

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.

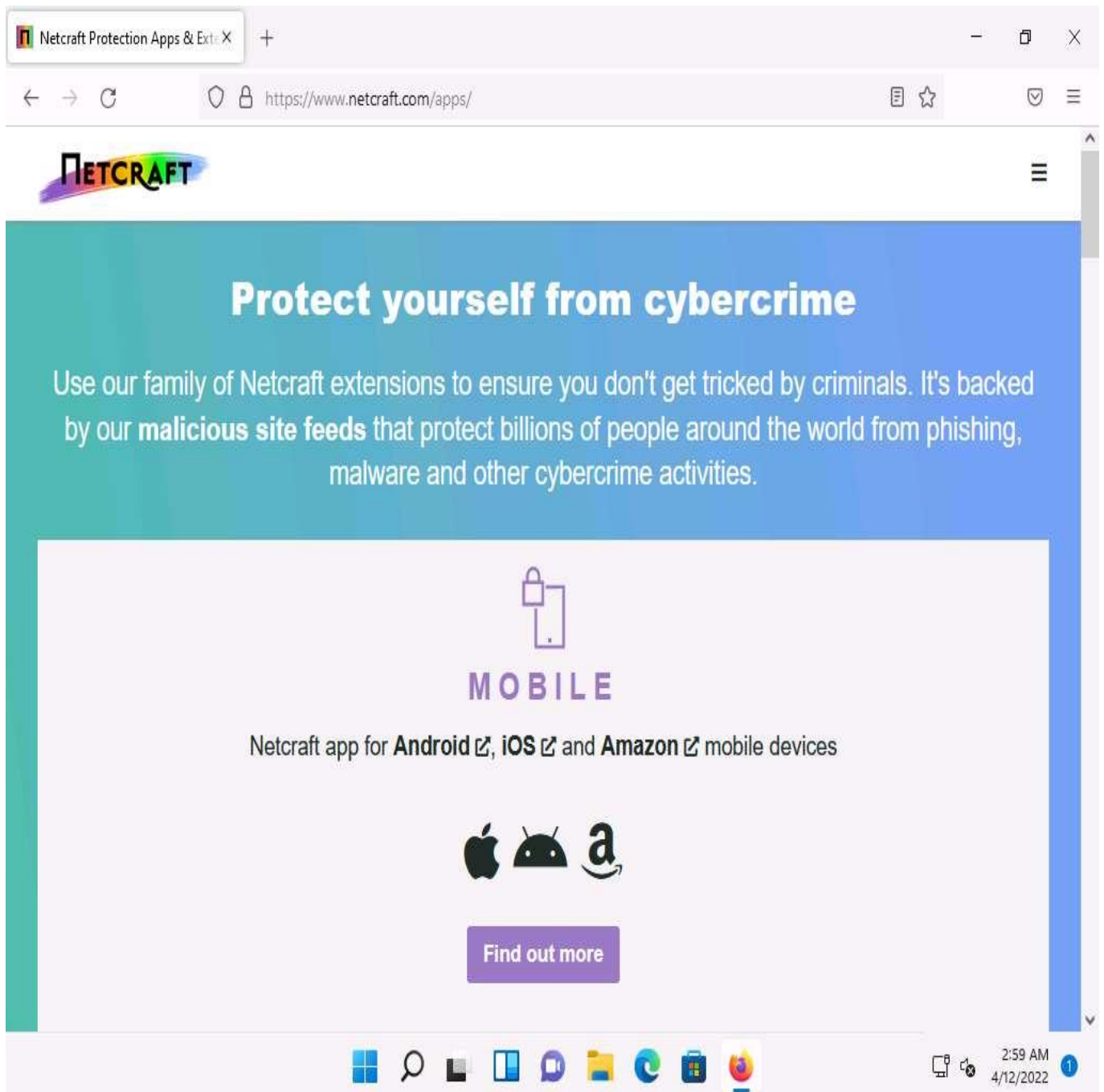
Task 1: Detect Phishing using Netcraft

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.

