

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.

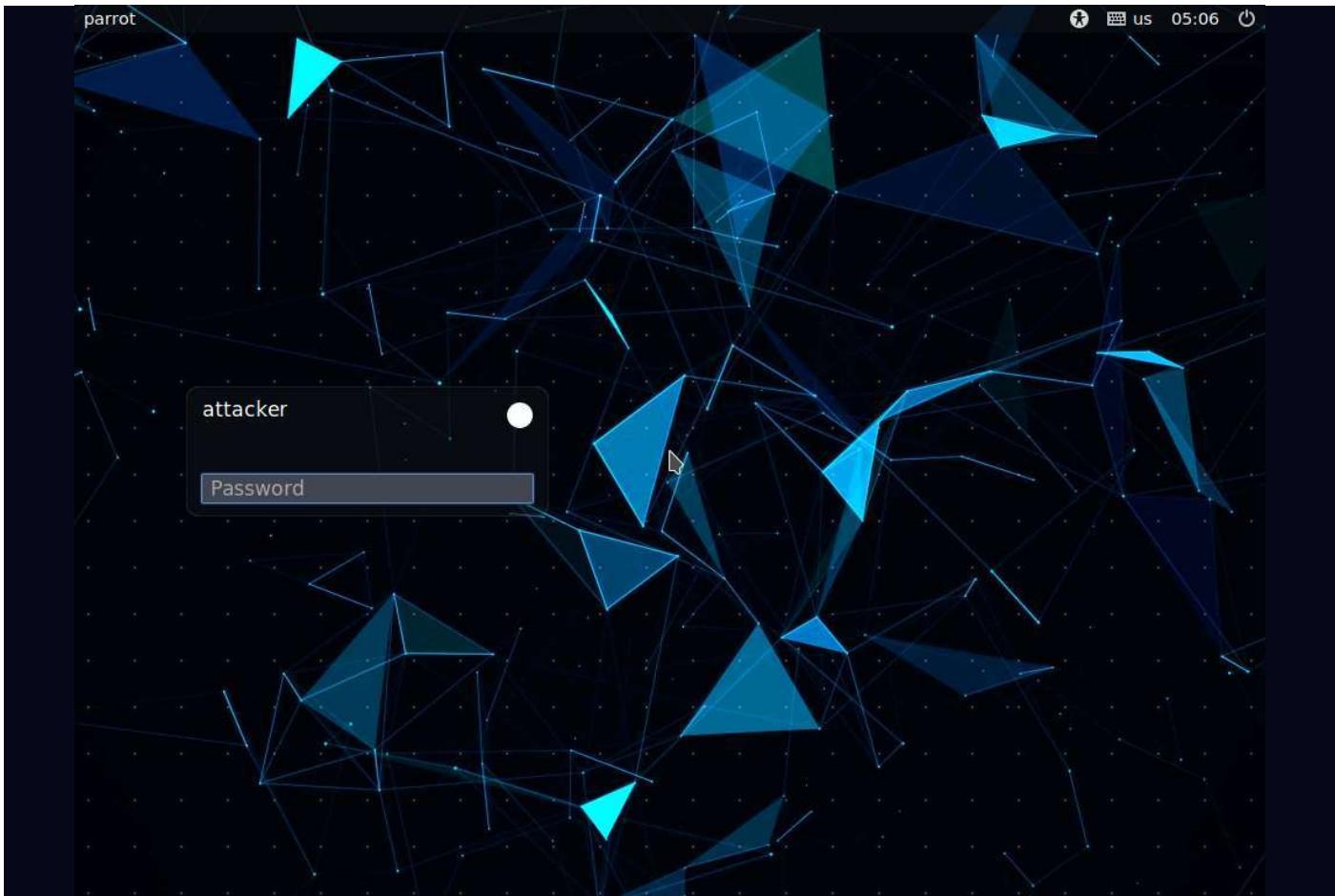
Although many kinds of attacks can be carried out using SET, it is also a must-have tool for penetration testers to check for vulnerabilities. For this reason, SET is the standard for social engineering penetration tests, and is strongly supported within the security community.

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.

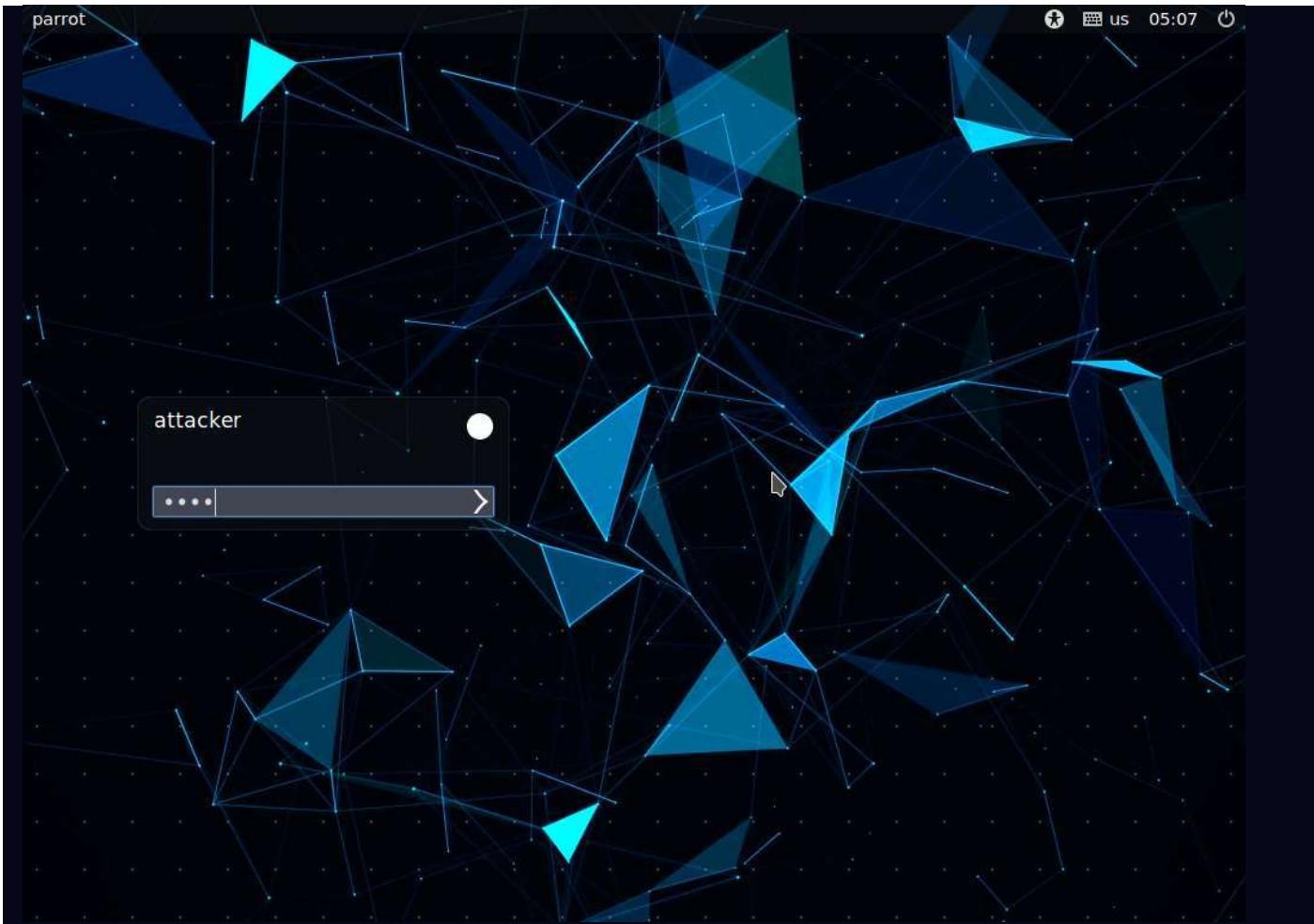




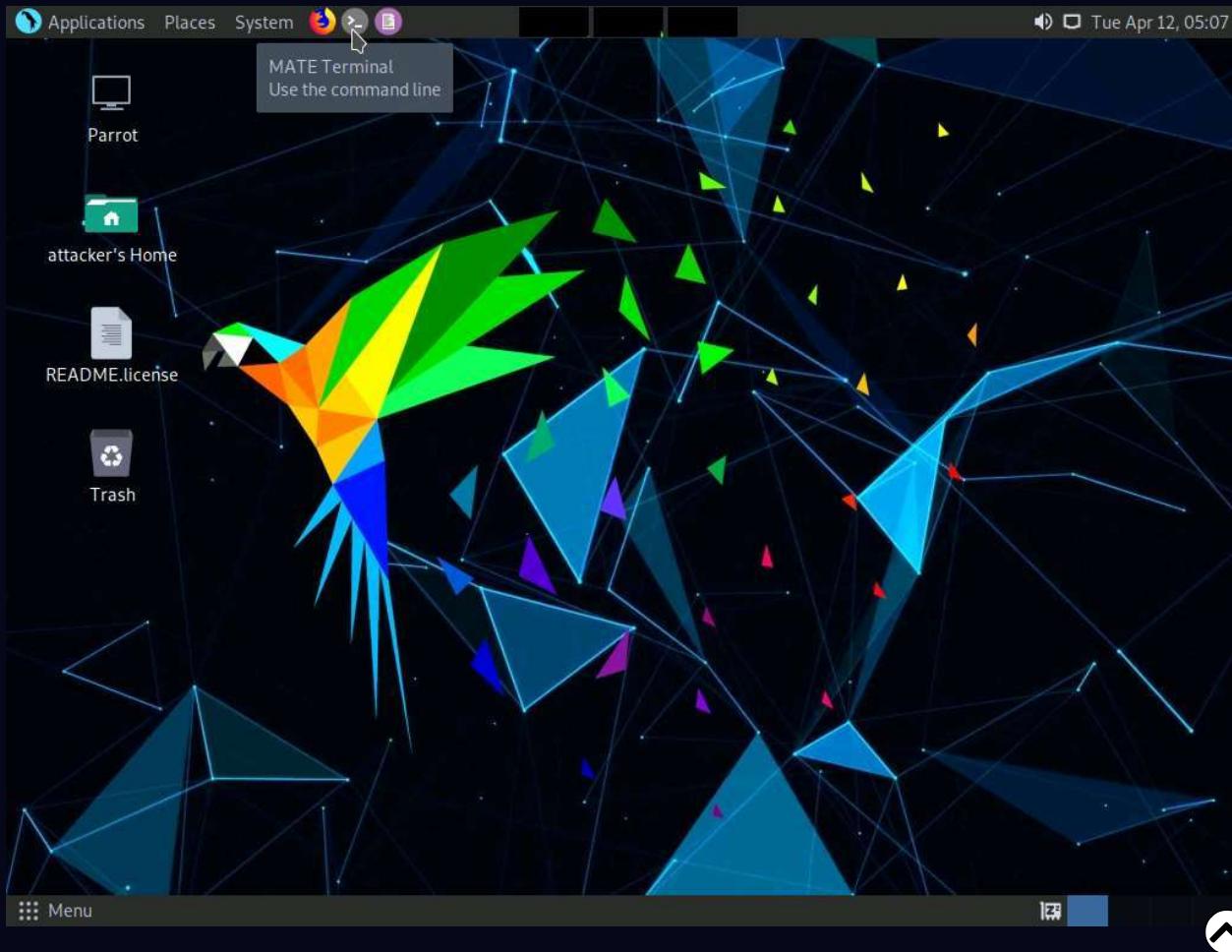
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the Password field and press Enter to log in to the machine.

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.

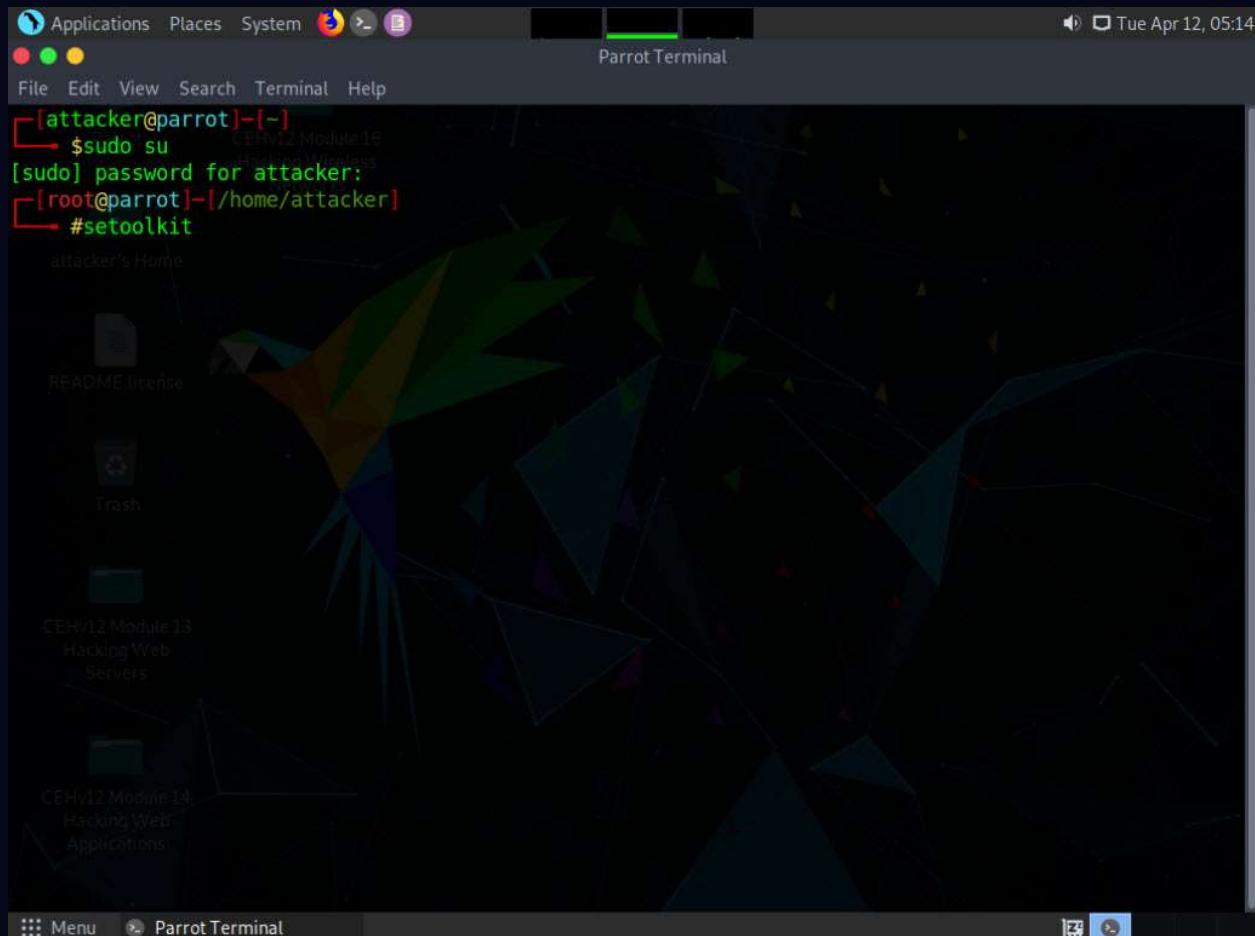


4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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**.



```
Applications Places System > /setoolkit - Parrot Terminal
File Edit View Search Terminal Help
[---] The Social-Engineer Toolkit (SET) [---]
[---] Parrot Created by: David Kennedy (ReL1K) [---]
      Version: 8.0.3
      Codename: 'Maverick'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

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

```
Applications Places System > /setoolkit - Parrot Terminal
File Edit View Search Terminal Help
[---] Follow us on Twitter: @TrustedSec [---]
[---] Parrot Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

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

```
Applications Places System ./setoolkit - Parrot Terminal
File Edit View Search Terminal Help
Tue Apr 12, 05:17

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

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

```
Applications Places System ./setoolkit - Parrot Terminal
File Edit View Search Terminal Help
Tue Apr 12, 05:17

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
```

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.

```
./setoolkit - Parrot Terminal
File Edit View Search Terminal Help
3) Custom Import
99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

----- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * -----
README/license

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 perspective, 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 [10.10.1.13]:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: http://www.moviescope.com
```

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.



