After cloning is completed, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.



15. Having successfully cloned a website, you must now send the IP address of your **Parrot Security** machine to a victim and try to trick him/her into clicking on the link.

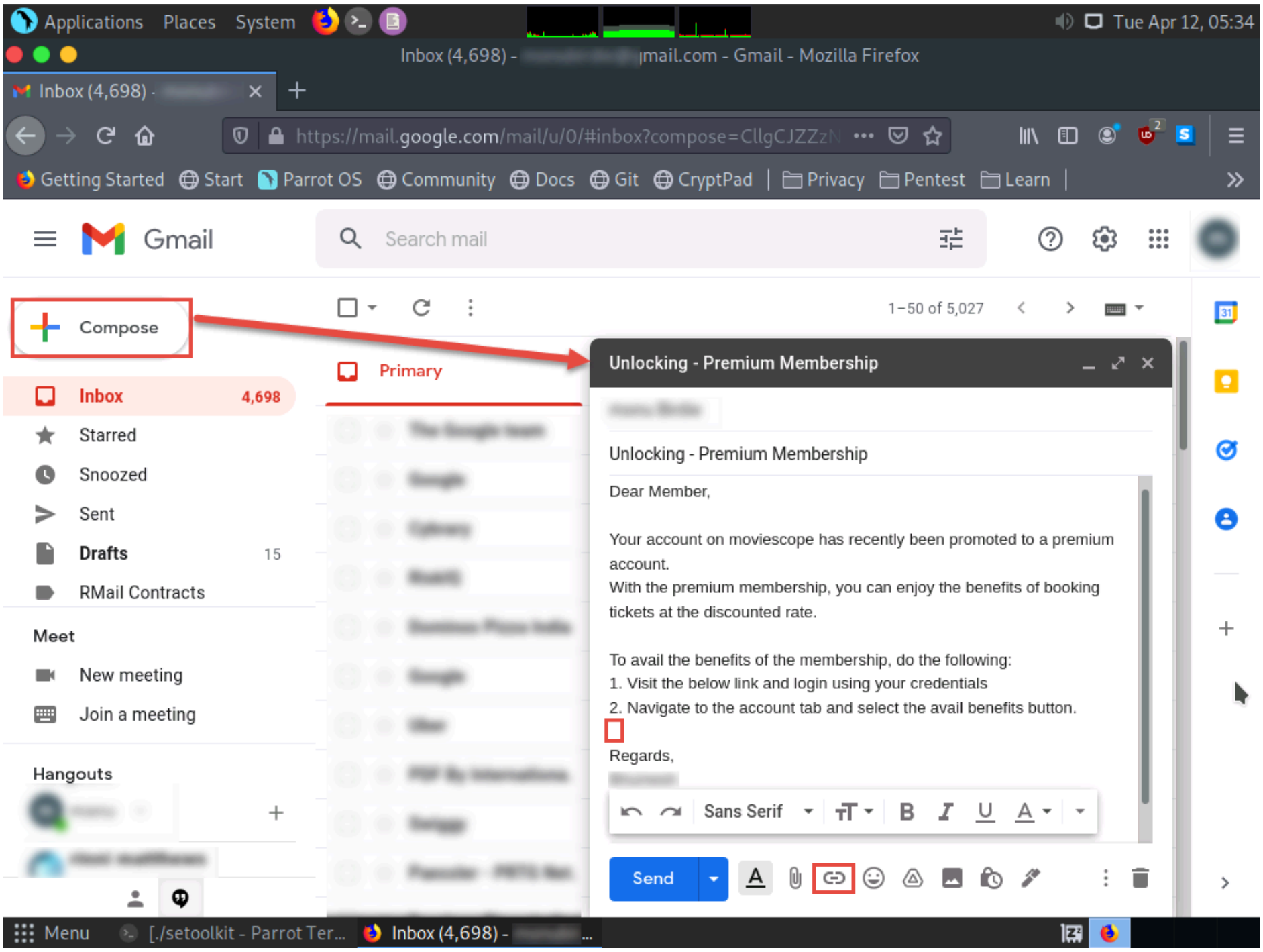
16. Click **Firefox** icon from the top-section of the **Desktop** to launch a web browser window and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively). Log in, and compose an email.

> Note: You can log in to any email account of your choice.

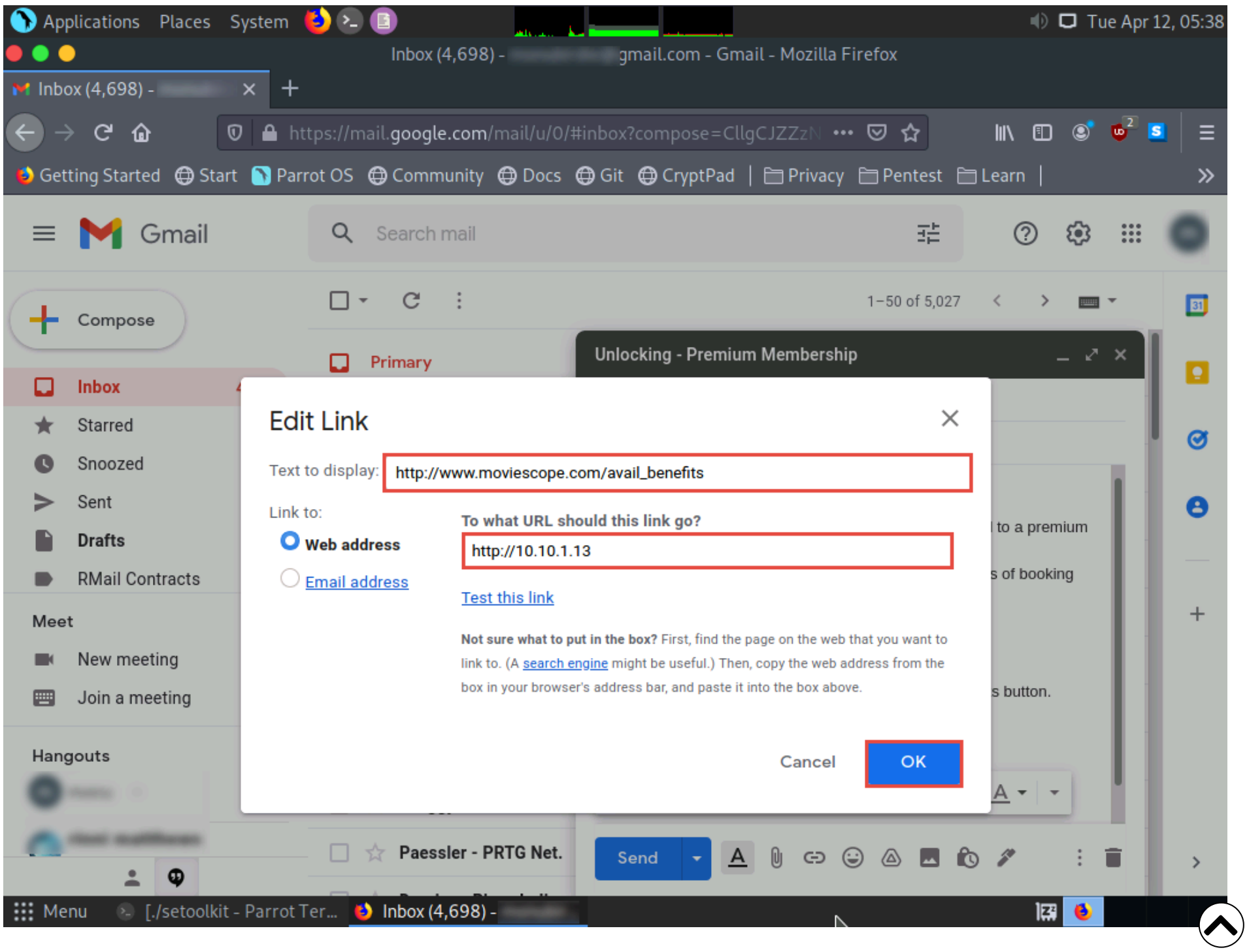
17. After logging into your email account, click the **Compose** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

> Note: A good way to conceal a malicious link in a message is to insert text that looks like a legitimate MovieScope URL (in this case), but that actually links to your malicious cloned MovieScope page.

18. Position the cursor just above Regards to place the fake URL, then click the **Insert link** icon.

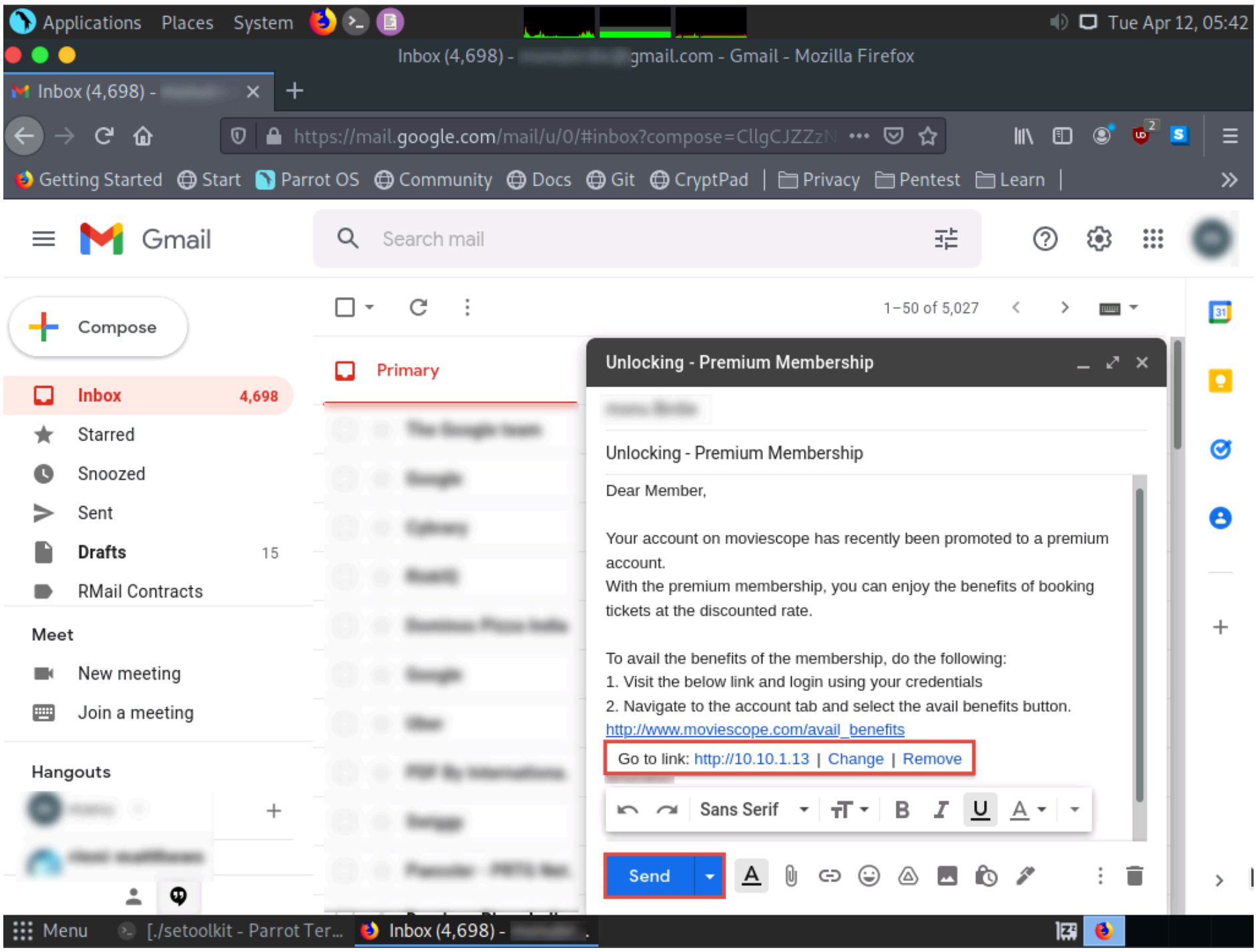


19. In the **Edit Link** window, first type the actual address of your cloned site in the **Web address** field under the **Link to** section. Then, type the fake URL in the **Text to display** field. In this case, the actual address of our cloned MovieScope site is **http://10.10.1.13**, and the text that will be displayed in the message is **http://www.moviescope.com/avail_benefits**; click **OK**.



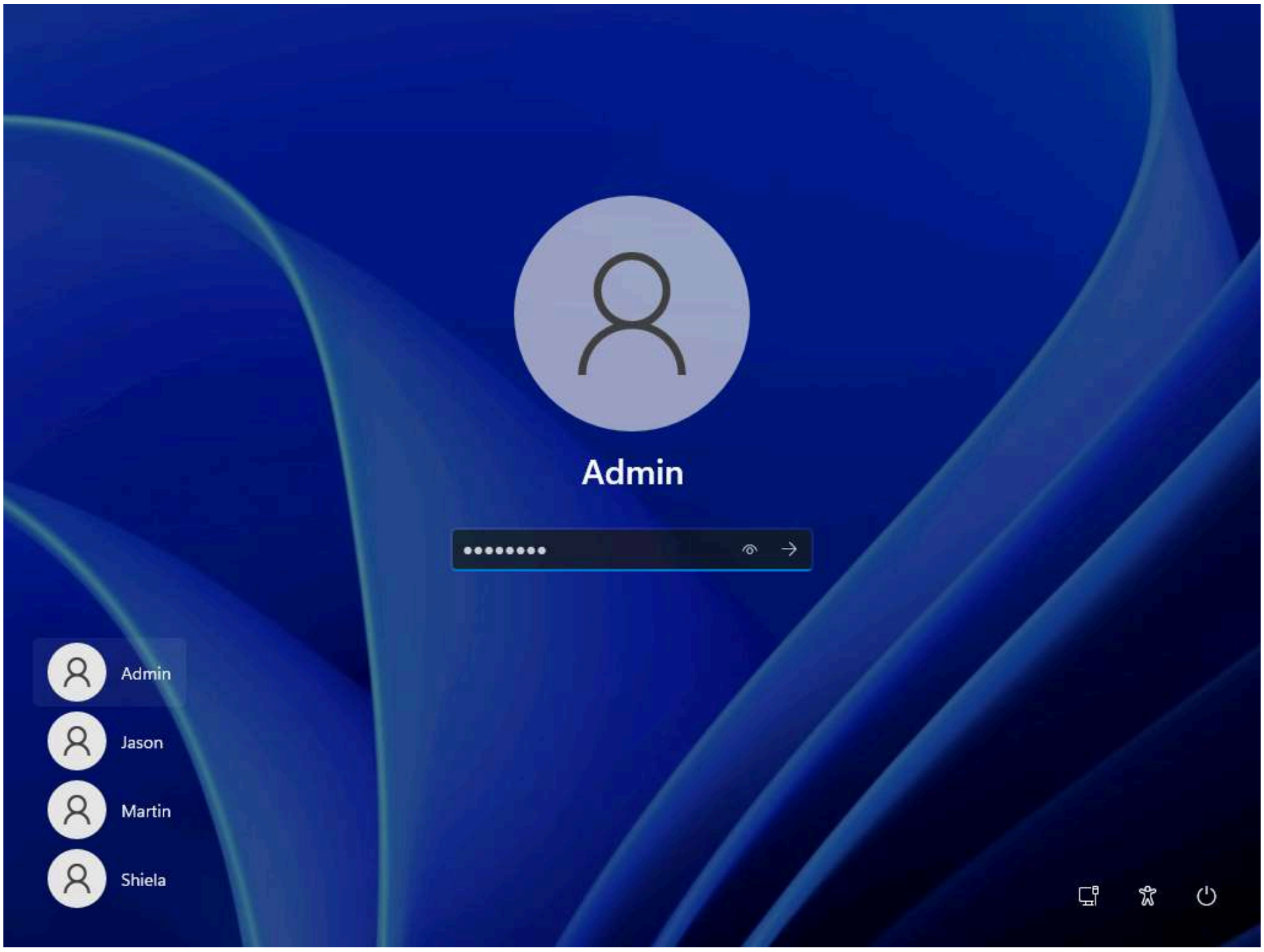
20. The fake URL should appear in the message body, as shown in the screenshot.

21. Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "**Go to link**" pop-up. Once verified, send the email to the intended user.

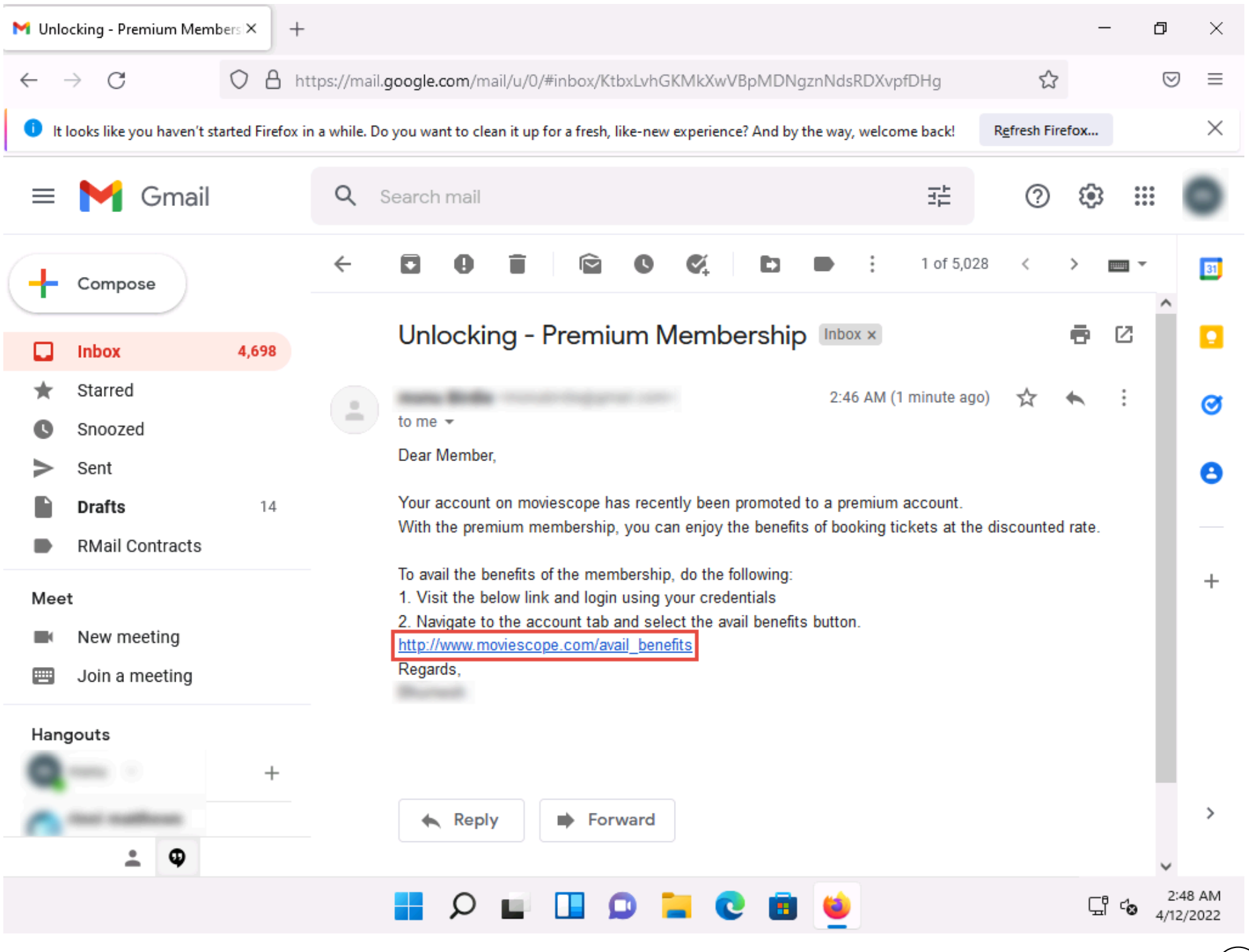


22. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine and click **Ctrl+Alt+Del**. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.

> Note: If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.
>
> Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

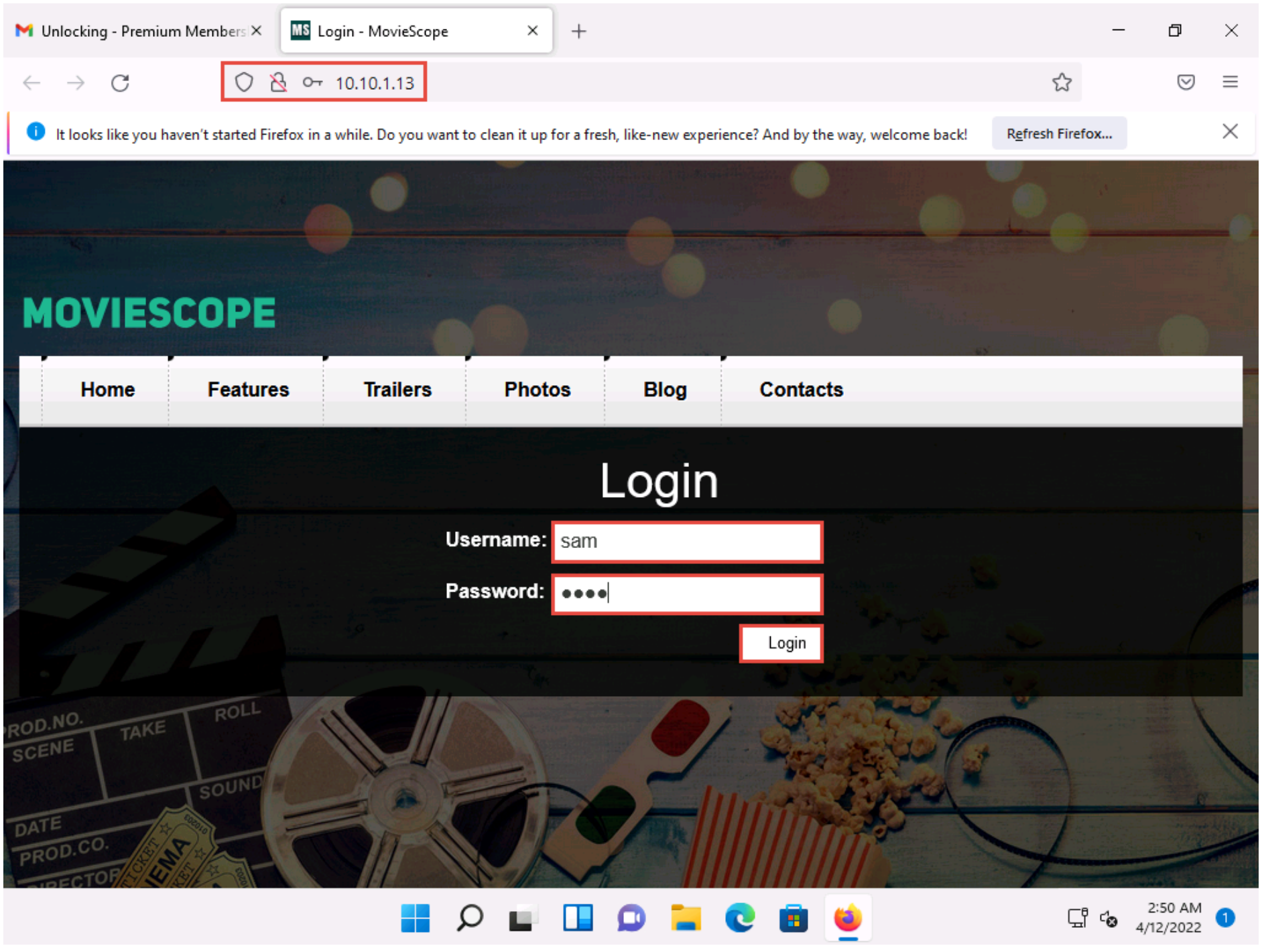


23. Open any web browser (here, we are using **Mozilla Firefox**), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.

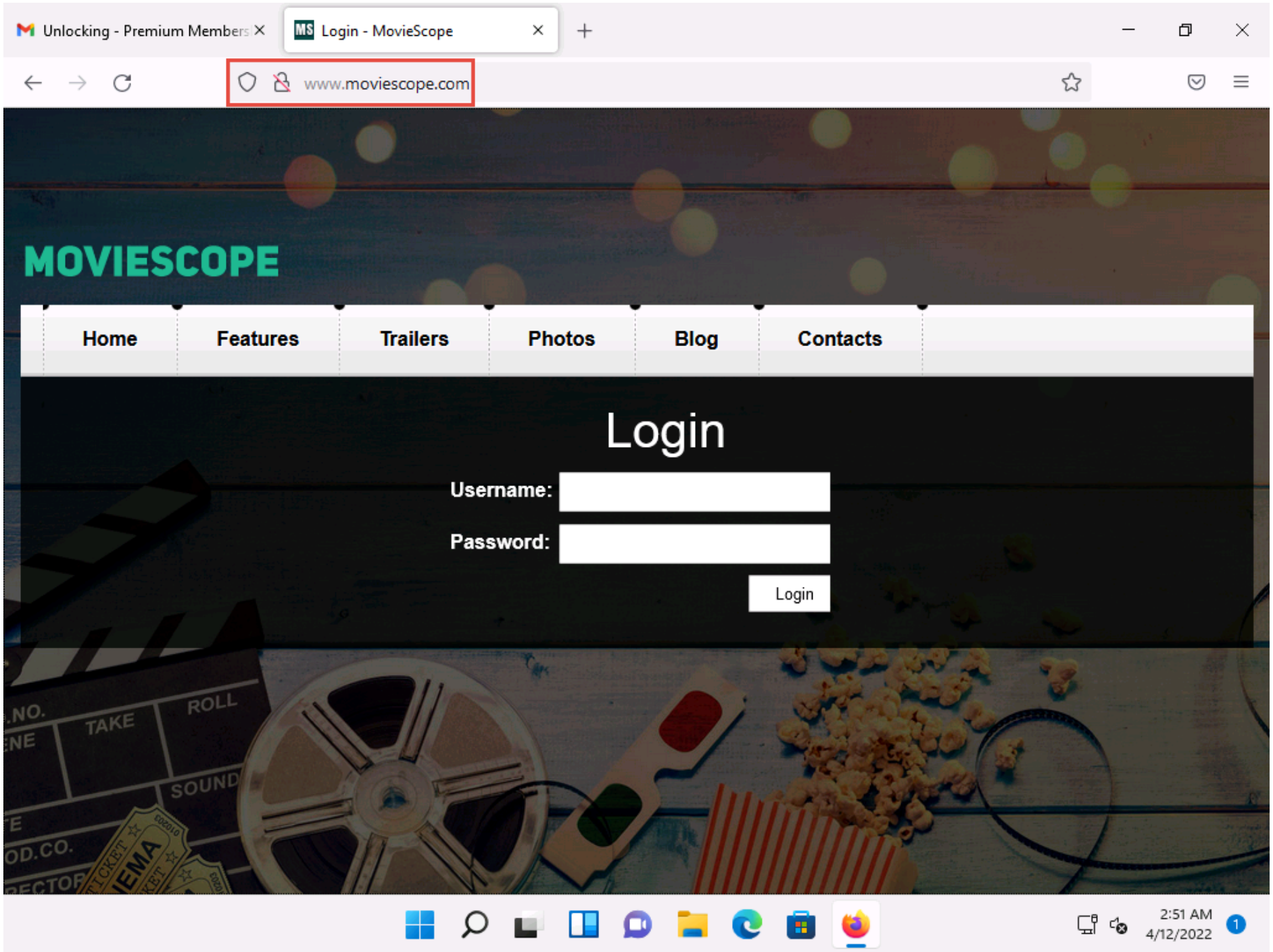


24. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of **www.moviescope.com**.

25. The victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, he/she will be redirected to the legitimate **MovieScope** login page. Note the different URLs in the browser address bar for the cloned and real sites.



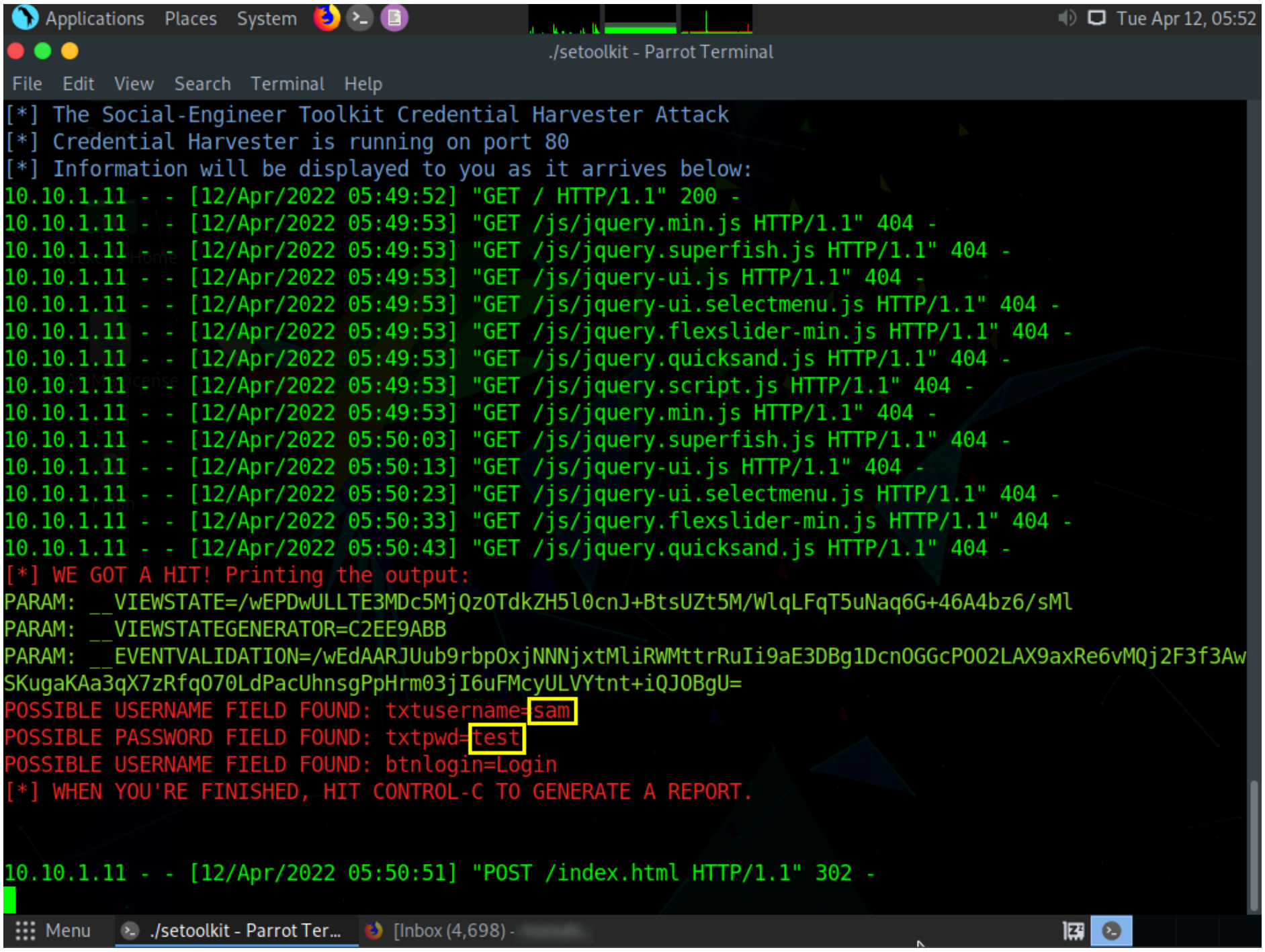
Note: If save credentials notification appears, click **Don't Save**.