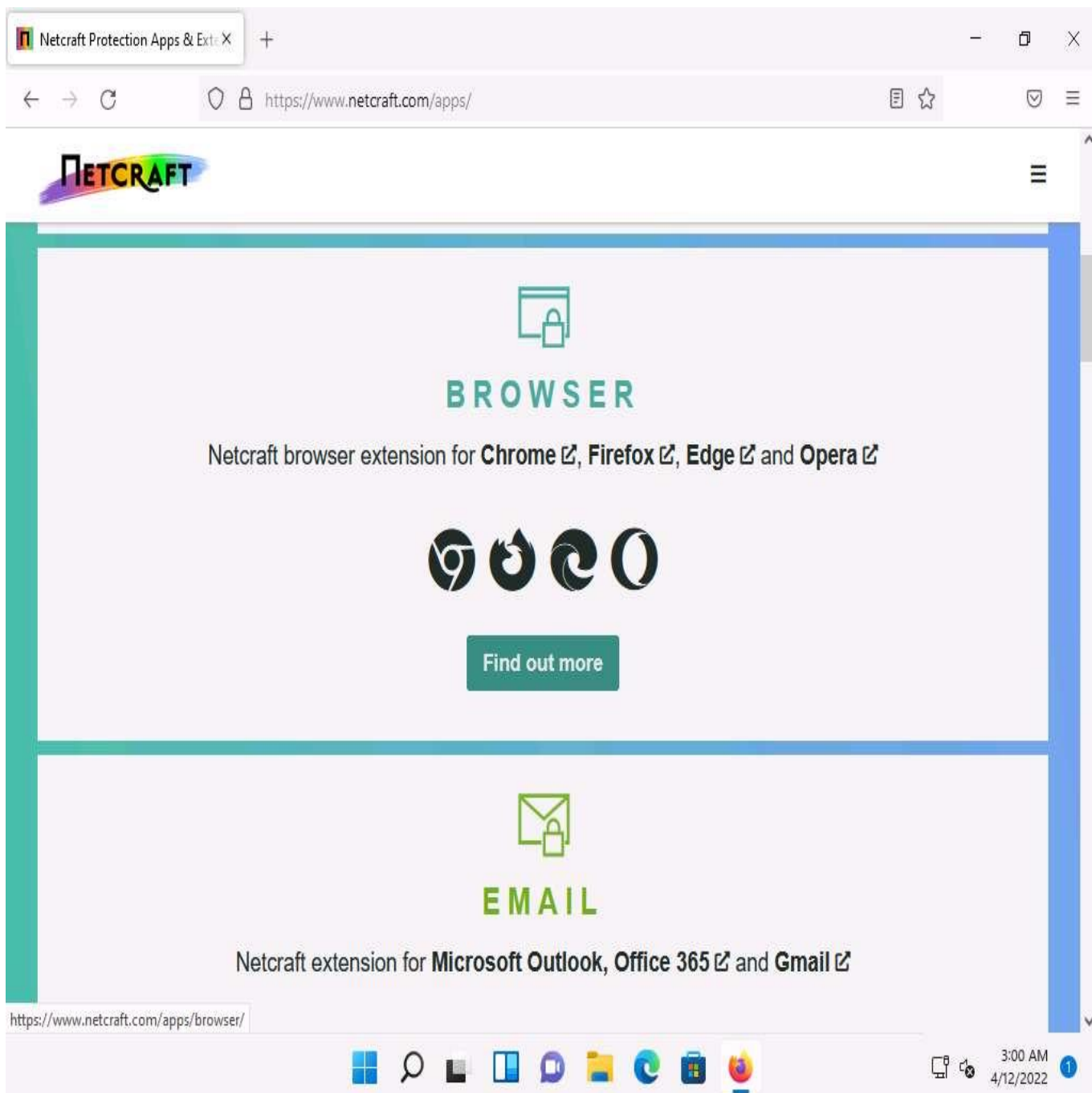
Here, we will use the Netcraft Extension to detect phishing sites.


1. ☐ Click on the [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.

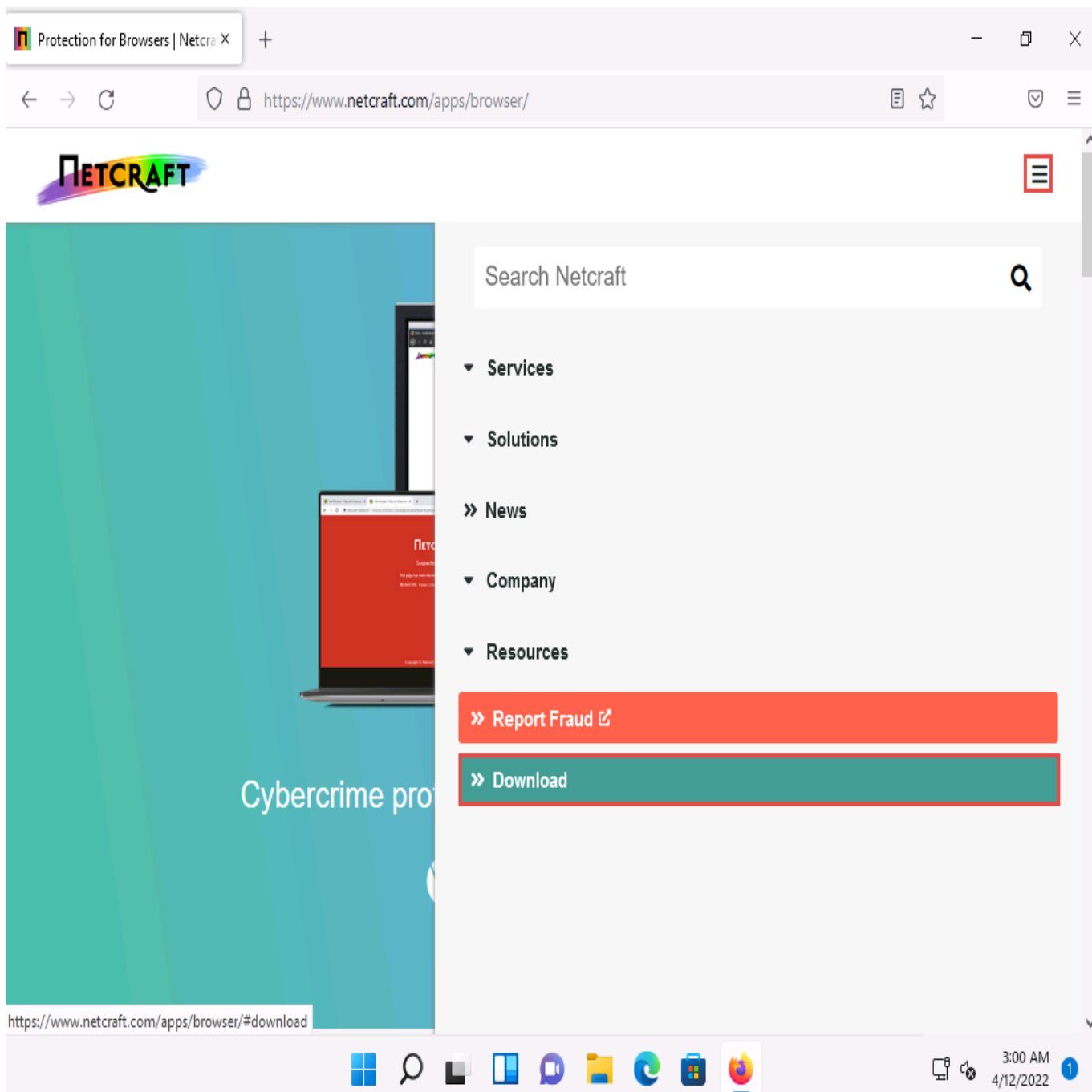
Click **Accept** in the cookie notification in the lower section of the browser.




