

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

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.

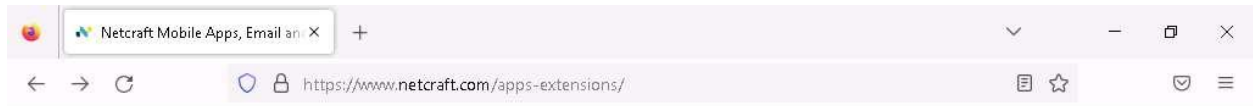
Task 1: Detect Phishing using Netcraft

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 web browser, and go to <https://www.netcraft.com/apps-extensions> (here, we are using **Mozilla Firefox**).
3. The **Netcraft** website appears, as shown in the screenshot. Scroll-down and click **LEARN MORE** button under **Browser Protection** section on the webpage.

If the cookie pop-up appears, click **ACCEPT** to continue.



Browser Protection

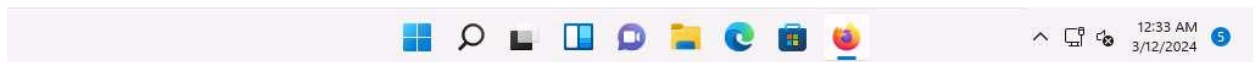
Netcraft's free browser extension provides real-time enhanced protection from malicious sites defending you from phishing, fake shops, and malicious scripts such as JavaScript skimmers and cryptocurrency miners.

The browser extension works with all major browsers, including Chrome, Firefox, Edge, and Opera.