26. Now, click **CEHv12 Parrot Security** to switch back to the **Parrot Security** machine and switch to the **terminal** window.

27. As soon as the victim types in his/her **Username** and **Password** and clicks **Login**, **SET** extracts the typed credentials. These can now be used by the attacker to gain unauthorized access to the victim's account.

28. Scroll down to find **Username** and **Password** displayed in plain text, as shown in the screenshot.



29. This concludes the demonstration of phishing user credentials using the SET.

30. Close all open windows and document all the acquired information.

Lab 2: Detect a Phishing Attack

Lab Scenario

With the tremendous increase in the use of online banking, online shares trading, and e-commerce, there has been a corresponding growth in incidents of phishing being used to carry out financial fraud.

As a professional ethical hacker or penetration tester, you must be aware of any phishing attacks that occur on the network and implement anti-phishing measures. Be warned, however, that even if you employ the most sophisticated and expensive technological solutions, these can all be bypassed and compromised if employees fall for simple social engineering scams.

The success of phishing scams is often due to users' lack of knowledge, being visually deceived, and not paying attention to security indicators. It is therefore imperative that all people in your organization are properly trained to recognize and respond to phishing attacks. It is your responsibility to educate employees about best practices for protecting systems and information.

In this lab, you will learn how to detect phishing attempts using various phishing detection tools.

Lab Objectives

- Detect phishing using Netcraft
- Detect phishing using PhishTank

Overview of Detecting Phishing Attempts

Phishing attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much like the other kinds of attacks used to extract a company's valuable data. To guard against phishing attacks, a company needs to evaluate the risk of different kinds of attacks, estimate possible losses and spread awareness among its employees.

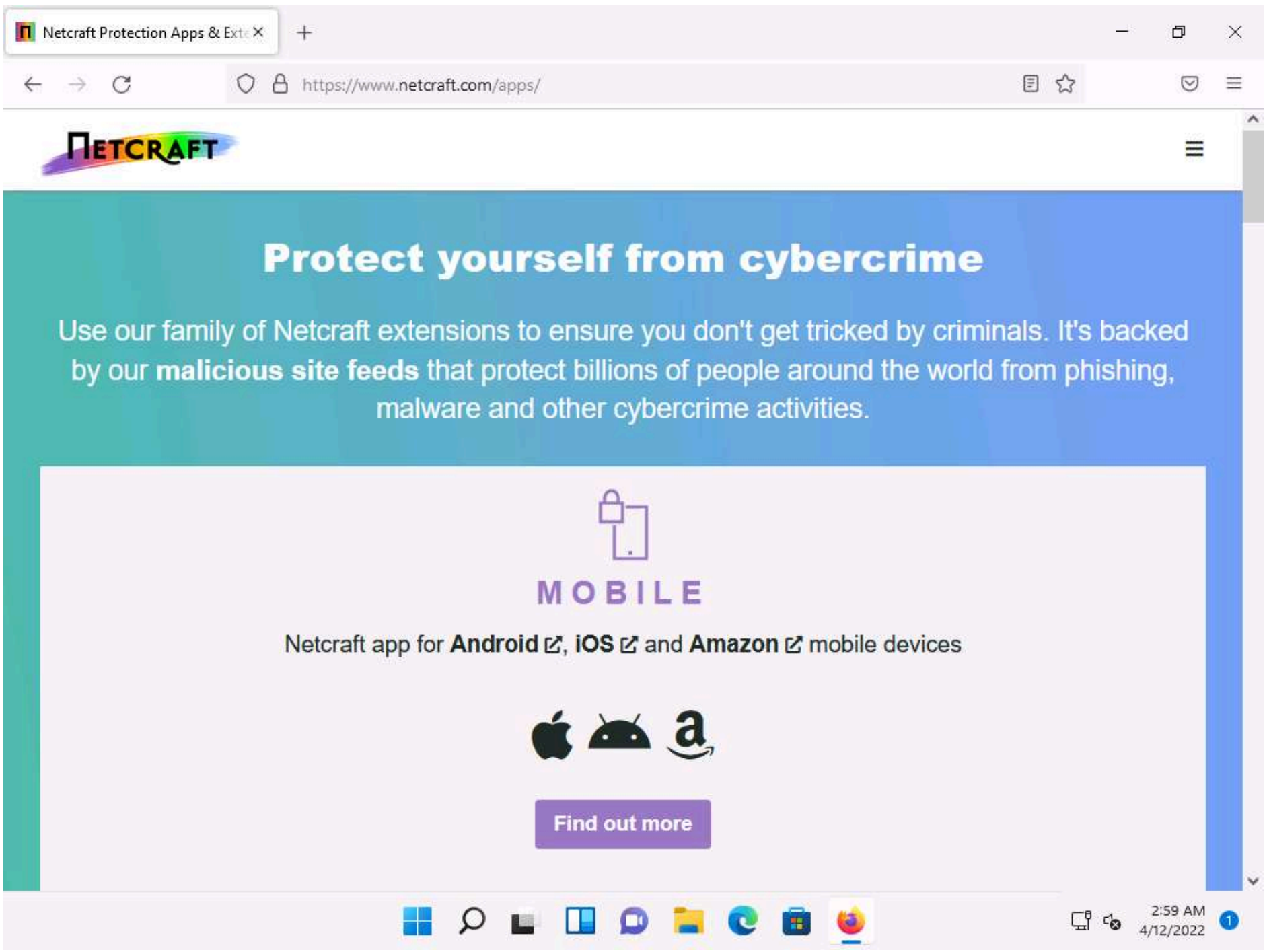
Task 1: Detect Phishing using Netcraft

The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks. The Netcraft Extension provides updated and extensive information about sites that users visit regularly; it also blocks dangerous sites. This information helps users to make an informed choice about the integrity of those sites.

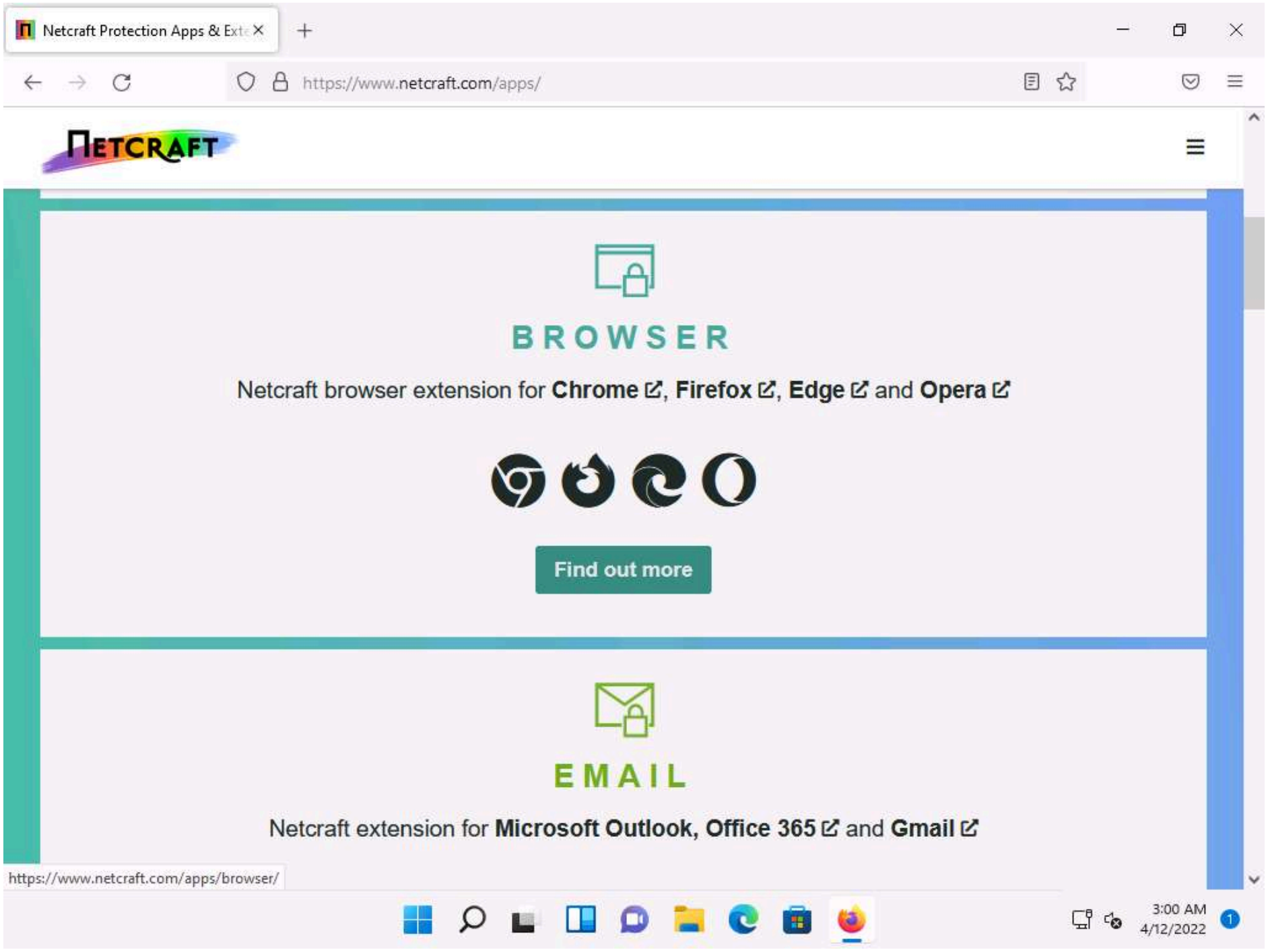
Here, we will use the Netcraft Extension to detect phishing sites.

1. Click on the **CEHv12 Windows 11** to switch to the **Windows 11** machine.
2. First, it is necessary to install the Netcraft extension. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **https://www.netcraft.com/apps/** and press **Enter**.
3. The **Netcraft** website appears, as shown in the screenshot.

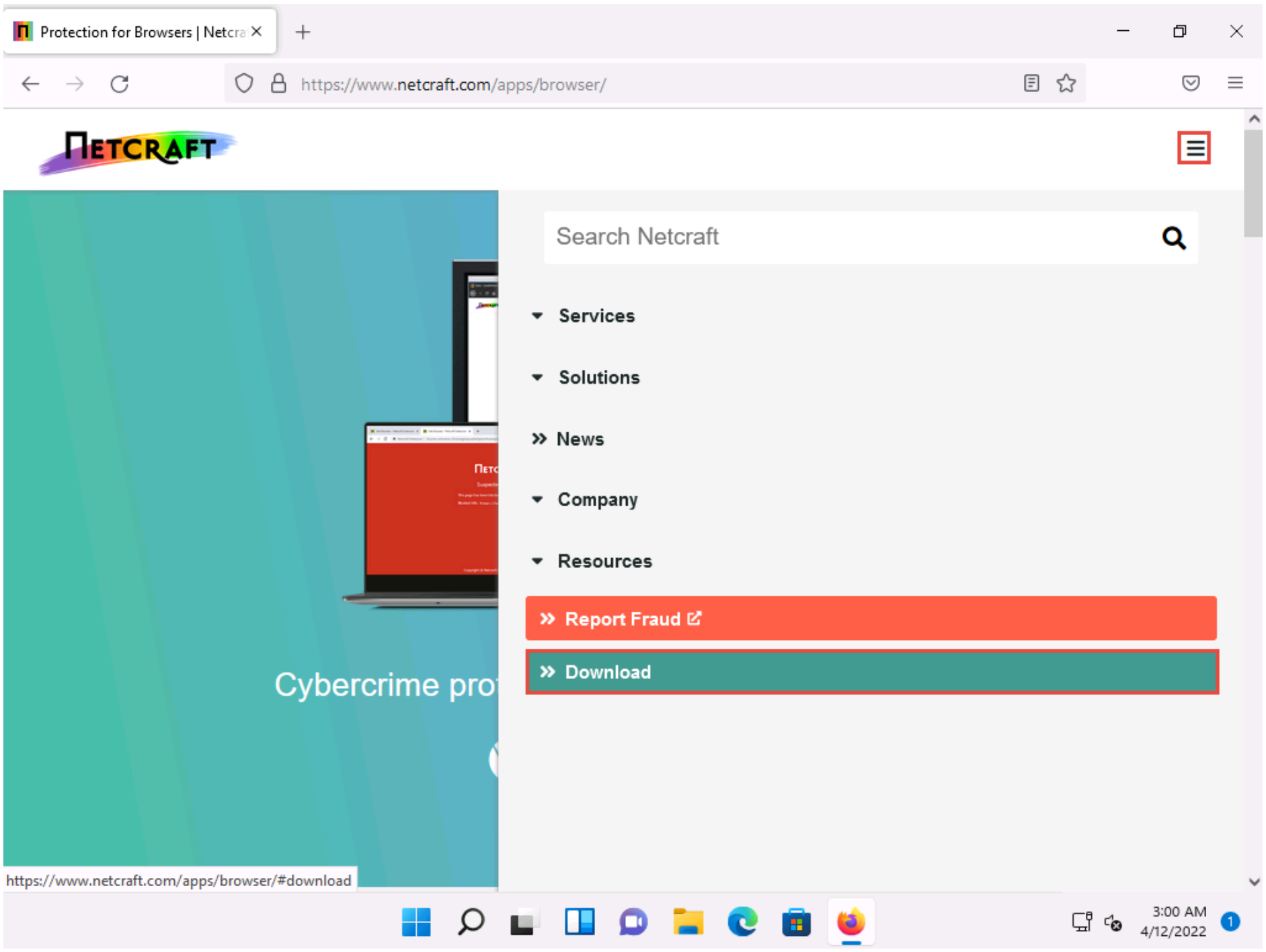
> Note: Click **Accept** in the cookie notification in the lower section of the browser.



4. Scroll-down and click **Find out more** button under **BROWSER** option on the webpage.

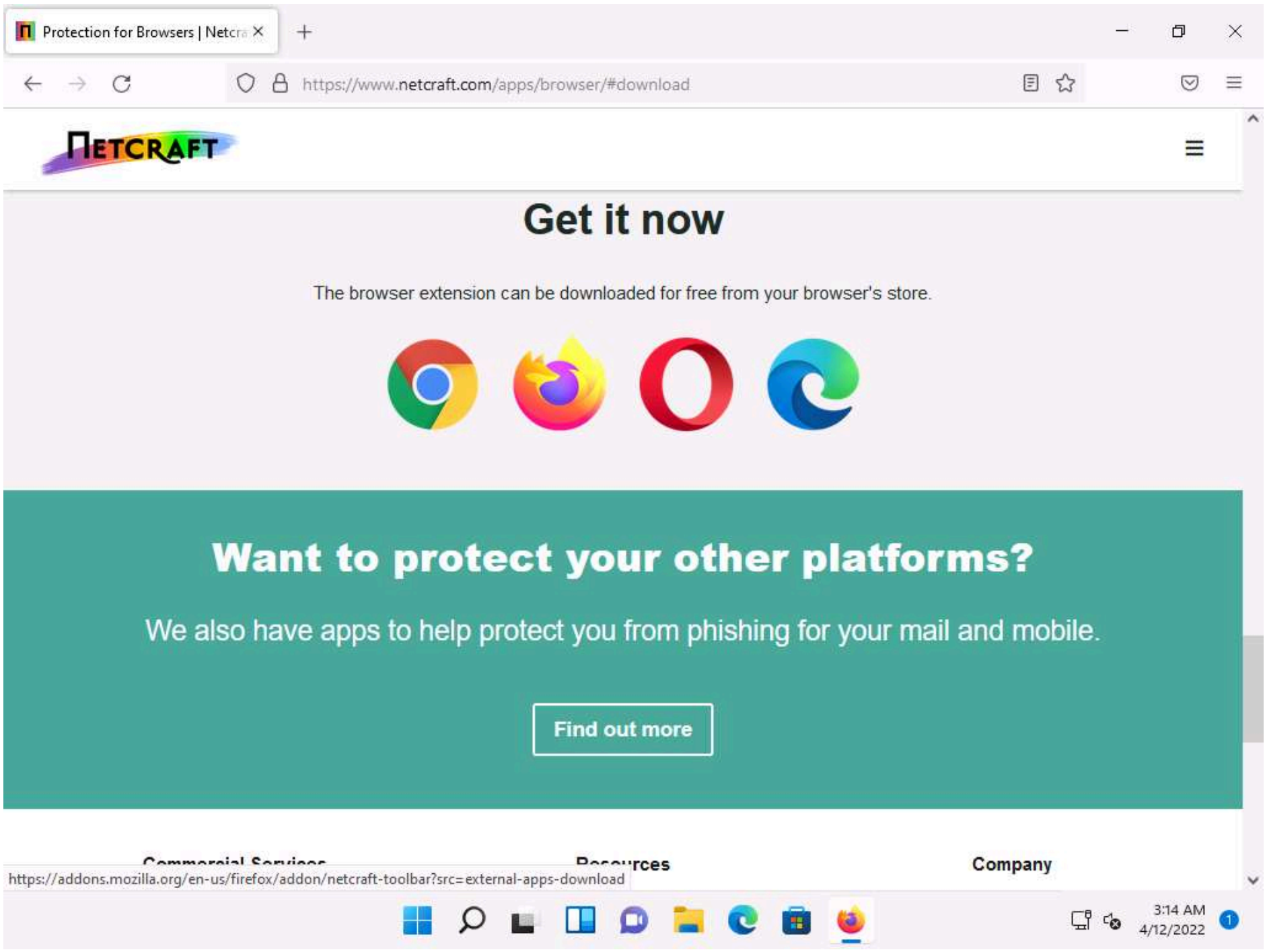


5. Click ellipses icon (☰) from the top-right corner of the webpage and click **Download** button.

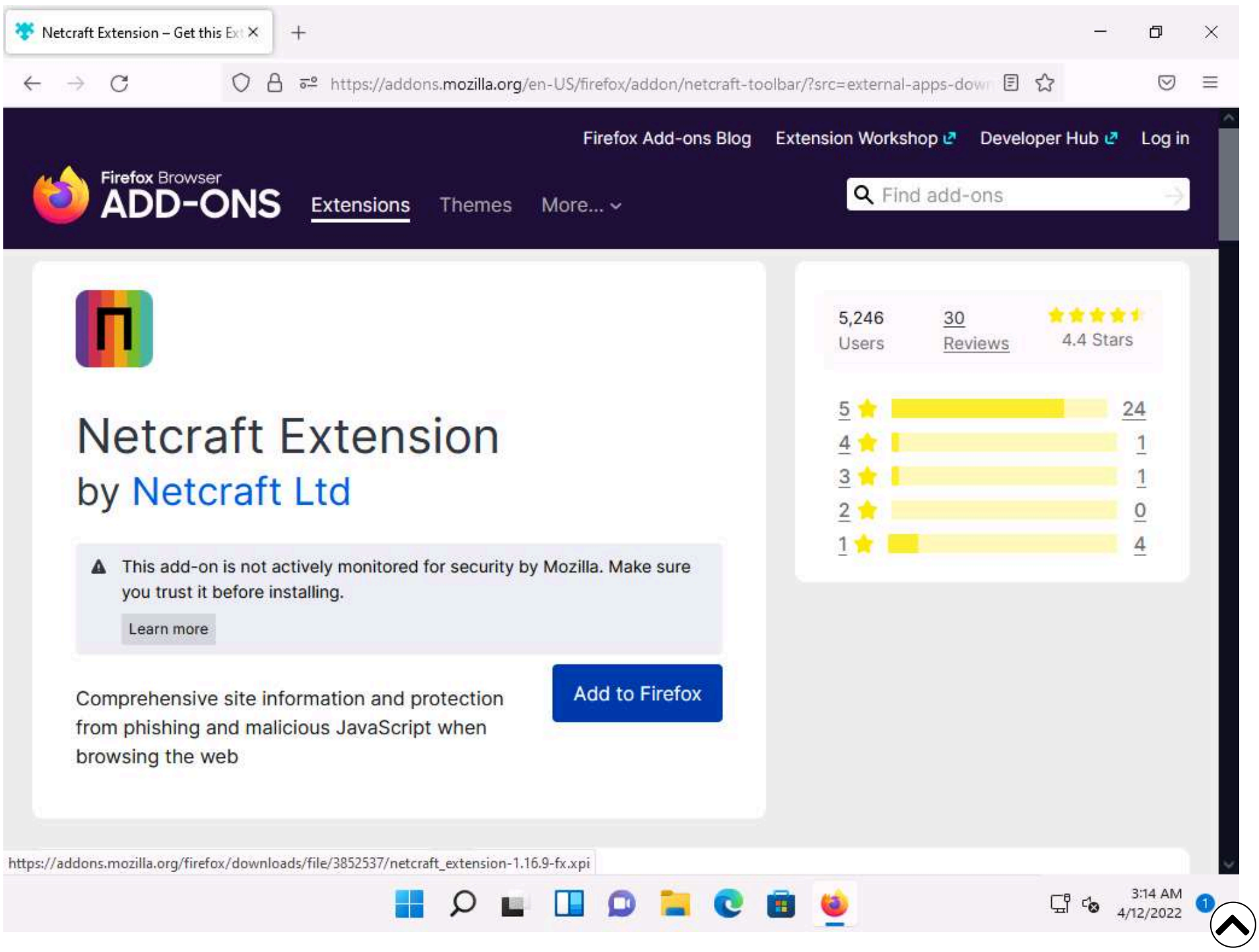


6. Click ellipses icon (☰) again to close the menu.

7. You will be directed to the **Get it now** section; click the **Firefox** browser icon.

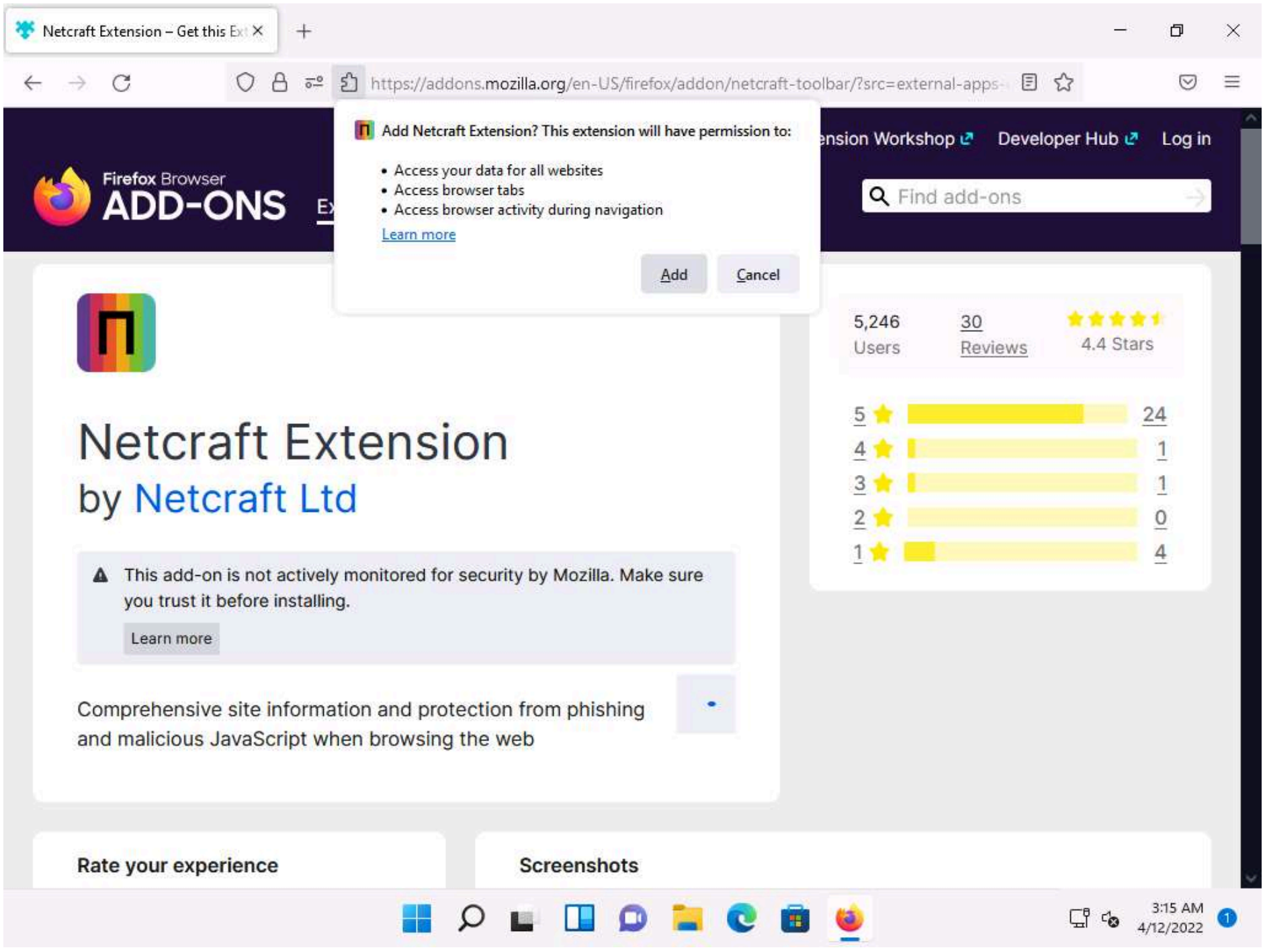


8. On the next page, click the **Add to Firefox** button to install the Netcraft extension.



9. When the **Add Netcraft Extension?** notification pop-up appears on top of the window, click **Add**.

Note: If the **Netcraft Extension has been added to Firefox** pop-up appears in the top section of the browser, click **Okay**.