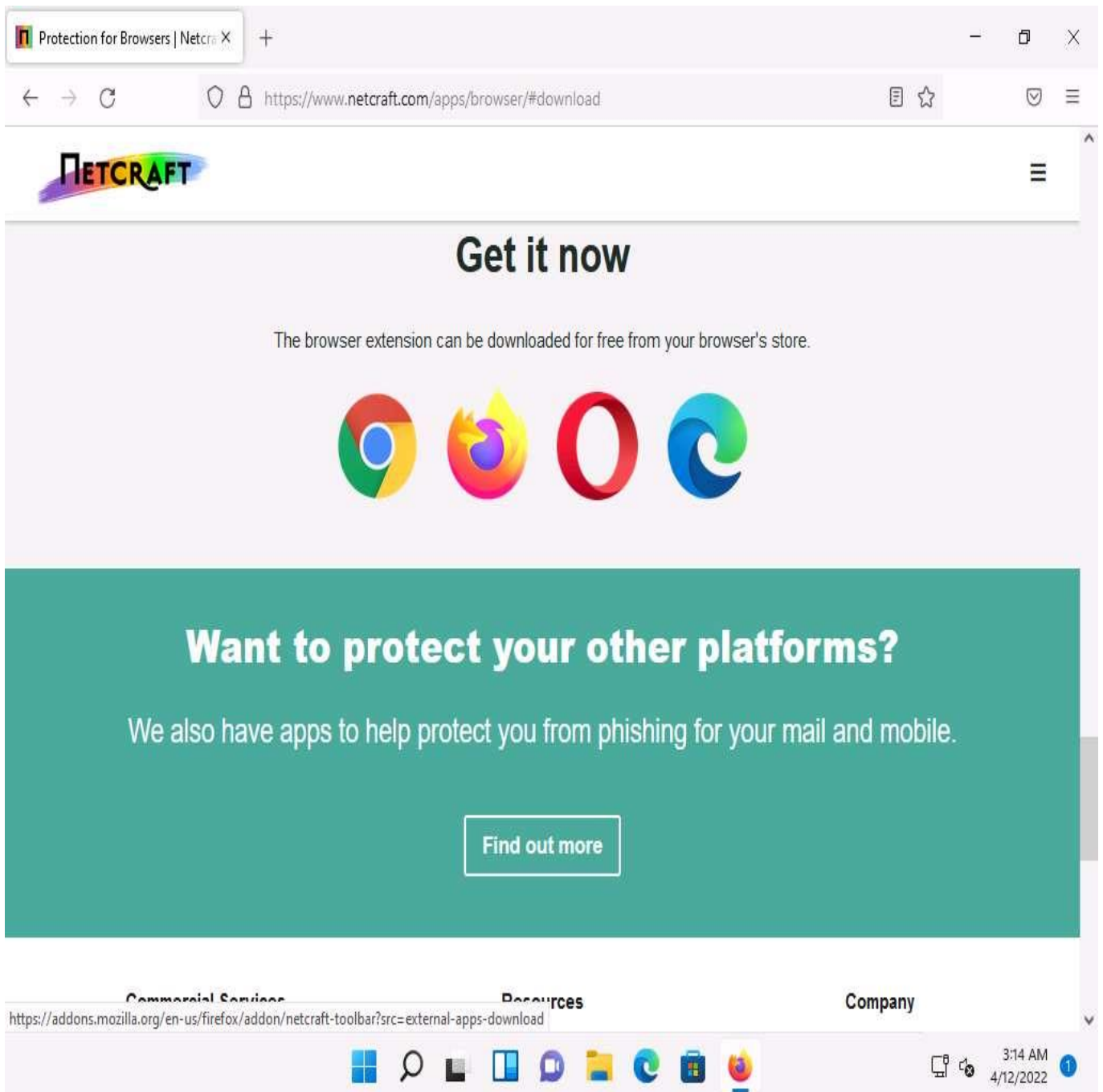
4. ☐ Scroll-down and click **Find out more** button under **BROWSER** option on the webpage.