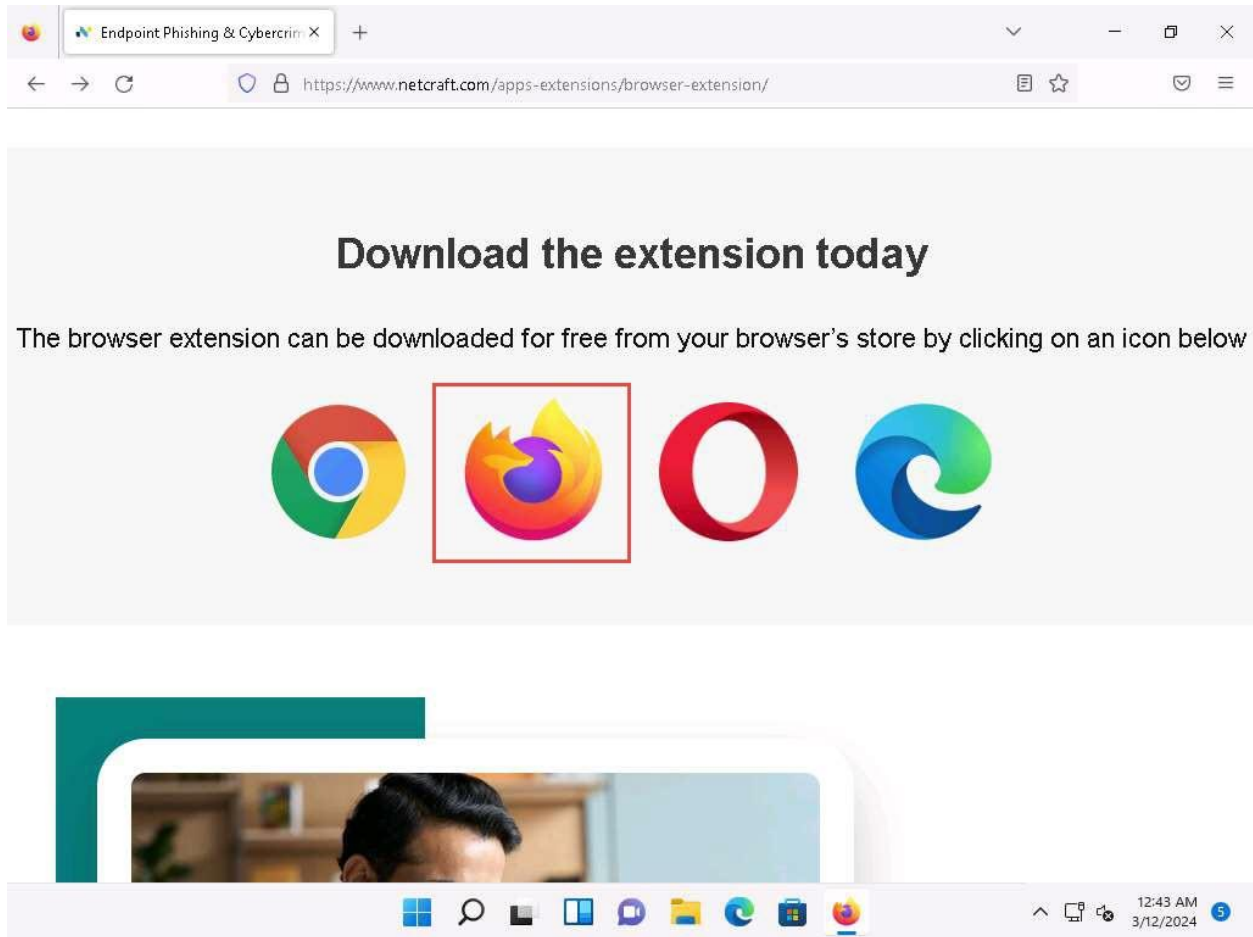


[LEARN MORE](#)