```
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: Home

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 perspective, 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 [10.10.1.13]:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.moviescope.com

[*] Cloning the website: http://www.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:
```

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.

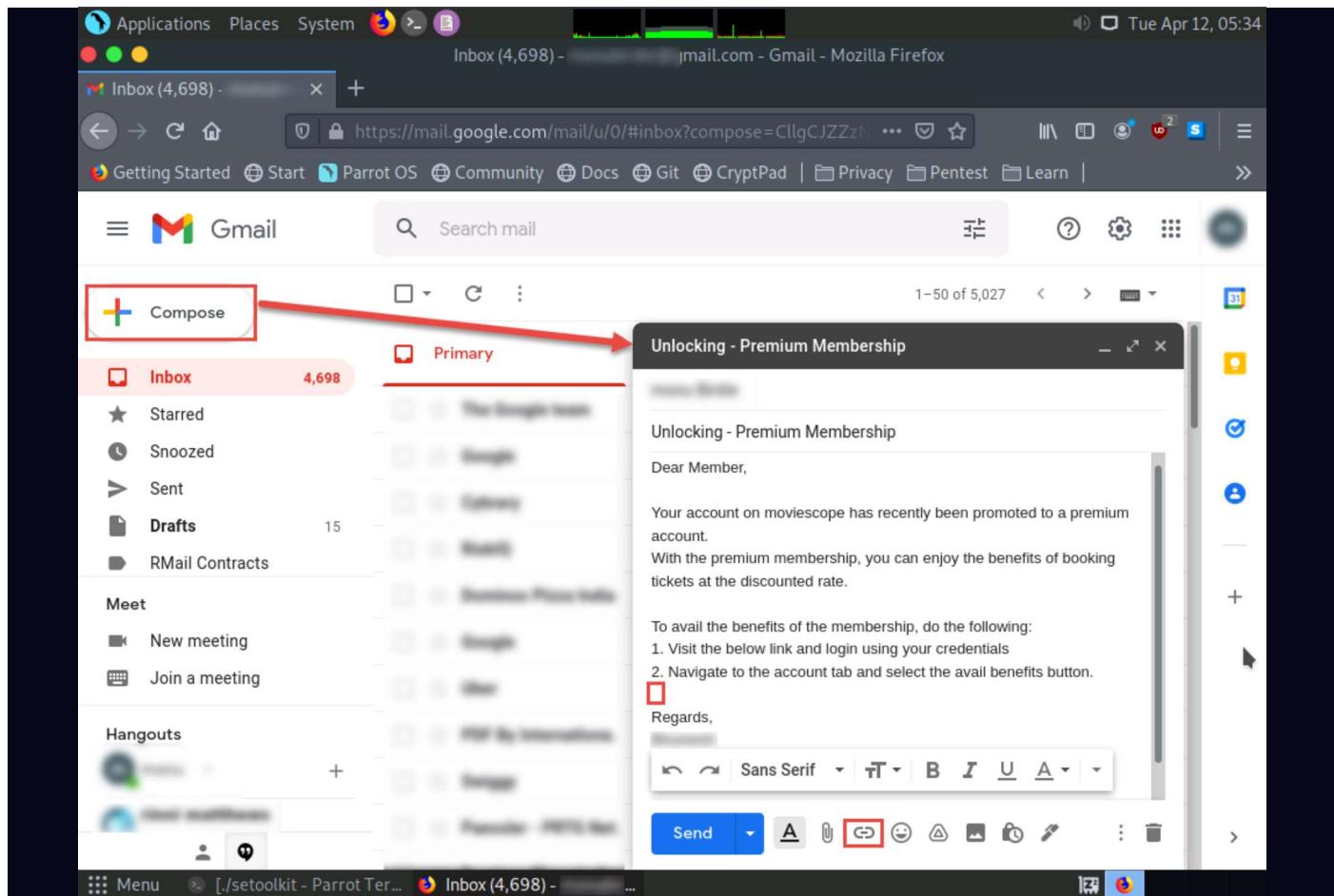
16. Click **Firefox** icon from the top-section of the **Desktop** to launch a web browser window and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively). Log in, and compose an email.

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

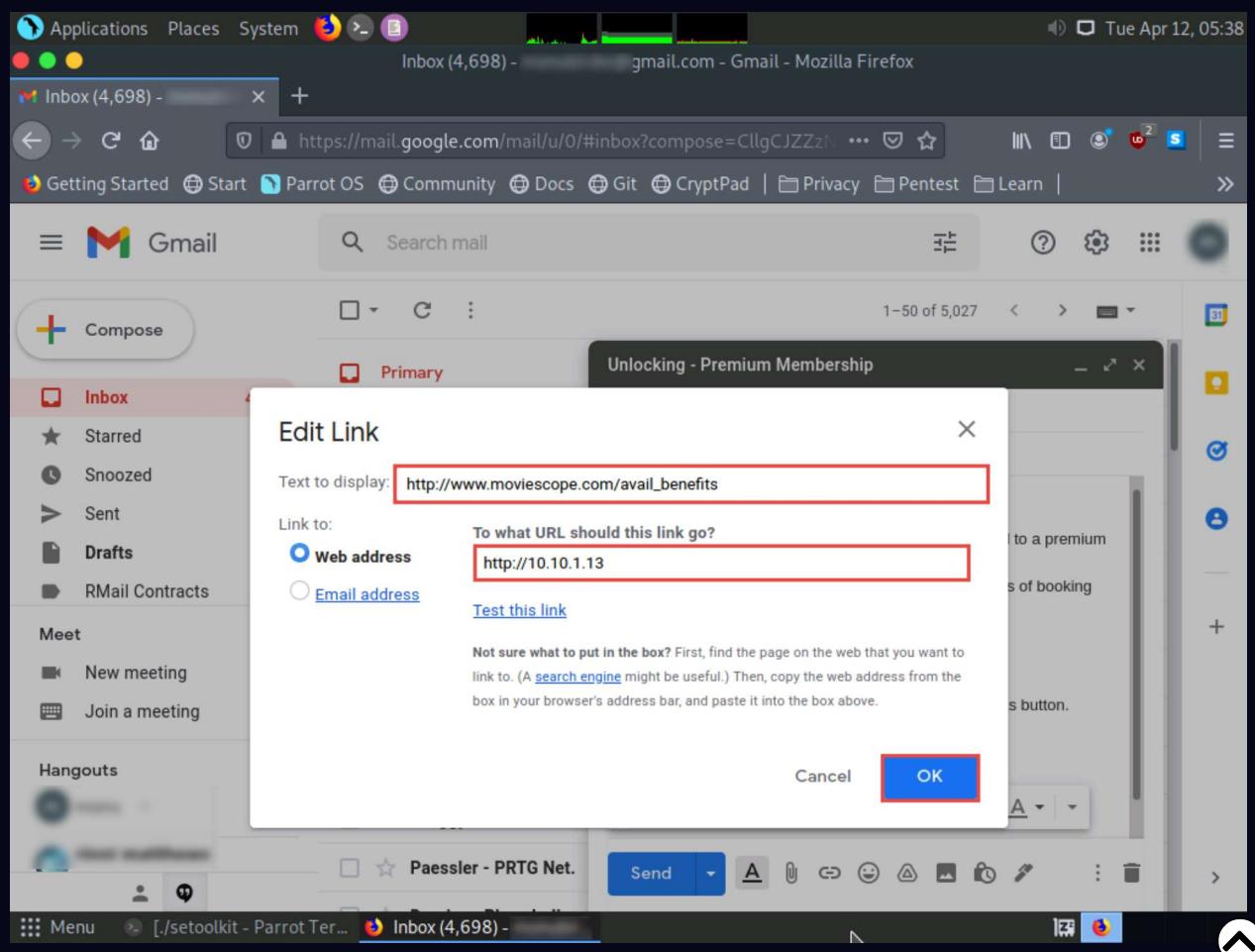
17. After logging into your email account, click the **Compose** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

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.

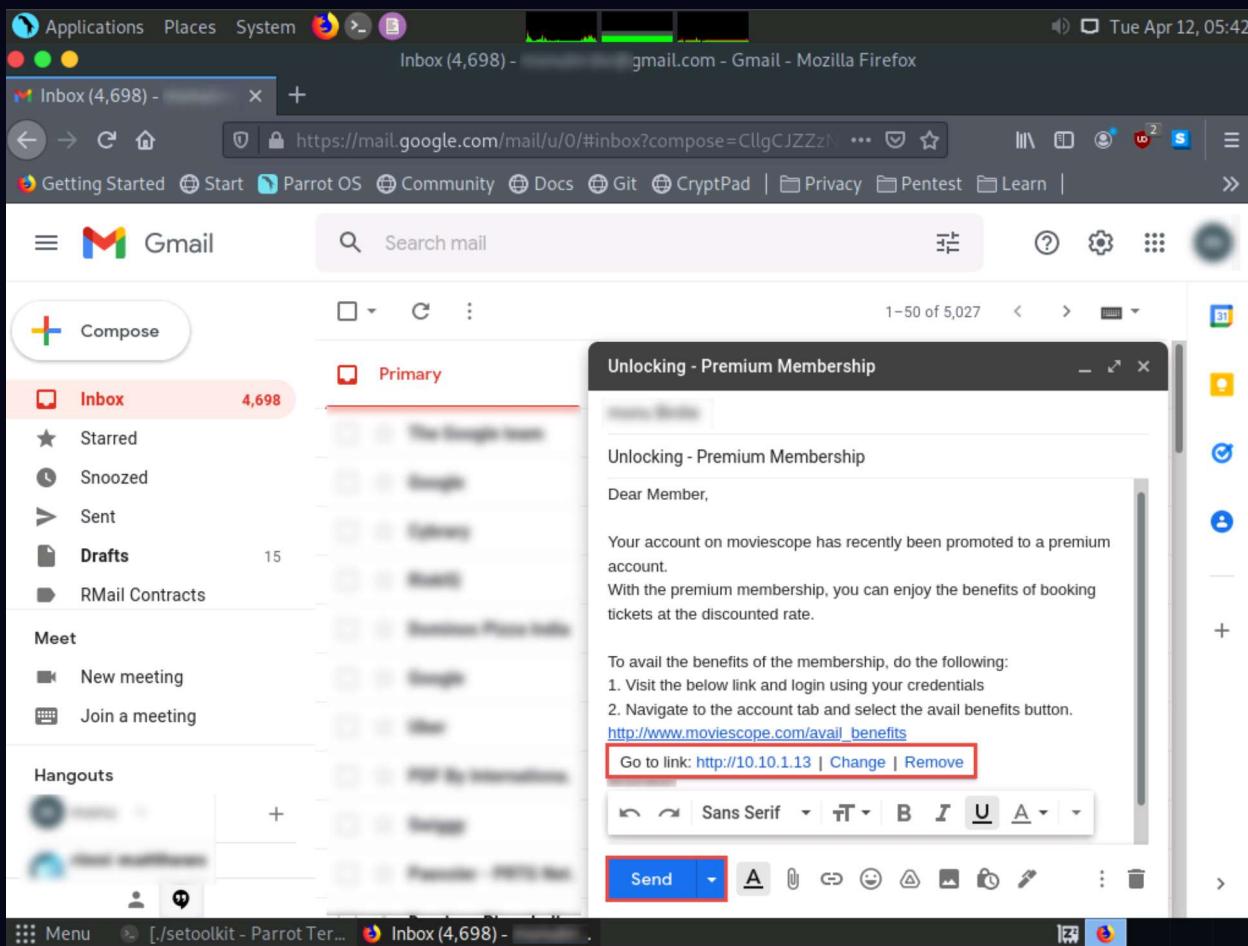


19. In the **Edit Link** window, first type the actual address of your cloned site in the **Web address** field under the **Link to** section. Then, type the fake URL in the **Text to display** field. In this case, the actual address of our cloned MovieScope site is <http://10.10.1.13>, and the text 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.

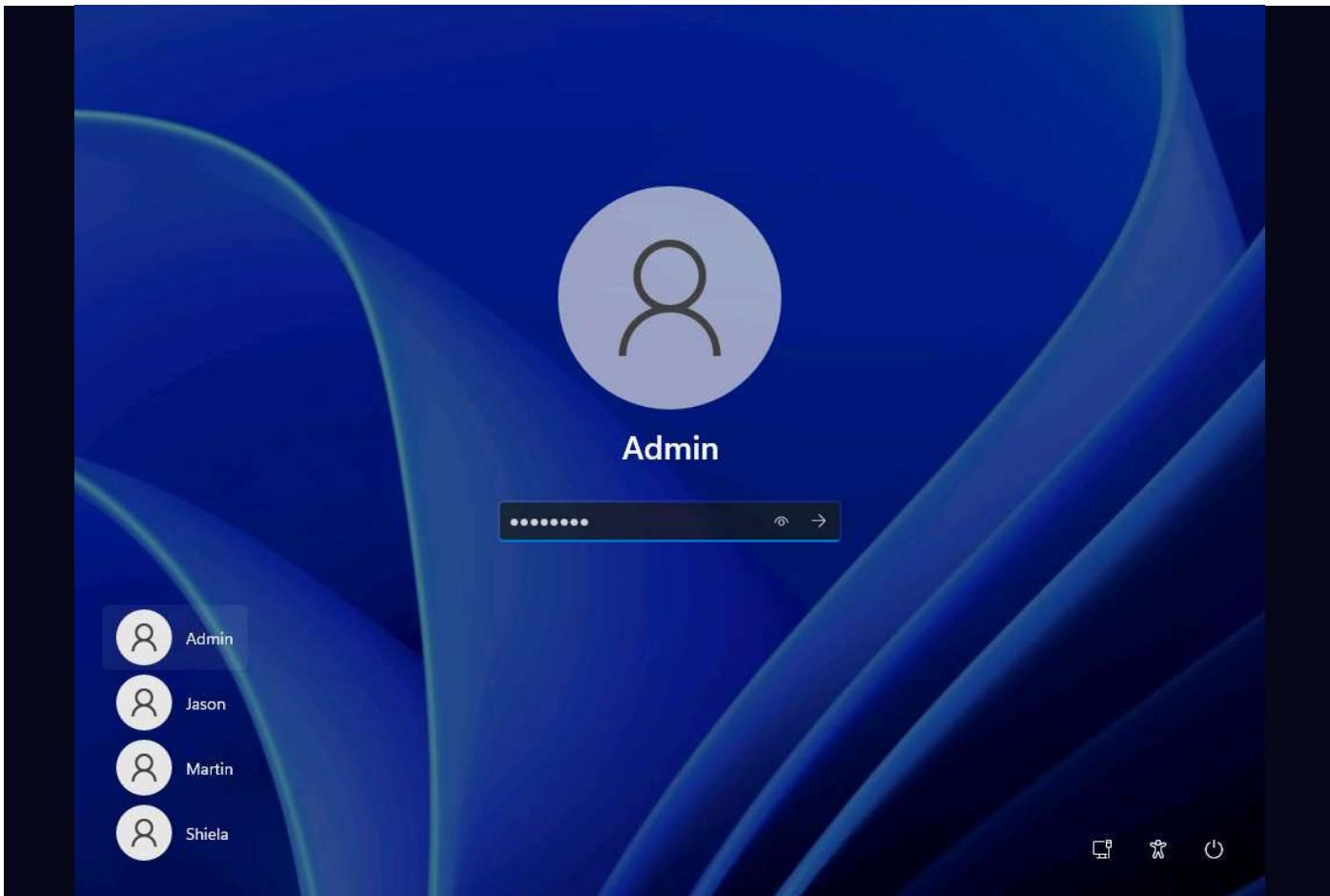
21. Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "Go to link" pop-up. Once verified, send the email to the intended user.



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.

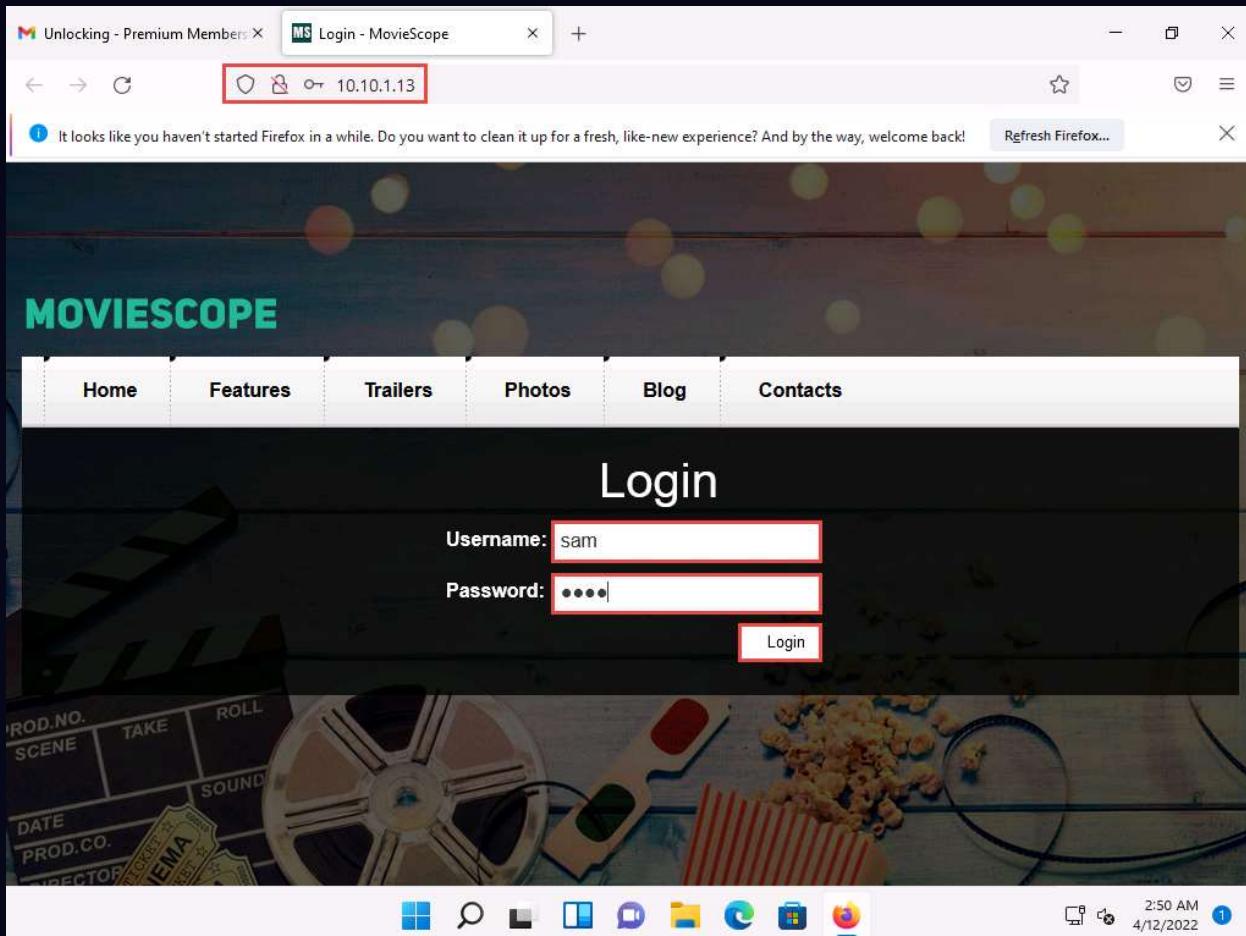


23. Open any web browser (here, we are using **Mozilla Firefox**), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.

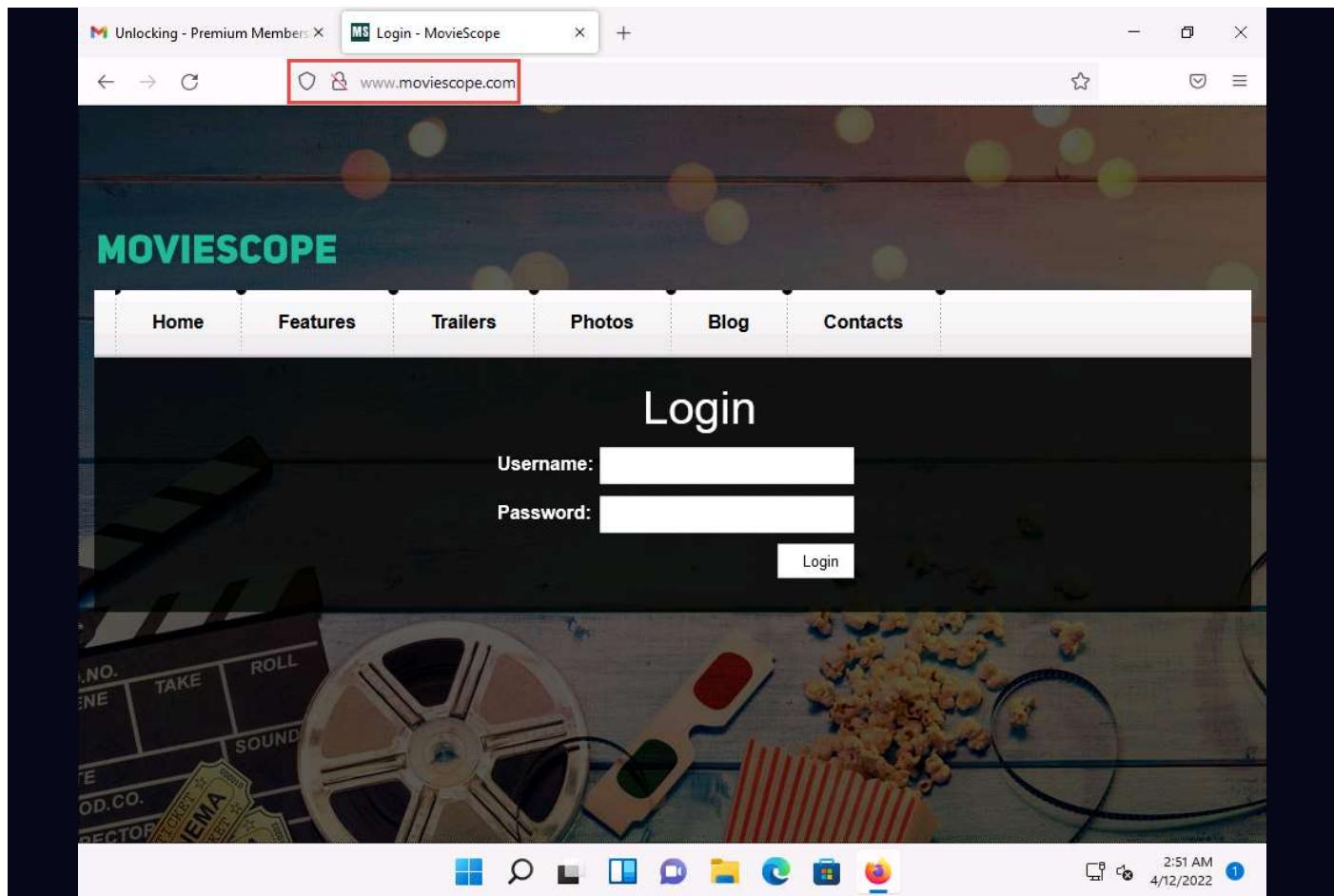
A screenshot of a Mozilla Firefox browser window. The address bar shows the URL https://mail.google.com/mail/u/0/#inbox/KtbxLvhGKMKxwVBlMDNgznNdsRDXvpfDHg. The main content area displays an email from "Unlocking - Premium Membership" to "to me". The email body reads: "Your account on moviescope has recently been promoted to a premium account. With the premium membership, you can enjoy the benefits of booking tickets at the discounted rate. To avail the benefits of the membership, do the following:
1. Visit the below link and login using your credentials
2. Navigate to the account tab and select the avail benefits button." A red box highlights the URL "http://www.moviescope.com/avail_benefits". The Firefox taskbar at the bottom shows various pinned icons.

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.