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.


Netcraft Extension – Get this Ext X

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... v

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](#)

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

Add to Firefox

5,246 Users 30 Reviews 4.4 Stars

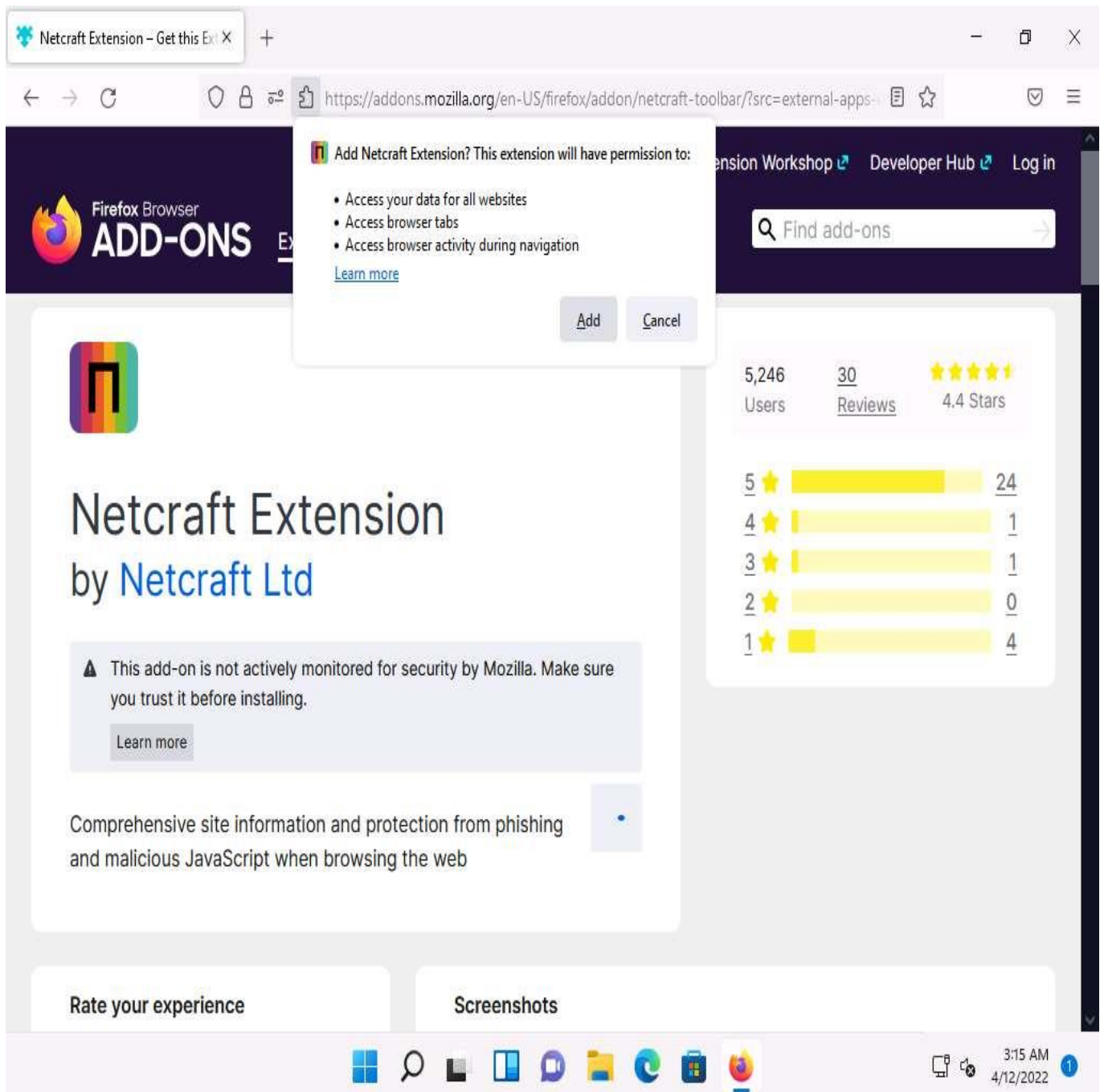
Star Rating	Count
5 Stars	24
4 Stars	1
3 Stars	1
2 Stars	0
1 Star	4