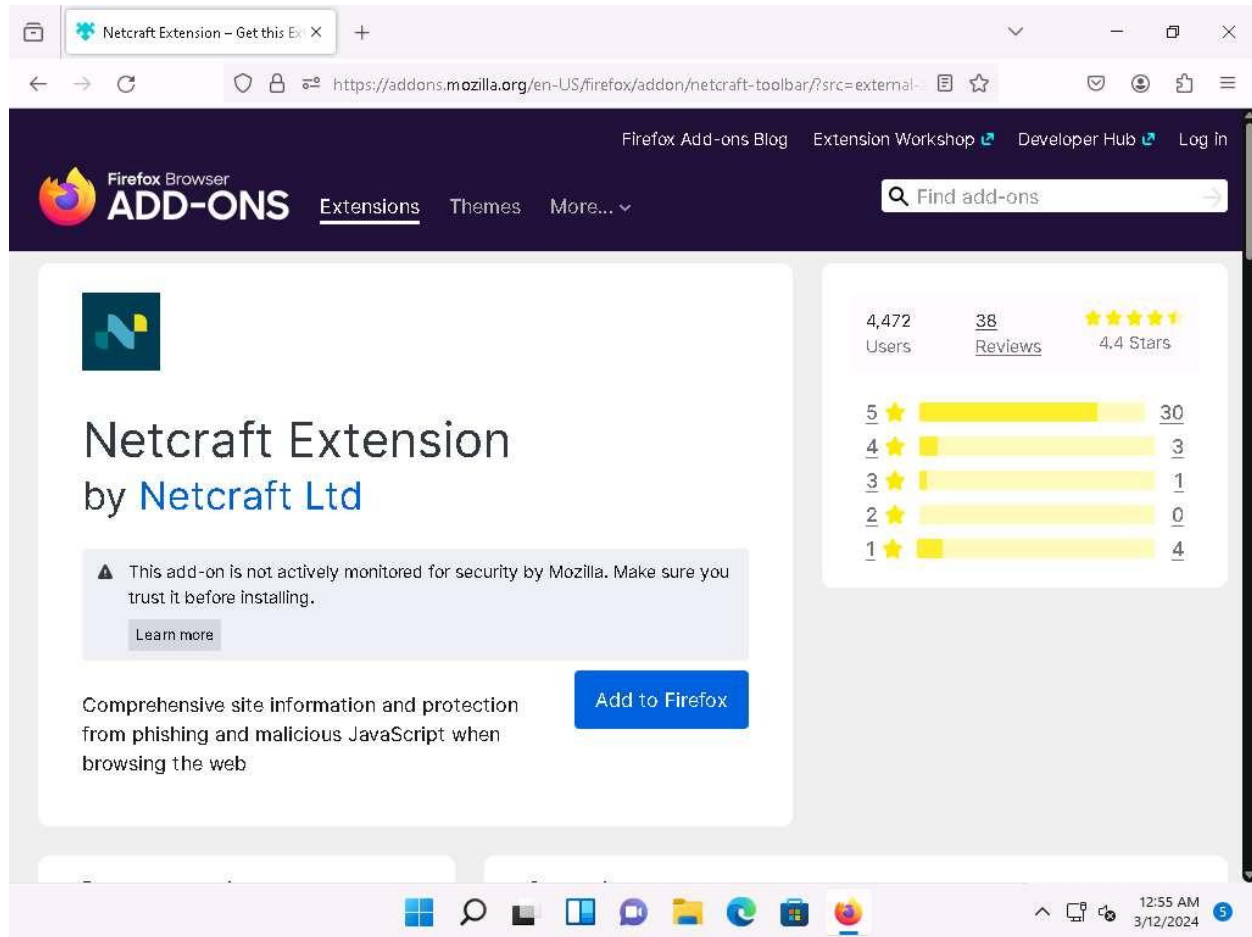
No audio device is installed



4. Scroll-down to **Download the extension today** and click on **Firefox** logo, as shown in the screenshot.