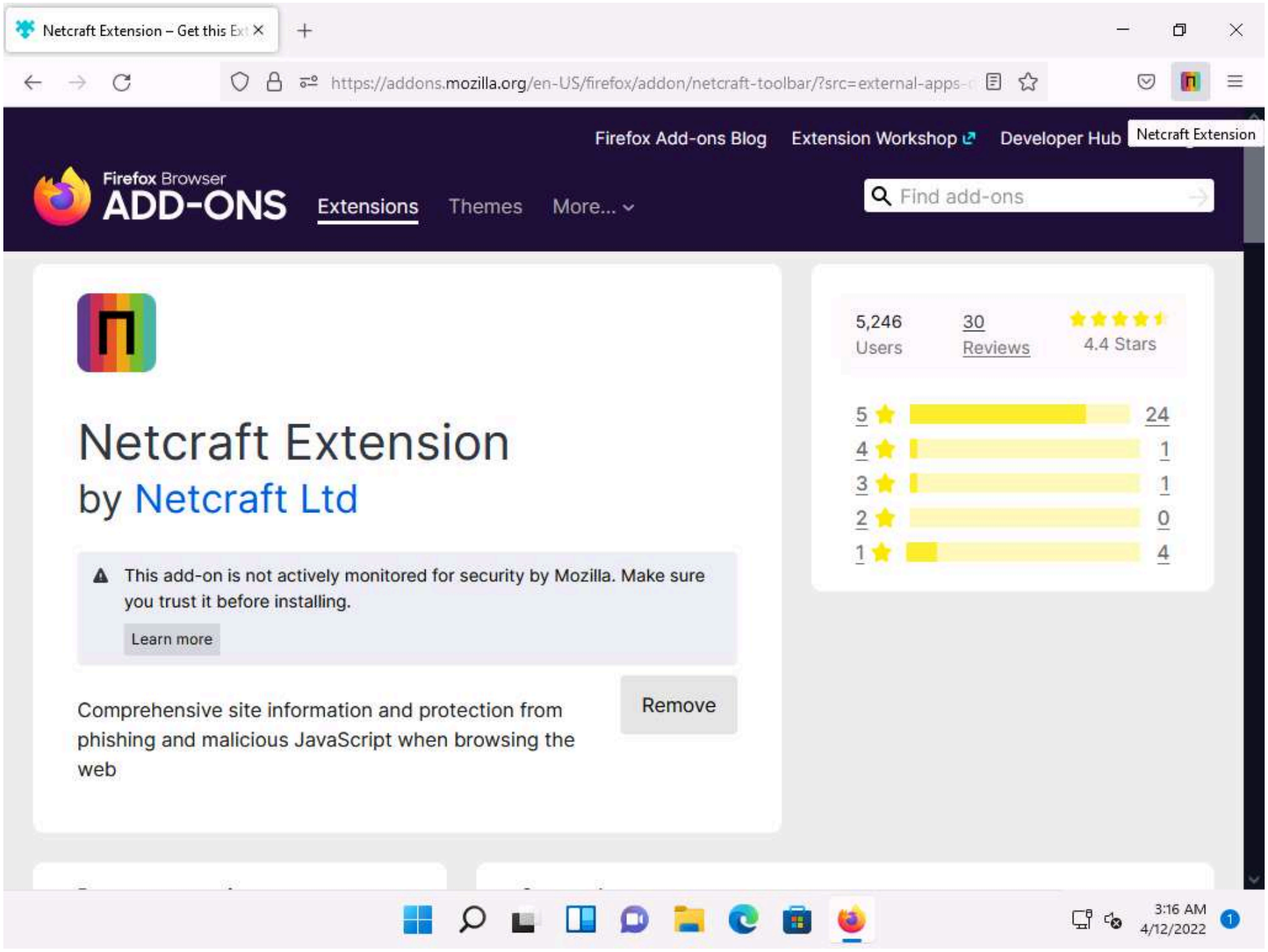


10. After the installation finishes, you may be asked to restart the browser. If so, click **Restart Now**.

11. If **Netcraft Extension has been added to Firefox** notification appears, click **Okay**, **Got it**.

12. The **Netcraft Extension** icon now appears on the top-right corner of the browser, as shown in the screenshot.

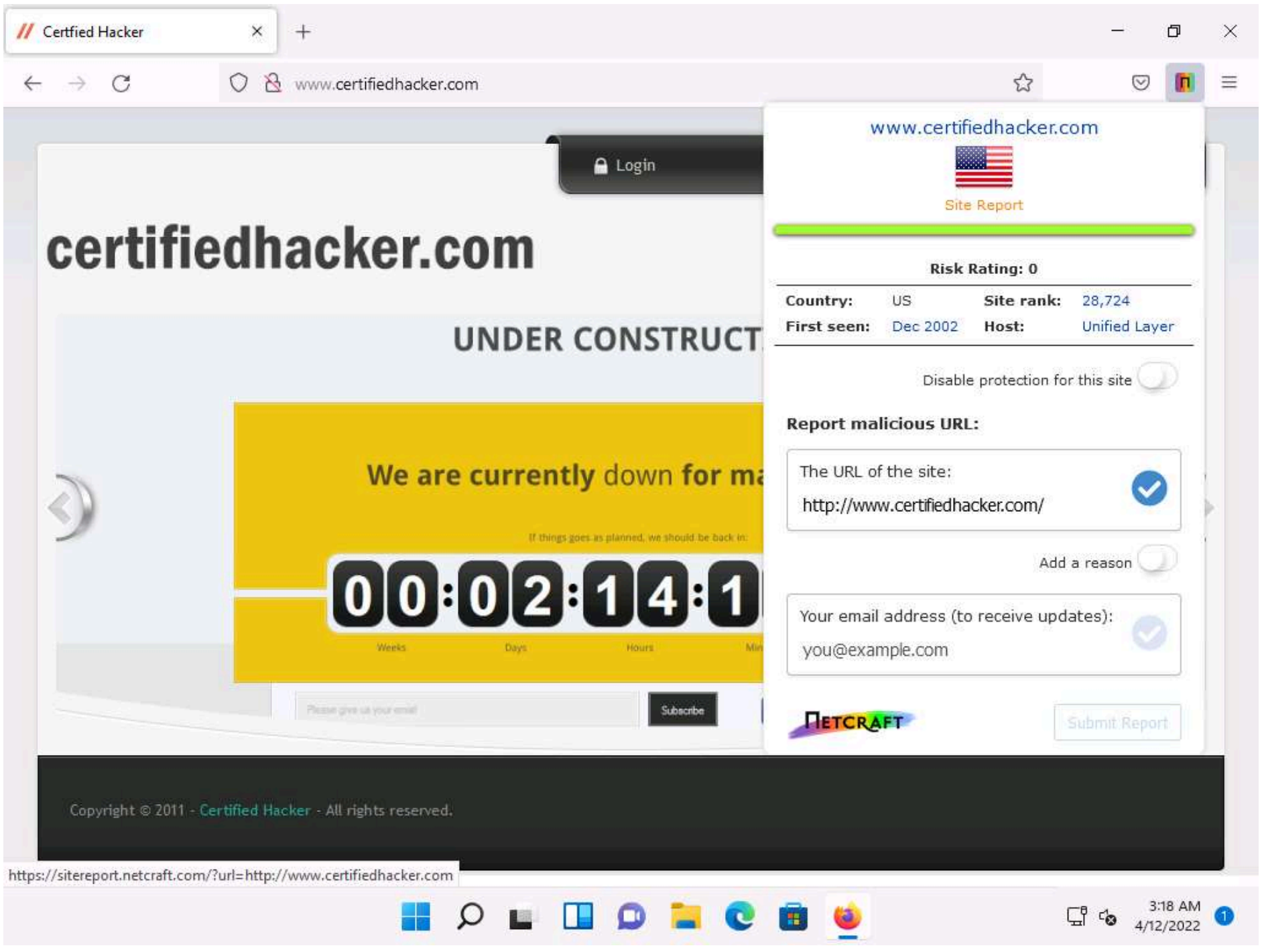
Note: Screenshots may differ with newer versions of Firefox.



13. Now, In the address bar of the browser place your mouse cursor, type **http://www.certifiedhacker.com/** and press **Enter**.

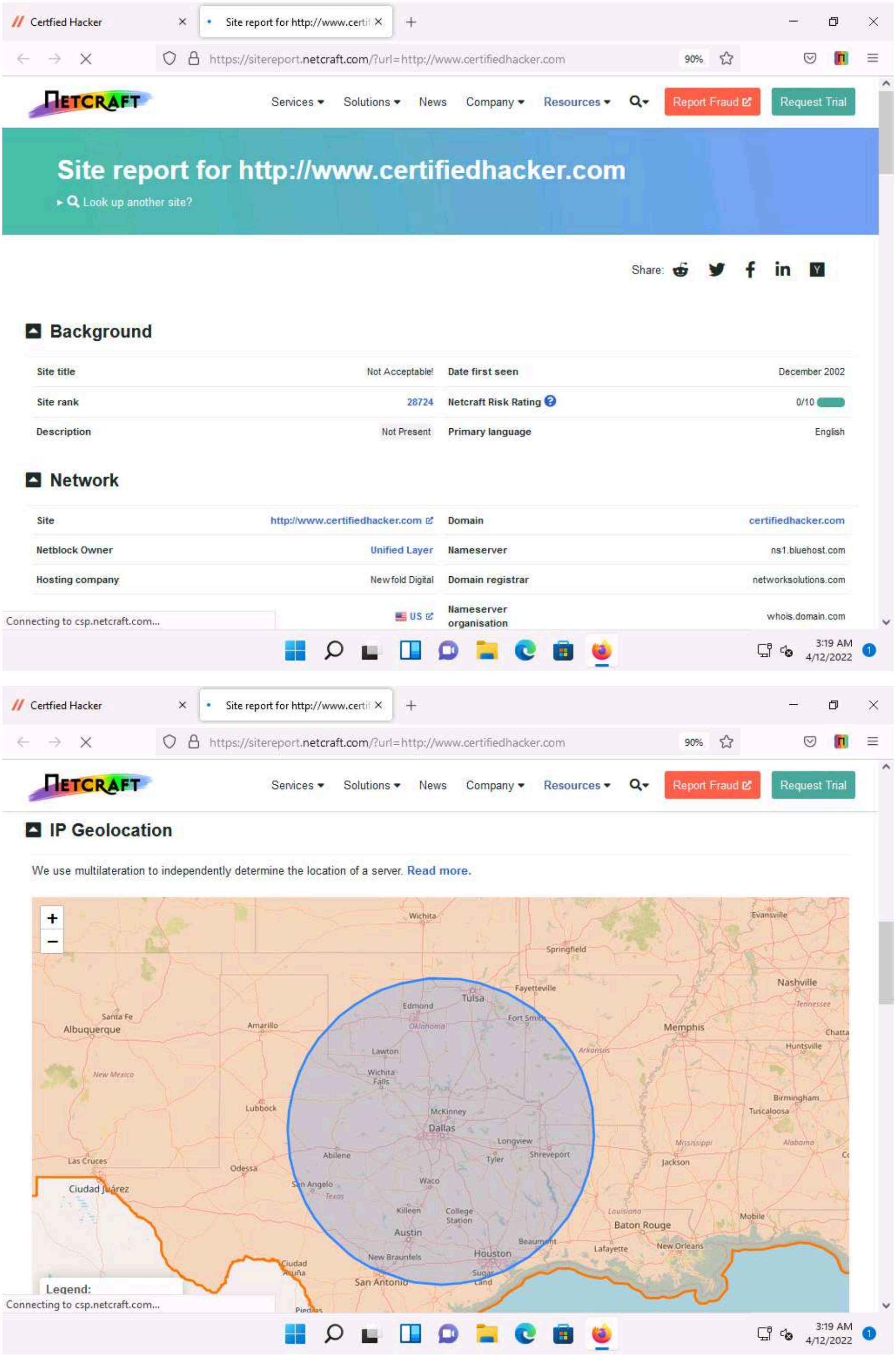
14. The **certifiedhacker.com ** webpage appears. Click the Netcraft **Extension** icon in the top-right corner of the browser. A dialog box appears, displaying a summary of information such as **Risk Rating**, **Site rank**, **First seen**, and **Host** about the searched website.

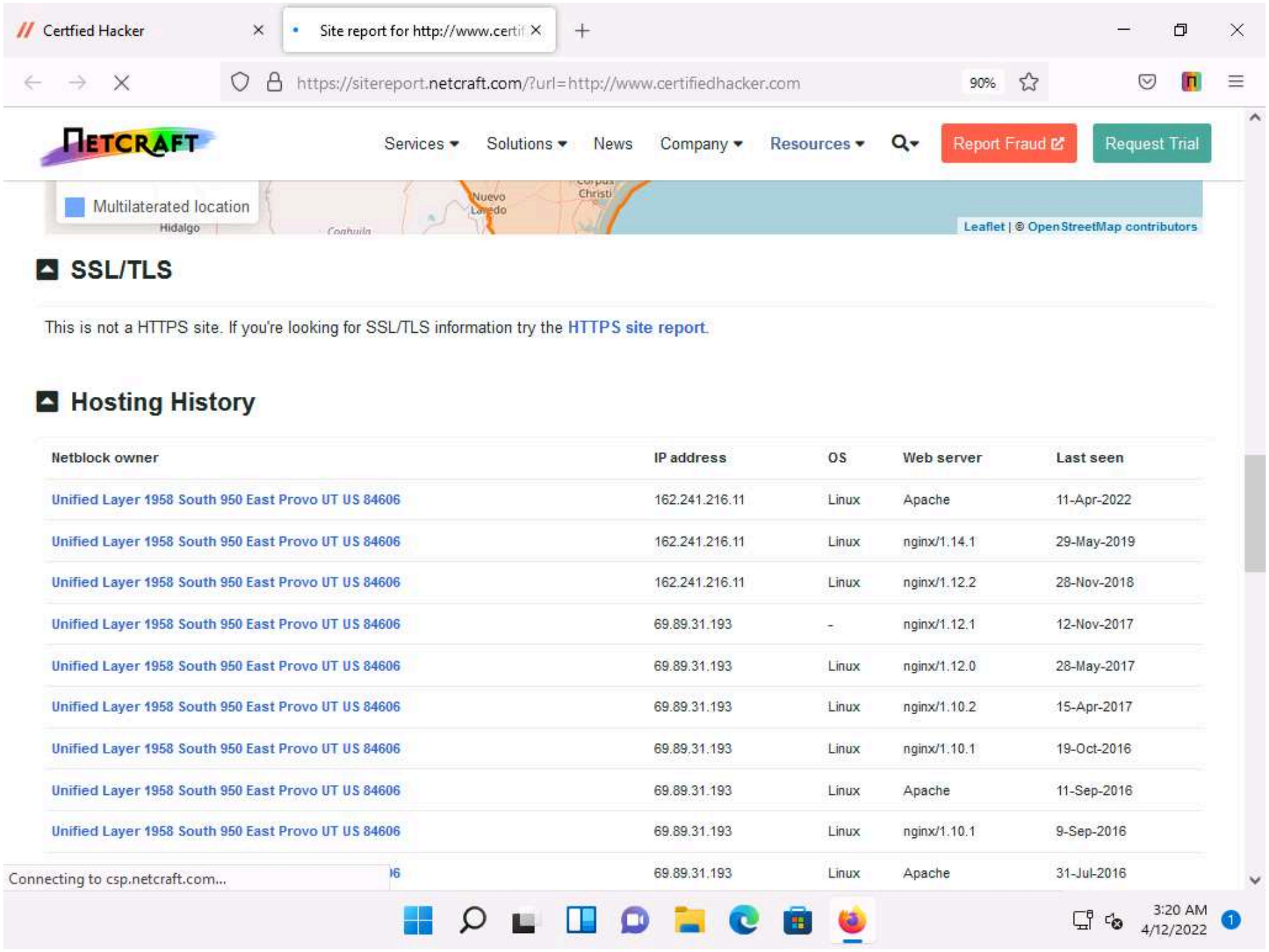
15. Now, click the **Site Report** link from the dialog-box to view a report of the site.



16. The **Site report for certifiedhacker.com** page appears, displaying detailed information about the site such as **Background, Network**, **IP Geolocation**, **SSL/TLS** and **Hosting History**

Note: If a **Site information not available** pop-up appears, ignore it.


Certfied Hacker
Site report for http://www.certif
https://sitereport.netcraft.com/?url=http://www.certifiedhacker.com
90%
NETCRAFT
Services
Solutions
News
Company
Resources
Report Fraud
Request Trial
Site report for http://www.certifiedhacker.com
Look up another site?
Share:
Background
Site title
Not Acceptable!
Date first seen
December 2002
Site rank
28724
Netcraft Risk Rating
0/10
Description
Not Present
Primary language
English
Network
Site
http://www.certifiedhacker.com
Domain
certifiedhacker.com
Netblock Owner
Unified Layer
Nameserver
ns1.bluehost.com
Hosting company
Newfold Digital
Domain registrar
networksolutions.com
US
Nameserver organisation
whois.domain.com
Connecting to csp.netcraft.com...
3:19 AM
4/12/2022
IP Geolocation
We use multilateration to independently determine the location of a server. Read more.
Wichita
Evansville
Springfield
Nashville
Fayetteville
Tulsa
Edmond
Oklahoma
Fort Smith
Santa Fe
Albuquerque
Amarillo
Memphis
Tennessee
Lawton
Arkansas
Huntsville
New Mexico
Wichita Falls
Lubbock
McKinney
Dallas
Birmingham
Tuscaloosa
Longview
Mississippi
Alabama
Abilene
Tyler
Shreveport
Las Cruces
Odessa
Jackson
San Angelo
Waco
Ciudad Juárez
Texas
Killeen
College Station
Louisiana
Baton Rouge
Mobile
Austin
Beaumont
Lafayette
New Orleans
Houston
New Braunfels
Ciudad Acuña
Sugar Land
San Antonio
Legend:



17. 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**.

18. Now, in the browser window open a new tab, type **https://sfrclients.ml/** and press **Enter**.

> Note: Here, for demonstration purposes, we are using **https://sfrclients.ml/** phishing website to trigger Netcraft Extension to obtain desired results. You can use the same website or any other website to perform this task.

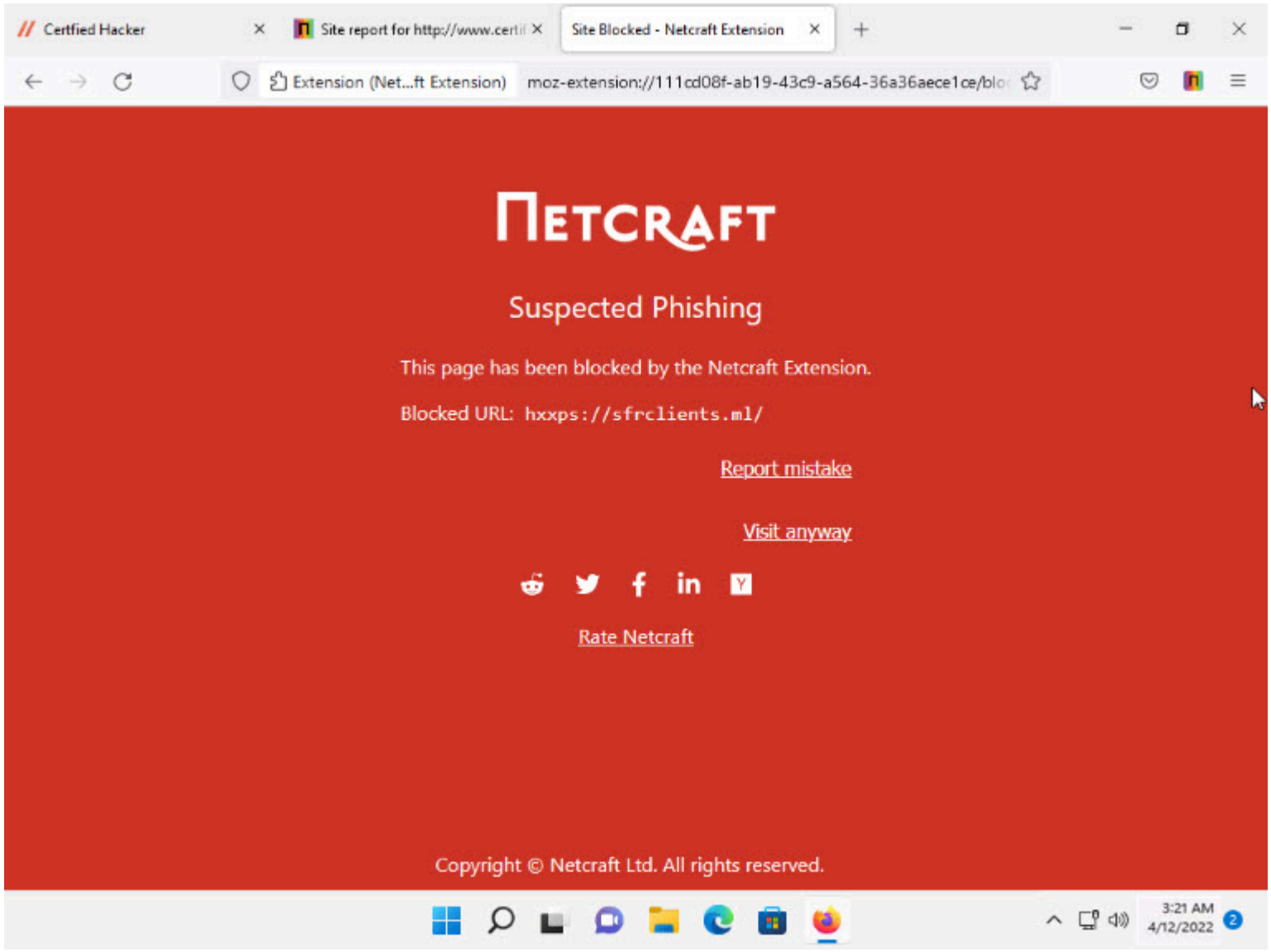
19. The Netcraft Extension automatically blocks phishing sites. However, if you trust the site, click **Visit anyway** to browse it; otherwise, click **Report mistake** to report an incorrectly blocked URL.

> Note: If you are getting an error in opening the website (**https://sfrclients.ml/**), try to open other phishing website.

OR

You will get a **Suspected Phishing** page in the **Firefox** browser.

> Note: If you get **Secure Connection Failed** webpage, then use some other phishing website to get the result, as shown in the screenshot.



20. This concludes the demonstration of detecting phishing using Netcraft Extension.
21. Close all open windows and document all the acquired information.

Task 2: Detect Phishing using PhishTank

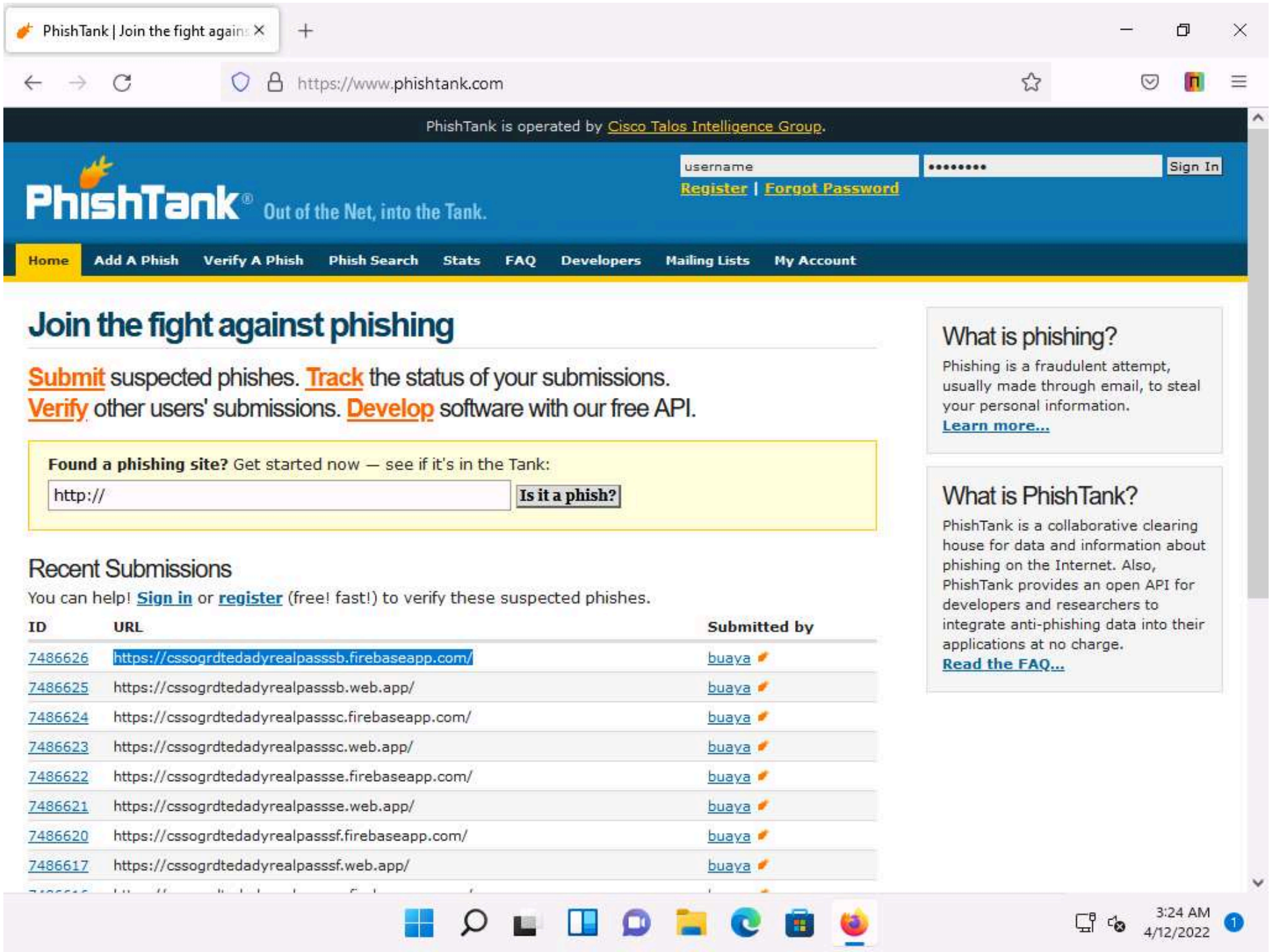
PhishTank is a free community site on which anyone can submit, verify, track, and share phishing data. As the official website notes, "it is a collaborative clearing house for data and information about phishing on the Internet." PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications.

In this task, we will use PhishTank to detect phishing.

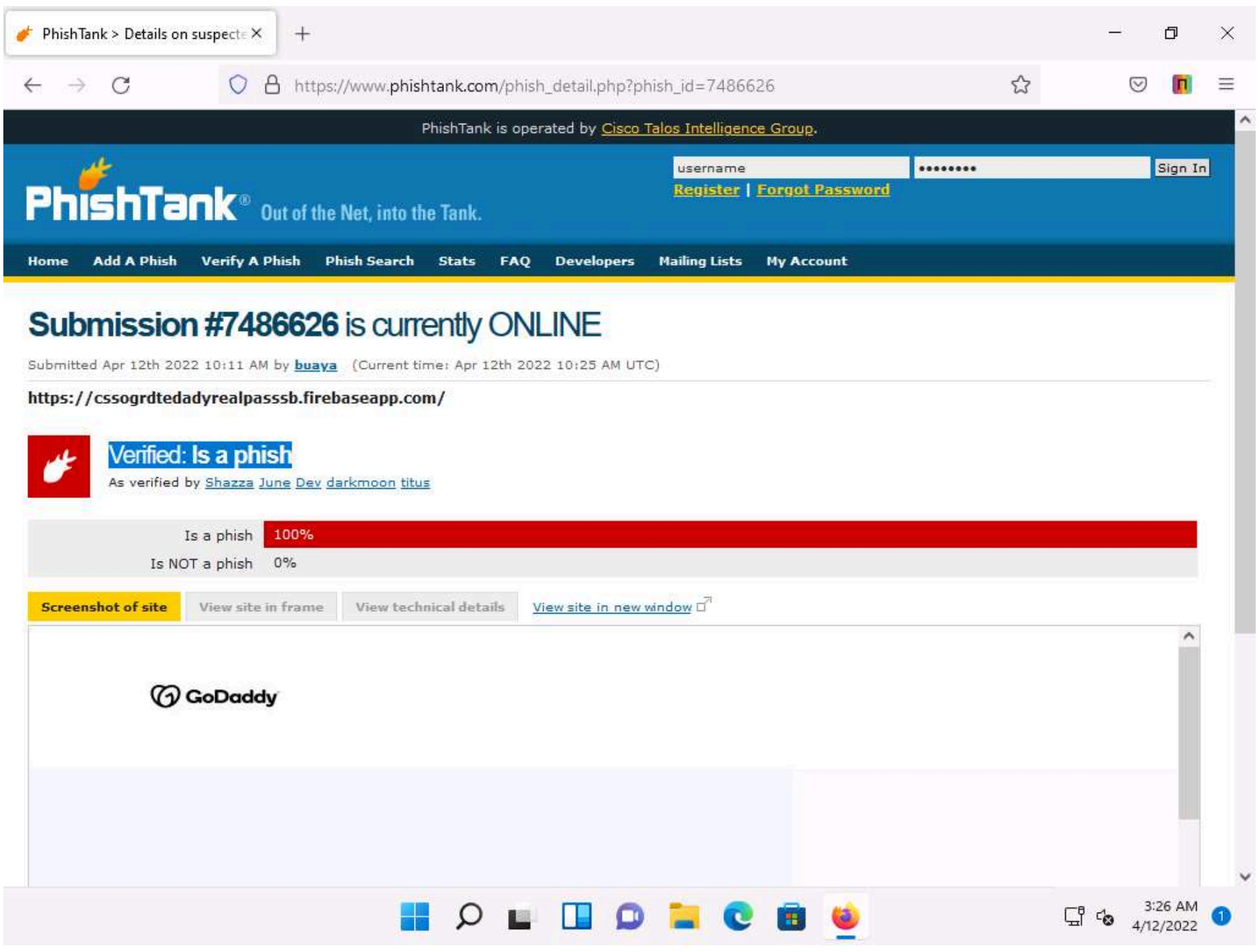
1. In the **Windows 11** machine, Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type **https://www.phishtank.com** and press **Enter**.
2. The **PhishTank** webpage appears, displaying a list of phishing websites under **Recent Submissions**.
3. Click on any phishing website **ID** in the **Recent Submissions** list (in this case, **7486626**) to view detailed information about it.

Note: If a notification appears asking **Would you like Firefox to save this login for phishtank.com?**, click **Don't Save**.

Note: If you are redirected to the page asking captcha, enter the captcha to proceed.