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

3:14 AM 4/12/2022

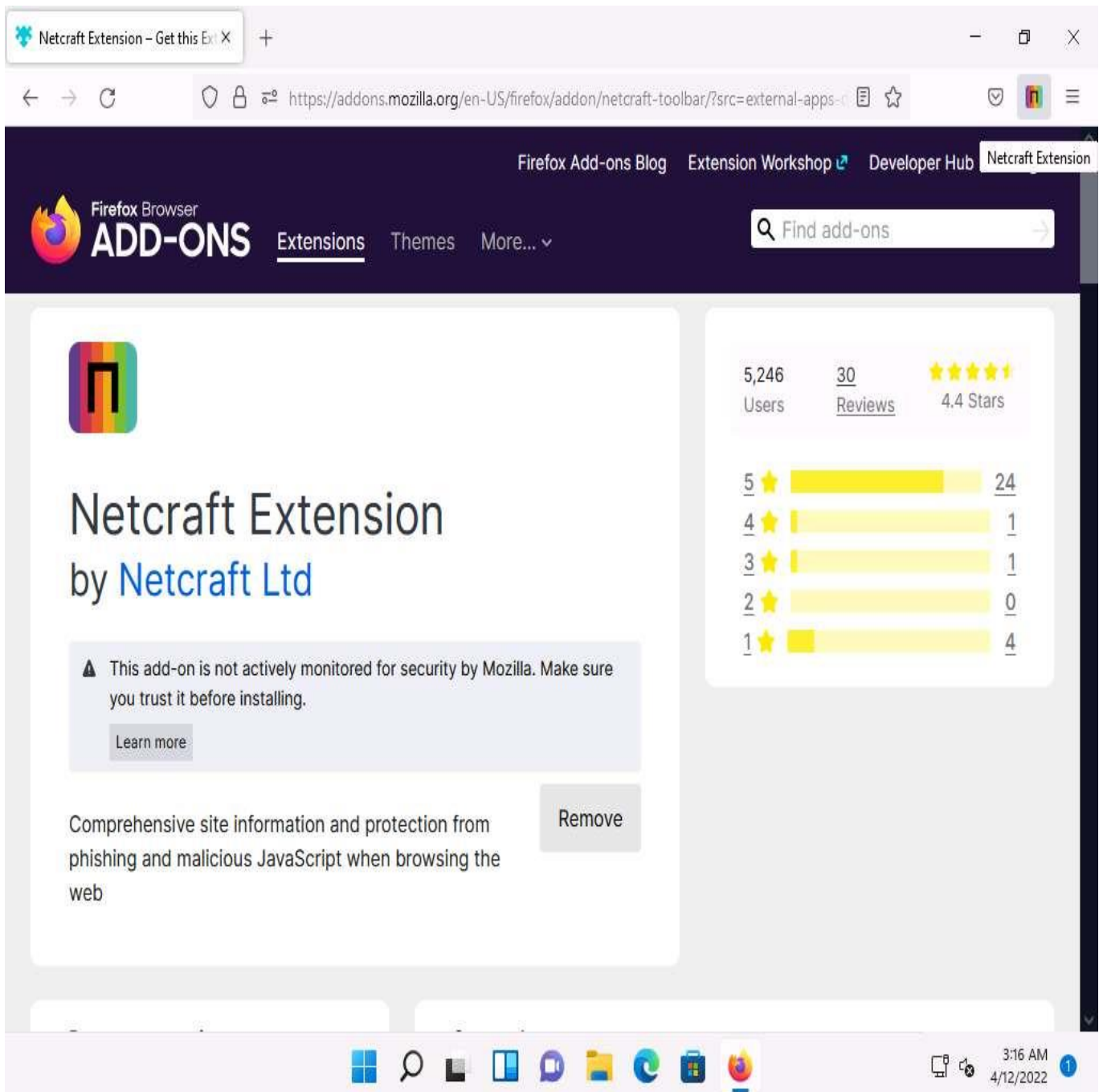
9. ☐ When the **Add Netcraft Extension?** notification pop-up appears on top of the window, click **Add**.

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.

Screenshots may differ with newer versions of Firefox.