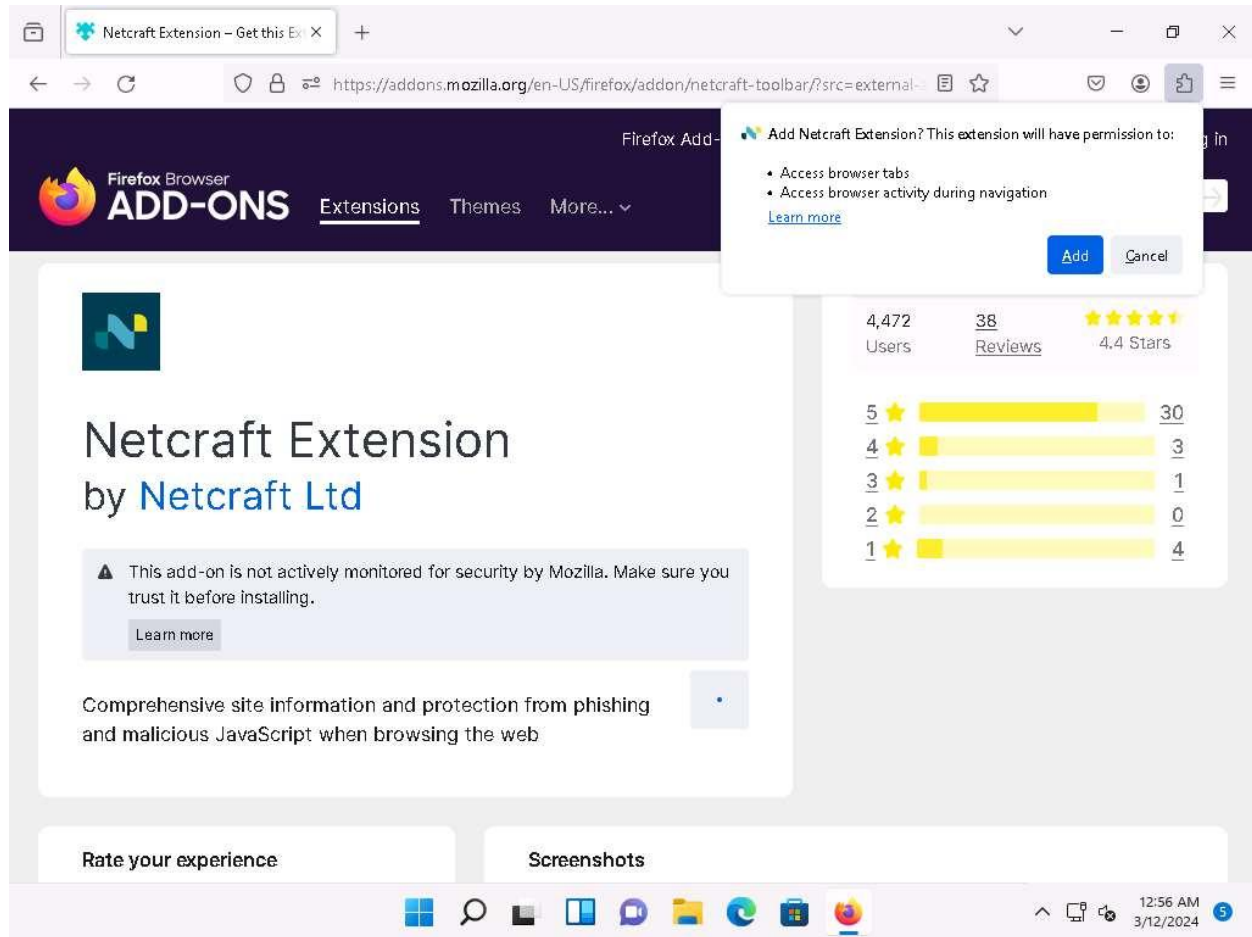


5. On the next page, click the **Add to Firefox** button to install the Netcraft extension.



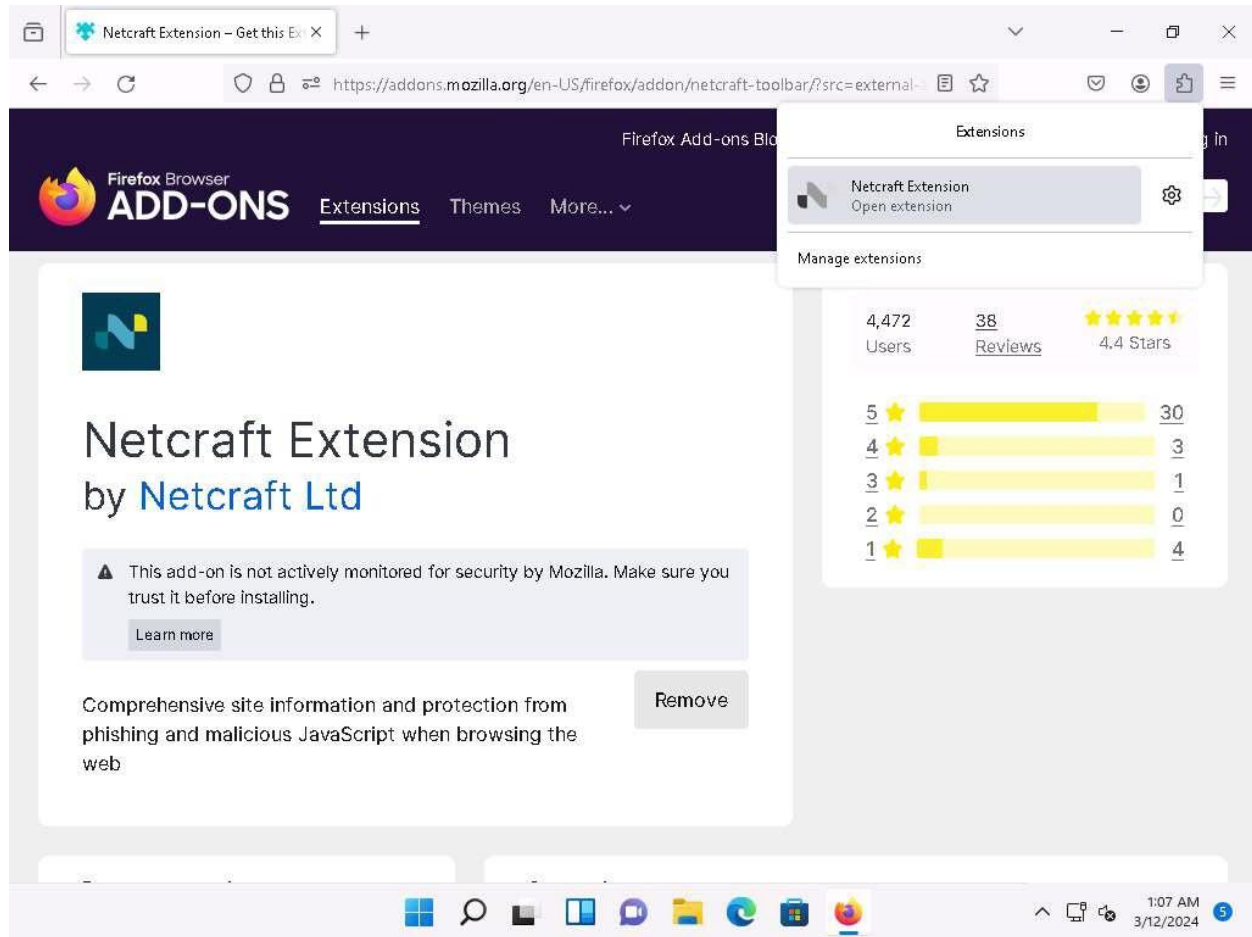
6. When the **Add Netcraft Extension?** notification pop-up appears on top of the window, click **Add**. If **Access your data for all websites**, pop-up appears, click **Allow**.