```
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.10.1.11 - - [12/Apr/2022 05:49:52] "GET / HTTP/1.1" 200 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery-ui.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery-ui.selectmenu.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.quicksand.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.script.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:49:53] "GET /js/jquery.min.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:50:03] "GET /js/jquery.superfish.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:50:13] "GET /js/jquery-ui.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:50:23] "GET /js/jquery-ui.selectmenu.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:50:33] "GET /js/jquery.flexslider-min.js HTTP/1.1" 404 -
10.10.1.11 - - [12/Apr/2022 05:50:43] "GET /js/jquery.quicksand.js HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: __VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZH5l0cnJ+BtsUZt5M/WlqLFqT5uNaq6G+46A4bz6/sML
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdAARJUub9rbp0xjNNNjxtMliRWMttrRuIi9aE3DBg1Dcn0GGcP002LAX9axRe6vMQj2F3f3AwSKugaKAa3qX7zRfq070LdPacUhnsPpHrm03jI6uFMcyULVYtnt+iQJOBgU=
POSSIBLE USERNAME FIELD FOUND: txtusername=sam
POSSIBLE PASSWORD FIELD FOUND: txtpwd=test
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.10.1.11 - - [12/Apr/2022 05:50:51] "POST /index.html HTTP/1.1" 302 -
```

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.



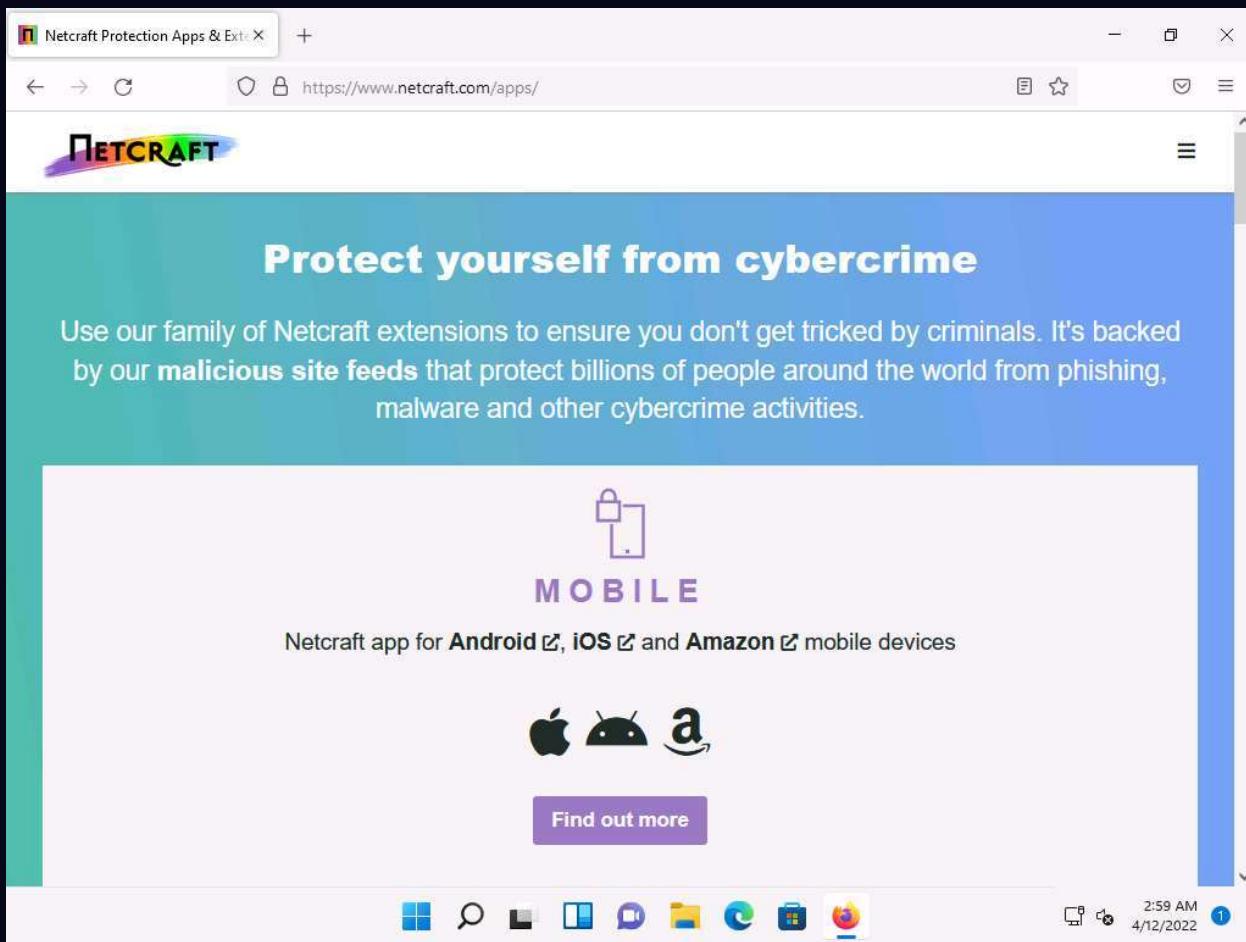
Task 1: Detect Phishing using Netcraft

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.

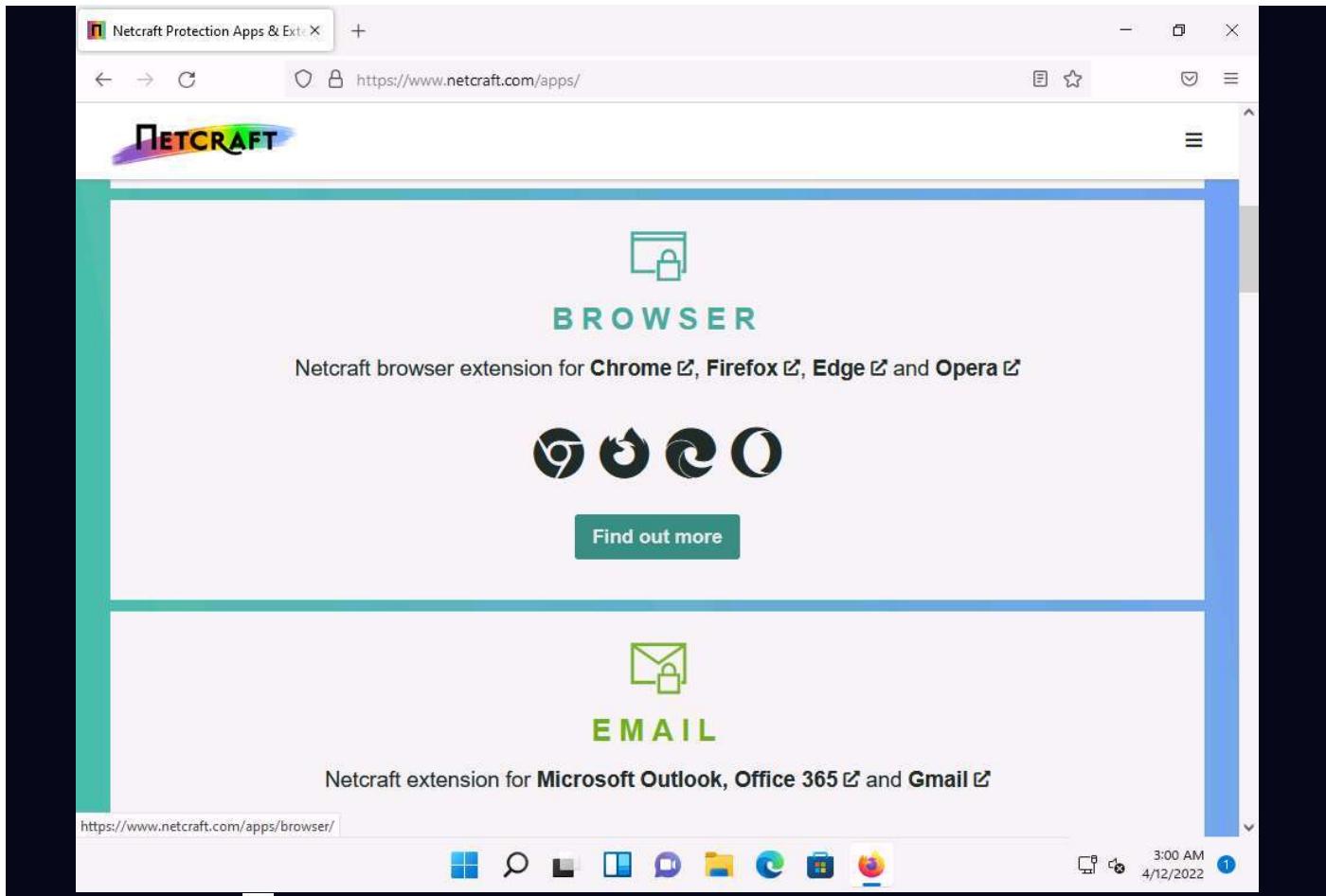
1. Click on the **CEHv12 Windows 11** to switch to the **Windows 11** machine.
2. First, it is necessary to install the Netcraft extension. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor, type <https://www.netcraft.com/apps/>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

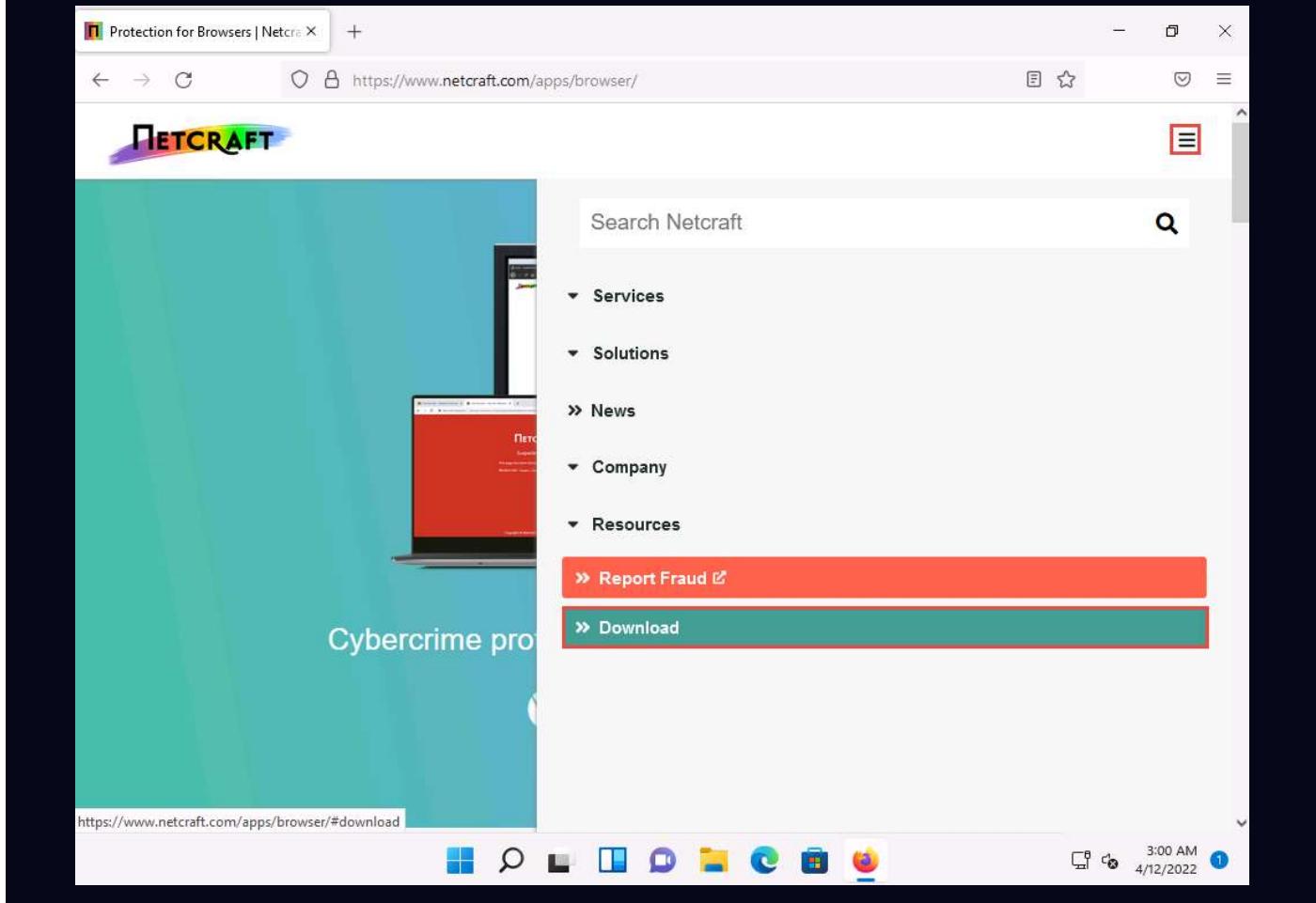


4. Scroll-down and click **Find out more** button under **BROWSER** option on the webpage.





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.

The browser extension can be downloaded for free from your browser's store.

Want to protect your other platforms?

We also have apps to help protect you from phishing for your mail and mobile.

[Find out more](#)

Commercial Services Resources Company

https://addons.mozilla.org/en-us/firefox/addon/netcraft-toolbar?src=external-apps-download

3:14 AM 4/12/2022 1

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

Netcraft Extension – Get this Ext

https://addons.mozilla.org/en-US/firefox/addon/netcraft-toolbar/?src=external-apps-down

Firefox Add-ons Blog Extension Workshop Developer Hub Log in

Firefox Browser ADD-ONS Extensions Themes More... Find add-ons

Netcraft Extension by Netcraft Ltd

This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.

Learn more

5,246 Users 30 Reviews 4.4 Stars

Rating	Count
5★	24
4★	1
3★	1
2★	0
1★	4

Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web

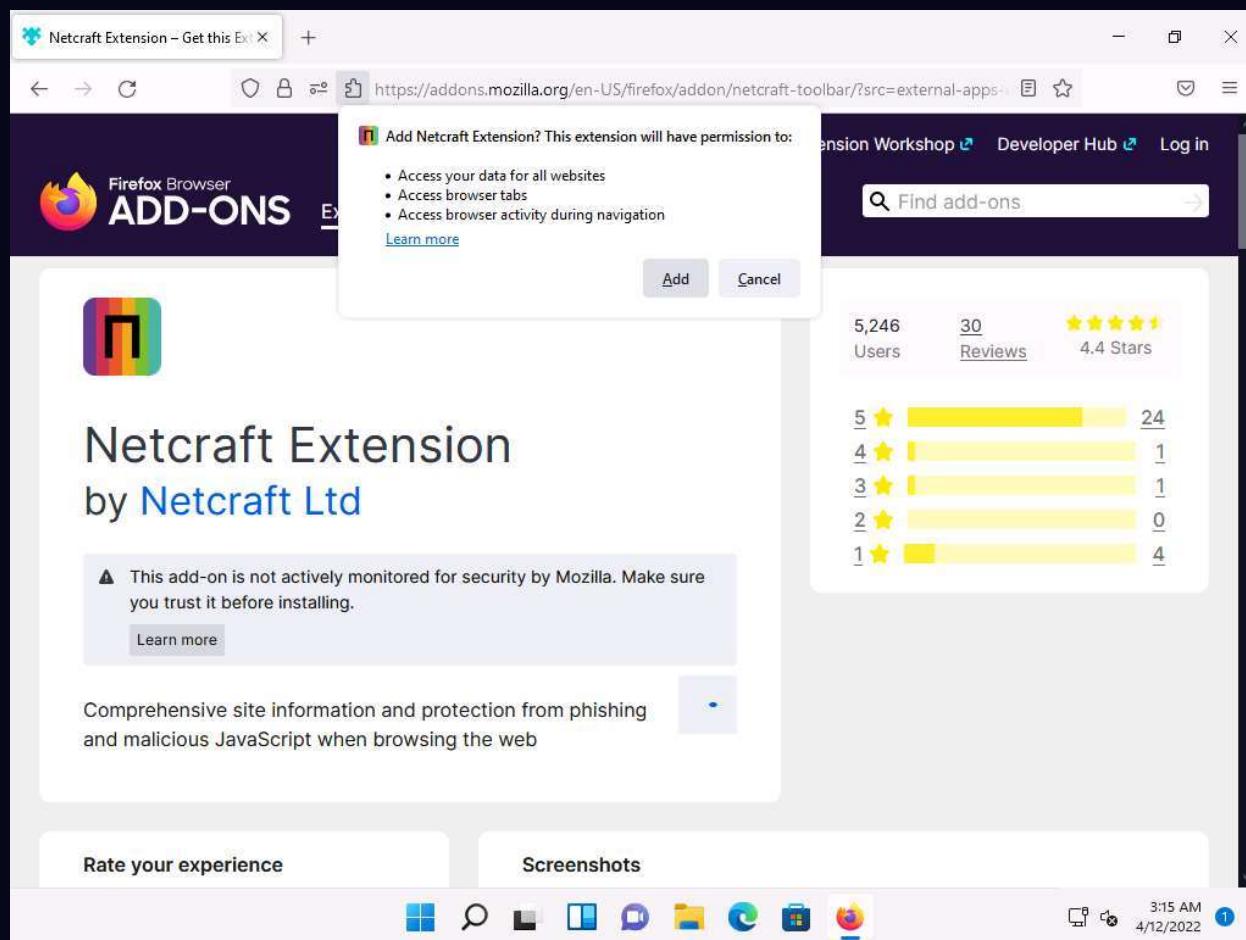
Add to Firefox

https://addons.mozilla.org/firefox/downloads/file/3852537/netcraft_extension-1.16.9-fx.xpi

3:14 AM 4/12/2022 1

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.

The screenshot shows the Firefox Add-ons page for the Netcraft Extension. The extension icon is a colorful 'N' shape. The title is "Netcraft Extension by Netcraft Ltd". A warning message states: "⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing." Below the warning, a description says: "Comprehensive site information and protection from phishing and malicious JavaScript when browsing the web". To the right, there are statistics: 5,246 users, 30 reviews, and a 4.4 Stars rating. A star rating breakdown shows: 5★ (24), 4★ (1), 3★ (1), 2★ (0), and 1★ (4). The browser taskbar at the bottom shows various pinned icons.

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.

The screenshot shows the Firefox browser window. The main page is the homepage of [certifiedhacker.com](http://www.certifiedhacker.com). On the right side of the screen, a Netcraft extension dialog box is open. The dialog box displays the following information:

- www.certifiedhacker.com**
- Site Report**
- Risk Rating: 0**
- Country: US**
- Site rank: 28,724**
- First seen: Dec 2002**
- Host: Unified Layer**
- Disable protection for this site** (with a checkbox)
- Report malicious URL:**
 - The URL of the site: <http://www.certifiedhacker.com/> (with a checked checkbox)
 - Add a reason (with a checkbox)
- Your email address (to receive updates):** you@example.com (with a checked checkbox)
- Submit Report** button

The browser taskbar at the bottom shows various pinned icons.

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

The screenshot shows a Microsoft Edge browser window with two tabs open. The left tab is for 'certifiedhacker.com' and displays a 'UNDER CONSTRUCT' page with a yellow banner stating 'We are currently down for maintenance'. It includes a large digital clock showing '00:02:14:1' and a 'Please give us your email' input field. The right tab is a 'Site Report' from Netcraft for the same domain. This report includes a small American flag icon, the URL 'www.certifiedhacker.com', and a 'Site Report' button. Below this, it shows a 'Risk Rating: 0', 'Country: US', 'Site rank: 28,724', 'First seen: Dec 2002', and 'Host: Unified Layer'. There is also a link to 'Disable protection for this site'. A 'Report malicious URL' section is present, with fields for the URL ('http://www.certifiedhacker.com/') and an email address ('you@example.com'), both of which have checked checkboxes. A 'NETCRAFT' logo is visible at the bottom of the report window. The browser's taskbar at the bottom shows various pinned icons and the system tray with the date and time '3:18 AM 4/12/2022'.