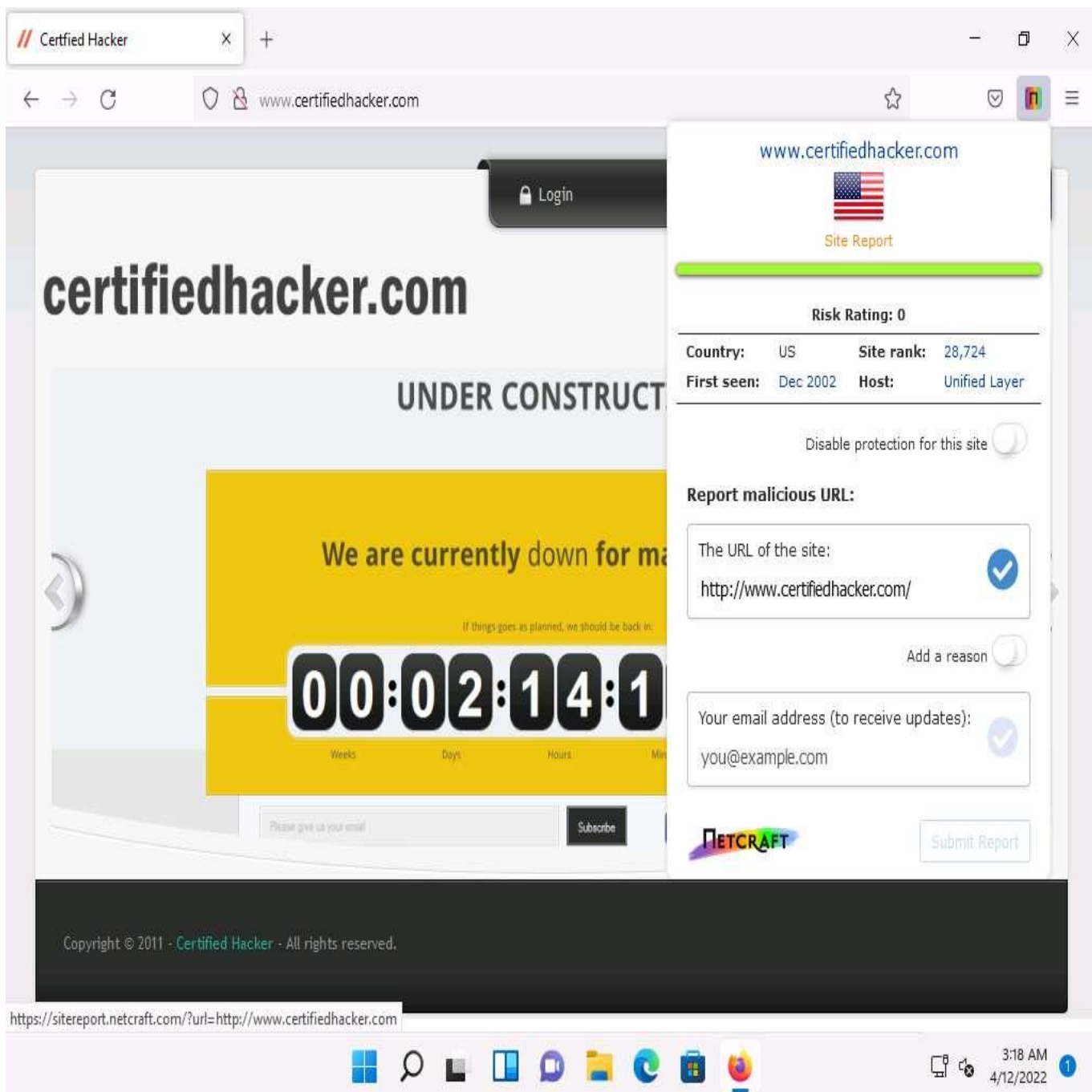
13. ☐ Now, In the address bar of the browser place your mouse cursor, type **http://www.certifiedhacker.com/** and press **Enter**.
14. ☐ The **certifiedhacker.com** webpage appears. Click the Netcraft **Extension** icon in the top-right corner of the browser. A dialog box appears, displaying a summary of information such as **Risk Rating**, **Site rank**, **First seen**, and **Host** about the searched website.

The screenshot shows a web browser window with the address bar displaying `www.certifiedhacker.com`. The website's main content area features a 'JuggyBoy Kitchen' banner and a 'Login' button. A 'Site Report' dialog box is open on the right side of the browser window. The dialog box contains the following information:

- URL: `http://www.certifiedhacker.com/`
- Risk Rating: 0
- Country: US
- Site rank: 28,724
- First seen: Dec 2002
- Host: Unified Layer
- Report malicious URL: ☒ (Add a reason toggle is off)
- Your email address (to receive updates): `you@example.com`
- Submit Report button

The website footer displays: Copyright © 2011 - Certified Hacker - All rights reserved.

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**

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

Certified Hacker

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

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


90%

☆

🔒

📄

☰








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
Connecting to csp.netcraft.com...		Nameserver organisation	whois.domain.com