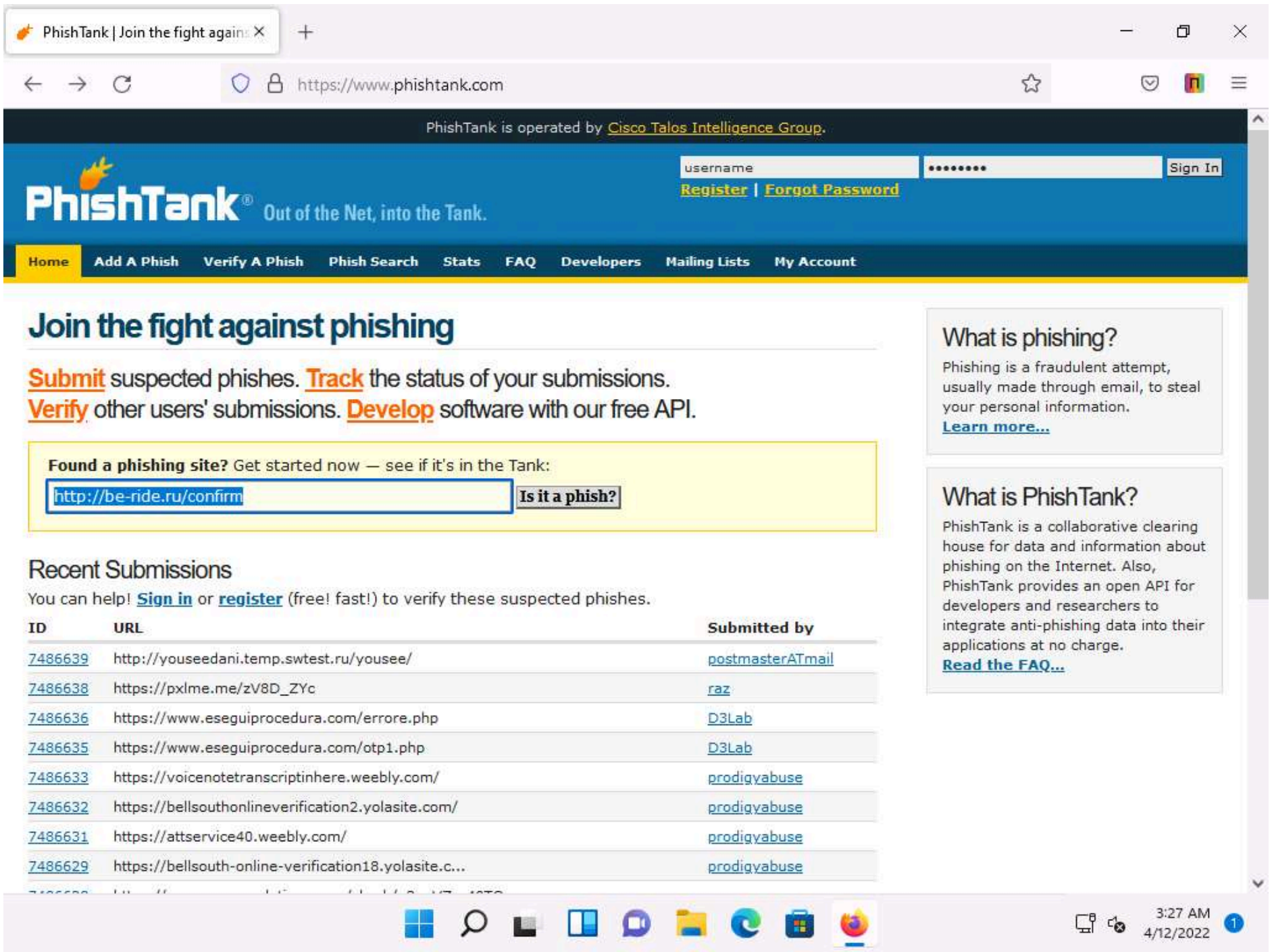


4. If the site is a phishing site, **PhishTank** returns a result stating that the website "**Is a phish**," as shown in the screenshot.



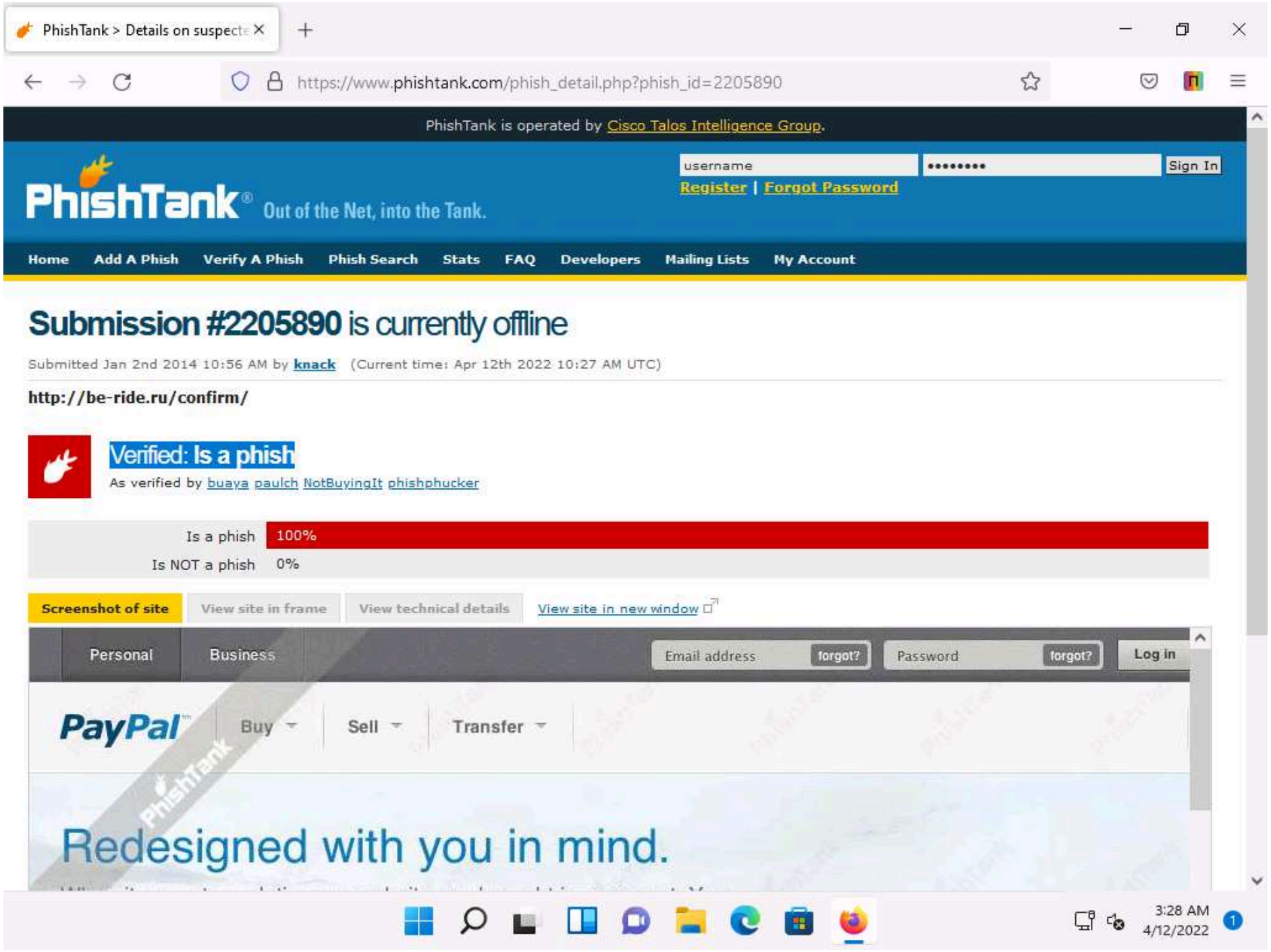
5. Navigate back to the **PhishTank** home page by clicking the **Back** button in the top-left corner of the browser.

6. In the **Found a phishing site?** text field, type a website URL to be checked for phishing (in this example, the URL entered is **be-ride.ru/confirm**). Click the **Is it a phish?** button.



Note: You can examine any website of your choice for phishing.

7. If the site is a phishing site, **PhishTank** returns a result stating that the website "**Is a phish**," as shown in the screenshot.



8. This concludes the demonstration of detecting phishing using PhishTank.

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

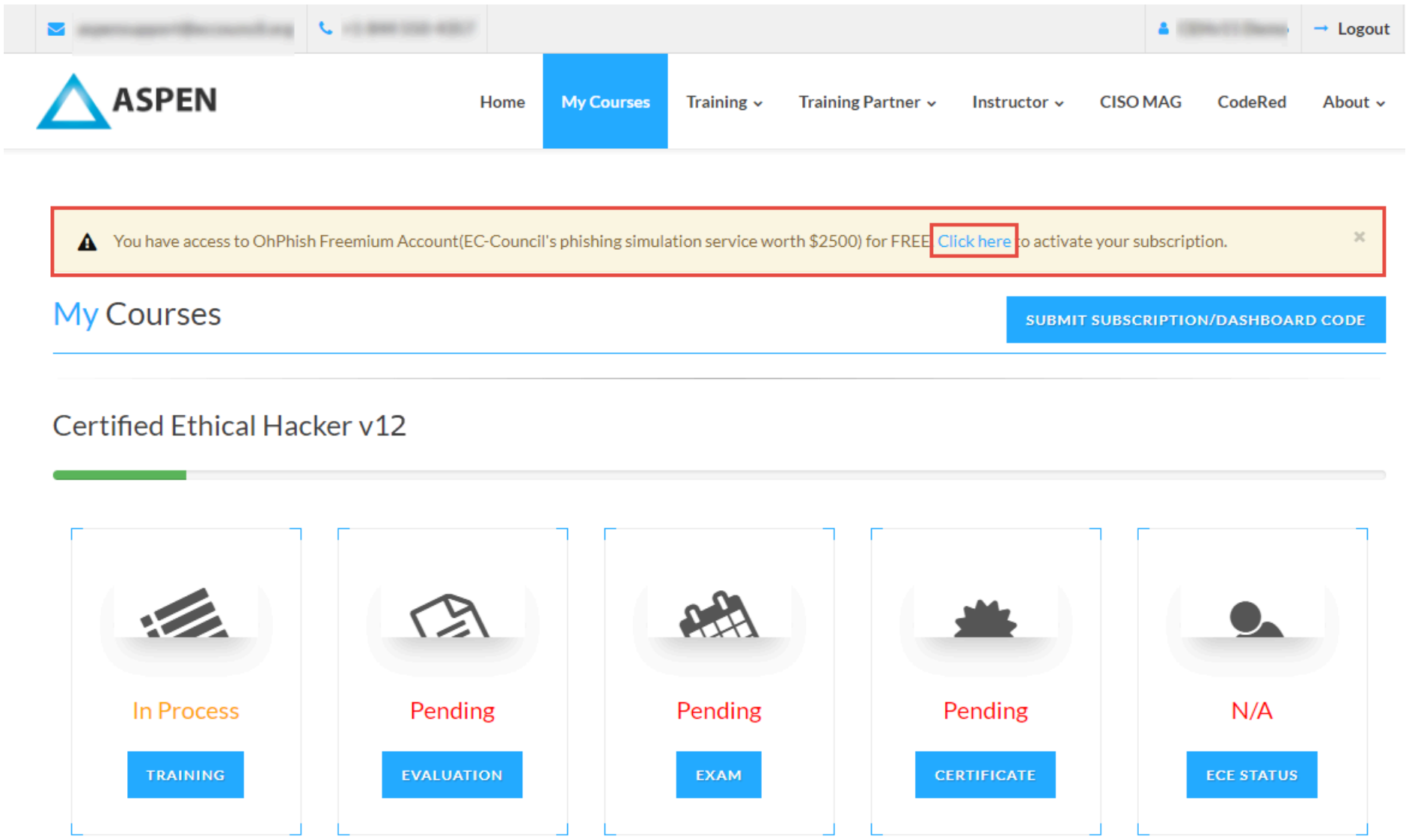
OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides an organization with a platform to launch phishing simulation campaigns on its employees. The platform captures the responses and provides MIS reports and 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.

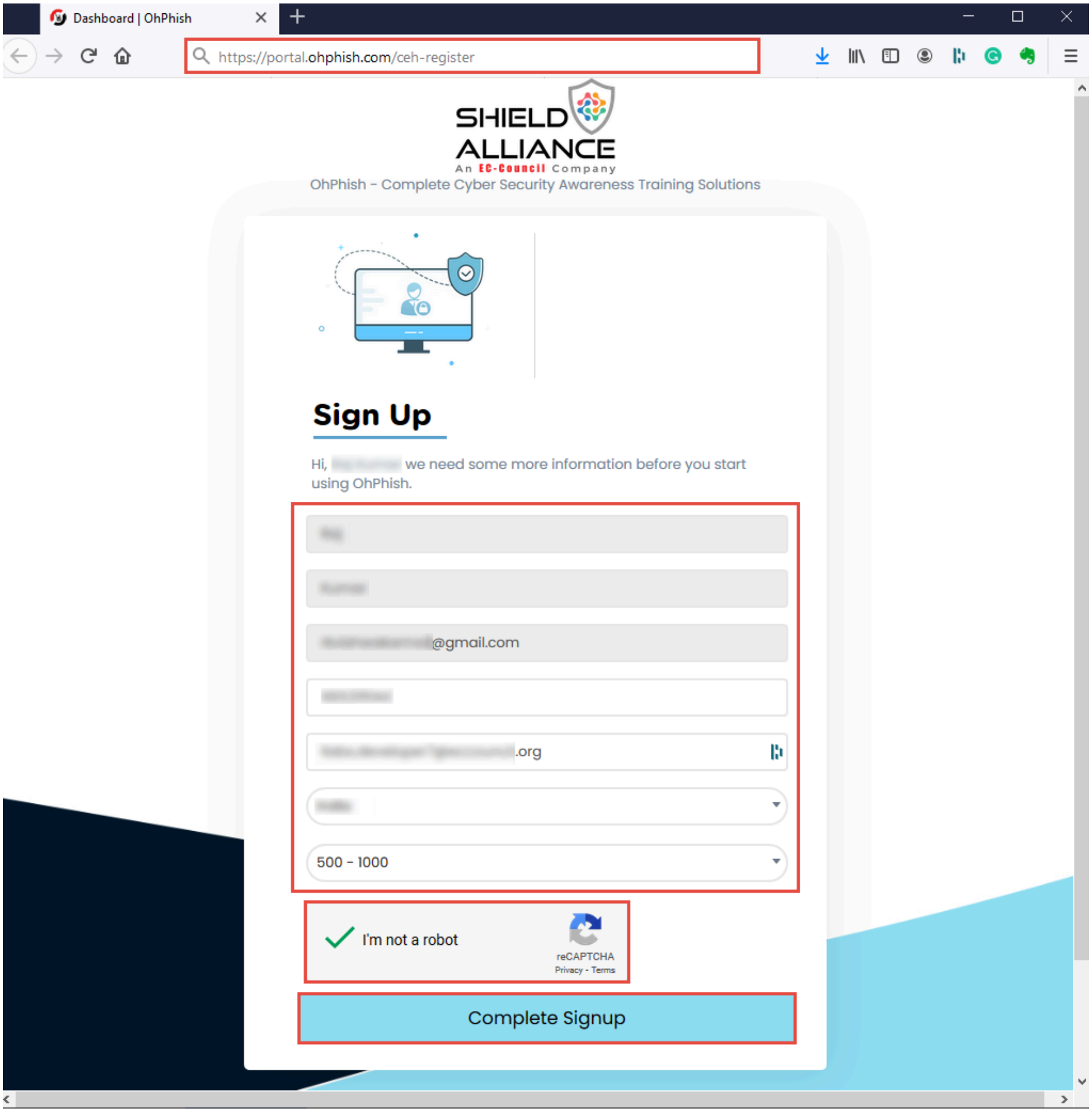
1. Before starting this task, you must activate your **OhPhish** account.
2. Open any web browser (here, **Mozilla Firefox**). Log in to your **ASPEN** account and navigate to **Certified Ethical Hacker v12** in the **My Courses** section.

   Note: 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.

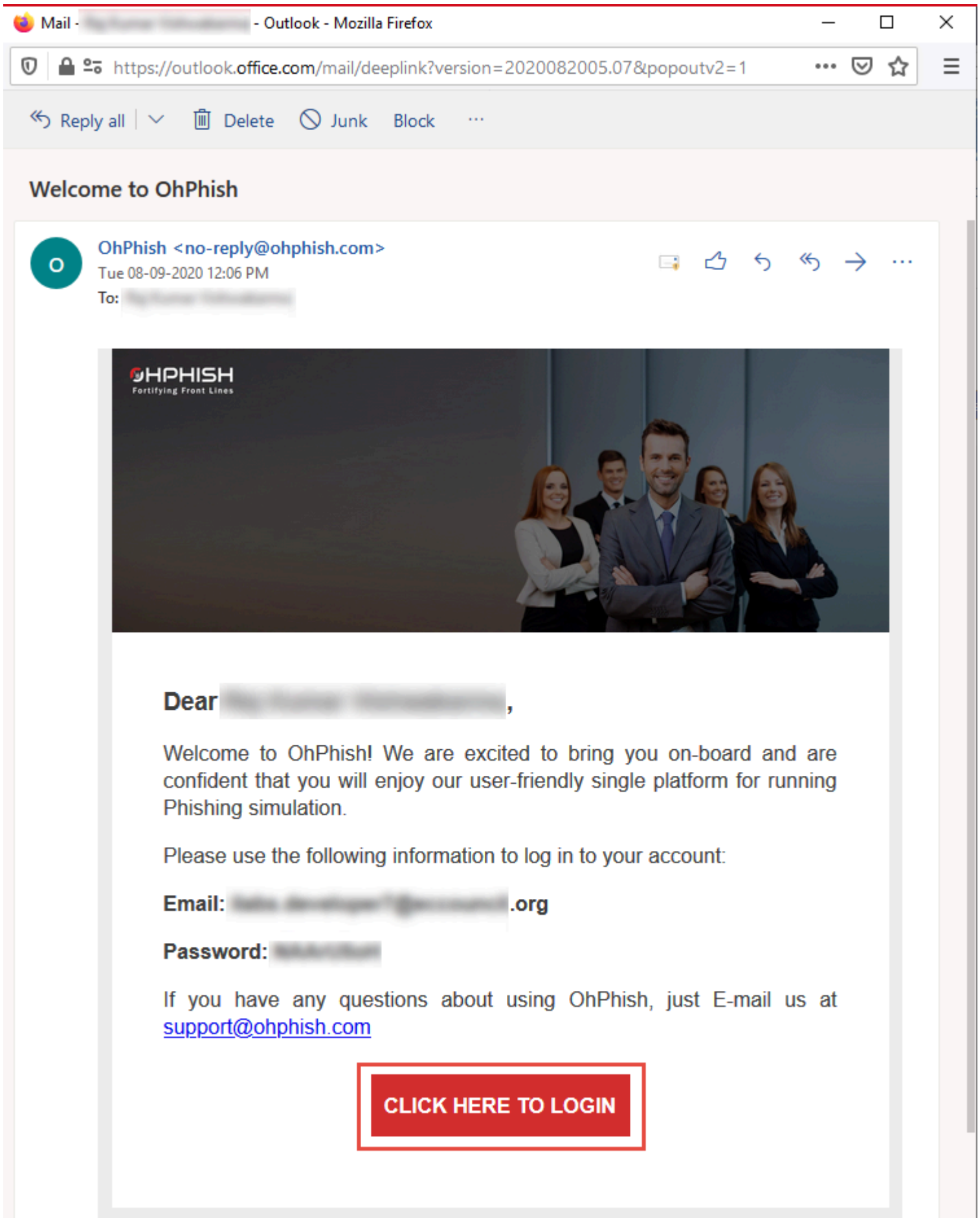


4. You will be redirected to the OhPhish **Sign Up** page. Enter the remaining personal details, check **I'm not a robot** checkbox and click **Complete Signup** button.



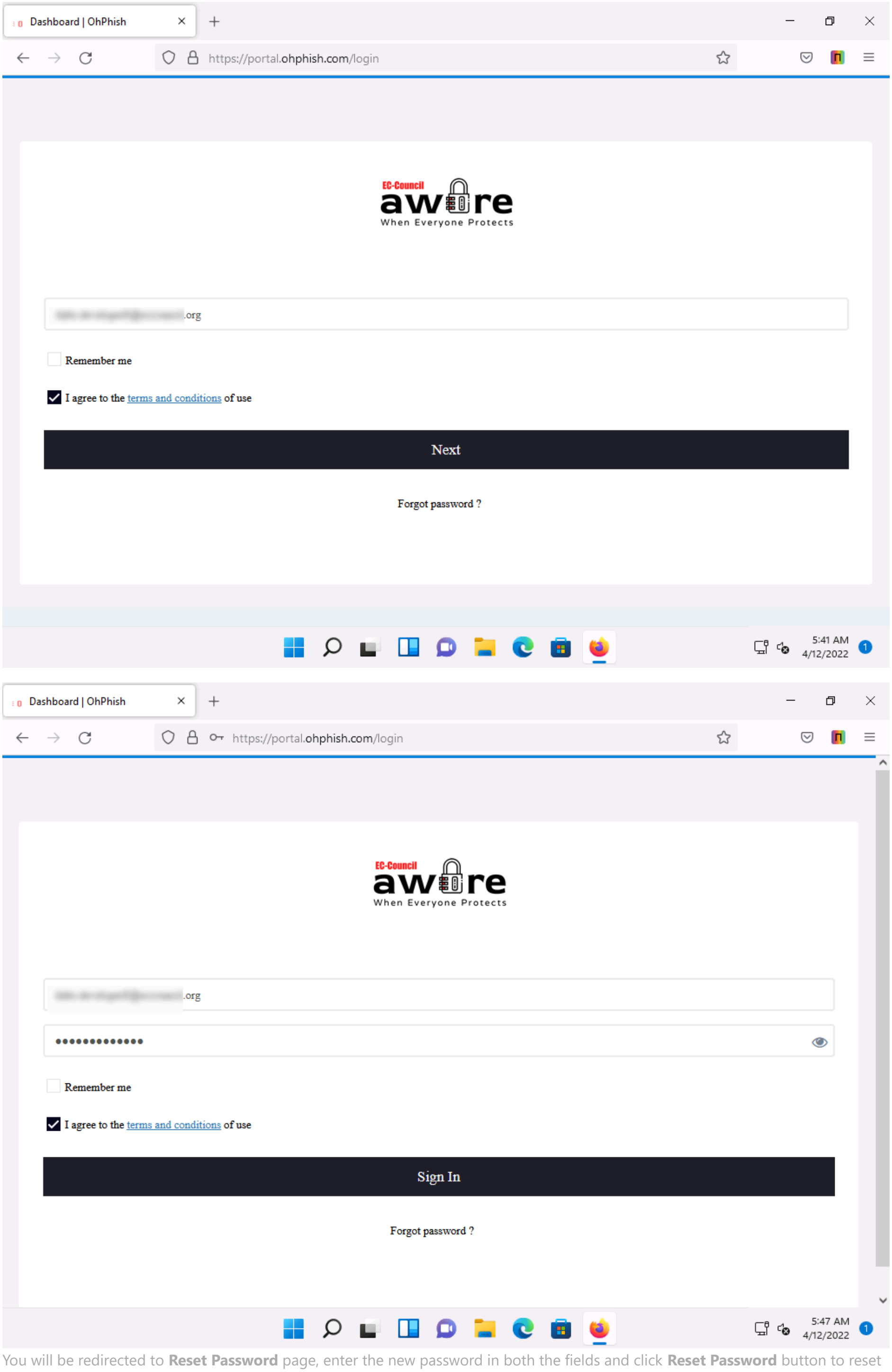
5. Account creation **Alert!** appears, click **OK**.

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.

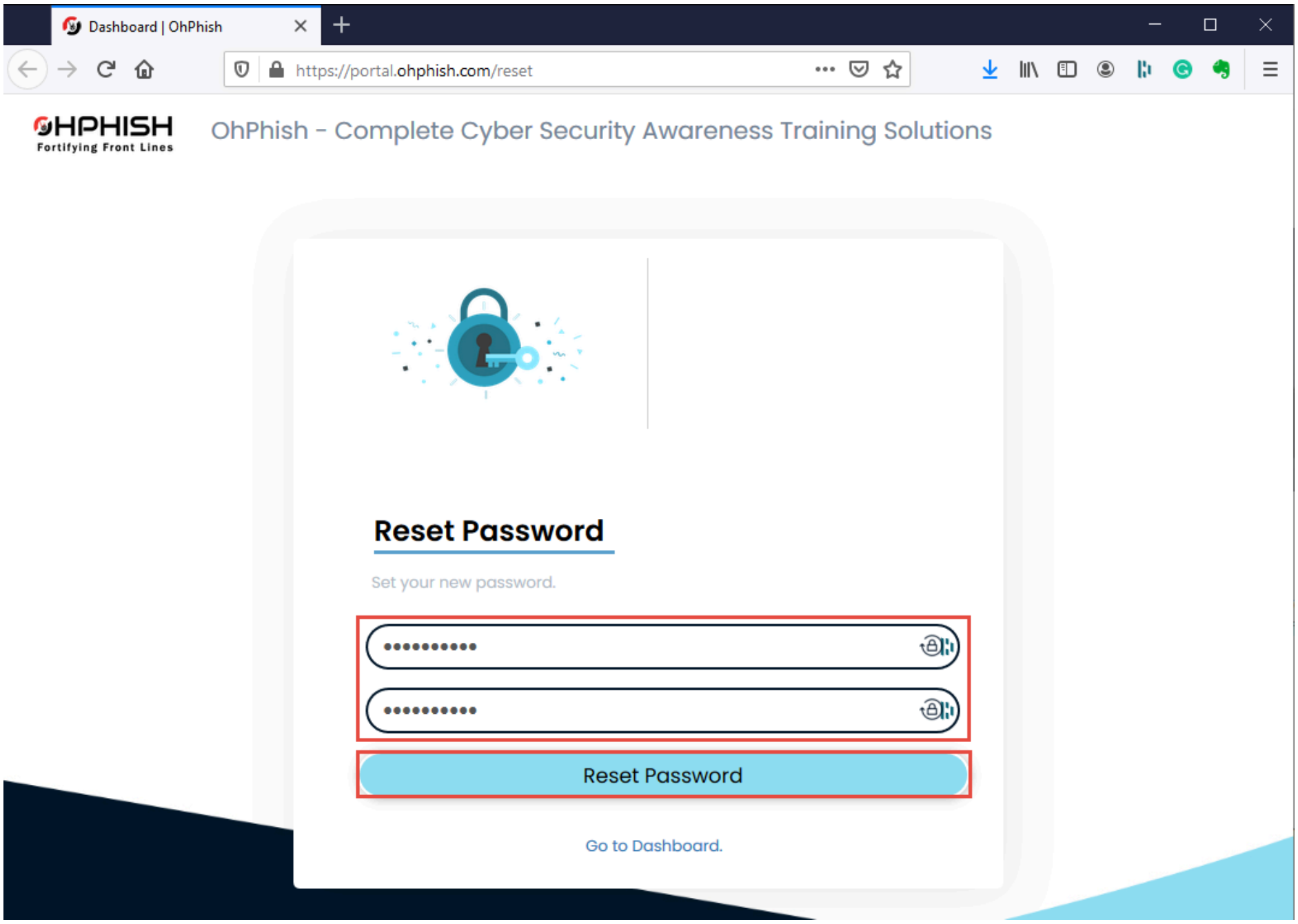


7. **EC-Council Aware** page appears, in the **Username** field enter your email address and click **Next**. In the next page, enter your password in the **Password** field and click **Sign In**.

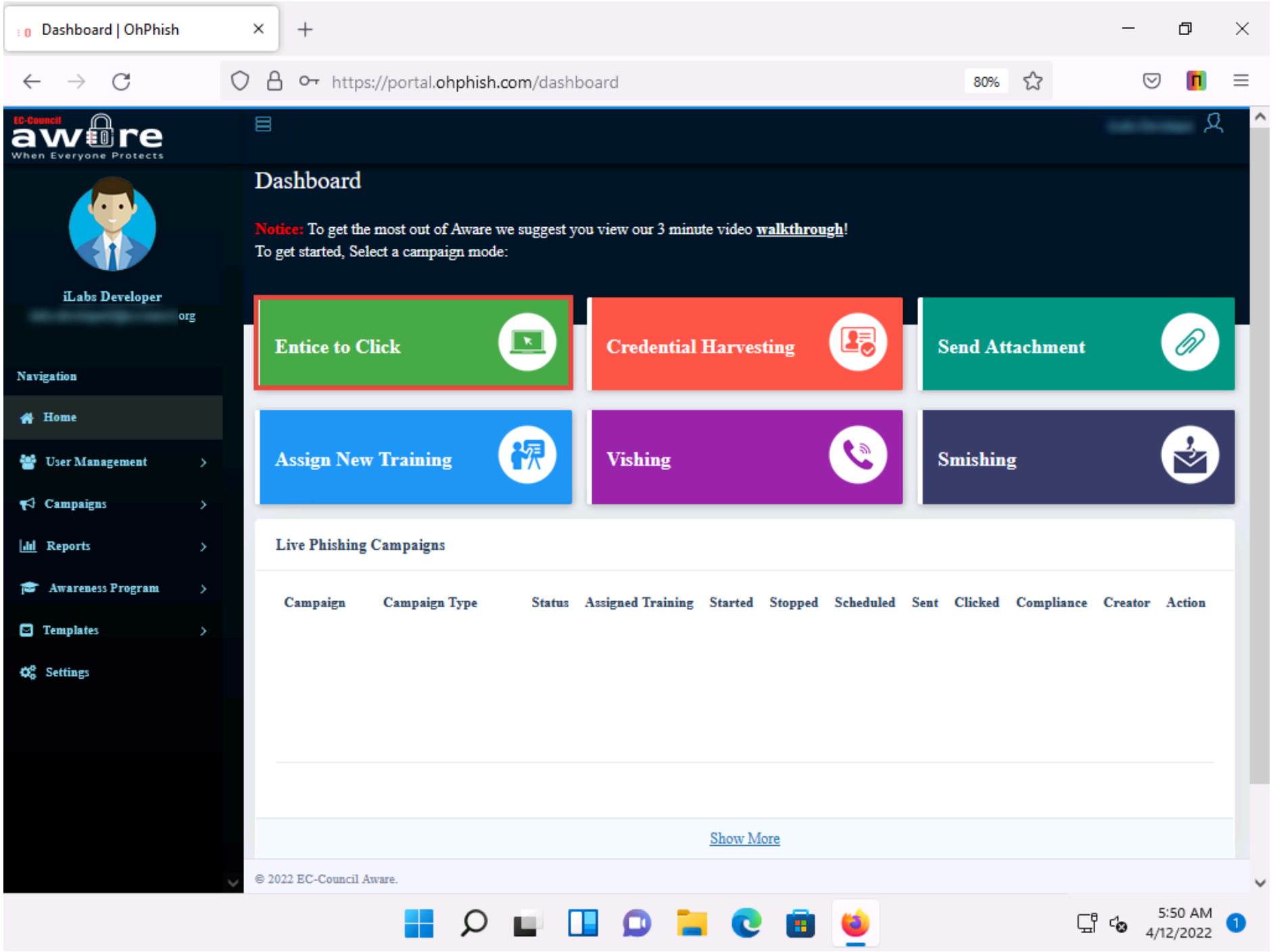
Note: If **Save login for ohphish.com?** notification appears, click **Don't Save**.