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

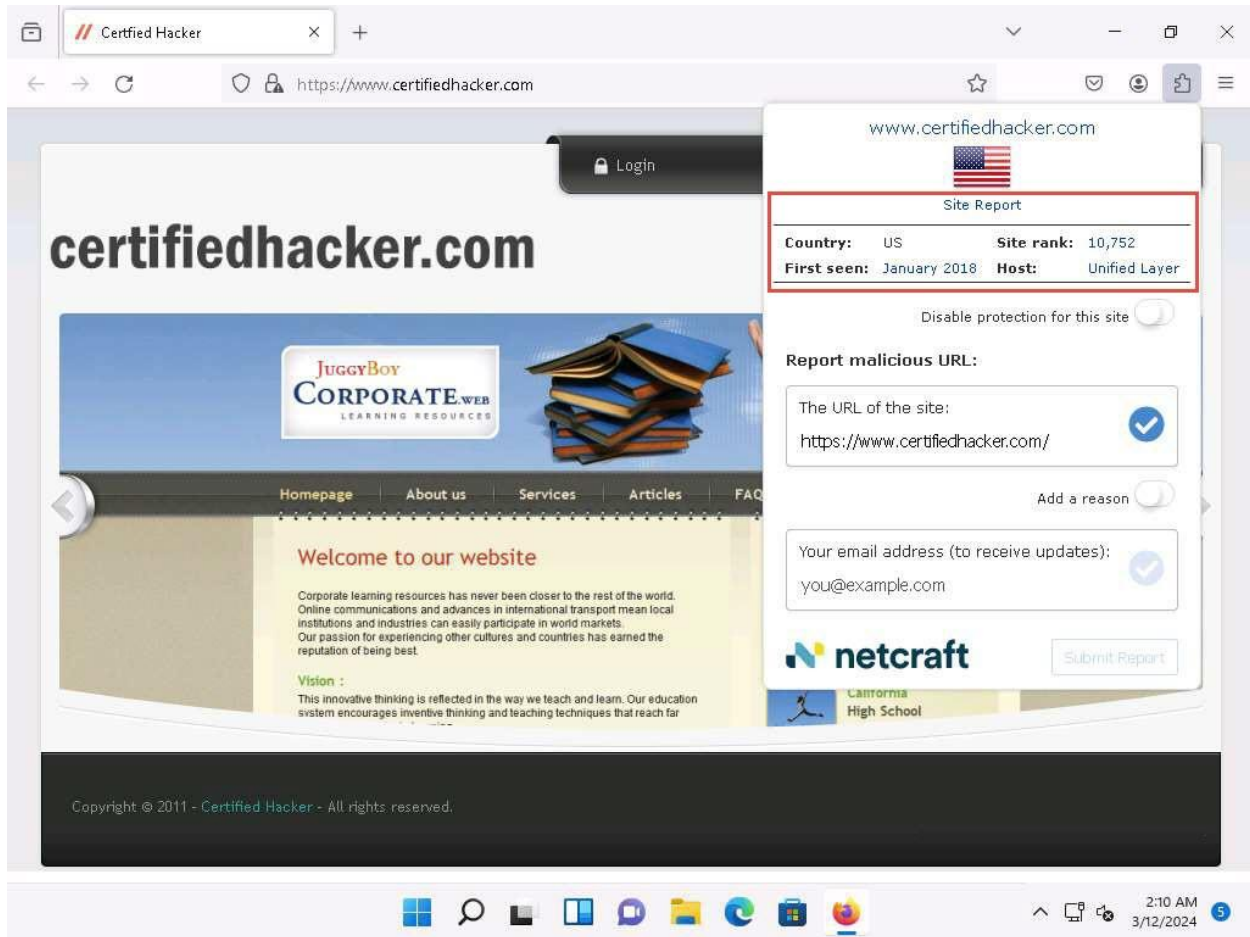


7. If **One step left to protect yourself** webpage appears, click on **Grant Permission** to provide permissions to the extension.
8. Click on **Extensions** button the top-right corner of the browser to view the **Netcraft Extension** icon, as shown in the screenshot.

Screenshots may differ with newer versions of Firefox.



9. Now, navigate to <https://www.certifiedhacker.com> and click the **Extension** icon in the top-right corner of the browser and open Netcraft extension. A dialog box appears, displaying a summary of information such as **Site Report**, **Country**, **Site rank**, **First seen**, and **Host** about the searched website.
10. Now, click the **Site Report** link from the dialog-box to view a report of the site.



11. The **Site report** for **https://www.certifiedhacker.com** page appears, displaying detailed information about the site such as **Background, Network, IP Geolocation, and SSL/TLS**.

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

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

► 🔍 Look up another site?

Share:     

Background

Site title	Not Acceptable!	Date first seen	January 2018
Site rank	10752	Primary language	English
Description	Not Present		




Certified Hacker

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

https://sitereport.netcraft.com/?url=https://www.certifiedhacker.com

90%

 netcraft

LEARN MORE


REPORT FRAUD

IP Geolocation


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

+

-



Legend:



2:26 AM

3/12/2024










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	unknown	nginx/1.21.6	29-Jan-2024
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	unknown	nginx/1.19.10	6-Oct-2022
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	Apache	8-May-2022
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.14.1	12-Jan-2019
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.12.2	13-Aug-2018
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	Apache	1-Sep-2016

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of [rules](#). Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [open-spf.org](#).

Qualifier	Mechanism	Argument
	       	 

2:27 AM
3/12/2024

12. 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**.

13. Now, in the browser window open a new tab, and navigate to **https://end-authenticat.tftpd.net/**.

Here, for demonstration purposes, we are using **https://end-authenticat.tftpd.net/** phishing website to trigger Netcraft Extension to obtain desired results. You can use the same website or any other website to perform this task.