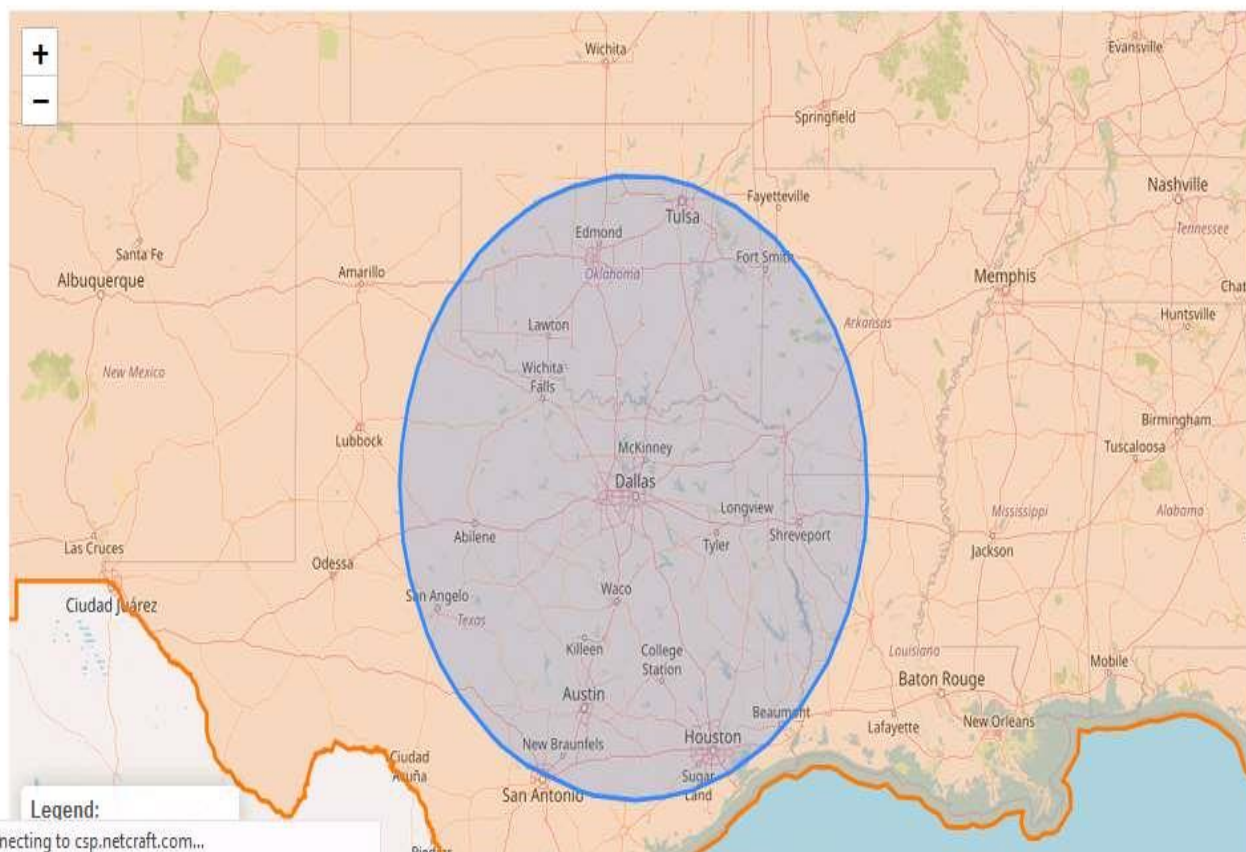


3:19 AM
4/12/2022



IP Geolocation

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



SSL/TLS

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://smbc.ctad-co.com/m** and press **Enter**.

Here, for demonstration purposes, we are using **https://smbc.ctad-co.com/m** phishing website to trigger Netcraft Extension to obtain desired results. You can use the same website or any other website to perform this task.

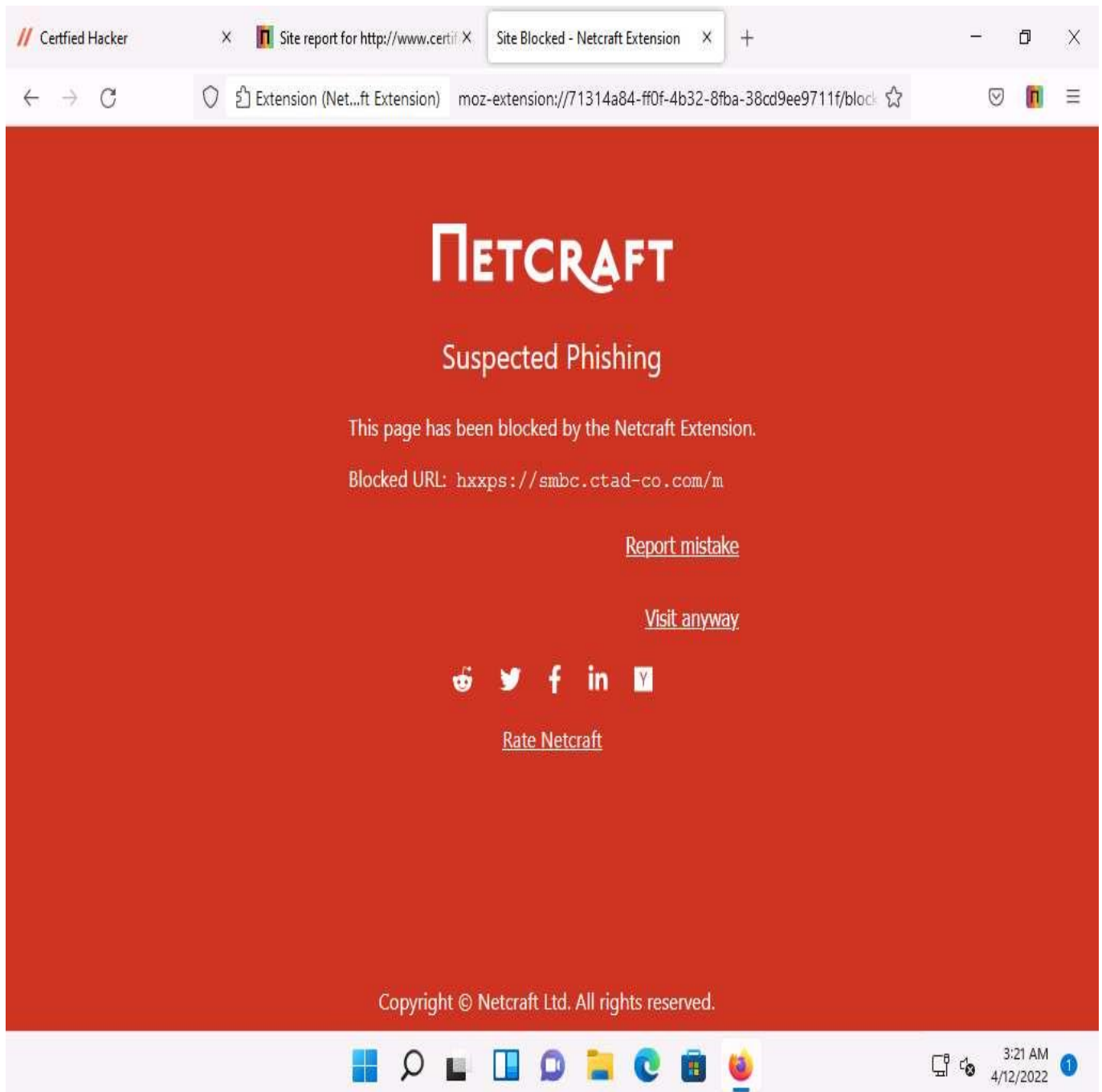
19. ☐ The Netcraft Extension automatically blocks phishing sites. However, if you trust the site, click **Visit anyway** to browse it; otherwise, click **Report mistake** to report an incorrectly blocked URL.