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.

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

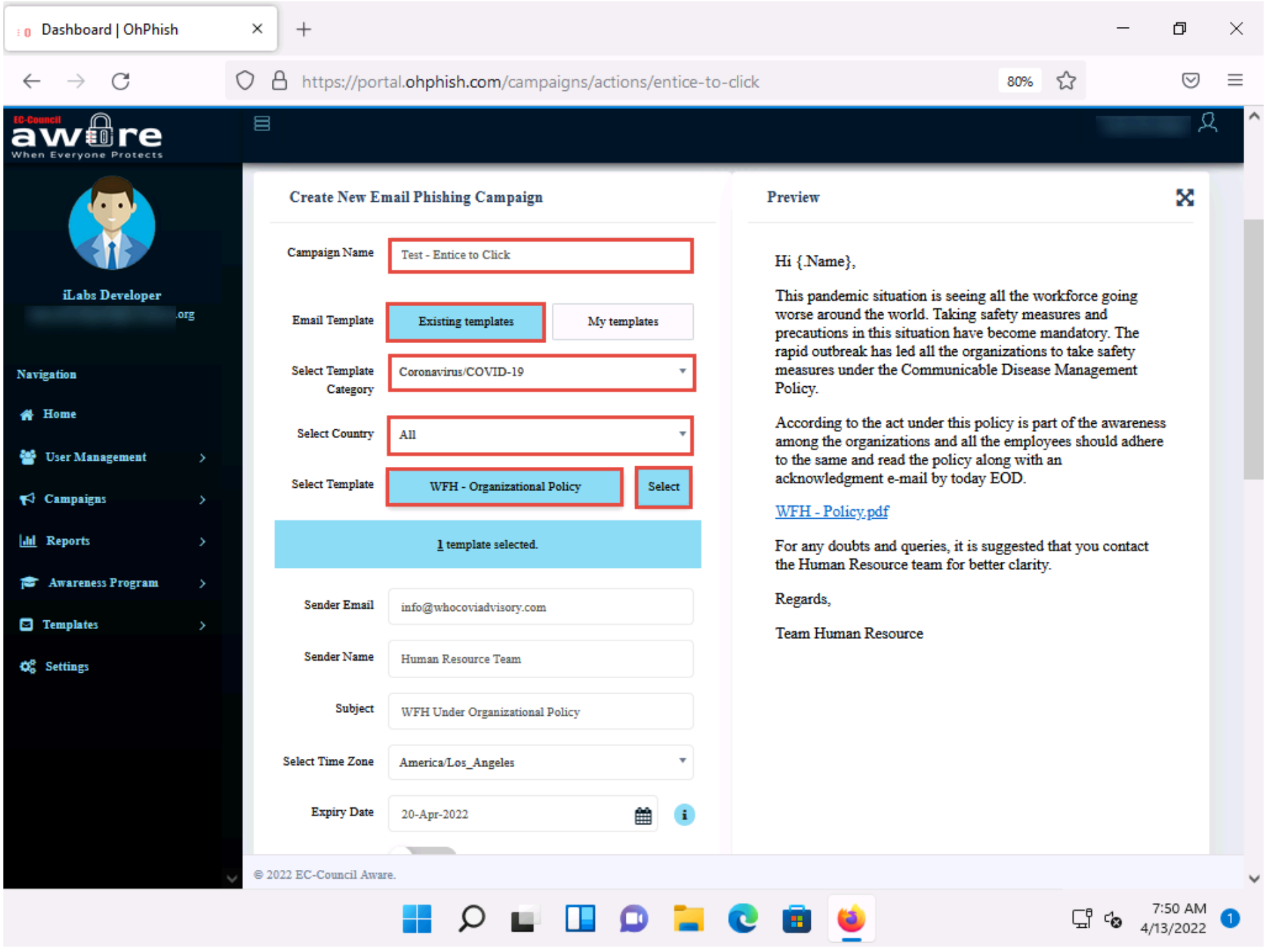
> Note: Ensure that the **Existing Template** is selected in the **Email Template** option.

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.

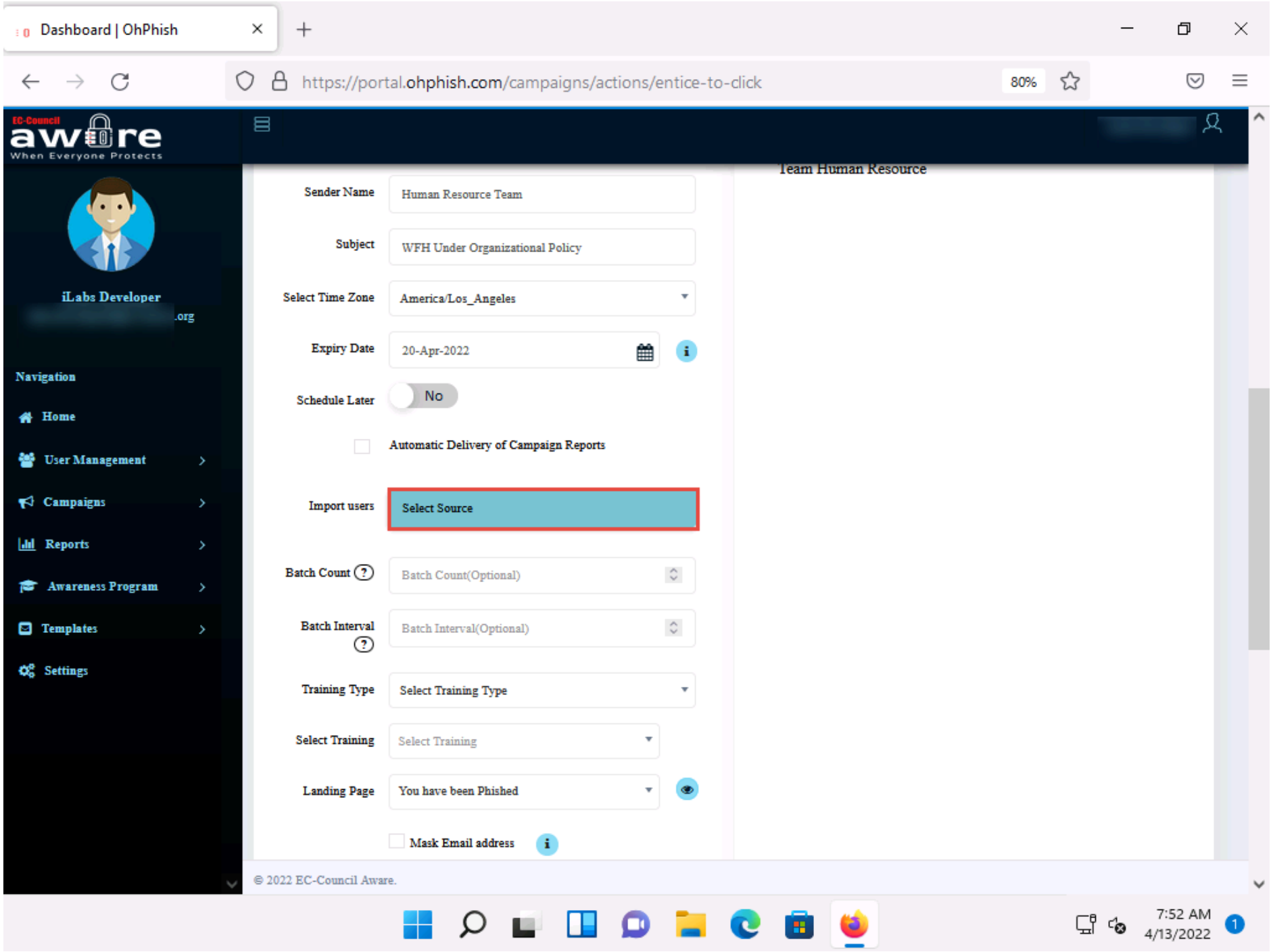
> Note: The **template selected** notification appears below the **Select Template** field.



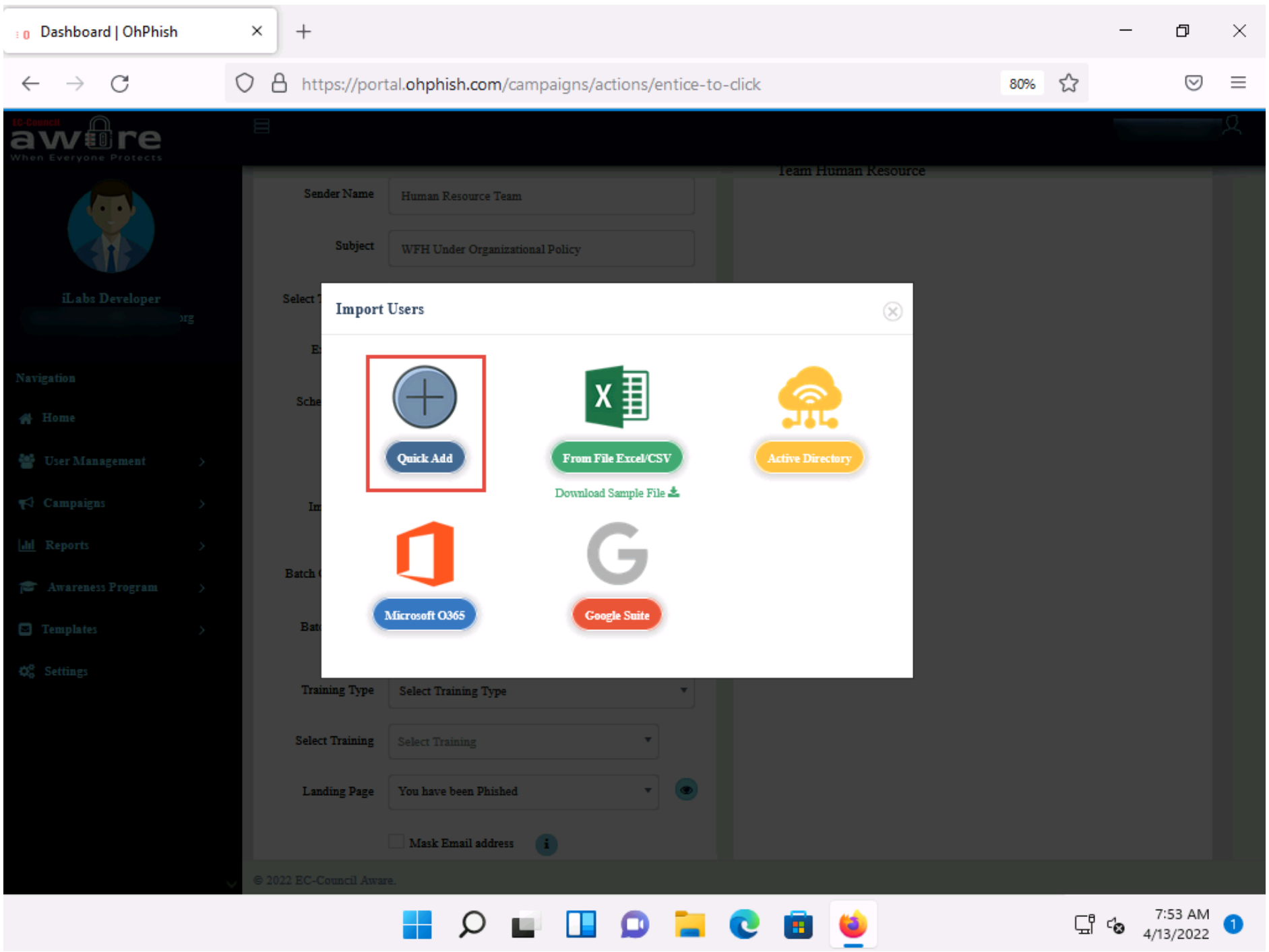
18. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

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

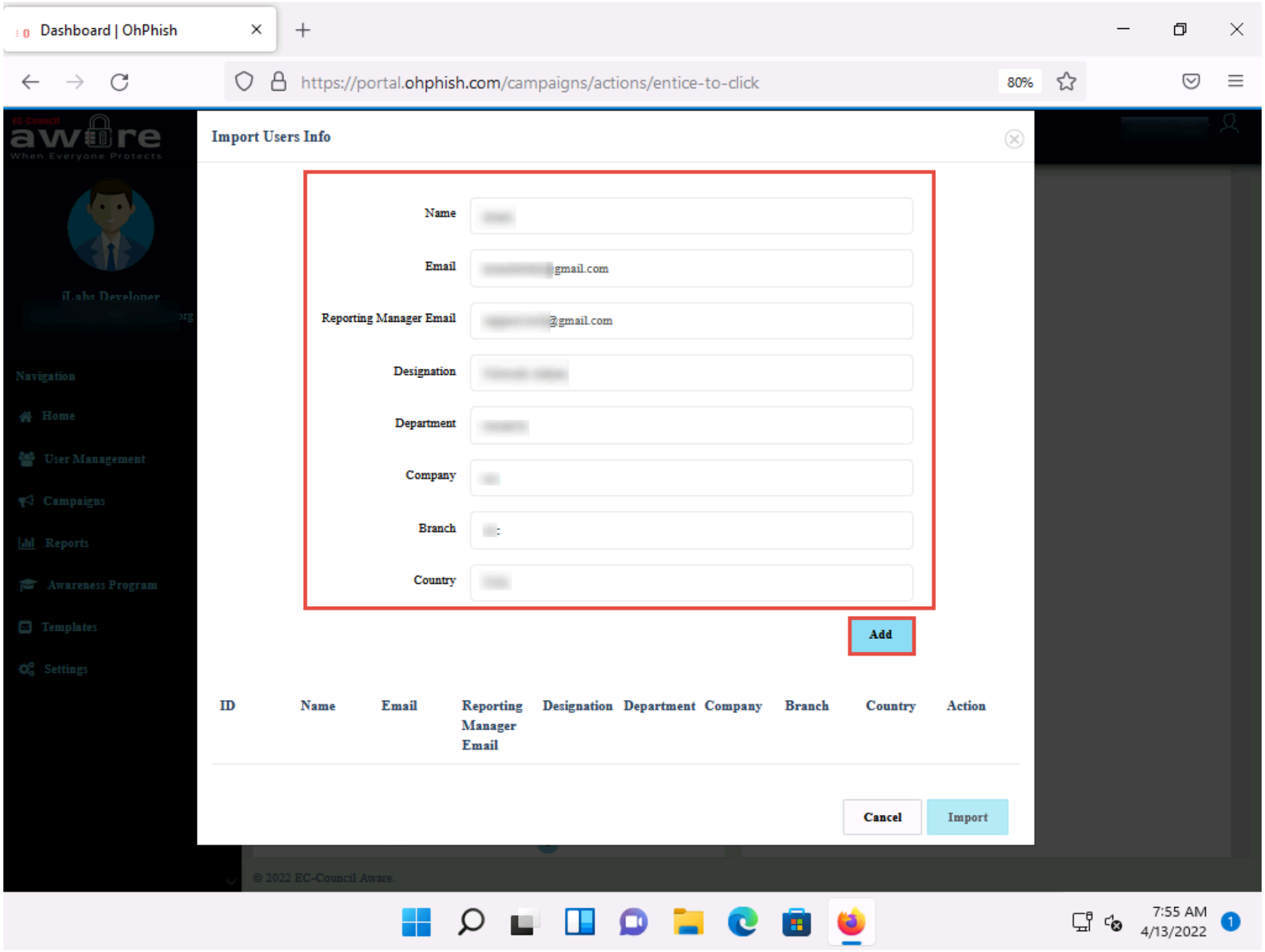
19. In the **Import users** field, click **Select Source**.



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

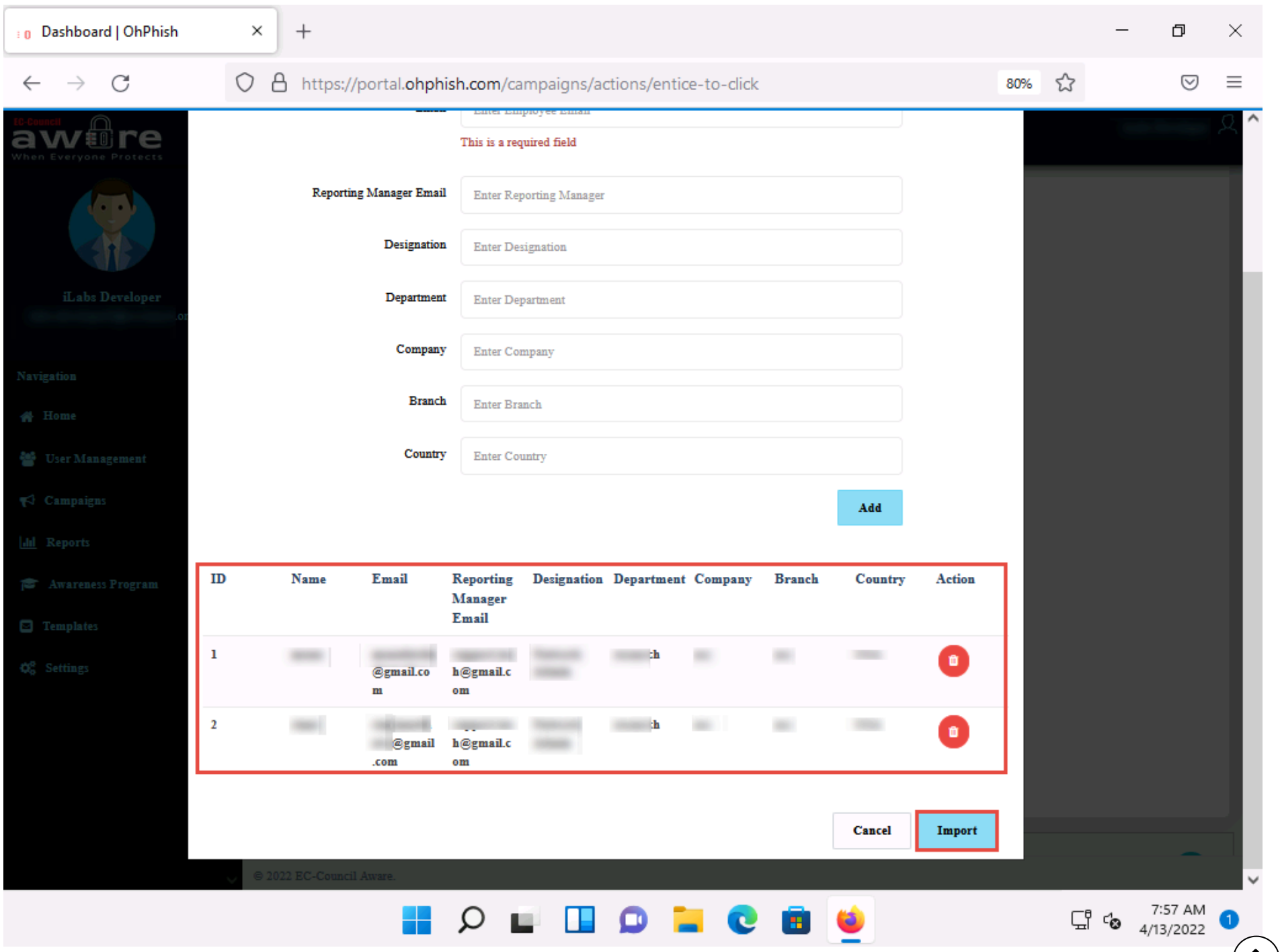


21. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.



22. Similarly, you can add the details of multiple users. Here, we added two users.

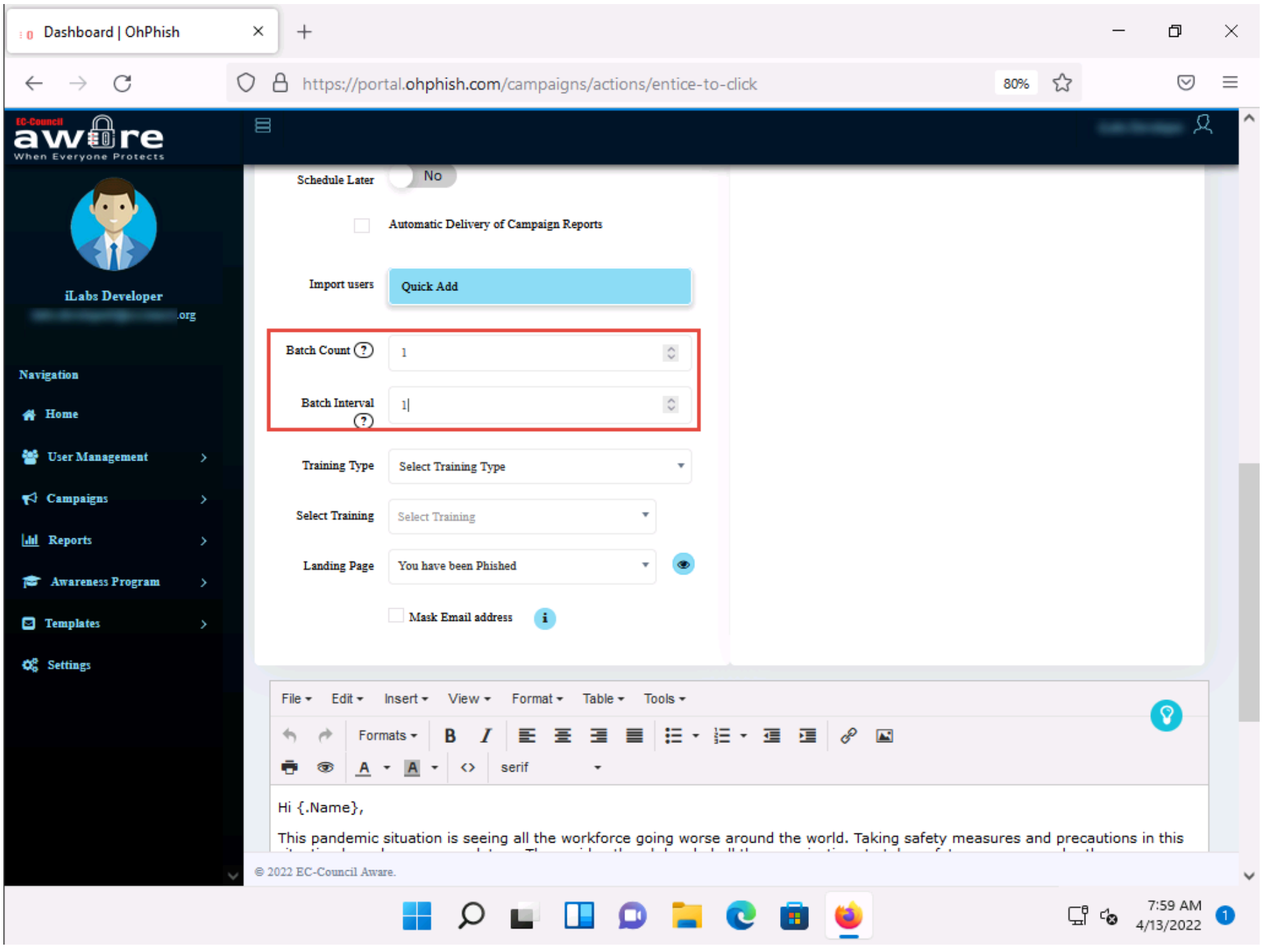
23. After adding the users' details, click **Import**.



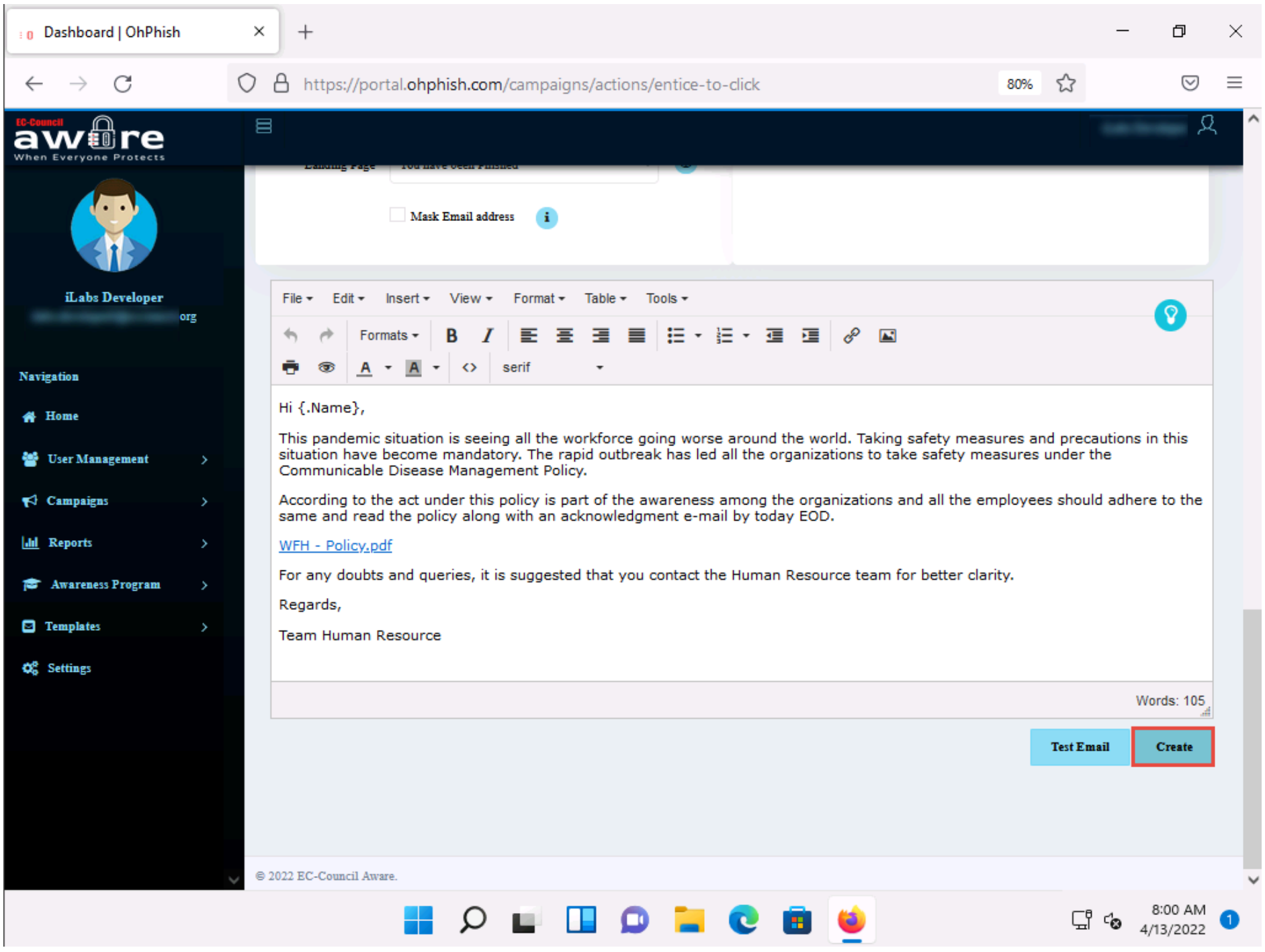
24. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

> Note: **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.
>
> Note: 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.