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.

Certified Hacker Site report for http://www.certifiedhacker.com

NETCRAFT Services Solutions News Company Resources Report Fraud Request Trial

Site report for http://www.certifiedhacker.com

Look up another site?

Share: [Link](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [YouTube](#)

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	New fold Digital	Domain registrar	networksolutions.com
Connecting to csp.netcraft.com...	US	Nameserver organisation	whois.domain.com

3:19 AM 4/12/2022

Certified Hacker Site report for http://www.certifiedhacker.com

NETCRAFT Services Solutions News Company Resources Report Fraud Request Trial

IP Geolocation

We use multilateration to independently determine the location of a server. [Read more.](#)

A map of the southern United States, centered on Dallas, Texas. A large blue circle is drawn around Dallas, representing the geolocation radius. The map shows state boundaries and major cities. A legend in the bottom left corner indicates the scale and provides a link to the CSP. The status bar at the bottom shows "Connecting to csp.netcraft.com..." and the time "3:19 AM 4/12/2022".

This is not a HTTPS site. If you're looking for SSL/TLS information try the [HTTPS site report](#).

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	Apache	11-Apr-2022
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.14.1	29-May-2019
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.12.2	28-Nov-2018
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	-	nginx/1.12.1	12-Nov-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.12.0	28-May-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.10.2	15-Apr-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.10.1	19-Oct-2016
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	Apache	11-Sep-2016
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.10.1	9-Sep-2016
Connecting to csp.netcraft.com...	69.89.31.193	Linux	Apache	31-Jul-2016

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.

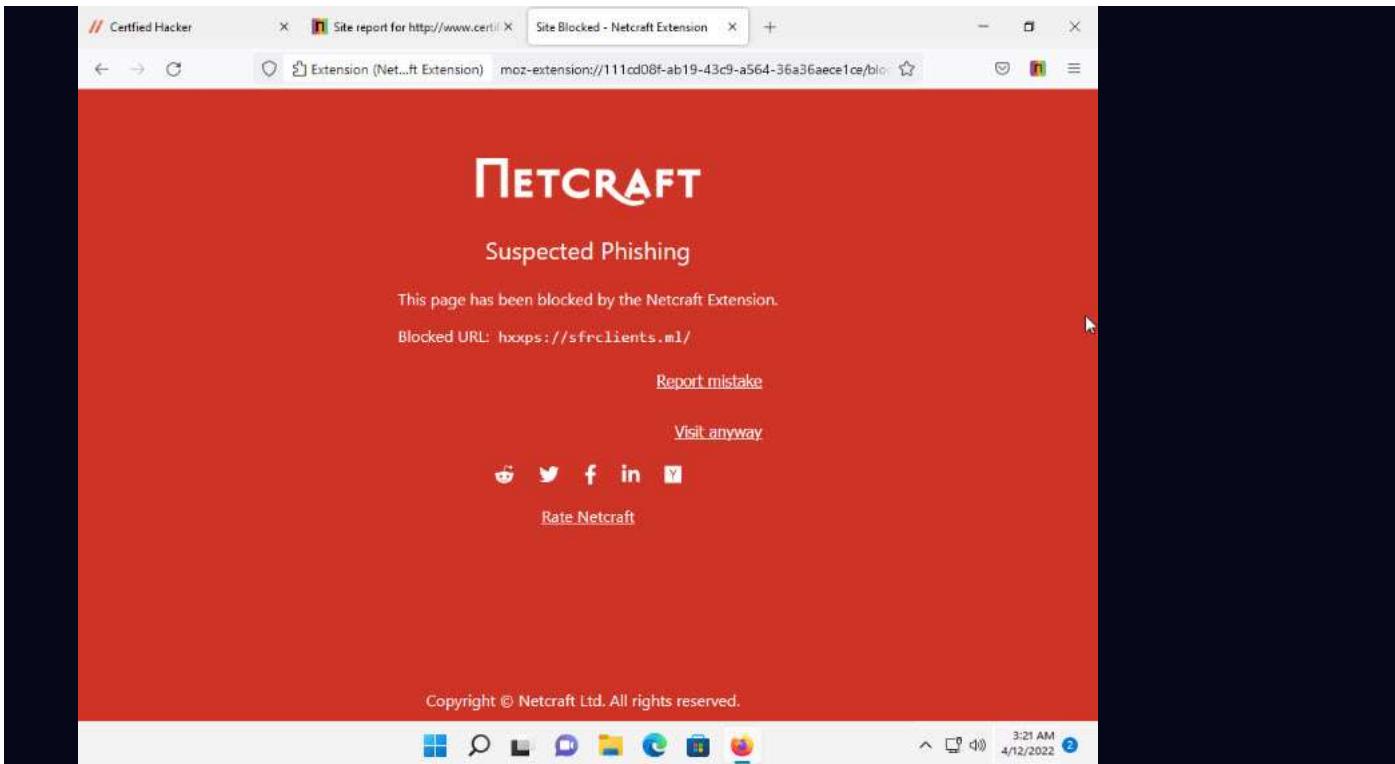
19. The Netcraft Extension automatically blocks phishing sites. However, if you trust the site, click **Visit anyway** to browse it; otherwise, click **Report mistake** to report an incorrectly blocked URL.

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.



The screenshot shows the PhishTank homepage. At the top, there's a search bar with the URL <https://www.phishtank.com>. Below the search bar, the PhishTank logo and slogan "Out of the Net, into the Tank." are displayed. A navigation menu includes Home, Add A Phish, Verify A Phish, Phish Search, Stats, FAQ, Developers, Mailing Lists, and My Account. On the left, a section titled "Join the fight against phishing" encourages users to submit suspected phishes and verify others. It features a yellow box with a "Is it a phish?" button and a list of recent submissions. On the right, two boxes provide information about what phishing is and what PhishTank does. The taskbar at the bottom shows various pinned icons.

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

The screenshot shows the "Details on suspect" page for submission ID 7486626. The URL is https://www.phishtank.com/phish_detail.php?phish_id=7486626. The page title is "Submission #7486626 is currently ONLINE". It shows the submission was submitted on April 12th, 2022, at 10:11 AM by user [buaya](#). The URL is <https://cssogrtdedadrealpasssb.firebaseioapp.com/>. A large red banner at the top says "Verified: Is a phish" with the note "As verified by Shazza June Dev darkmoon titus". Below this, a progress bar shows 100% for "Is a phish" and 0% for "Is NOT a phish". There are buttons for "Screenshot of site", "View site in frame", "View technical details", and "View site in new window". The GoDaddy logo is visible in the screenshot preview. The taskbar at the bottom shows various pinned icons.

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.

The screenshot shows a Microsoft Edge browser window displaying the PhishTank website at https://www.phishtank.com. The page header includes the PhishTank logo, a navigation bar with links like Home, Add A Phish, Verify A Phish, Phish Search, Stats, FAQ, Developers, Mailing Lists, and My Account. A login form with fields for 'username' and 'password' is visible. The main content area features a section titled 'Join the fight against phishing' with calls to action for submitting and verifying phishing sites. A yellow-highlighted box contains the URL 'http://be-ride.ru/confirm' and a button labeled 'Is it a phish?'. Below this is a table of 'Recent Submissions' with columns for ID, URL, and Submitted by. The table lists several URLs, mostly from prodigvabuse, such as 'http://youseedani.temp.swtest.ru/yousee/' and 'https://pxlme.me/zV8D_ZYc'. To the right, two boxes provide information about what phishing is and what PhishTank does, including links to 'Learn more...' and 'Read the FAQ...'. The bottom right corner of the screen shows the Windows taskbar with the date and time (3:27 AM, 4/12/2022).