If you are getting an error in opening the website (**https://smbc.ctad-co.com/m**), try to open other phishing website.

OR

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

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.

- ☐ 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**.
- ☐ The **PhishTank** webpage appears, displaying a list of phishing websites under **Recent Submissions**.
- ☐ Click on any phishing website **ID** in the **Recent Submissions** list (in this case, **7486626**) to view detailed information about it.

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

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

PhishTank is operated by [Cisco Talos Intelligence Group](#).

PhishTank® Out of the Net, into the Tank.

username: Sign In
[Register](#) | [Forgot Password](#)

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

Join the fight against phishing

[Submit](#) suspected phishes. [Track](#) the status of your submissions.
[Verify](#) other users' submissions. [Develop](#) software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

[Is it a phish?](#)

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
7486626	https://cssogrdtedadyrealpasssb.firebaseio.com/	buaya
7486625	https://cssogrdtedadyrealpasssb.web.app/	buaya
7486624	https://cssogrdtedadyrealpasssc.firebaseio.com/	buaya
7486623	https://cssogrdtedadyrealpasssc.web.app/	buaya
7486622	https://cssogrdtedadyrealpasse.firebaseio.com/	buaya
7486621	https://cssogrdtedadyrealpasse.web.app/	buaya
7486620	https://cssogrdtedadyrealpasssf.firebaseio.com/	buaya
7486617	https://cssogrdtedadyrealpasssf.web.app/	buaya

What is phishing?
Phishing is a fraudulent attempt, usually made through email, to steal your personal information.
[Learn more...](#)

What is PhishTank?
PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.
[Read the FAQ...](#)

Windows taskbar: 3:24 AM 4/12/2022

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

PhishTank > Details on suspect X

https://www.phishtank.com/phish_detail.php?phish_id=7486626

PhishTank is operated by [Cisco Talos Intelligence Group](#).

PhishTank® Out of the Net, into the Tank.


username Sign In
[Register](#) | [Forgot Password](#)

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

Submission #7486626 is currently ONLINE


Submitted Apr 12th 2022 10:11 AM by [buaya](#) (Current time: Apr 12th 2022 10:25 AM UTC)

<https://cssogrdtedadyrealpasssb.firebaseio.com/>

 **Verified: Is a phish**
As verified by [Shazza](#) [June Dev](#) [darkmoon](#) [titus](#)

Is a phish 100%
Is NOT a phish 0%

Screenshot of site View site in frame View technical details View site in new window



3:26 AM 4/12/2022

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.

PhishTank | Join the fight against phishing X

https://www.phishtank.com

PhishTank is operated by [Cisco Talos Intelligence Group](#).

PhishTank® Out of the Net, into the Tank.

username Sign In
[Register](#) | [Forgot Password](#)

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

Join the fight against phishing

[Submit](#) suspected phishing sites. [Track](#) the status of your submissions.
[Verify](#) other users' submissions. [Develop](#) software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

[Is it a phish?](#)

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishing sites.

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

3:27 AM 4/12/2022

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.

PhishTank > Details on suspect X

https://www.phishtank.com/phish_detail.php?phish_id=2205890

PhishTank is operated by [Cisco Talos Intelligence Group](#).

PhishTank® Out of the Net, into the Tank.


username Sign In
[Register](#) | [Forgot Password](#)

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

Submission #2205890 is currently offline

Submitted Jan 2nd 2014 10:56 AM by [knack](#) (Current time: Apr 12th 2022 10:27 AM UTC)

<http://be-ride.ru/confirm/>

 **Verified: Is a phish**
As verified by [buaya](#) [paulch](#) [NotBuyingIt](#) [phishohucker](#)

Is a phish 100%
Is NOT a phish 0%

Screenshot of site View site in frame View technical details View site in new window

Personal Business Email address forgot? Password forgot? Log in

PayPal™ Buy Sell Transfer

Redesigned with you in mind.

Windows taskbar: 3:28 AM 4/12/2022

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