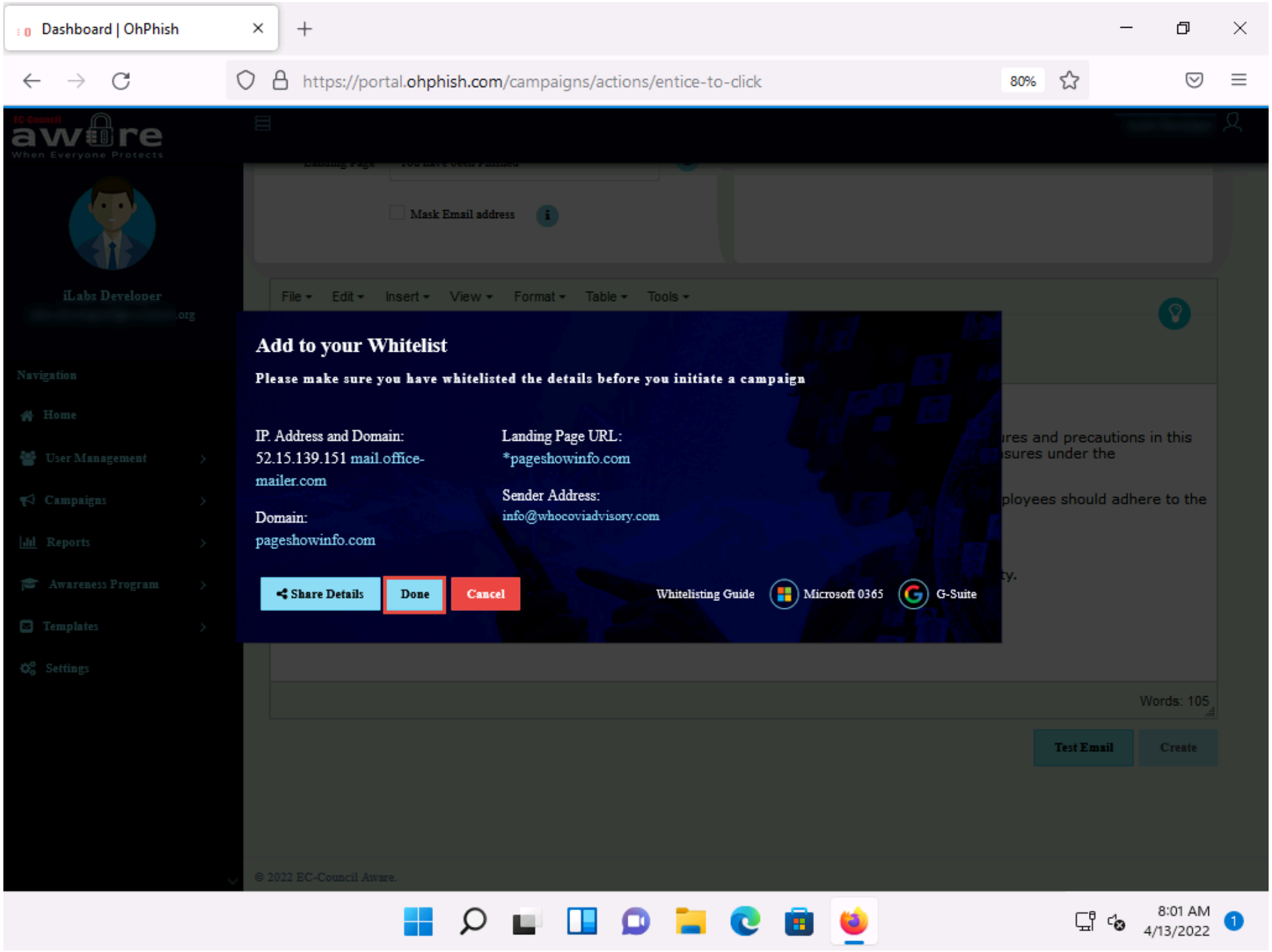


26. Now, scroll down to the end of the page and click **Create** to create the phishing campaign.

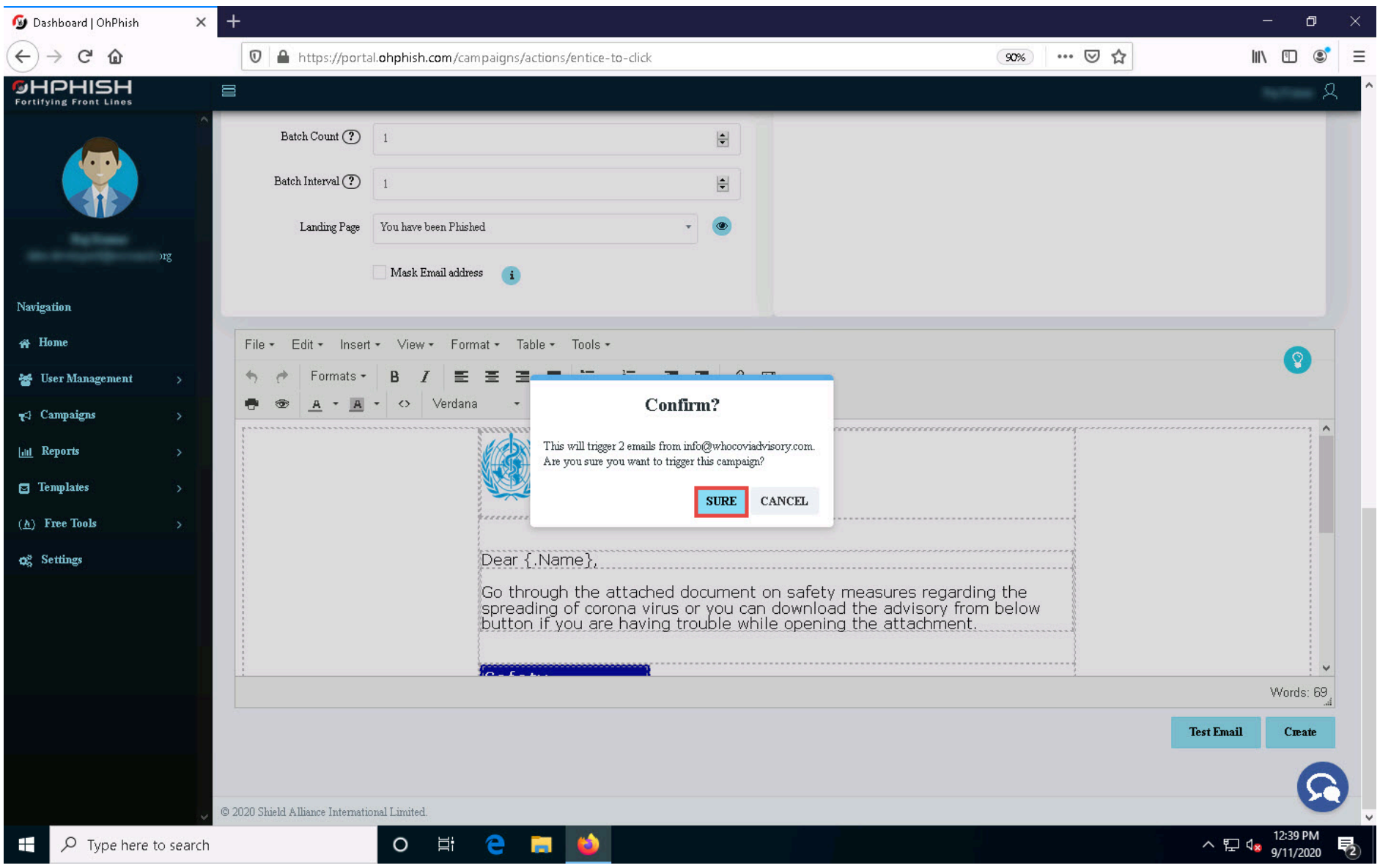


27. **Add to your Whitelist** pop-up appears, click **Done**.

Note: 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.

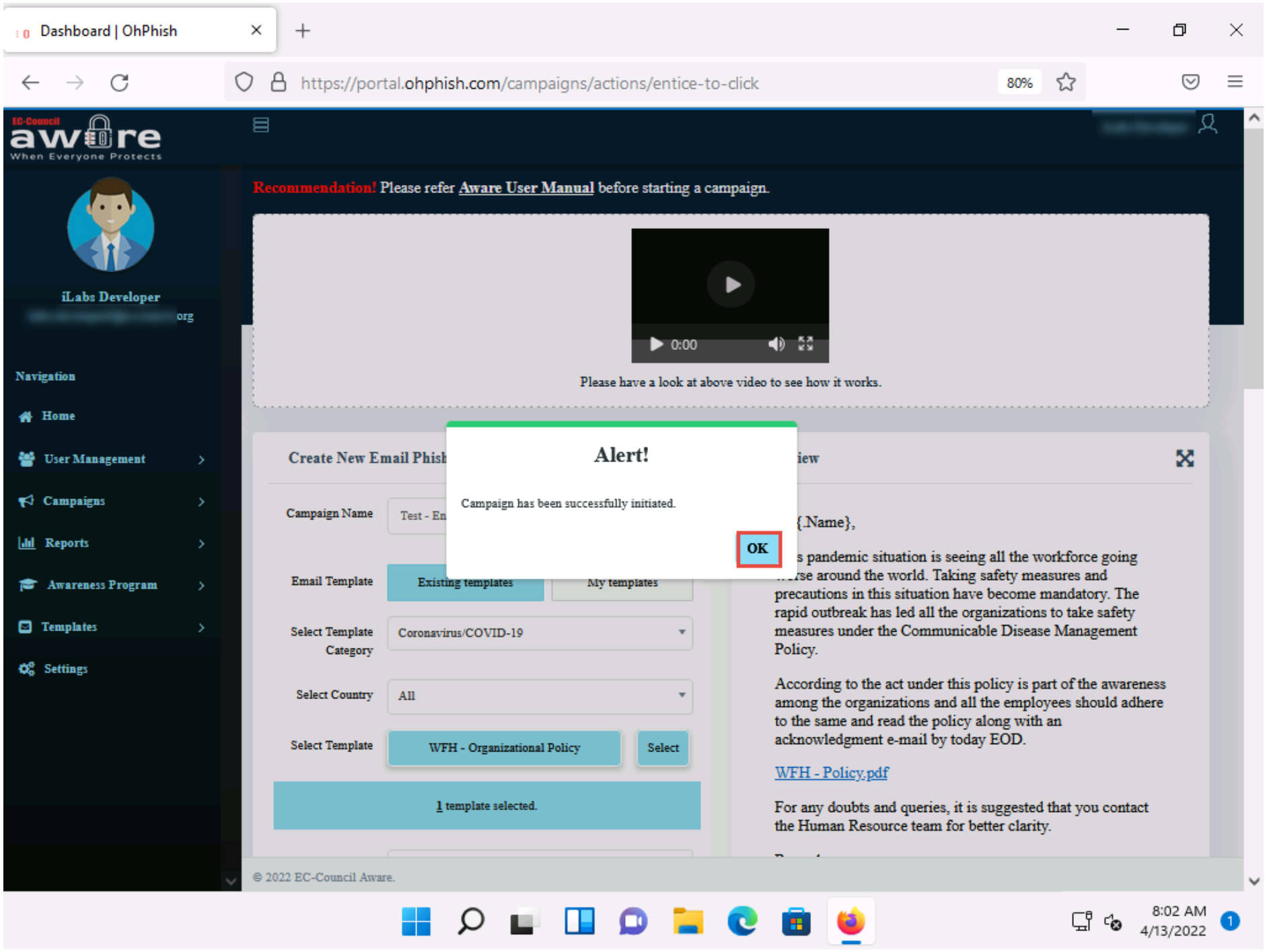


28. The **Confirm?** pop-up appears; click **SURE**.

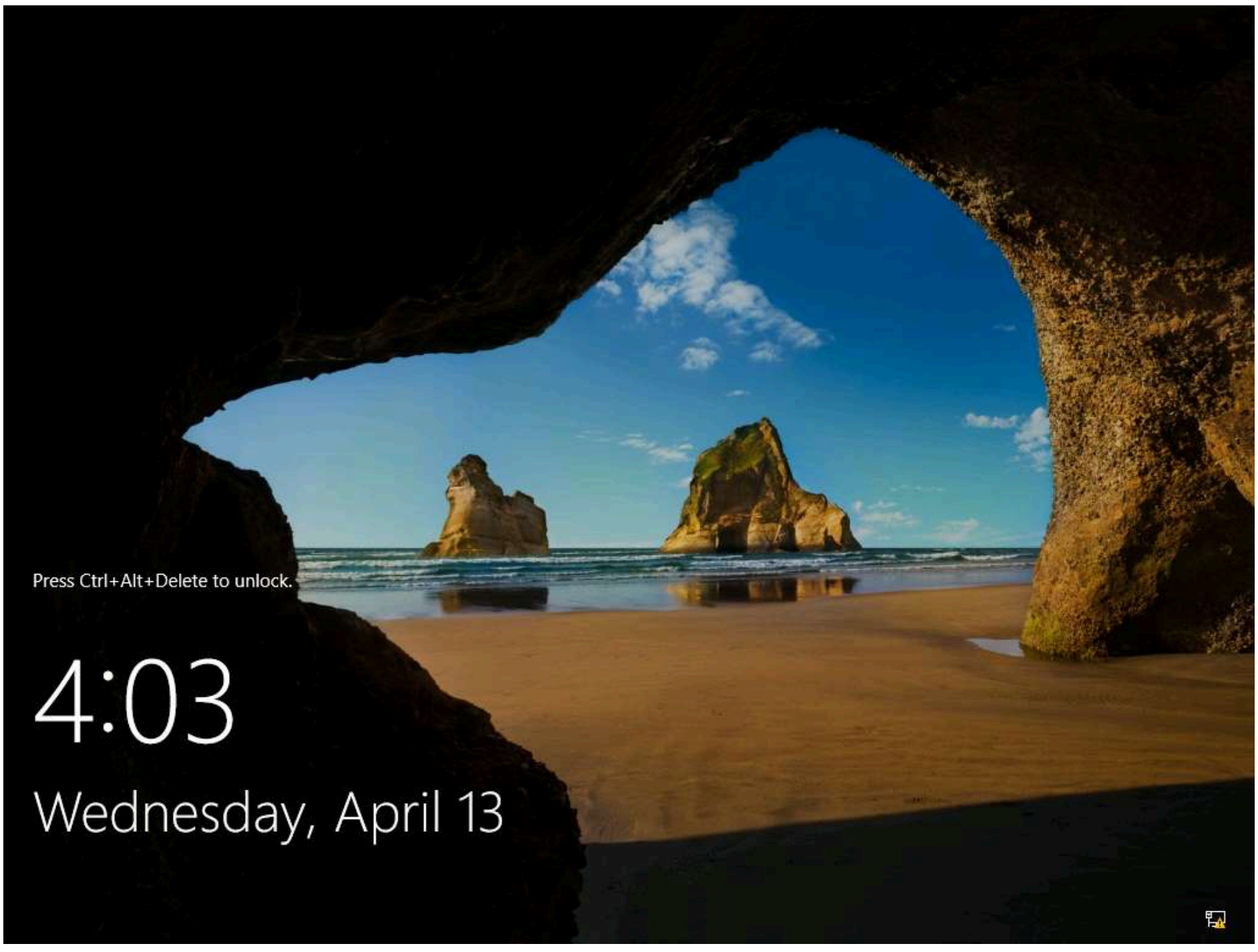


29. A count down timer appears and phishing campaign initiates in ten seconds.

30. The **Alert!** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.

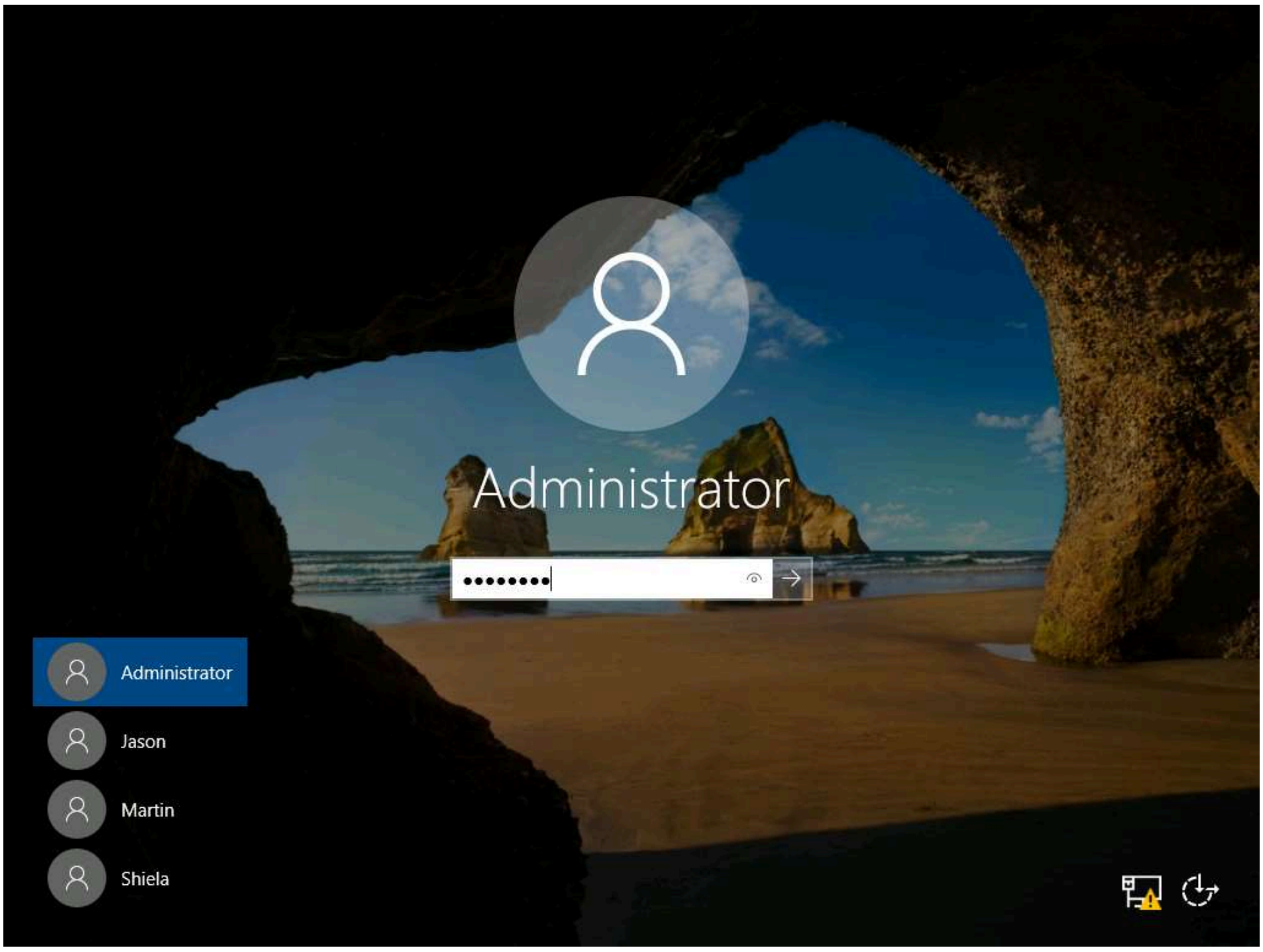


31. Now, we must open the phishing email as a victim (here, an employee of the organization). To do so, click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.



32. Click on **Ctrl+Alt+Del** to activate it, by default, **Administrator** profile is selected type **Pa$$w0rd** in the Password field and press **Enter** to login.

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



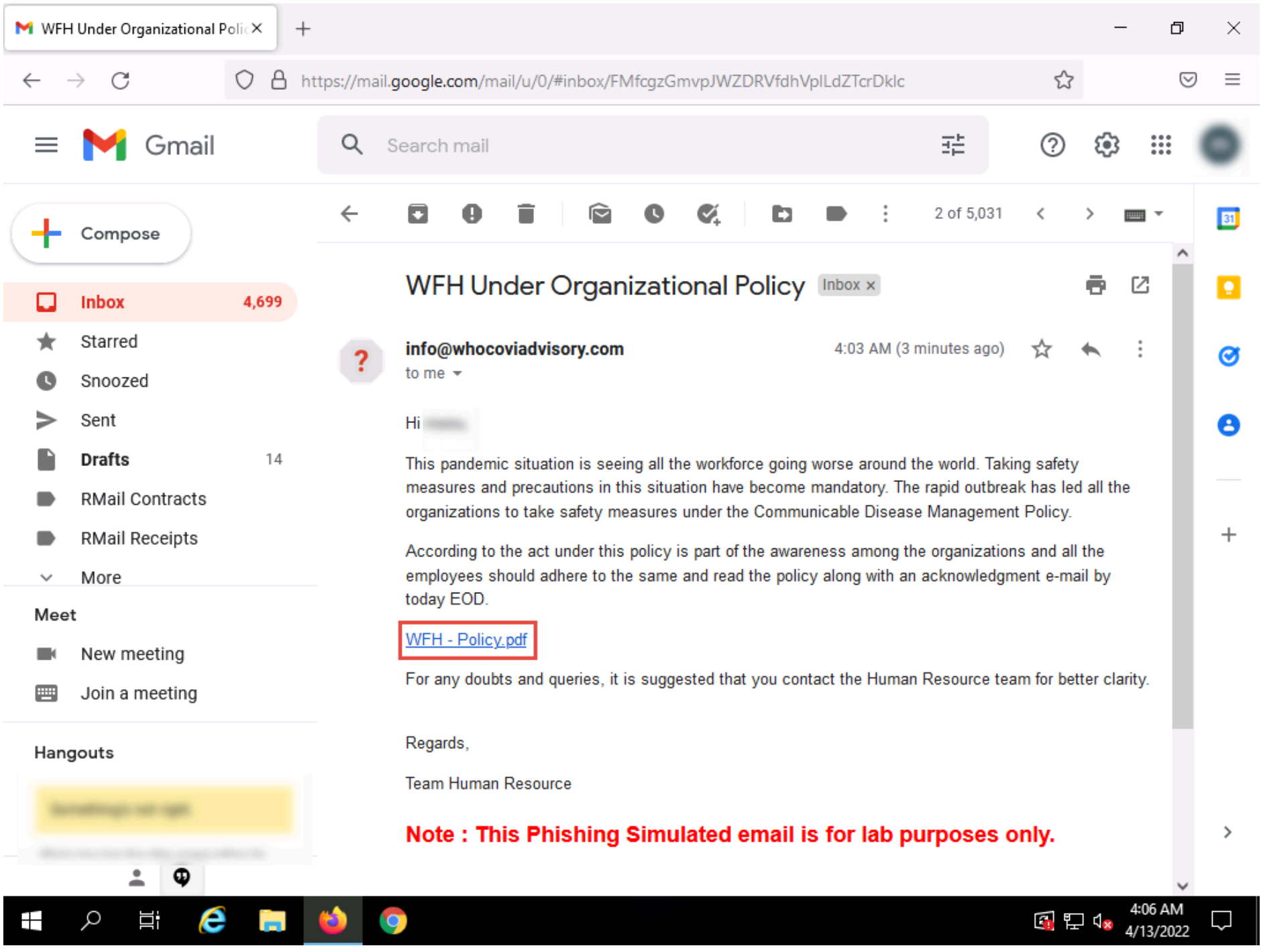
33. Open any web browser (here, **Mozilla Firefox**) and then open the email client provided while creating the phishing campaign (here, **Gmail**).

34. After you login to your **Gmail** account, search for an email with the subject **WFH Under Organizational Policy** in the **Inbox**.

Note: 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.

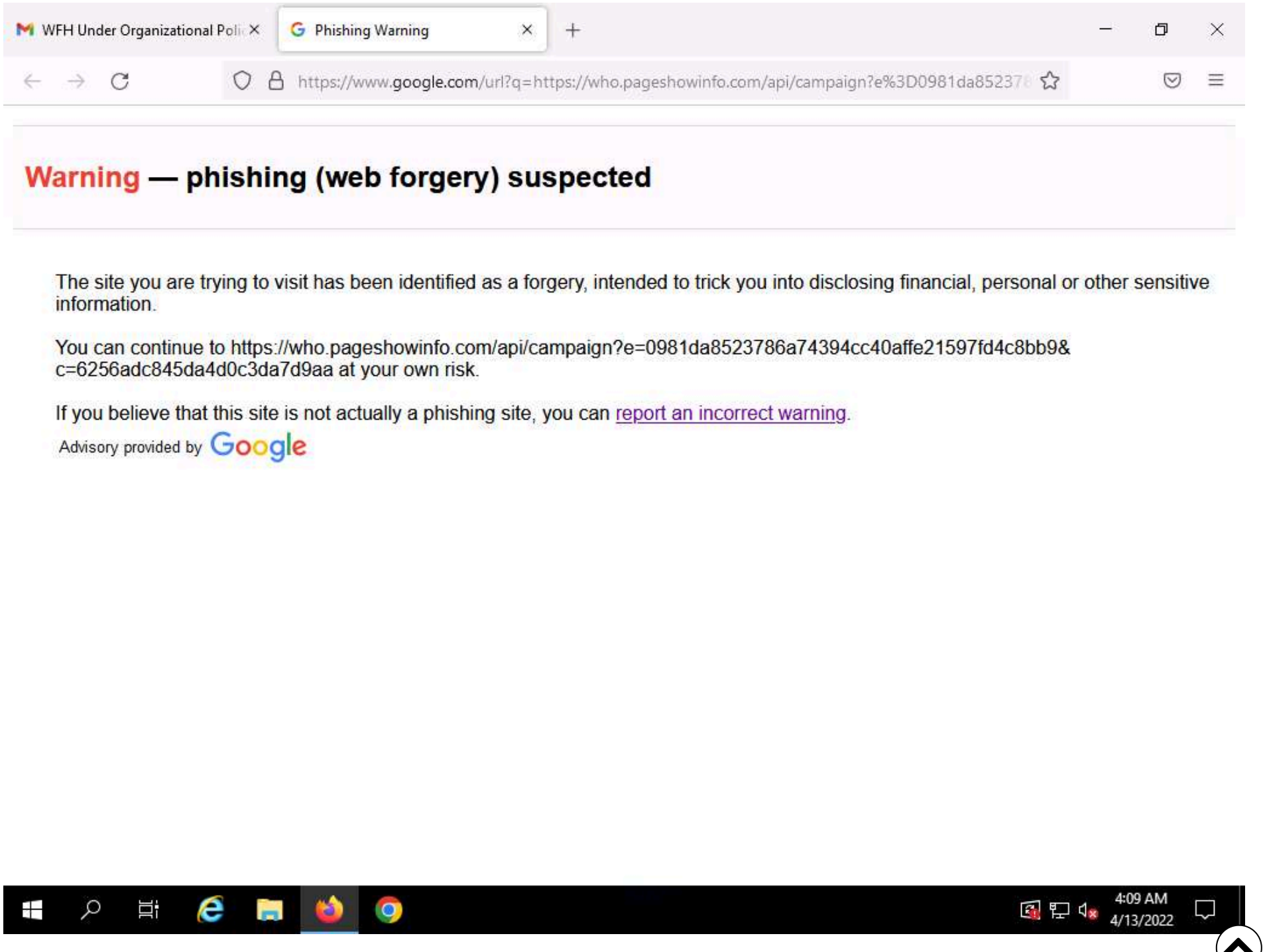
Note: If the email is not present in the **Inbox** folder, then check your **Spam** folder.

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.

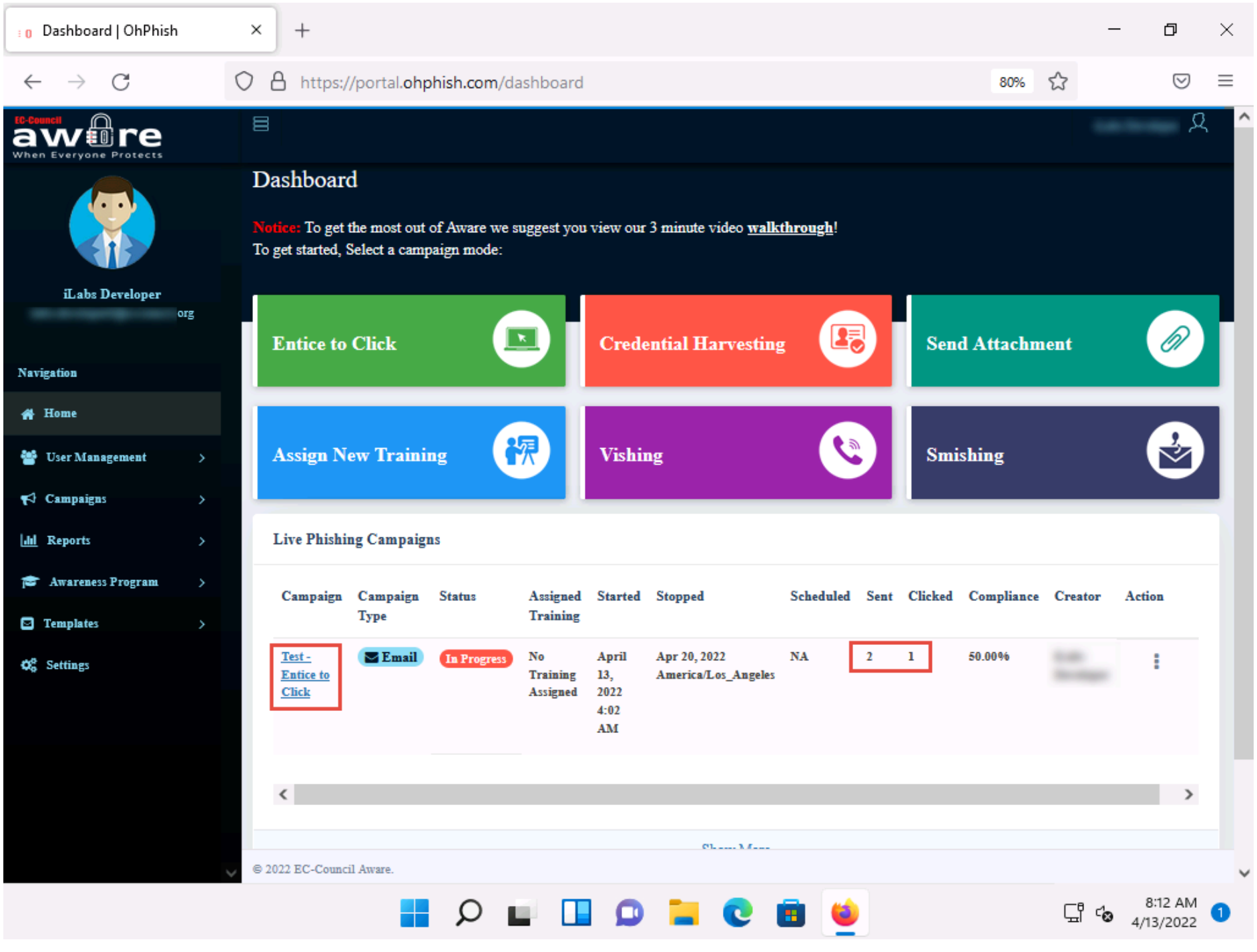


38. Close the current tab.

39. Now, click **CEHv12 Windows 11** to switch back to the **Windows 11** machine.

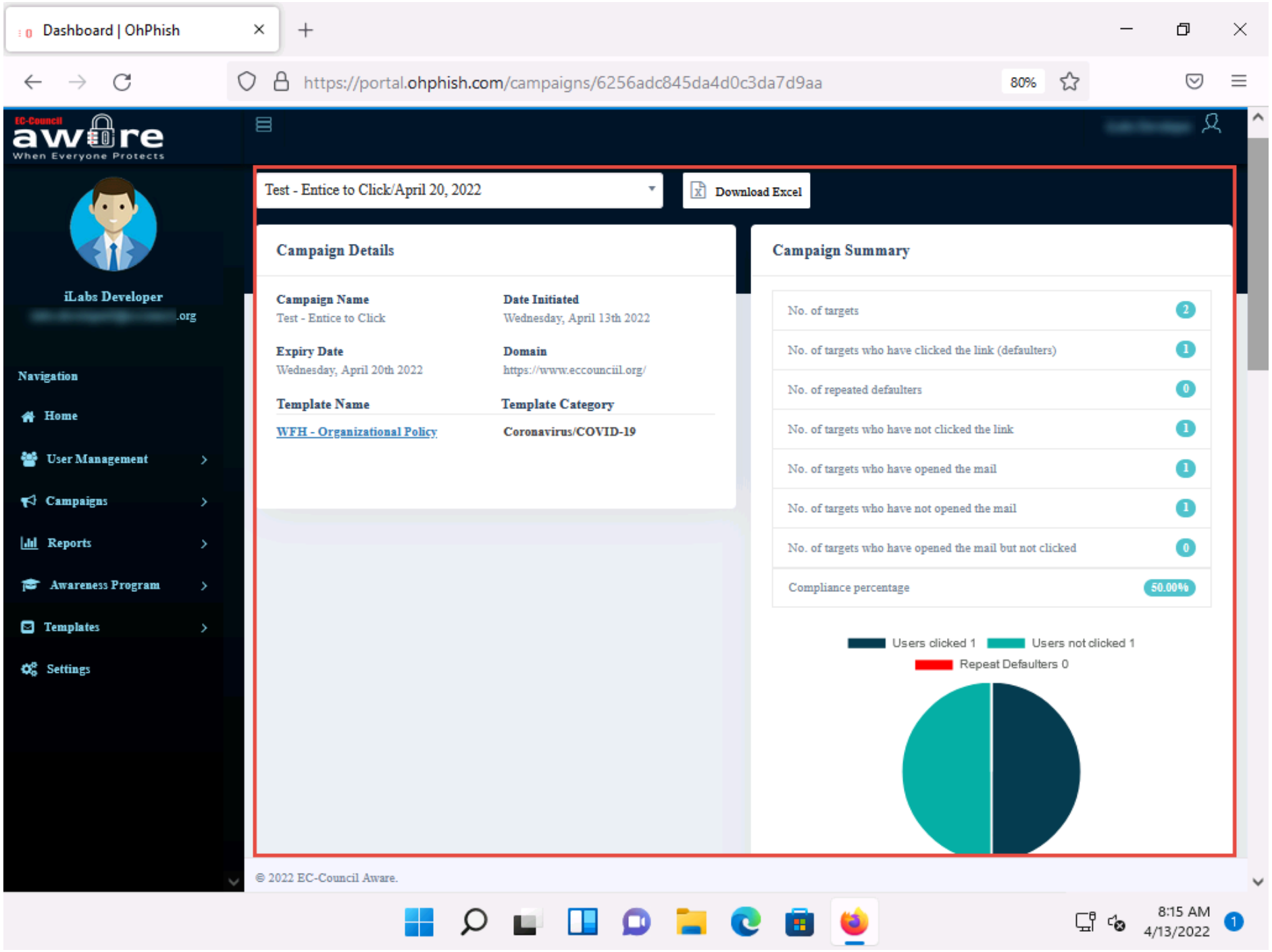
40. Click on the **Test – Entice to Click** campaign present on the **OhPhish Dashboard**. You can observe that one person has clicked the link.