ID	URL	Submitted by
7486639	http://youseedani.temp.swtest.ru/yousee/	postmasterATmail
7486638	https://pxlme.me/zV8D_ZYc	raz
7486636	https://www.eseguiprocedura.com/errore.php	D3Lab
7486635	https://www.eseguiprocedura.com/otp1.php	D3Lab
7486633	https://voicenotetranscriptinhere.weebly.com/	prodigvabuse
7486632	https://bellsouthonlineverification2.yolasite.com/	prodigvabuse
7486631	https://attservice40.weebly.com/	prodigvabuse
7486629	https://bellsouth-online-verification18.yolasite.c...	prodigvabuse

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.

The screenshot shows a browser window with the URL https://www.phishtank.com/phish_detail.php?phish_id=2205890. The page title is "PhishTank > Details on suspect". The main content area displays a submission status: "Submission #2205890 is currently offline". Below this, it says "Submitted Jan 2nd 2014 10:56 AM by [knack](#) (Current time: Apr 12th 2022 10:27 AM UTC)". A link "<http://be-ride.ru/confirm/>" is provided. A red square icon with a white flame symbol is followed by the text "Verified: Is a phish". Below it, smaller text reads "As verified by [buaya](#) [paulch](#) [NotBuyingIt](#) [phishphucker](#)". A progress bar shows "Is a phish" at 100% and "Is NOT a phish" at 0%. Below the progress bar are buttons for "Screenshot of site", "View site in frame", "View technical details", and "View site in new window". A preview of a PayPal-like login page is shown, featuring the PhishTank logo and the text "Redesigned with you in mind.". The bottom right corner of the screen shows the Windows taskbar with icons for File Explorer, Task View, Start, Taskbar settings, and a clock indicating 3:28 AM on 4/12/2022.

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.

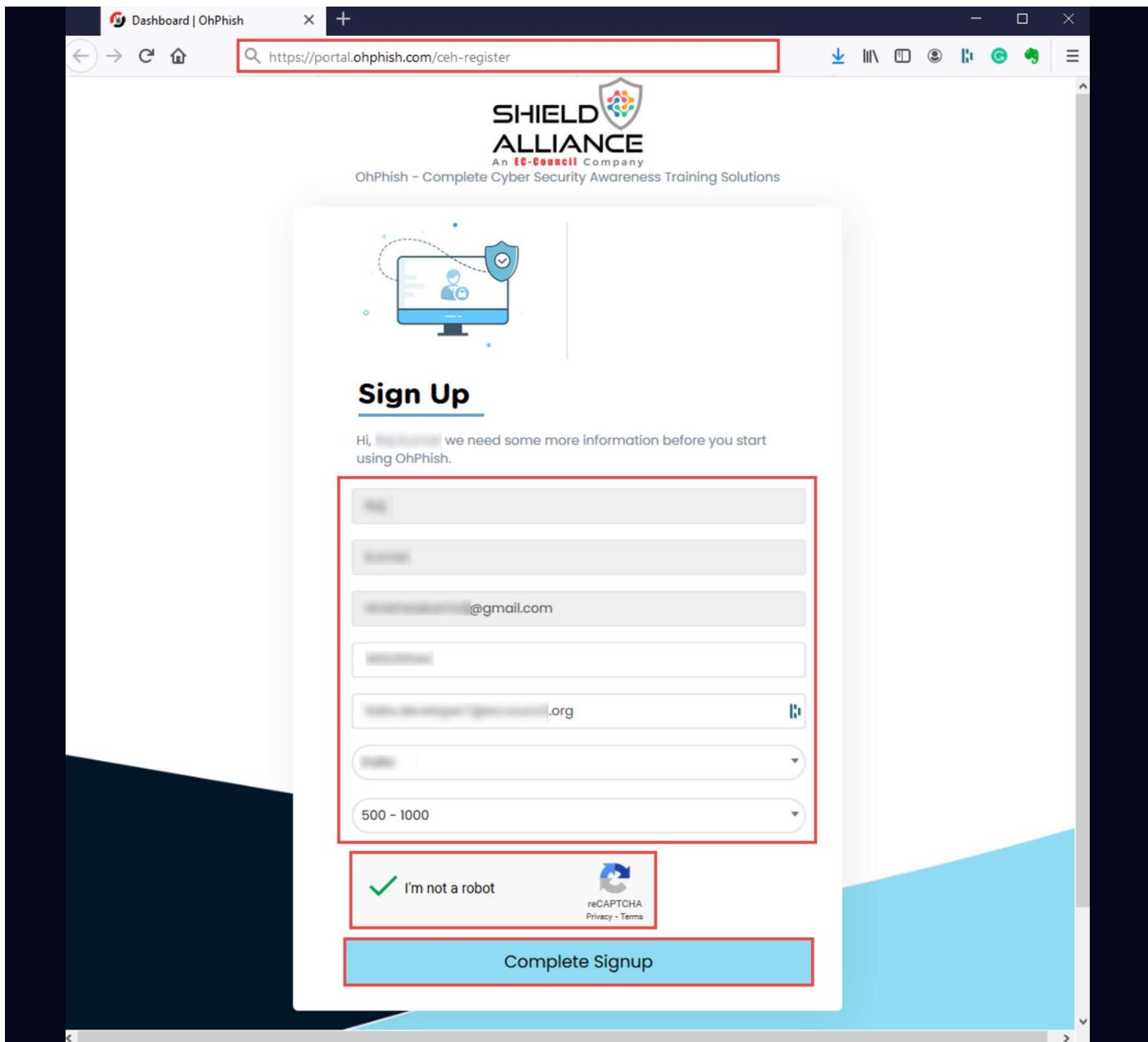
Note: If you do not have an ASPEN account or access to CEHv12 program on ASPEN, please write to support@eccouncil.org for an OhPhish account. Once your account is setup, you will receive an email from aware@eccouncil.org with an account activation link. Upon activation, continue from **STEP 12**.

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

Status	Action
In Process	TRAINING
Pending	EVALUATION
Pending	EXAM
Pending	CERTIFICATE
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.





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.

Mail - Outlook - Mozilla Firefox https://outlook.office.com/mail/deeplink?version=2020082005.07&popoutv2=1

Reply all | Delete | Junk | Block | ...

Welcome to OhPhish

OhPhish <no-reply@ohphish.com>
Tue 08-09-2020 12:06 PM
To: [REDACTED]

A professional photograph of five people in business attire standing in a row against a dark background. The OhPhish logo is visible in the top left corner of the image.

Dear [REDACTED],

Welcome to OhPhish! We are excited to bring you on-board and are confident that you will enjoy our user-friendly single platform for running Phishing simulation.

Please use the following information to log in to your account:

Email: [REDACTED].org

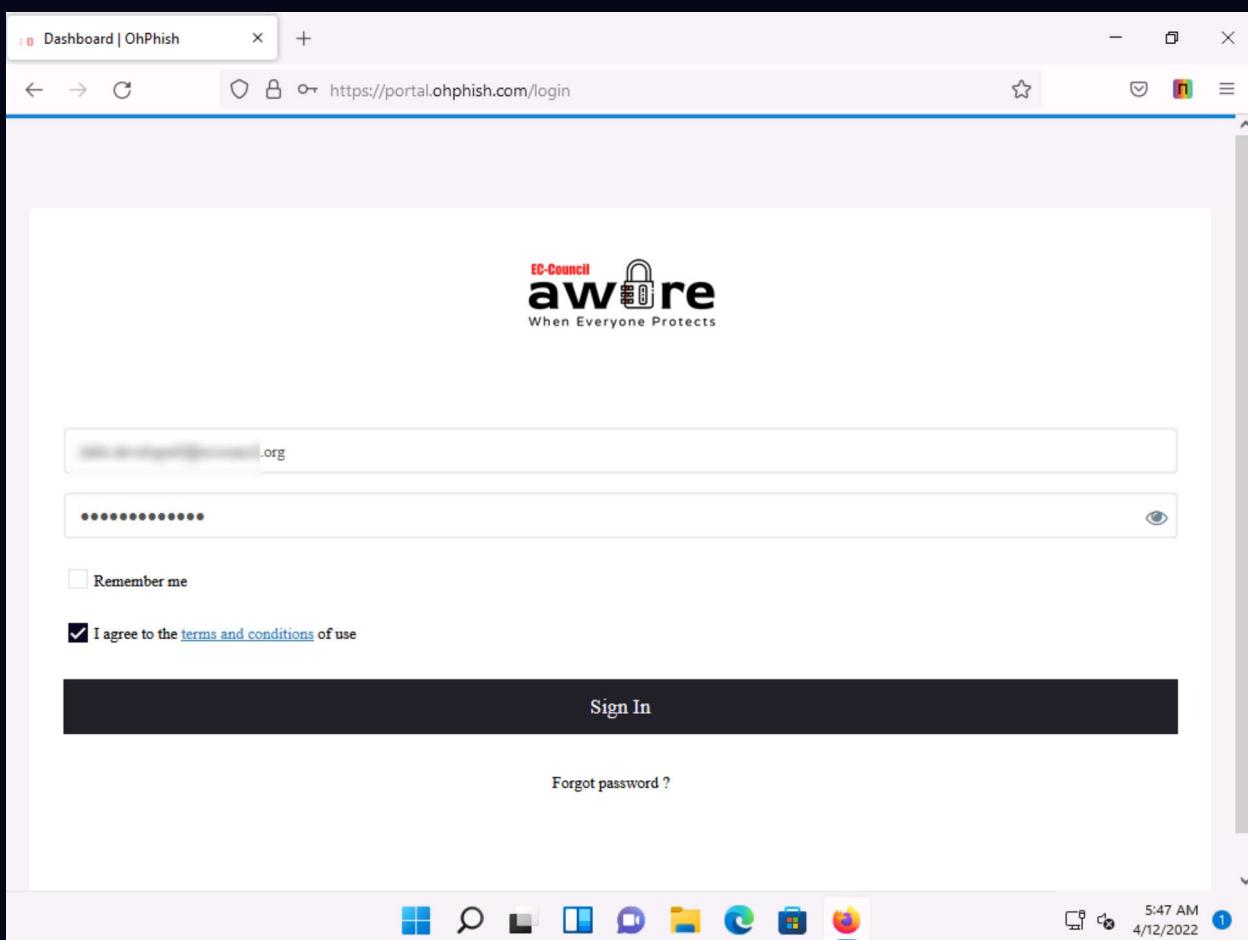
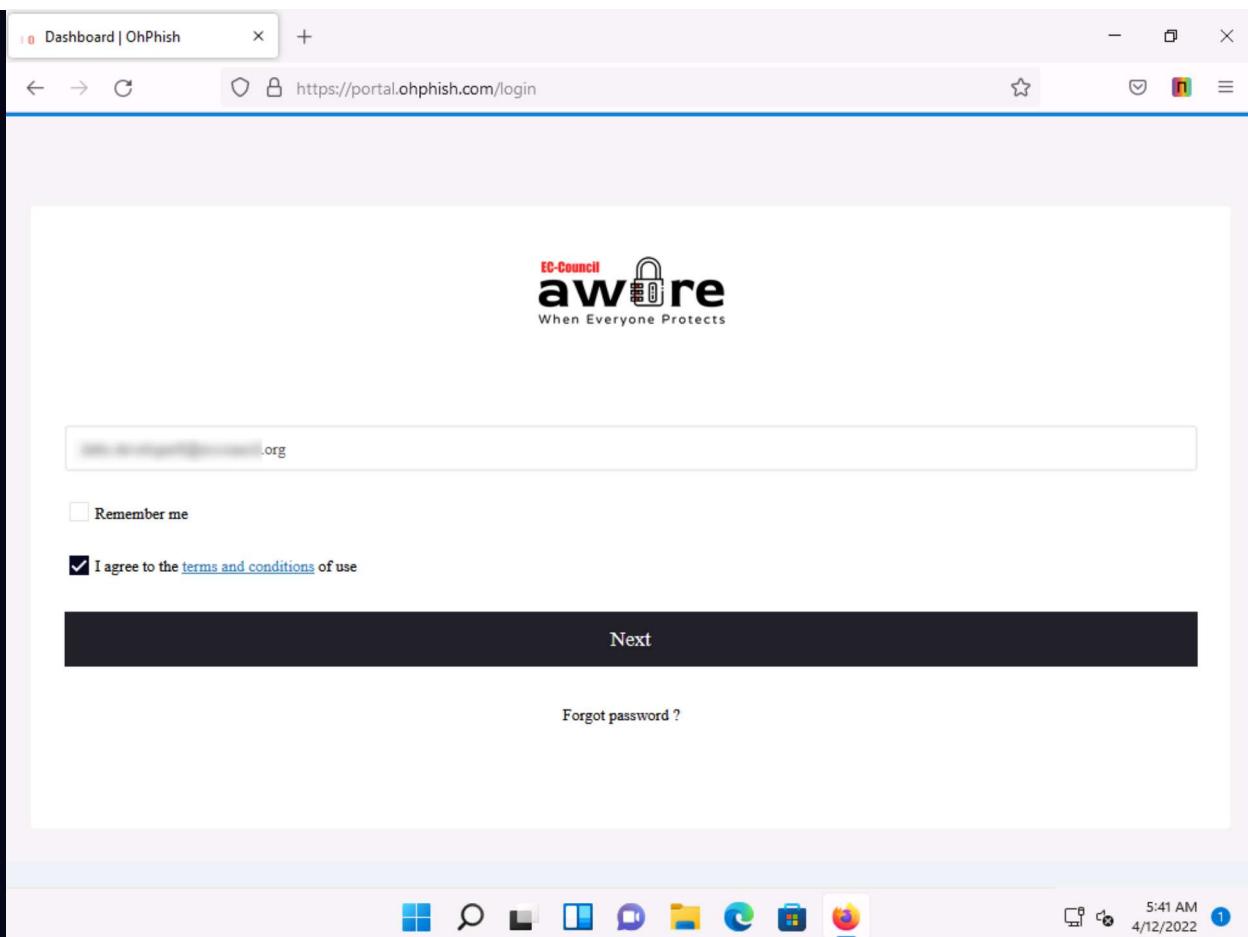
Password: [REDACTED]

If you have any questions about using OhPhish, just E-mail us at support@ohphish.com

CLICK HERE TO LOGIN

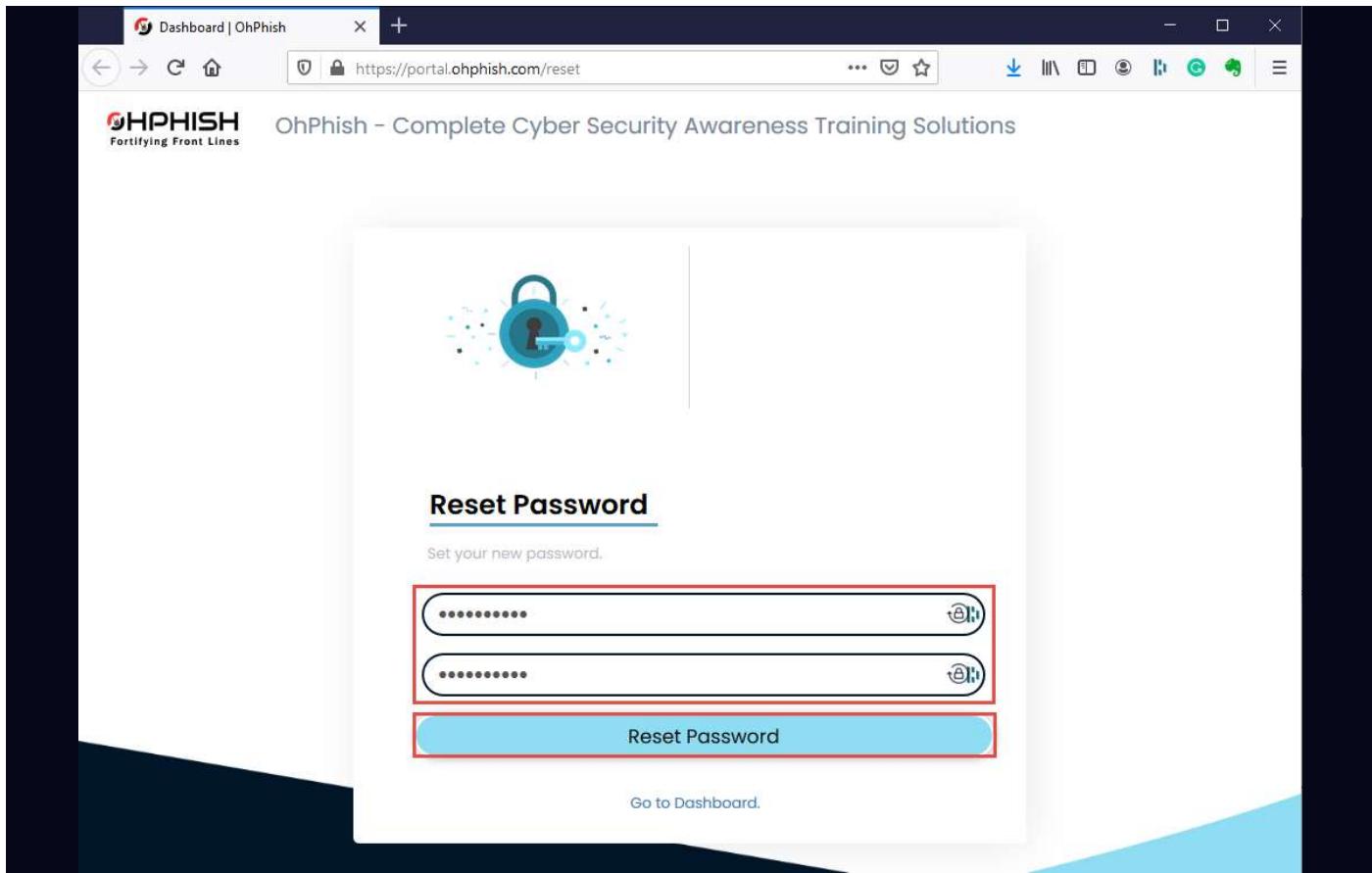
7. **EC-Council Aware** page appears, in the **Username** field enter your email address and click **Next**. In the next page, enter your password in the **Password** field and click **Sign In**.

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.



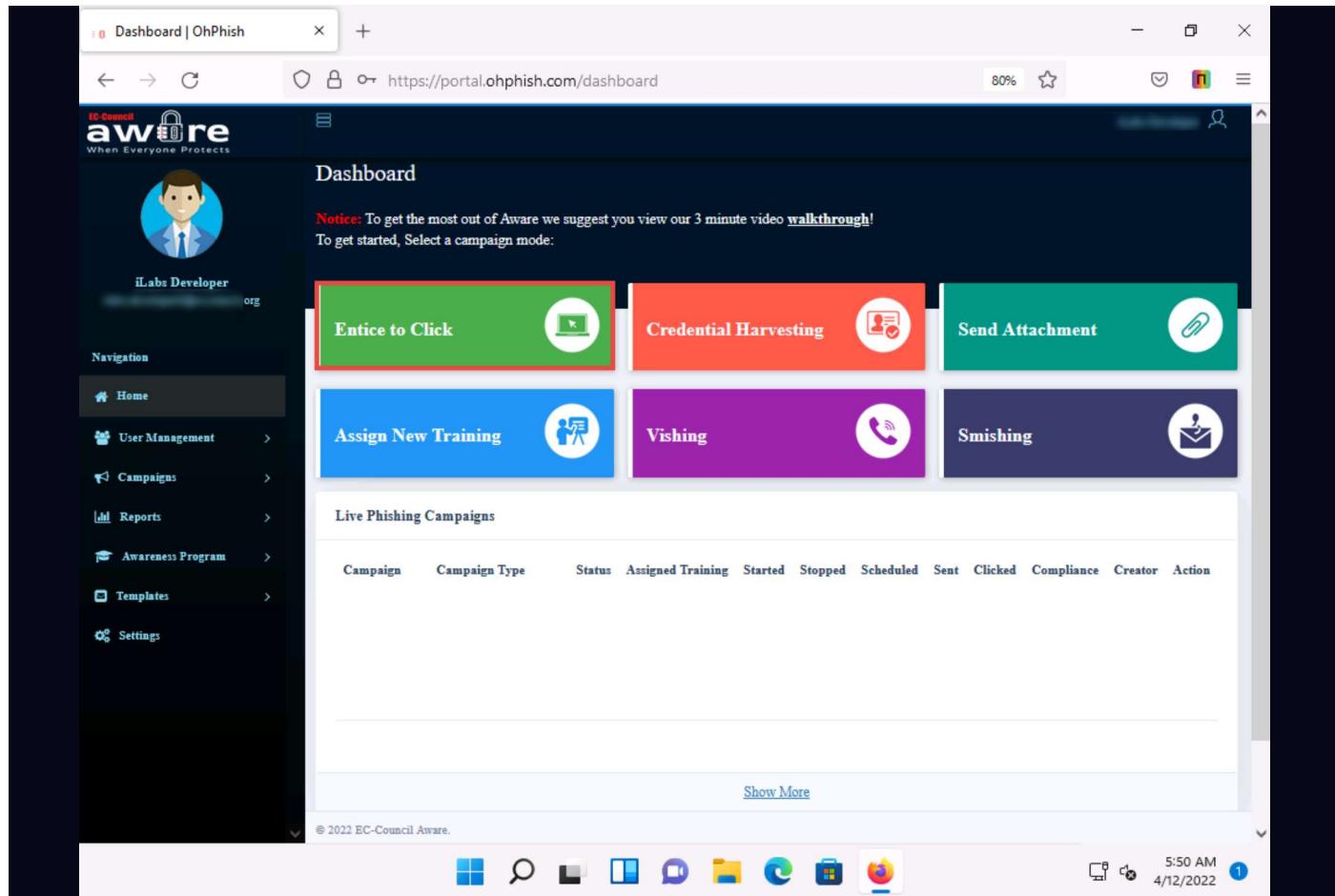


9. Your account password is changed successfully.

10. Now, you can login to your OhPhish account either by clicking on the **LOGIN TO OPHISH 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.

The screenshot shows the EC-Council Aware platform's 'Create New Email Phishing Campaign' interface. The campaign name is 'Test - Entice to Click'. The email template selected is 'WFH - Organizational Policy'. The preview window shows a phishing email template with a subject line 'WFH Under Organizational Policy' and a body containing a COVID-19 update.

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**.

The screenshot shows the EC-Council Aware platform interface. On the left, there's a sidebar with navigation links like Home, User Management, Campaigns, Reports, Awareness Program, Templates, and Settings. The main area is titled 'Team Human Resource' and contains fields for Sender Name (Human Resource Team), Subject (WFH Under Organizational Policy), Select Time Zone (America/Los_Angeles), Expiry Date (20-Apr-2022), and Schedule Later (No). There's also a checkbox for Automatic Delivery of Campaign Reports. Below these are sections for Import users (with a red box around the 'Select Source' button), Batch Count (Batch Count(Optional)), Batch Interval (Batch Interval(Optional)), Training Type (Select Training Type), Select Training (Select Training), and Landing Page (You have been Phished). At the bottom, there's a checkbox for Mask Email address.

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

This screenshot shows the same interface as the previous one, but with a modal window titled 'Import Users' overlaid. The modal contains five options: 'Quick Add' (highlighted with a red box), 'From File Excel/CSV' (with a 'Download Sample File' link), 'Active Directory', 'Microsoft O365', and 'Google Suite'. The background of the main interface is dimmed.

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

The screenshot shows a 'Import Users Info' dialog box over a dark-themed web interface. The dialog box contains fields for Name, Email, Reporting Manager Email, Designation, Department, Company, Branch, and Country, all of which are currently empty and highlighted with a red border. A blue 'Add' button is located at the bottom right of the input area. Below the input area is a table header with columns: ID, Name, Email, Reporting Manager Email, Designation, Department, Company, Branch, Country, and Action. The table body contains two rows of user data, each with a red-bordered 'Edit' icon in the Action column. At the bottom of the dialog box are 'Cancel' and 'Import' buttons.

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

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

The screenshot shows the same 'Import Users Info' dialog box after two users have been added. The 'Reporting Manager Email' field now has the value 'h@gmail.com'. The table below shows two rows of user data:

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

At the bottom of the dialog box, the 'Import' button is highlighted with a red border.

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.

The screenshot shows the EC-Council Aware platform interface for creating a phishing campaign. The left sidebar contains navigation links: Home, User Management, Campaigns, Reports, Awareness Program, Templates, and Settings. The main area is titled 'entice-to-click' and includes the following configuration fields:

- Schedule Later: No
- Automatic Delivery of Campaign Reports: Unchecked
- Import users: Quick Add (selected)
- Batch Count: 1 (highlighted with a red box)
- Batch Interval: 1 (highlighted with a red box)
- Training Type: Select Training Type
- Select Training: Select Training
- Landing Page: You have been Phished
- Mask Email address: Unchecked

Below these fields is a rich text editor toolbar with various formatting options like bold, italic, underline, and alignment. The editor content area displays a template message:

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.

The bottom right corner shows the system status: 7:59 AM, 4/13/2022, and a notification icon.

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

The screenshot shows a web browser window with the URL <https://portal.ohphish.com/campaigns/actions/entice-to-click>. The page is titled "Dashboard | OhPhish". On the left, there's a sidebar for "iLabs Developer" with navigation links: Home, User Management, Campaigns, Reports, Awareness Program, Templates, and Settings. The main content area shows an email editor with the following text:

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

At the bottom right of the editor, there are two buttons: "Test Email" and "Create". The "Create" button is highlighted with a red box.

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.

The screenshot shows a web browser window with the URL <https://portal.ohphish.com/campaigns/actions/entice-to-click>. The page title is "Dashboard | OhPhish". On the left, there's a sidebar with navigation links: Home, User Management, Campaigns, Reports, Awareness Program, Templates, and Settings. The main content area has a dark blue background with a grid pattern. It displays several configuration fields: "IP Address and Domain: 52.15.139.151 mail.office-mailer.com", "Landing Page URL: *pageshowinfo.com", "Sender Address: info@whocoviadvisory.com", and "Domain: pageshowinfo.com". Below these fields are three buttons: "Share Details" (blue), "Done" (red, highlighted), and "Cancel" (white). To the right of the buttons are links for "Whitelisting Guide", "Microsoft 365", and "G-Suite". At the bottom right of the main area, there are "Test Email" and "Create" buttons. The status bar at the bottom shows "Words: 105". The system tray at the bottom right indicates the date and time as 8:01 AM, 4/13/2022.

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

This screenshot shows the same OhPhish interface as the previous one, but with a "Confirm?" dialog box overlaid. The dialog contains the message: "This will trigger 2 emails from info@whocoviadvisory.com. Are you sure you want to trigger this campaign?". It features two buttons: "SURE" (highlighted with a red border) and "CANCEL". The main campaign setup page is visible in the background, showing the "Batch Count" set to 1 and "Batch Interval" set to 1. The "Landing Page" dropdown is set to "You have been Phished". The status bar at the bottom shows "Words: 69". The system tray at the bottom right shows the date and time as 12:39 PM, 9/11/2020.

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**.

EC-Council aware
When Everyone Protects

Recommendation! Please refer [Aware User Manual](#) before starting a campaign.

0:00

Please have a look at above video to see how it works.

Create New Email Phish

Campaign Name: Test - En

Email Template: Existing templates My templates

Select Template Category: Coronavirus/COVID-19

Select Country: All

Select Template: WFH - Organizational Policy Select

1 template selected.

© 2022 EC-Council Aware.

OK

Campaign has been successfully initiated.

{Name},