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



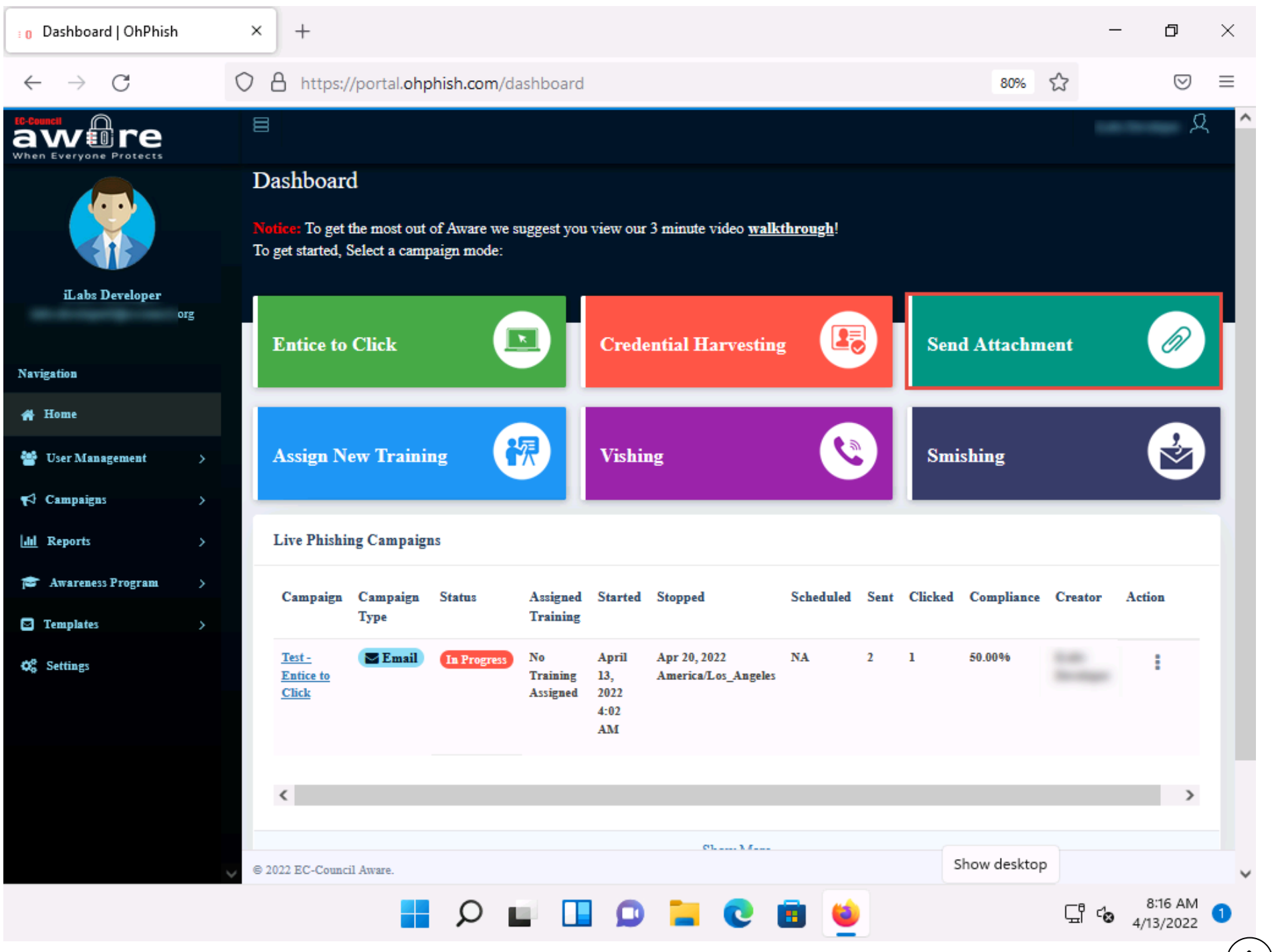
41. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.

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).



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.



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

> Note: **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.

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

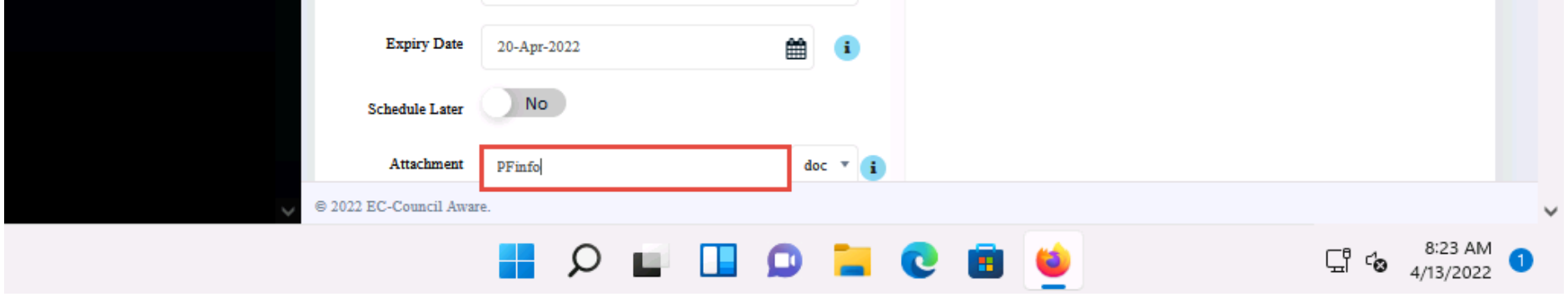
47. In the **Select Country** field, leave the default option selected (**All**).

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.

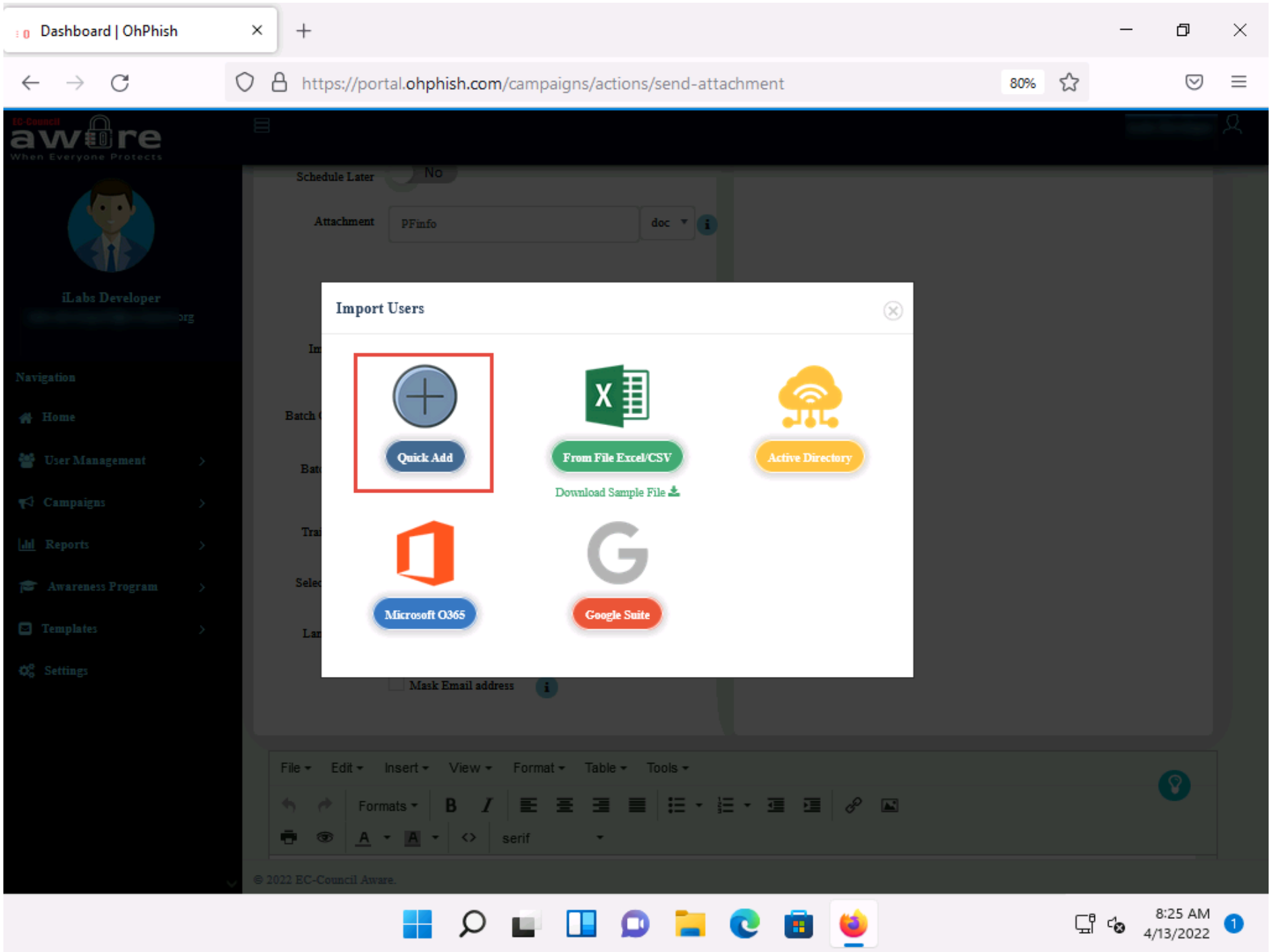
> Note: You can change the above-mentioned options if you want to.

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

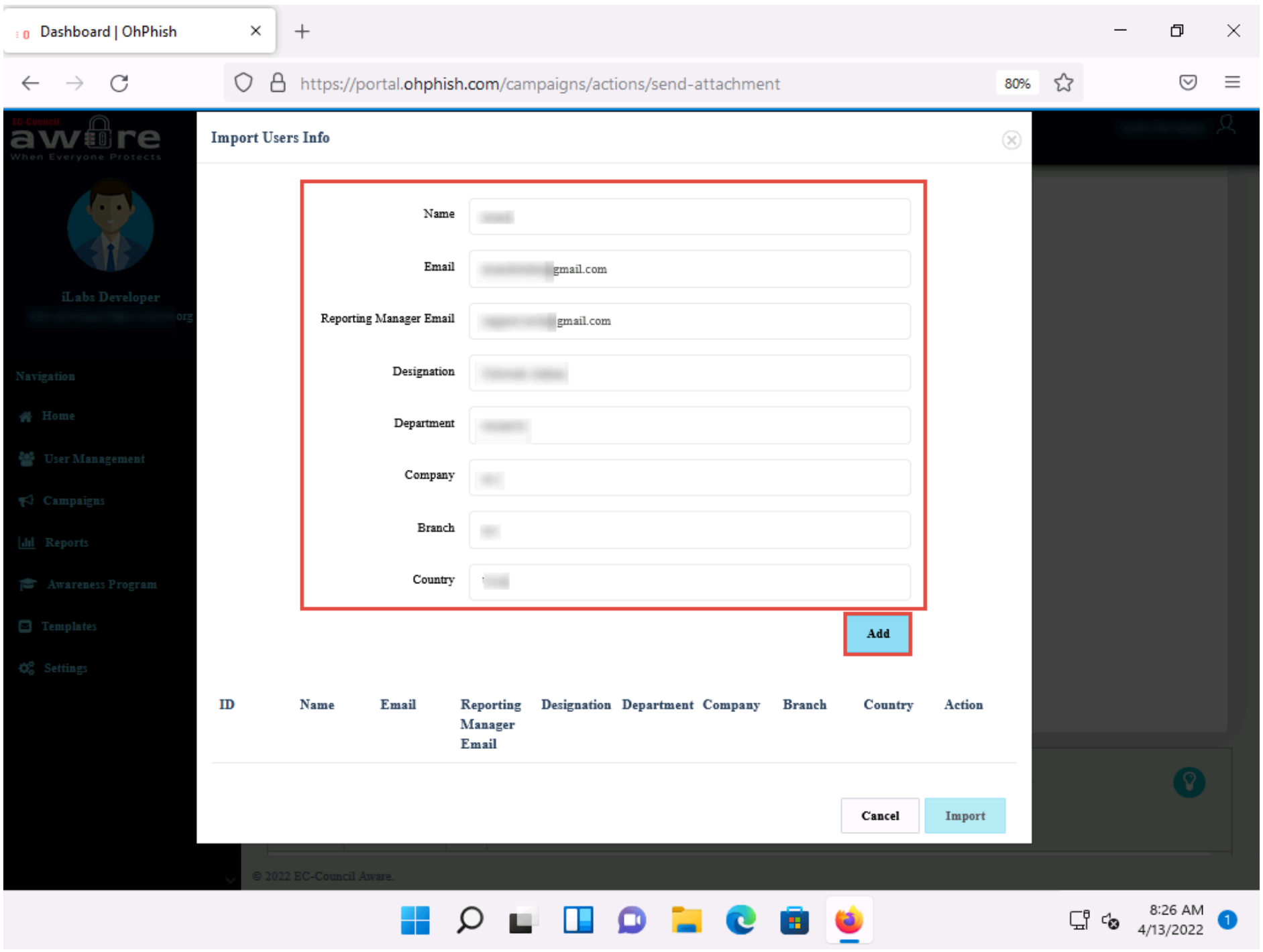


51. Click **Select Source** button under **Import users** field.

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.

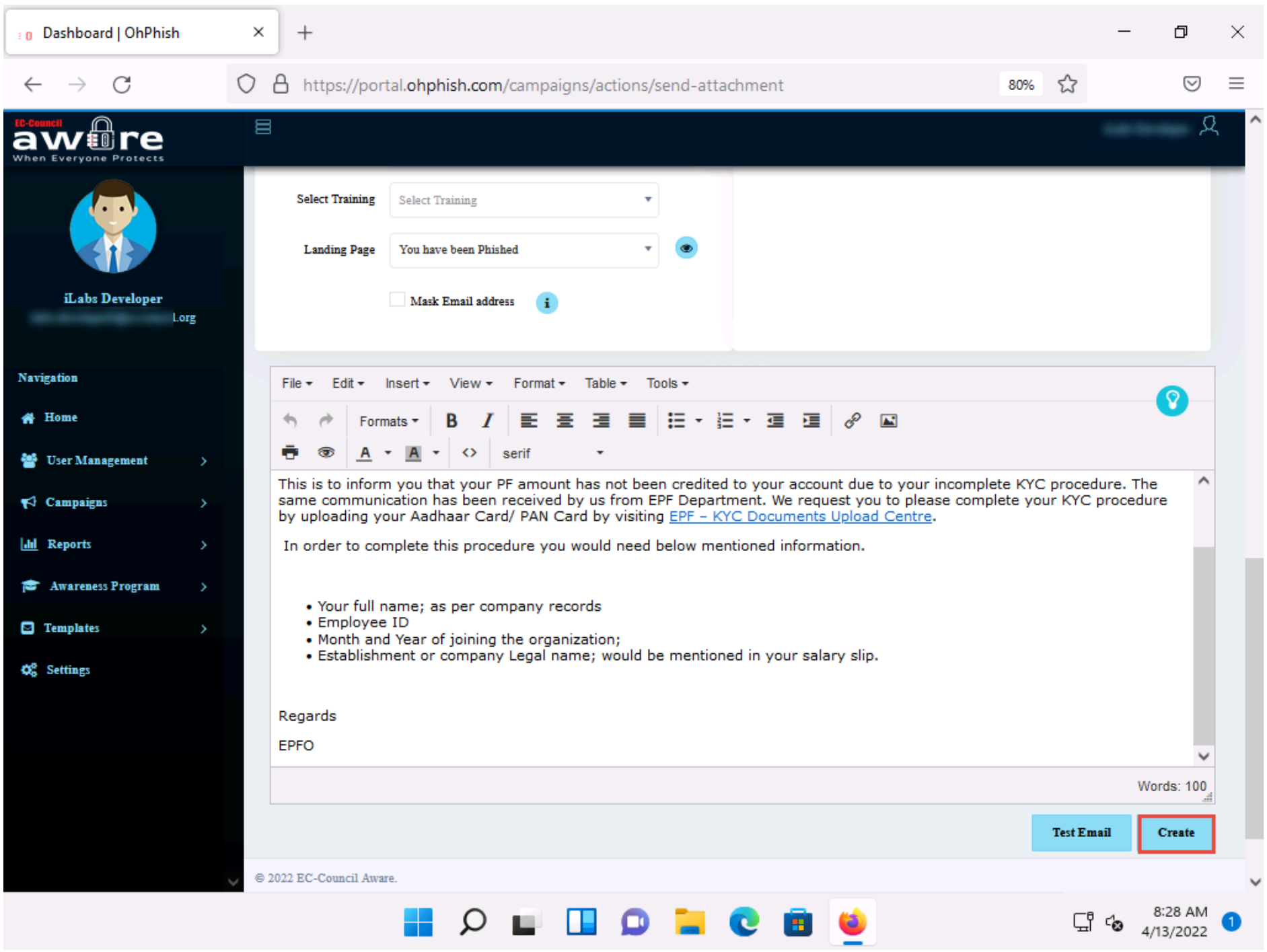
55. After adding the users' details, click **Import**.

56. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

> Note: 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**.

> Note: 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**.

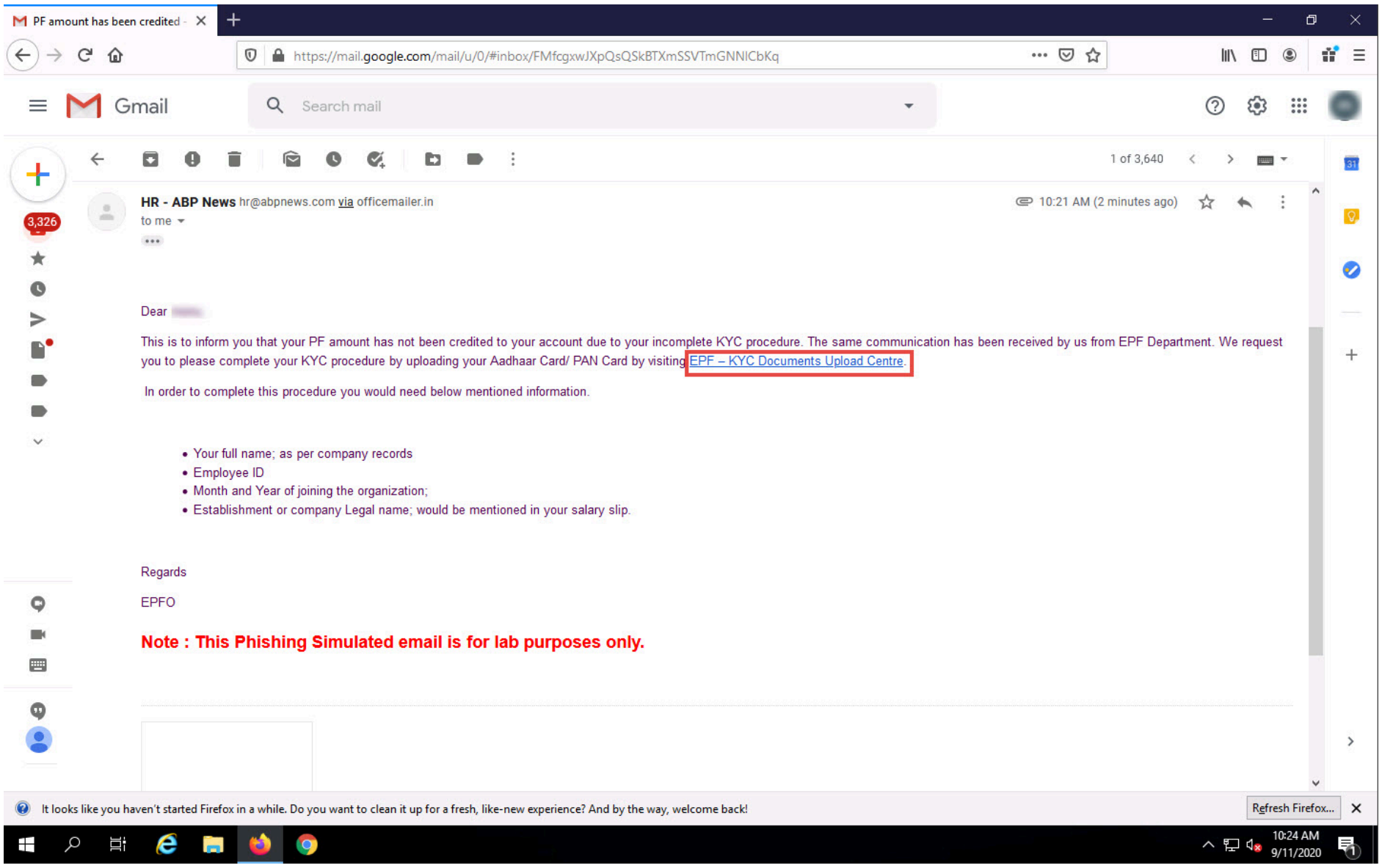
63. Now, click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.

> Note: If you are logged out of the **Windows Server 2019** machine, click **Ctrl+Alt+Del**, then login into **Administrator** user profile using **Pa$$w0rd** as password.

64. In the **Gmail** account opened previously, navigate to the **Inbox** folder.

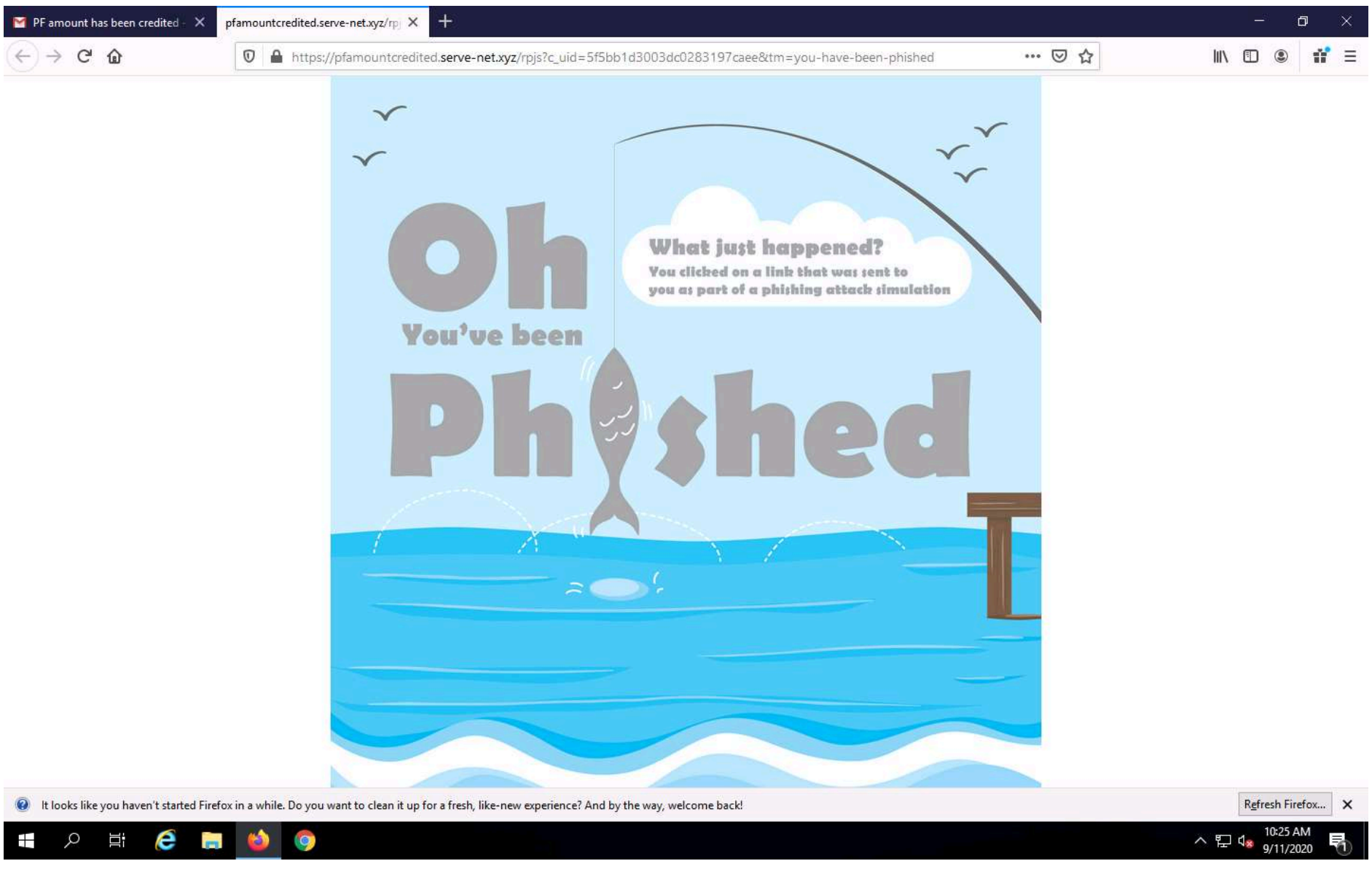
65. You will find an email from **HR – ABP News**, as shown in the screenshot.