This pandemic situation is seeing all the workforce going ... 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.

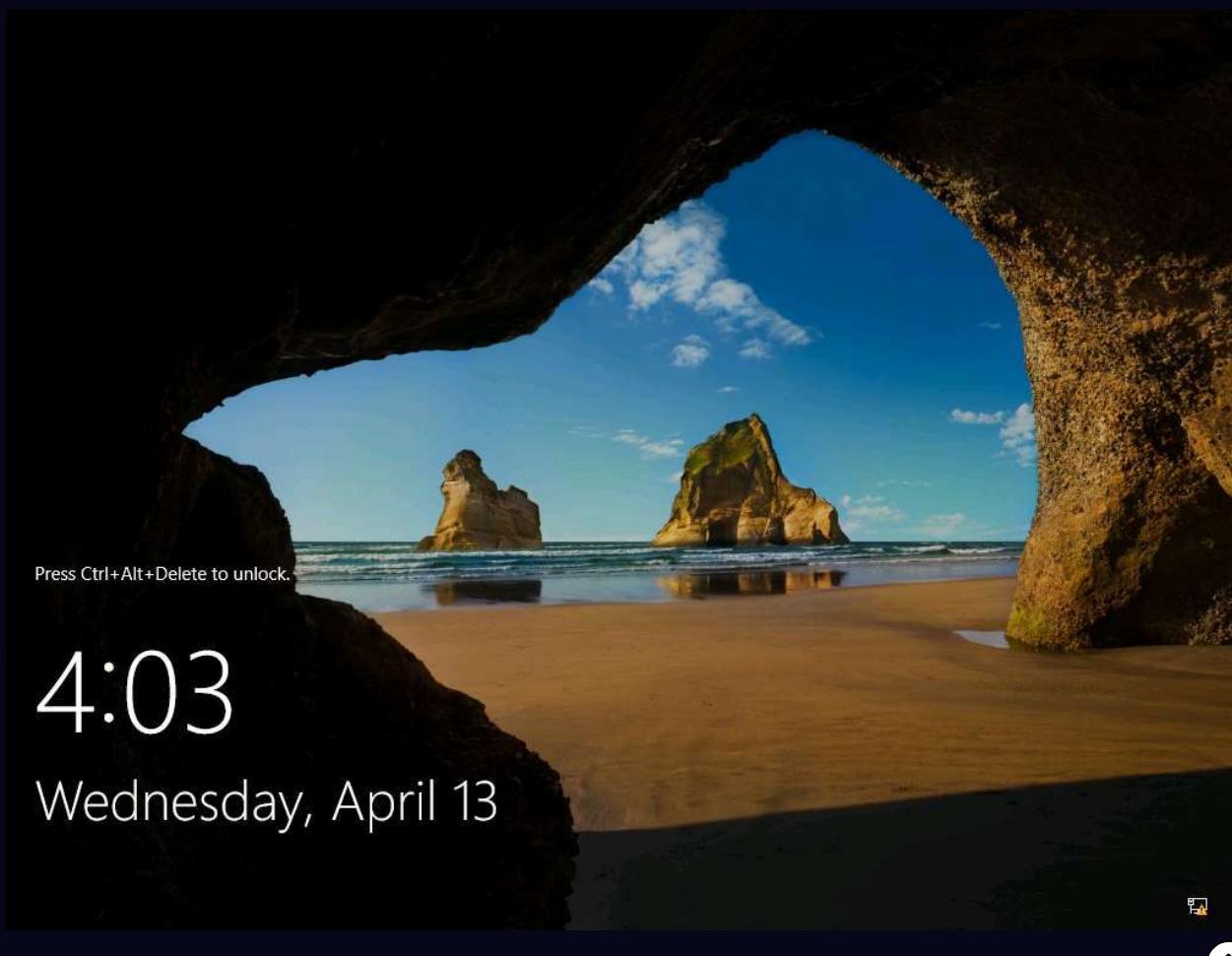
According to the act under this policy is part of the awareness among the organizations and all the employees should adhere to the same and read the policy along with an acknowledgment e-mail by today EOD.

[WFH - Policy.pdf](#)

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

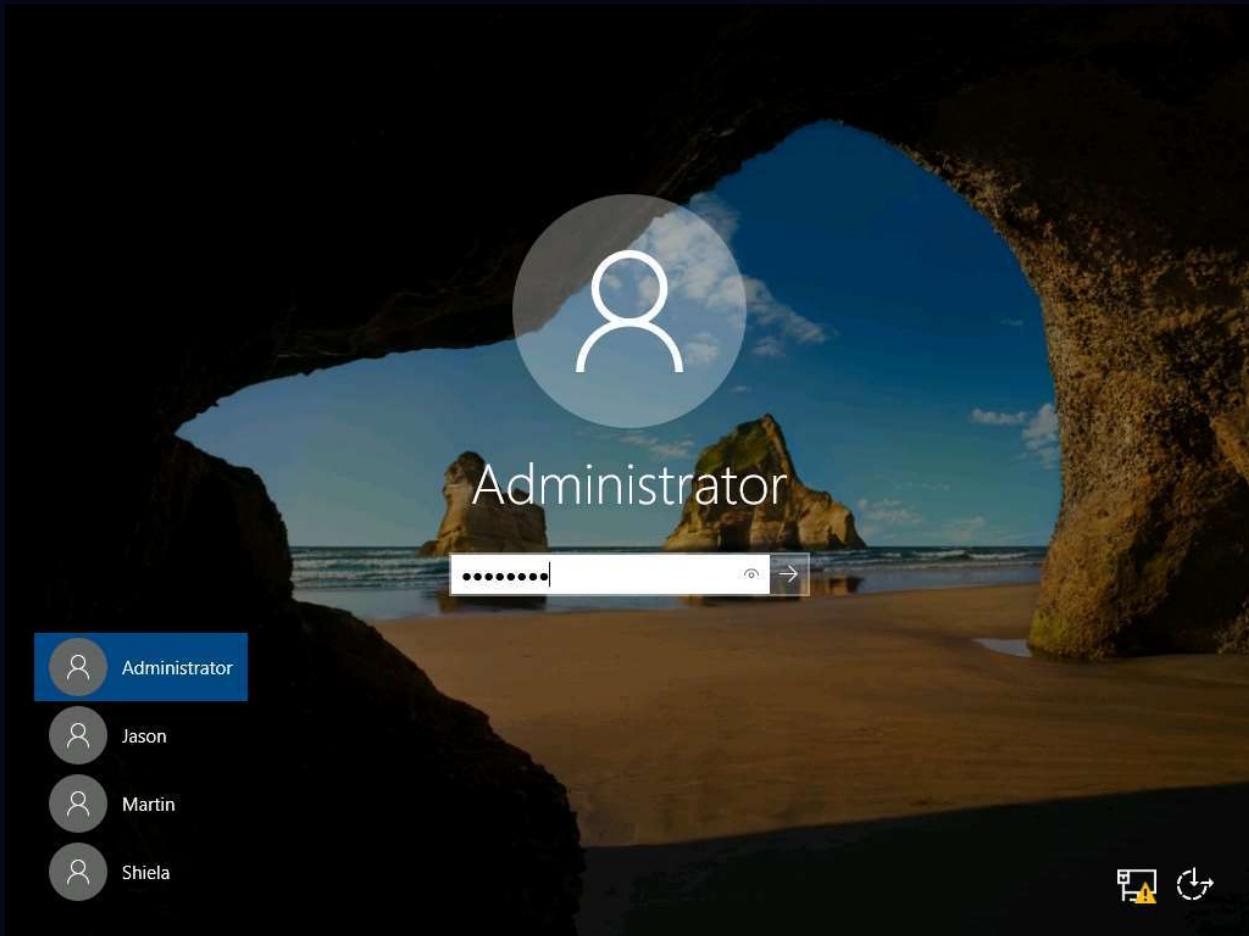
8:02 AM 4/13/2022

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.



WFH Under Organizational Policy

info@whocoviadvisory.com to me 4:03 AM (3 minutes ago)

Hi [REDACTED]

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

Note : This Phishing Simulated email is for lab purposes only.

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.

Phishing Warning

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 **Google**

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.

The screenshot shows the EC-Council Aware platform's OhPhish dashboard. On the left, a sidebar lists navigation options: Home, User Management, Campaigns, Reports, Awareness Program, Templates, and Settings. The main area is titled 'Dashboard' and features a notice about viewing a video walkthrough. Below this, there are six colored cards representing different campaign types: 'Entice to Click' (green), 'Credential Harvesting' (red), 'Send Attachment' (teal), 'Assign New Training' (blue), 'Vishing' (purple), and 'Smishing' (dark blue). A section titled 'Live Phishing Campaigns' displays a table with one row. The row details a campaign named 'Test - Entice to Click' (Status: In Progress), assigned to 'No Training' (Assigned Training), started on April 13, 2022, at 4:02 AM, and stopped on April 20, 2022, in America/Los_Angeles. It shows 2 targets sent 1 email, with 50.00% clicked. The table includes columns for Campaign Type, Status, Assigned Training, Started, Stopped, Scheduled, Sent, Clicked, Compliance, Creator, and Action. The bottom of the screen shows a taskbar with various icons and the system tray indicating the date and time as 8:12 AM on 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).

The screenshot shows the EC-Council Aware platform interface. On the left, there's a navigation sidebar with options like Home, User Management, Campaigns, Reports, Awareness Program, Templates, and Settings. The main content area displays a campaign named "Test - Entice to Click" from April 13, 2022, to April 20, 2022. It uses the "WFH - Organizational Policy" template under the "Coronavirus/COVID-19" category. The "Campaign Summary" section includes a pie chart showing 50.00% compliance (split evenly between users who clicked and those who did not). Below the chart is a legend: dark blue for "Users clicked 1", teal for "Users not clicked 1", and red for "Repeat Defaulters 0".

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. The left sidebar has the same navigation as the previous screen. The main dashboard features several buttons: "Entice to Click" (green), "Credential Harvesting" (red), "Send Attachment" (highlighted with a red border and green background), "Assign New Training" (blue), "Vishing" (purple), and "Smishing" (dark blue). Below these are sections for "Live Phishing Campaigns" and "Recent Activity". The "Live Phishing Campaigns" table shows one entry: "Test - Entice to Click" with status "In Progress", assigned to "No Training Assigned", started on April 13, 2022, at 4:02 AM, and stopped on April 20, 2022, at 11:59 PM. The "Send Attachment" button is clearly highlighted with a red border.

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**).

The screenshot shows the EC-Council Aware platform interface. On the left, there's a sidebar with navigation links like Home, User Management, Campaigns, Reports, Awareness Program, Templates, and Settings. The main area is titled 'Create New Email Phishing Campaign'. The form fields are as follows:

- Campaign Name:** Test - Send to Attachment
- Email Template:** Existing templates (selected)
- Select Template Category:** Office Mailers
- Select Country:** All
- Select Template:** PF Amount Credited (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)

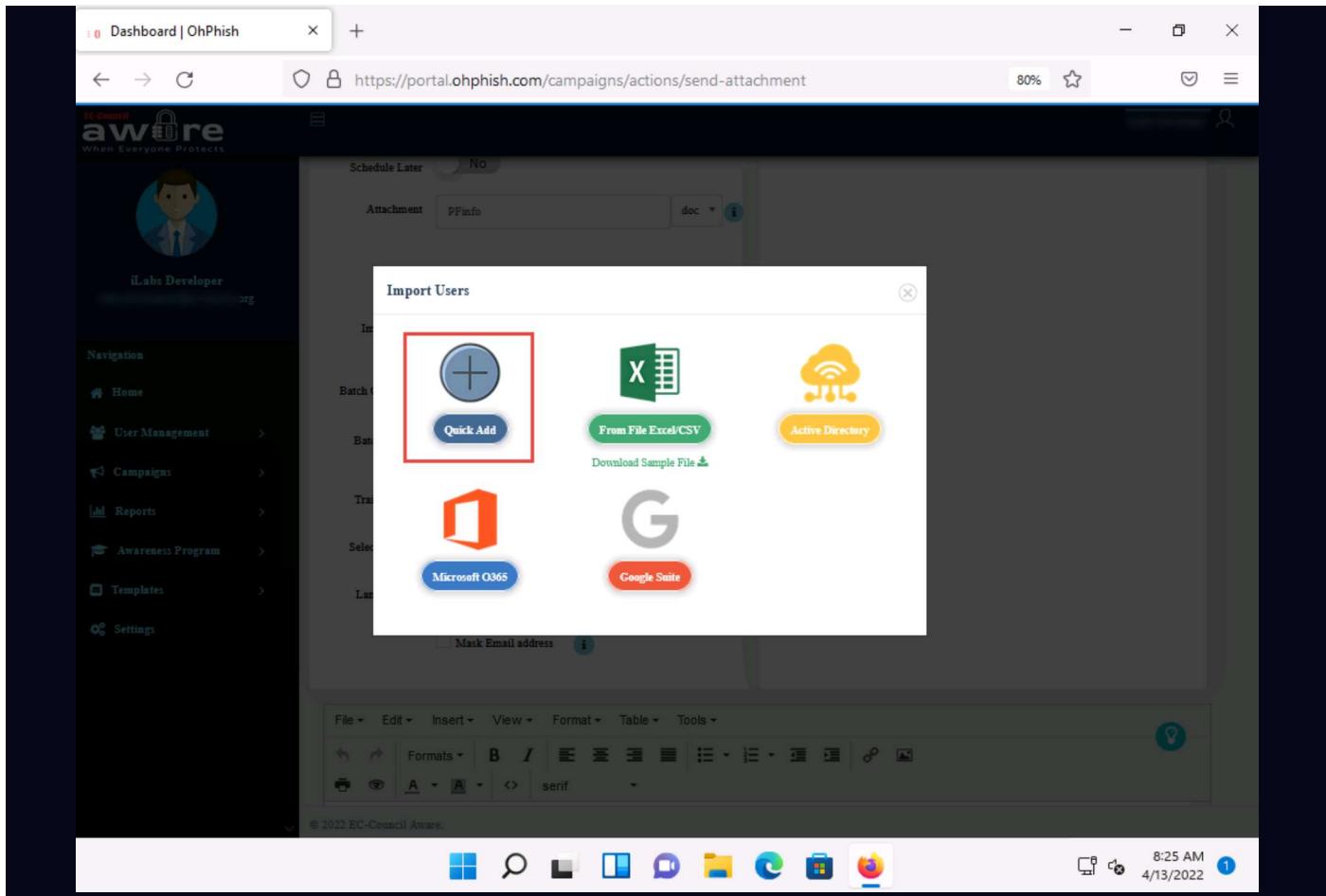
The generated email content on the right is:

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.

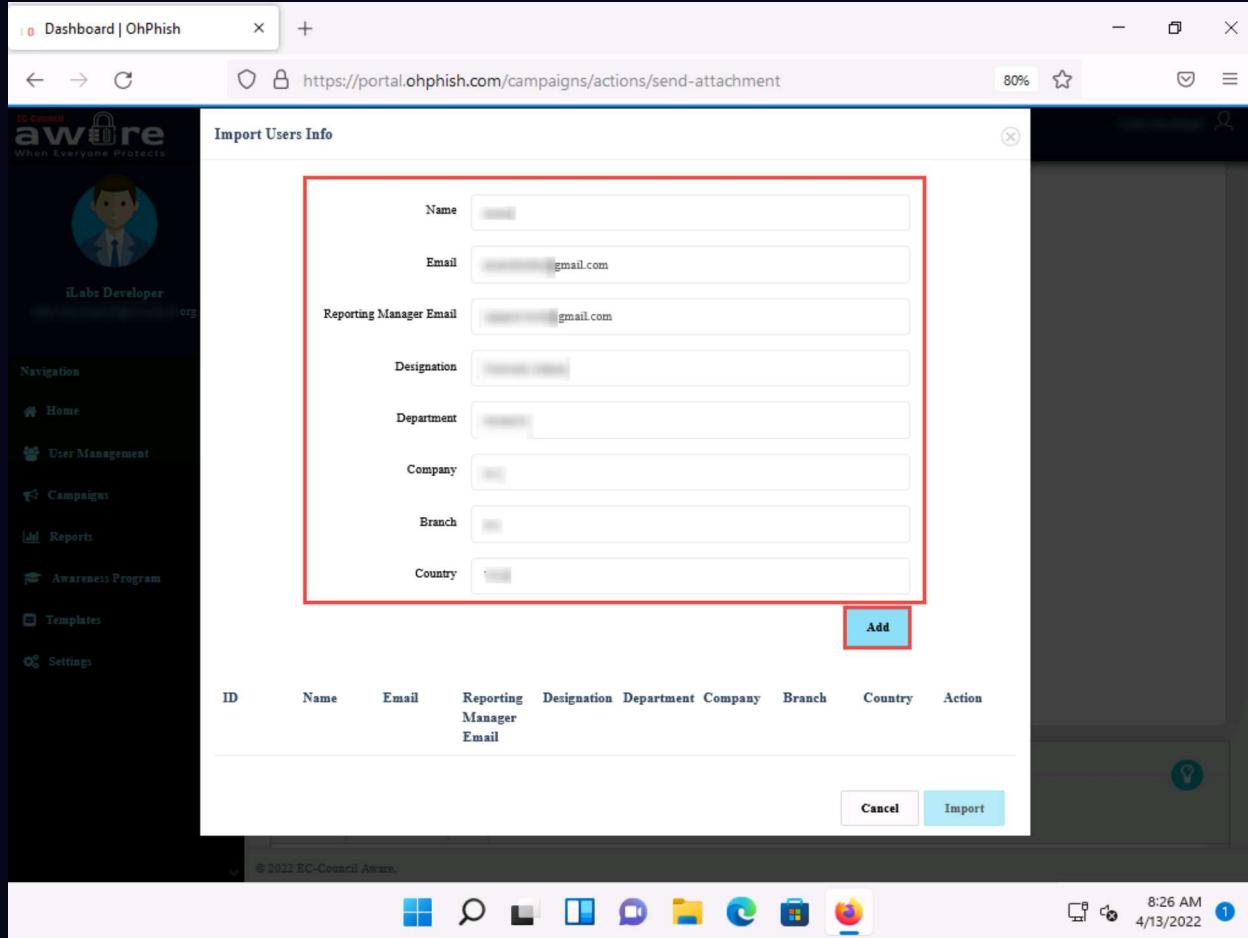
51. Click **Select Source** button under **Import users** field.

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



The screenshot shows a web browser window for the EC-Council Aware platform at the URL <https://portal.ohphish.com/campaigns/actions/send-attachment>. The page title is "Dashboard | OhPhish". A modal window titled "Import Users" is displayed in the center. The "Quick Add" button, which features a blue plus sign inside a red-bordered box, is highlighted. Other options shown include "From File Excel/CSV", "Active Directory", "Microsoft O365", and "Google Suite". Below the "Quick Add" button is a link to "Download Sample File". At the bottom of the modal, there is a checkbox for "Mask Email address" and a small information icon.

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



The screenshot shows the "Import Users Info" pop-up window. It contains fields for entering employee details: Name, Email, Reporting Manager Email, Designation, Department, Company, Branch, and Country. Each field has a placeholder value. A red box highlights the entire input area. To the right of the input fields is a blue "Add" button. Below the input area is a table with columns: ID, Name, Email, Reporting Manager Email, Designation, Department, Company, Branch, Country, and Action. The first row of the table is labeled with column headers. At the bottom of the pop-up are "Cancel" and "Import" buttons.

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

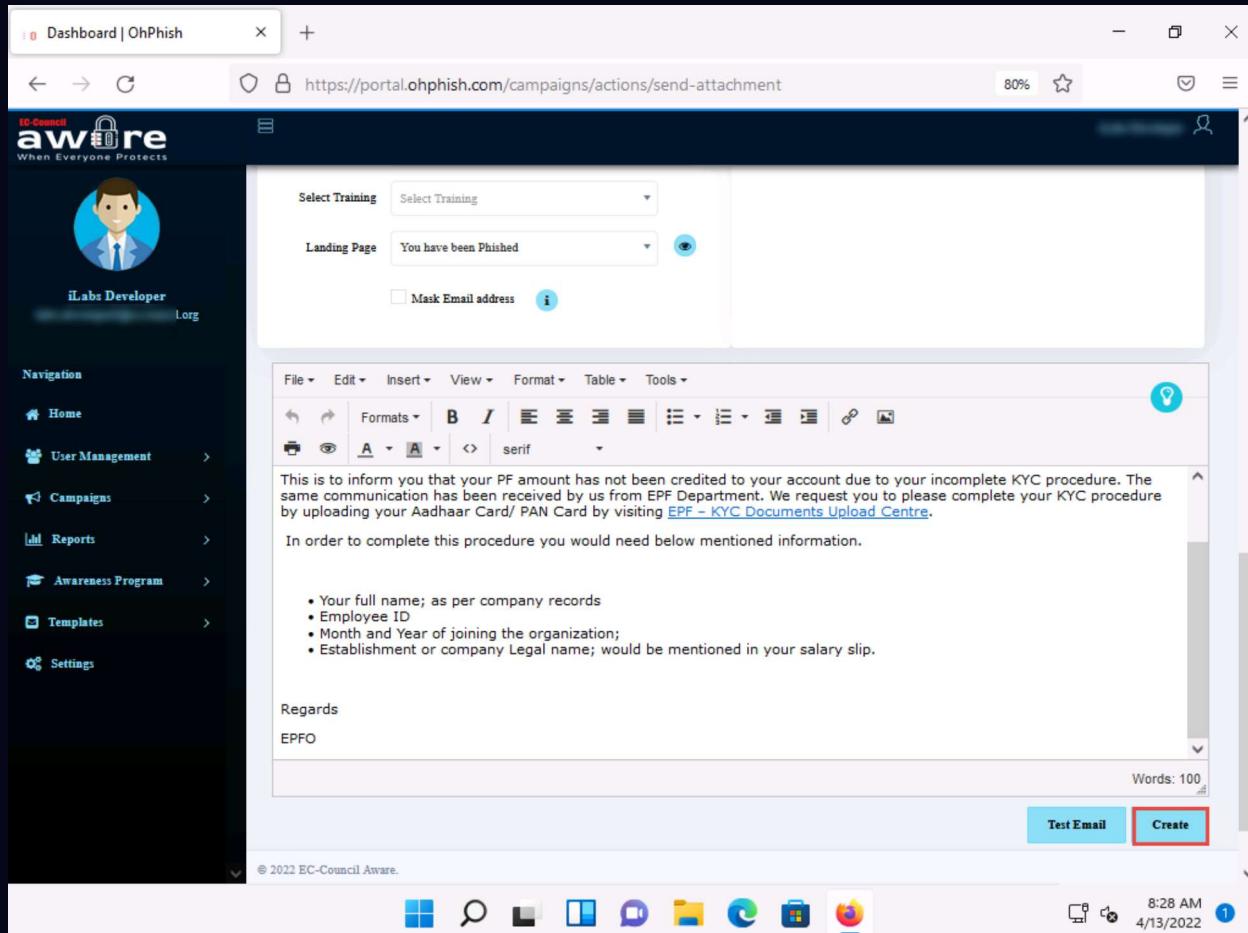
55. After adding the users' details, click **Import**.

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.



PF amount has been credited - + https://mail.google.com/mail/u/0/#inbox/FMfcgxwJXpQsQSkBTxmSSVTmGNNICbKq

Gmail Search mail

HR - ABP News hr@abpnews.com via officemailer.in to me 10:21 AM (2 minutes ago)

1 of 3,640

3,326

Dear [REDACTED]

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.

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... 10:24 AM 9/11/2020

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.

pfamountcredited.serv... https://pfamountcredited.serv... + https://pfamountcredited.serv.../rjs?c_uid=5f5bb1d3003dc0283197caee&tm=you-have-been-phished

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

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... 10:25 AM 9/11/2020

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**.

The screenshot shows the OhPhish dashboard interface. On the left, there's a navigation sidebar with options like Home, User Management, Campaigns, Reports, Templates, Free Tools, and Settings. The main area has several colored boxes representing different campaign types: 'Entice to Click' (green), 'Credential Harvesting' (red), 'Send Attachment' (teal), 'Training' (blue), 'Vishing' (purple), and 'Smishing' (dark blue). Below these are sections for 'Live Phishing Campaigns' and 'Recent Activity'. A specific campaign titled 'Test - Send to Attachment' is highlighted with a red box and is currently in progress.

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.

This screenshot shows the 'Campaign Detailed Report' page. It features two main sections: 'Campaign Details' and 'Campaign Summary'. The 'Campaign Details' section includes fields for Campaign Name (Test - Send to Attachment), Date Initiated (Friday, September 11th 2020), Expiry Date (Friday, September 18th 2020), Domain (https://www.eccouncil.org/), Template Name (PF_Amount_Credited), and Template Category (Office Mailers). The 'Campaign Summary' section displays various metrics: No. of targets (1), No. of targets who have clicked the link (defaulters) (1, highlighted with a red box), No. of repeated defaulters (1), 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 (1), and Compliance percentage (56.20%). A pie chart at the bottom illustrates the distribution of these metrics. A legend indicates: Users clicked 1 (dark blue), Users not clicked 1 (teal), and Repeat Defaulters 1 (red).

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.

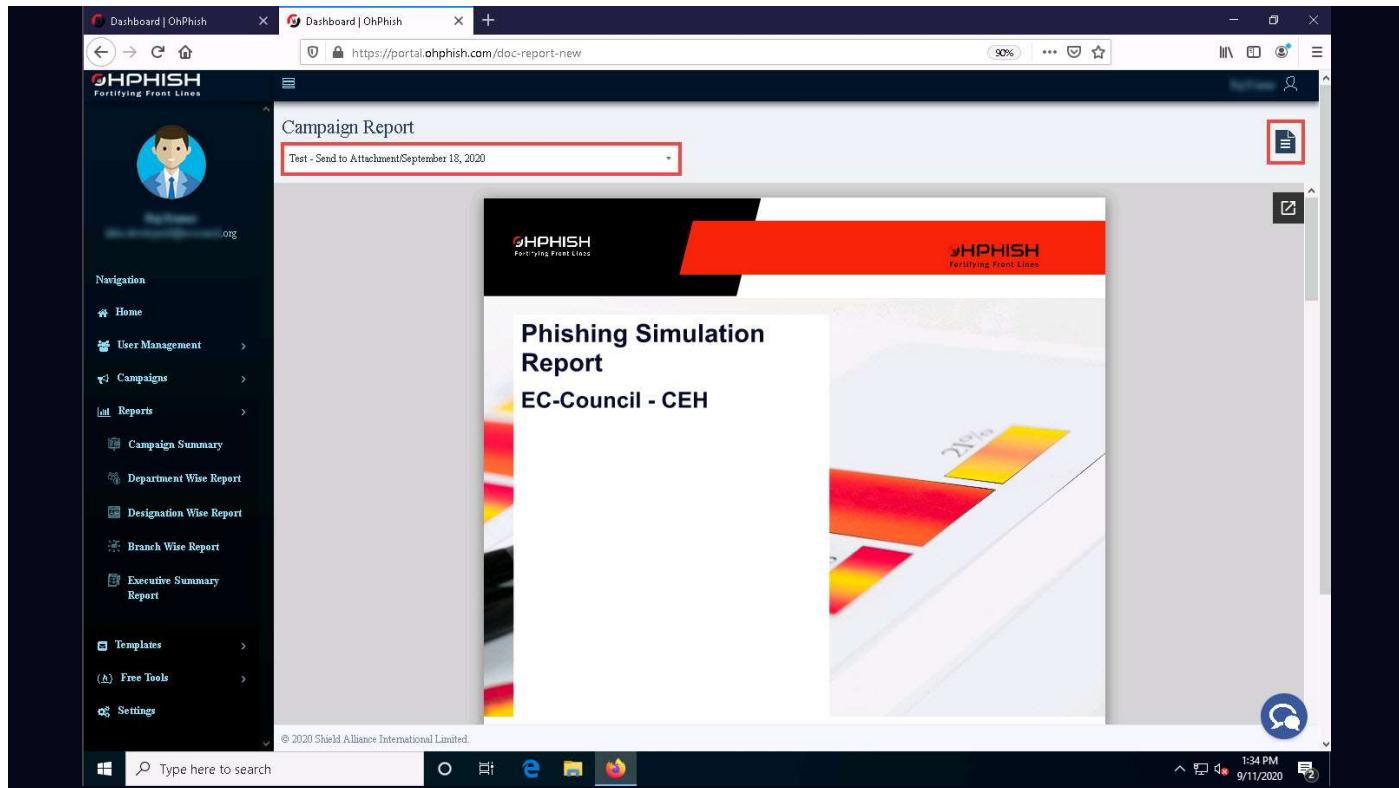
The screenshot shows the 'Campaigns Users' section of the OhPhish portal. On the left, there's a navigation sidebar with a user profile for 'Raj Kumar'. The main area displays a table titled 'Users Details' with one row of data. The table columns include Employee ID, Employee Name, Email, Designation, Department, Branch, Sent At, Opened At, Clicked At, Click Count, Risk Score, Template Used, IP Address, Location, Device, Status, and Attachment Open Time. The data in the table is as follows:

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	[REDACTED]	gmail.com	[REDACTED]	[REDACTED]	[REDACTED]	Fri, Sep 11, 2020 1:24 PM	Fri, Sep 11, 2020 1:25 PM	[REDACTED]	2	30	Office Mailers	66.102.8.217	United States	Desktop	Delivered	Nil

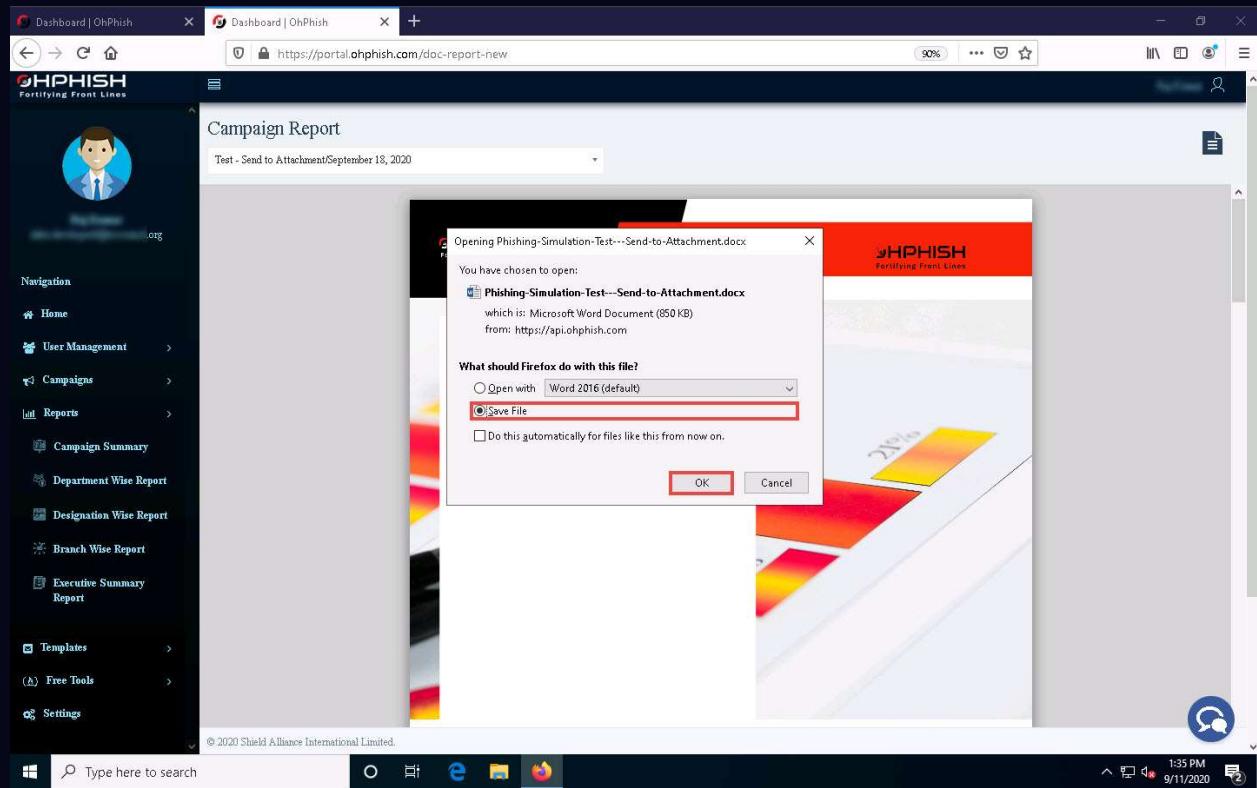
74. Now, click to expand the **Reports** section in the left pane and select the **Executive Summary Report** option.

The screenshot shows the 'Campaigns' section of the OhPhish portal. The left sidebar has a 'Reports' dropdown menu open, with the 'Executive Summary Report' option highlighted by a red box. Other options in the dropdown include 'Campaign Summary', 'Department Wise Report', 'Designation Wise Report', and 'Branch Wise Report'. The main content area shows the same 'Users Details' table as the previous screenshot, with one row of data. The data in the table is identical to the previous table.

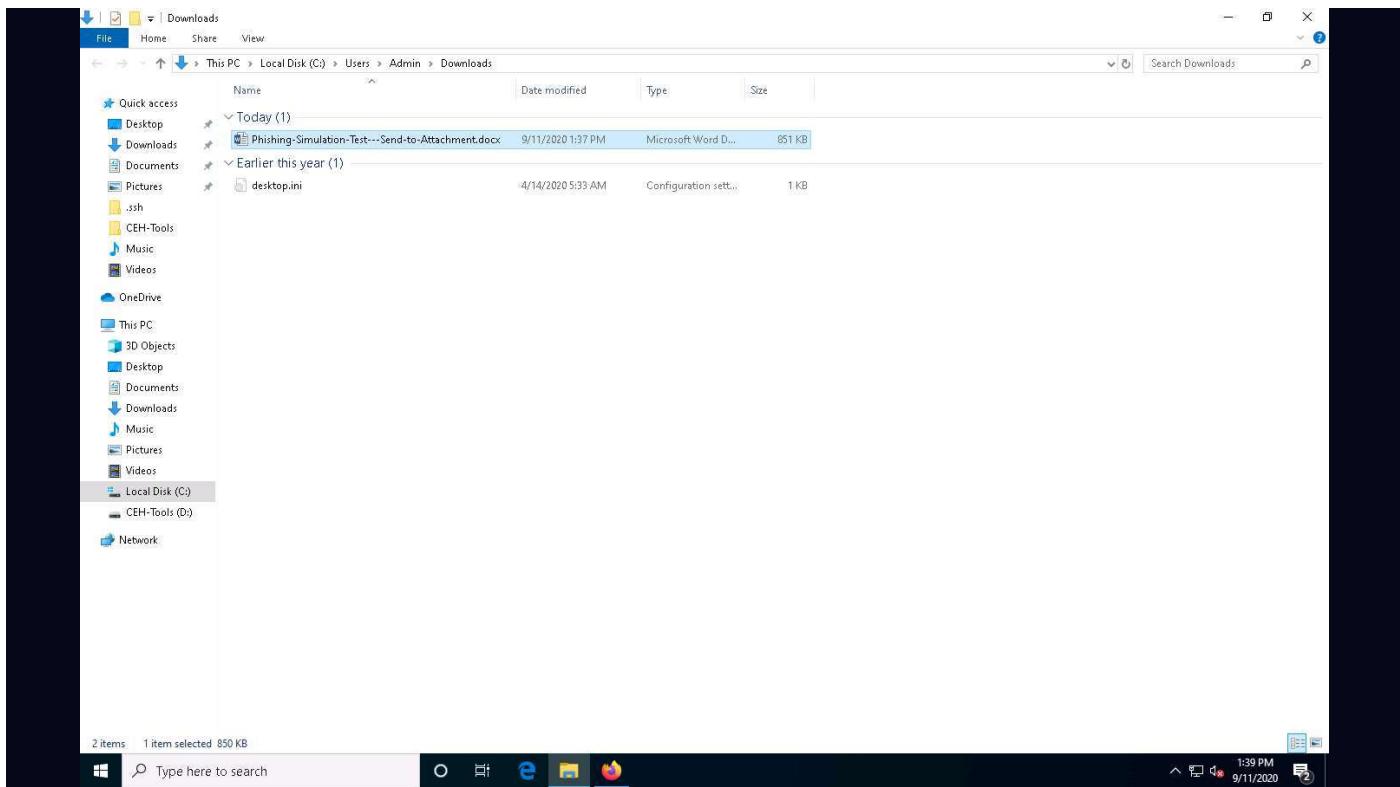
75. The **Campaign Report** page appears; select any phishing campaign from the drop-down list (here, **Test – Send to Attachment**) and click on the **Export** icon to export the report.



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**.

A screenshot of Microsoft Word displaying a document titled 'Phishing-Simulation-Test---Send-to-Attachment.docx'. The document is in 'Protected View', indicated by a yellow bar at the top. The content of the document is a professional-looking report with a red and white header featuring the 'OHPHISH Fortifying Front Lines' logo. The main title is 'Phishing Simulation Report' followed by 'EC-Council - CEH'. The Word ribbon is visible at the top, and the taskbar at the bottom shows the same icons as the previous screenshot.

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

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%

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.