66. Click on the **EPF – KYC Documents Upload Centre** hyperlink present in the email.



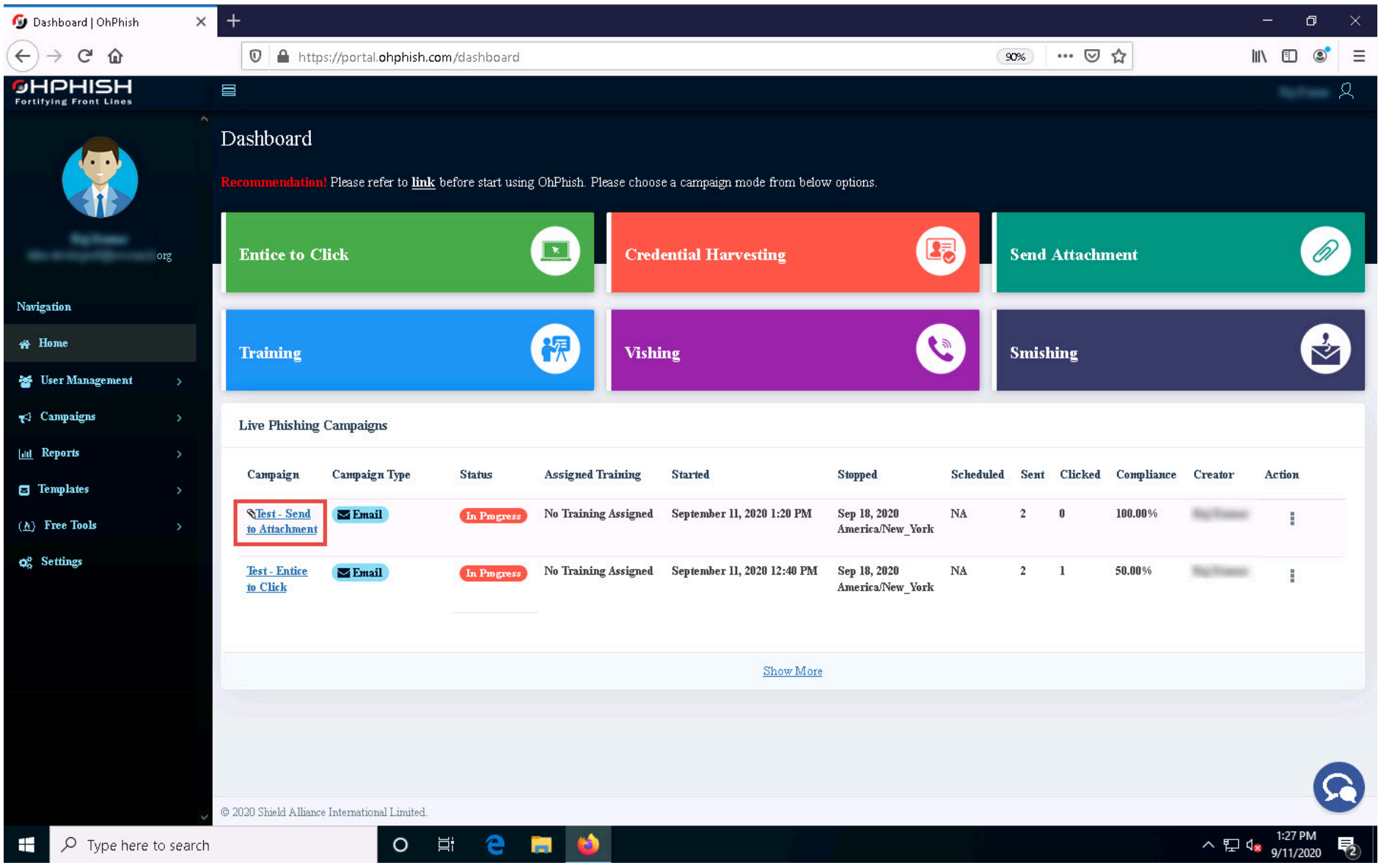
67. If a **Suspicious** link pop-up appears, click **Proceed**.

68. You will be re-directed to the **Oh You've been Phished** landing page, as shown in the screenshot.



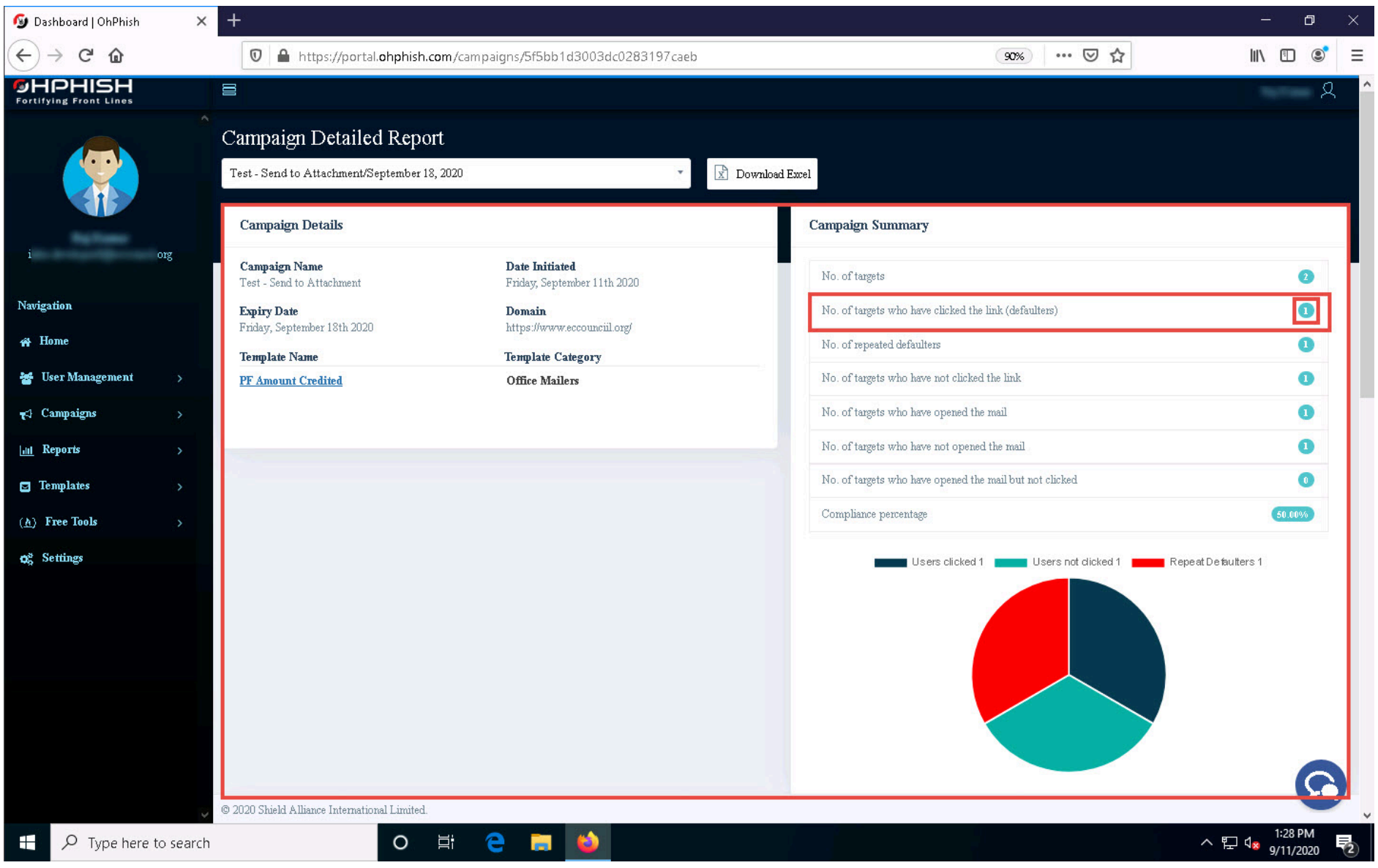
69. Now, click **CEHv12 Windows 11** to switch back to the **Windows 11** machine.

70. Click on the **Test – Send to Attachment** campaign present on the **OhPhish Dashboard**.

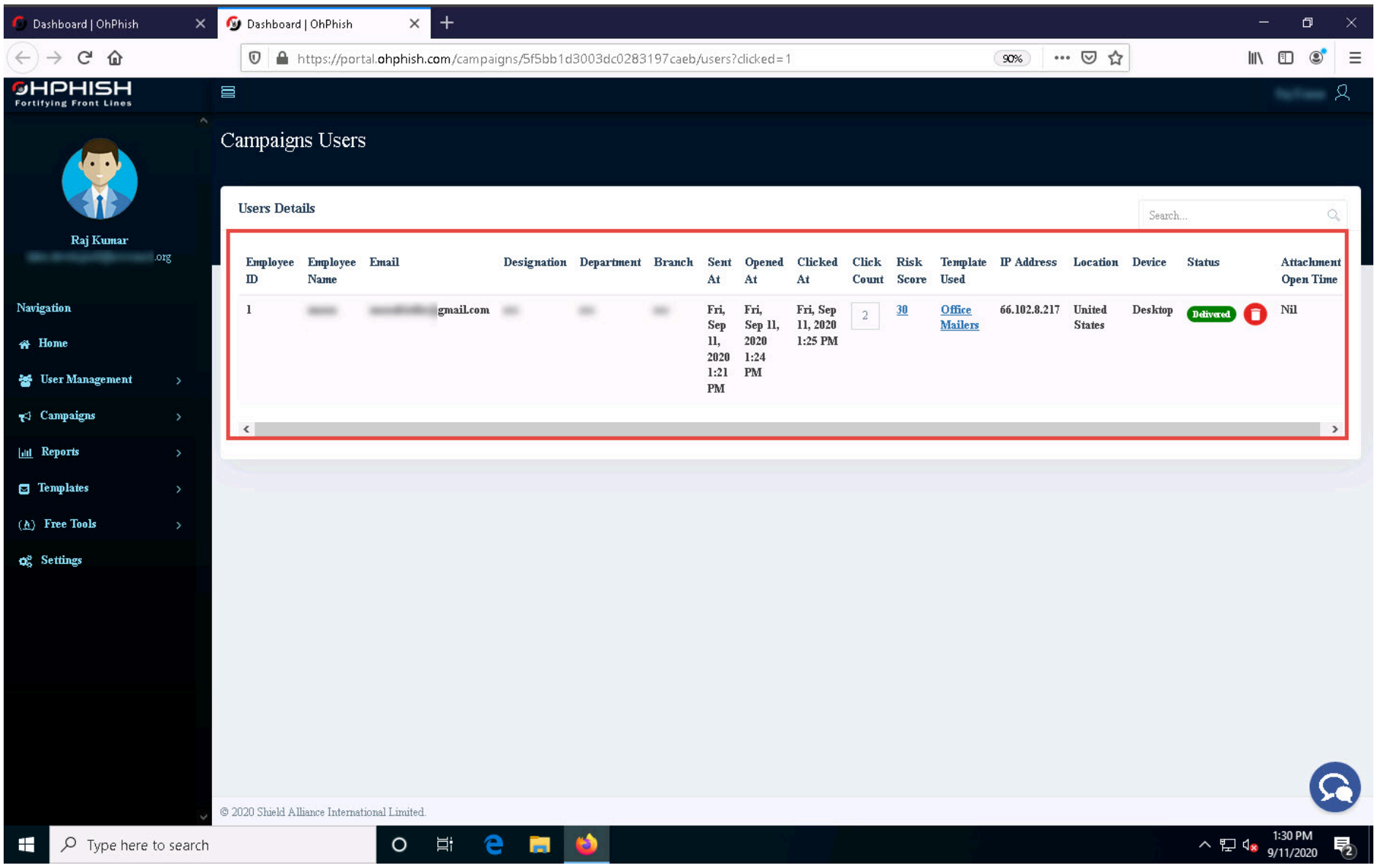


71. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.

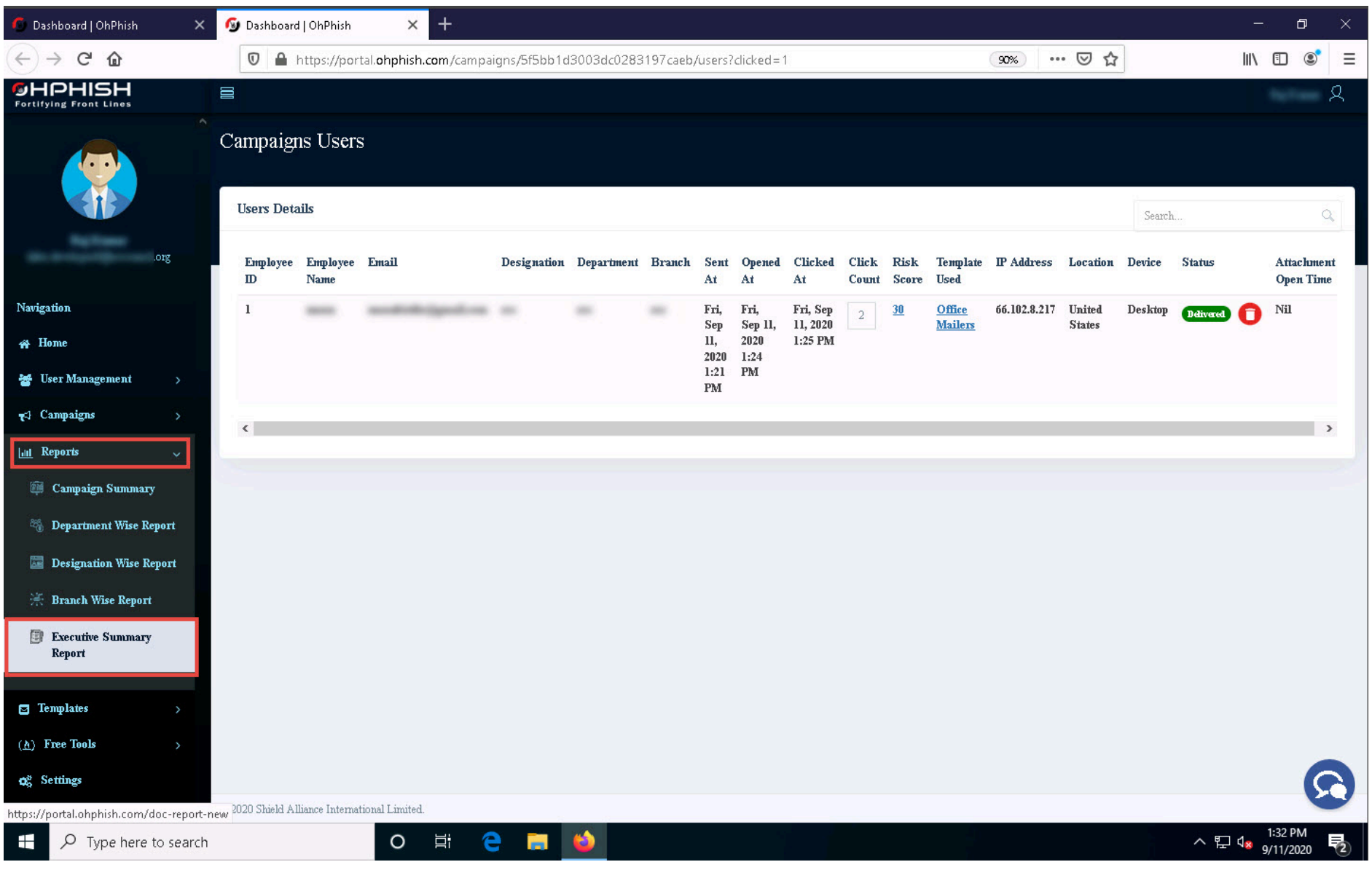
72. In the **Campaign Summary** section, you can observe that the value of **No. of targets who have clicked the link (defaulters)** is **1**. Click on **1** icon to see the defaulter.



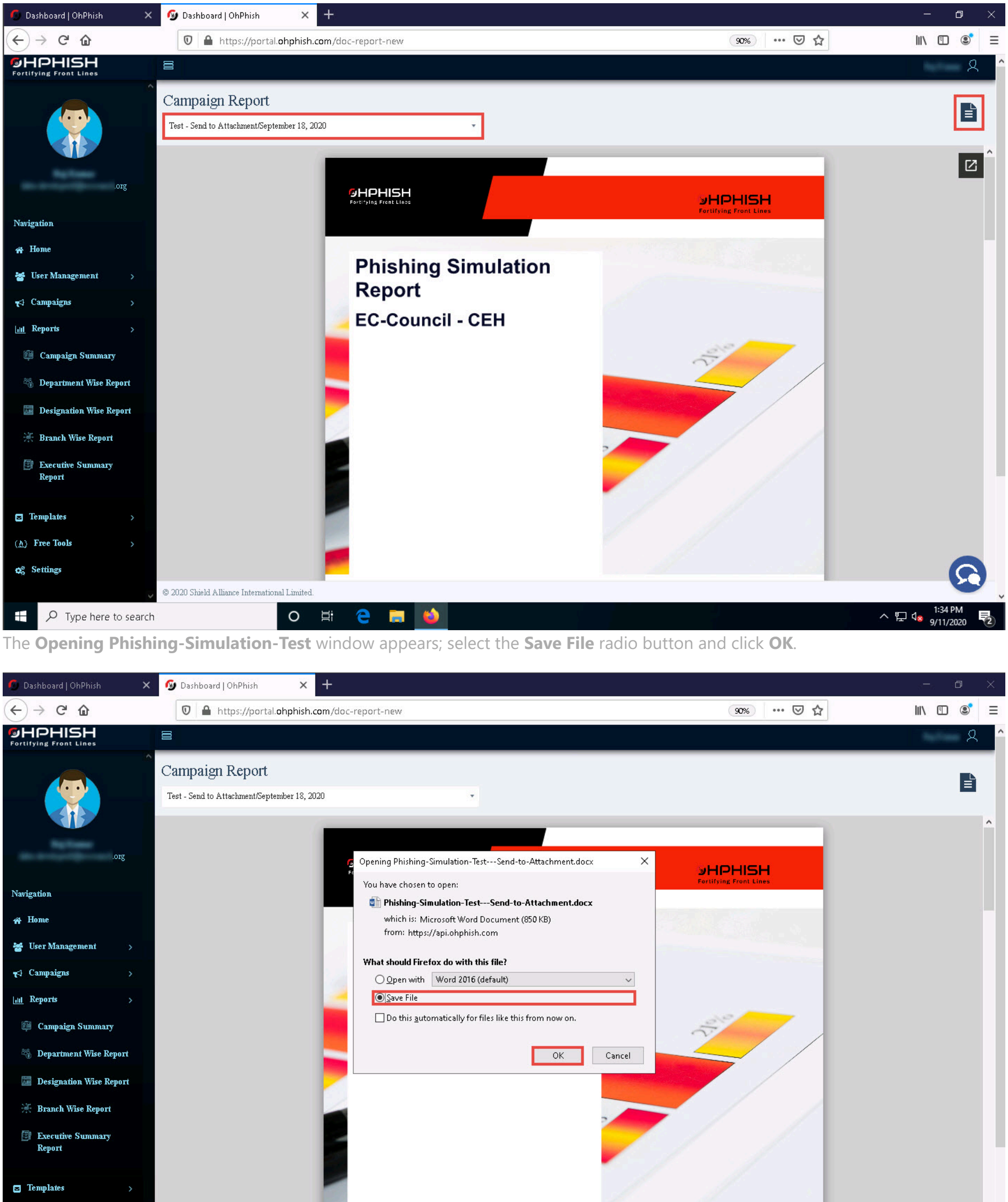
73. The **Campaigns Users** page appears, displaying the details of the defaulter, such as **Risk Score**, **Credentials**, **IP Address**, **Location**, etc., as shown in the screenshot.



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

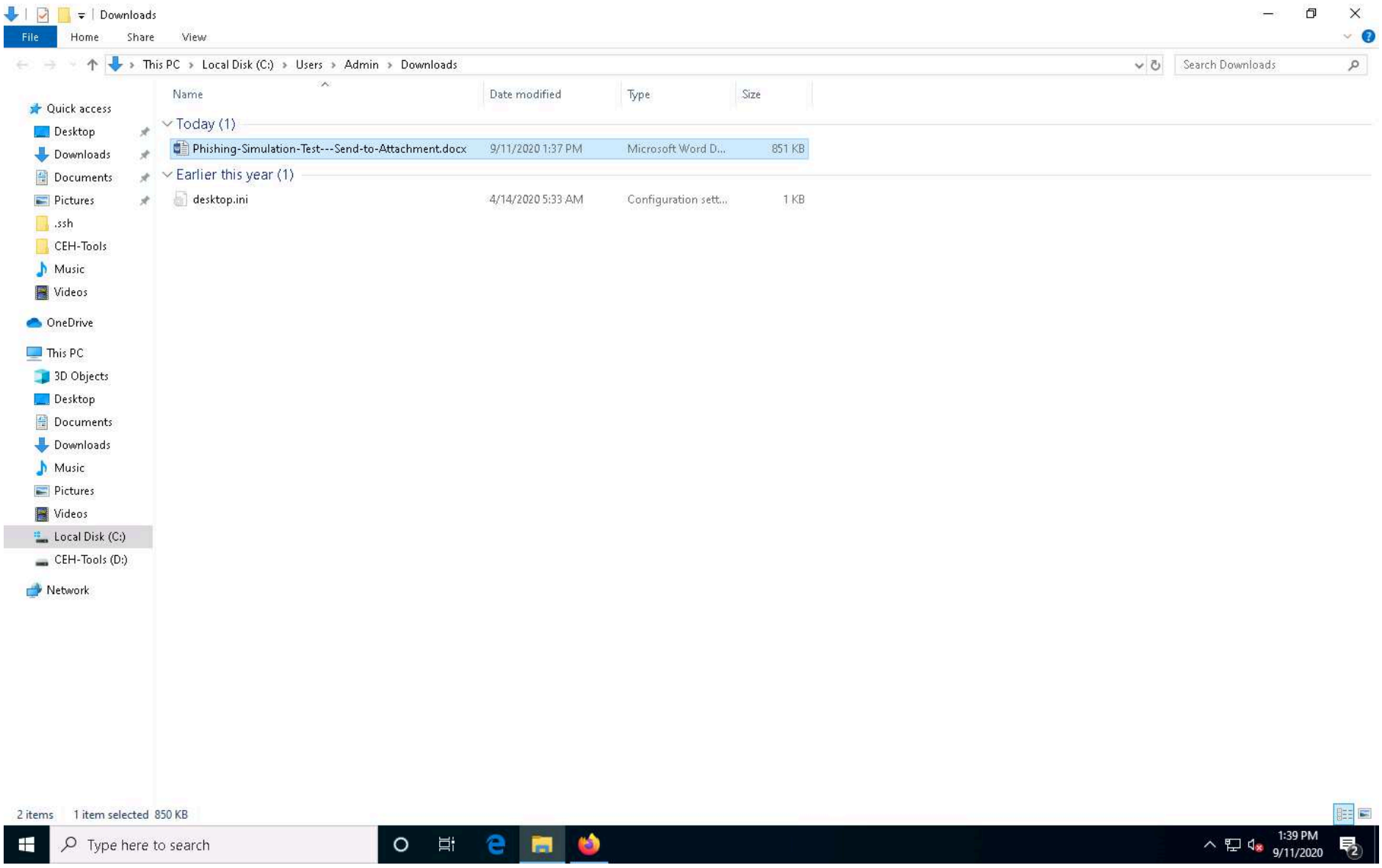


75. The **Campaign Report** page appears; select any phishing campaign from the drop-down list (here, **Test – Send to Attachment**) and click on the **Export** icon to export the report.



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

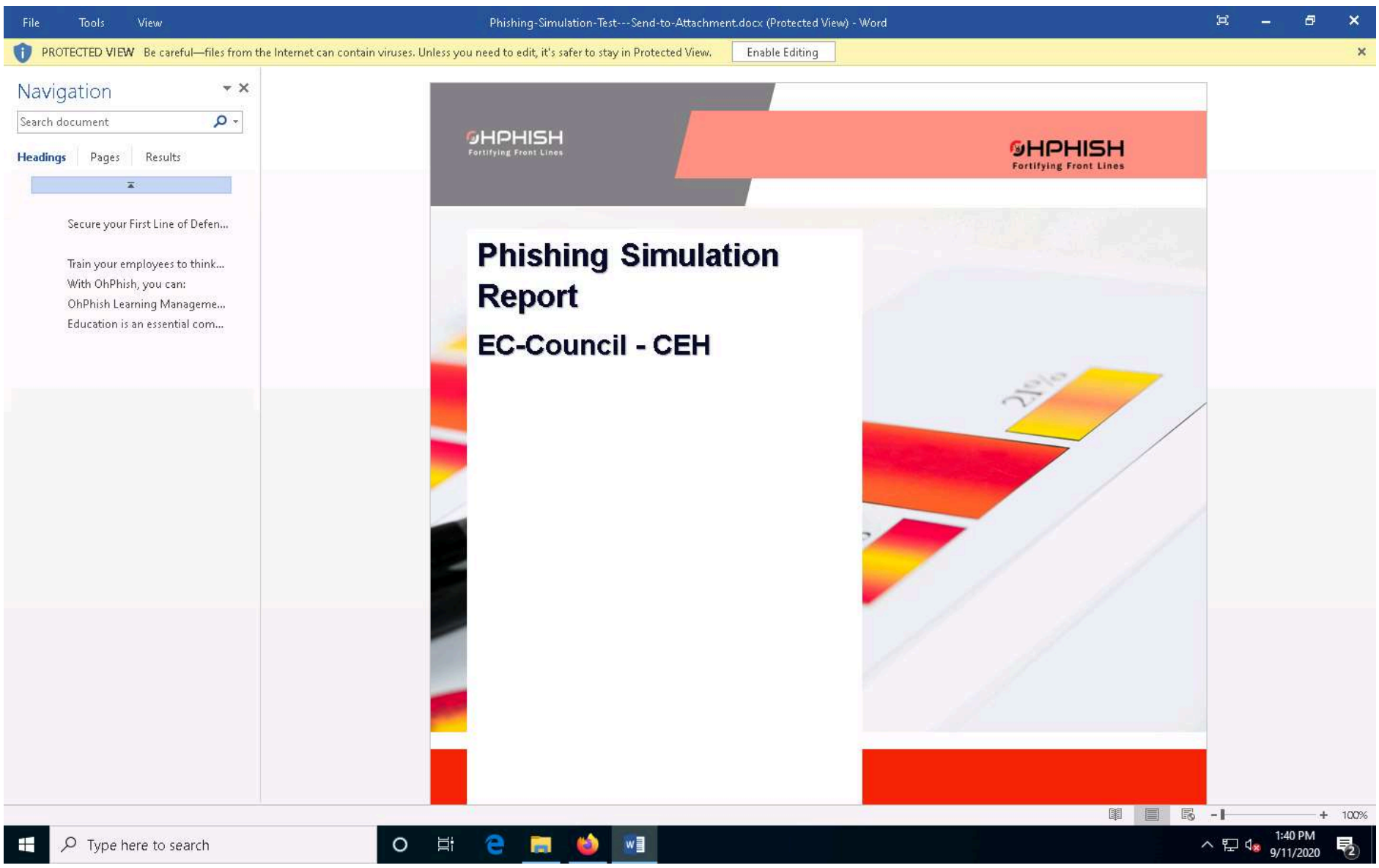
77. The file is downloaded to the default location (here, **Downloads**). Navigate to the download location and double-click the **Phishing-Simulation-Test---Send-Attachment** file to open it.

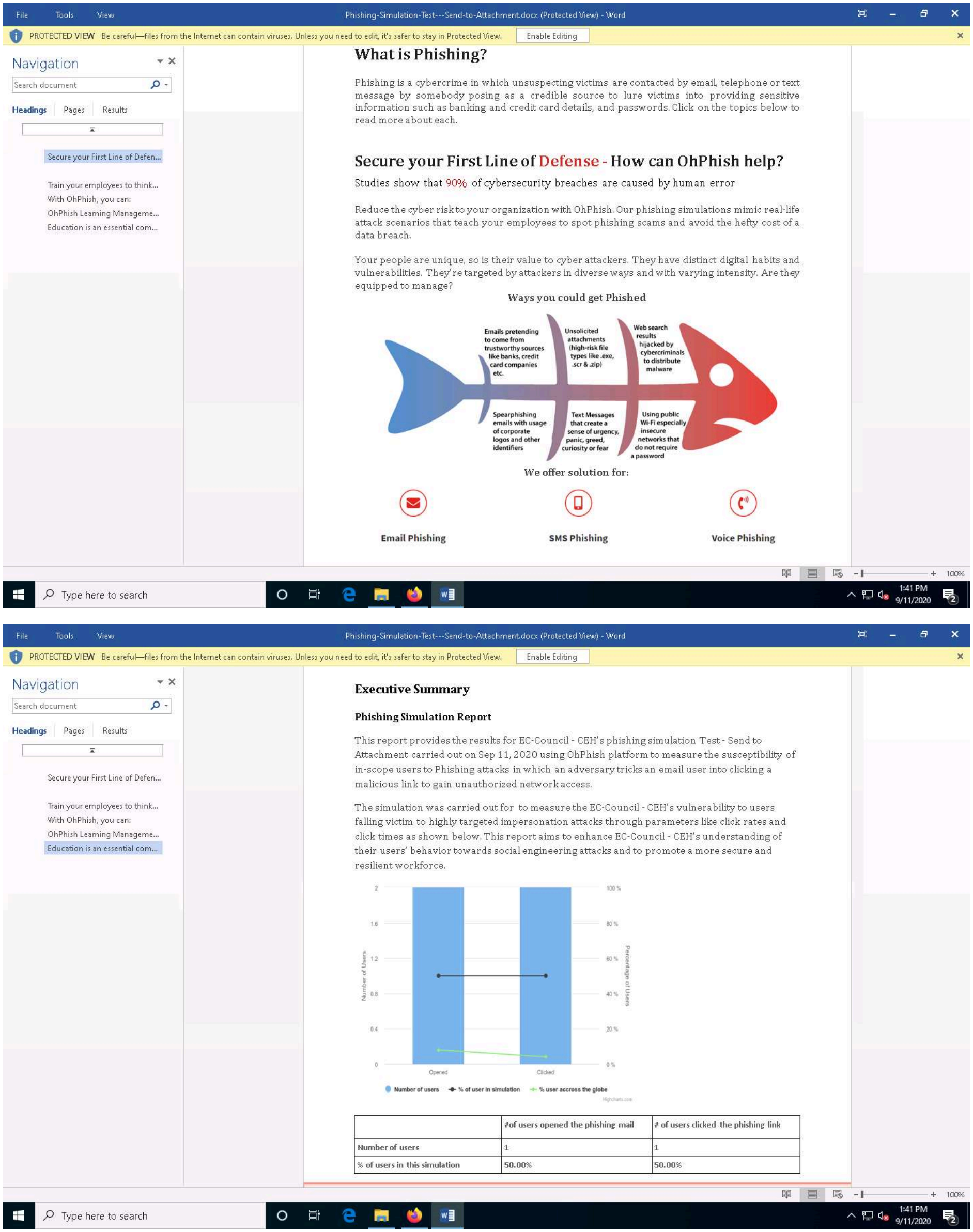


78. The executive phishing report appears in the document, as shown in the screenshot.

Note: If **Microsoft Word** pop-up appears, click **OK**. In the second **Microsoft Word** pop-up, click **Yes**.

Note: 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 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.