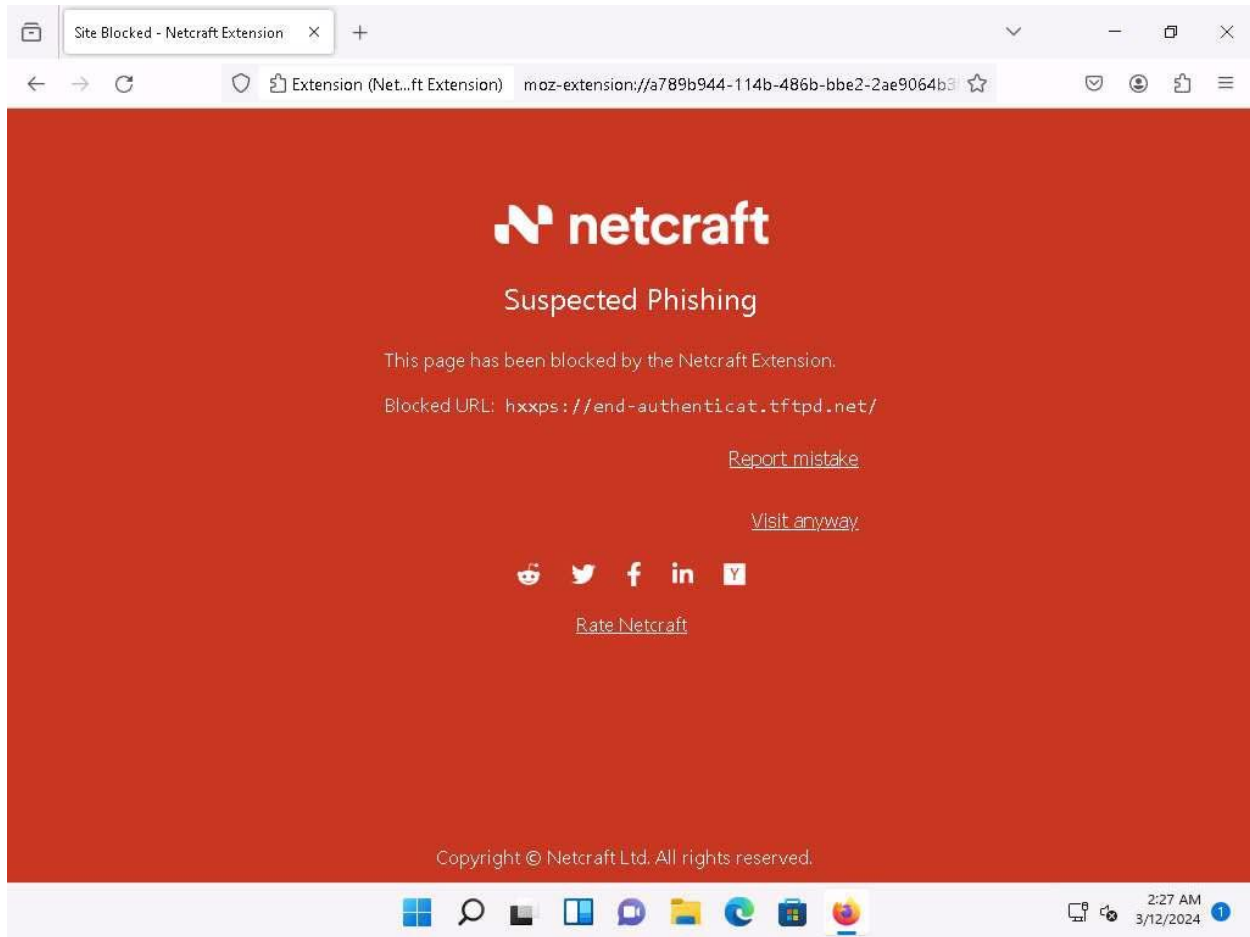
14. The Netcraft Extension automatically blocks phishing sites. However, if you trust the site, click **Visit anyway** to browse it; otherwise, click **Report mistake** to report an incorrectly blocked URL.

If you are getting an error in opening the website (**https://end-authenticat.tftpd.net/**), 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.



15. This concludes the demonstration of detecting phishing using Netcraft Extension.

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

Question 9.2.1.1

If Netcraft identifies any site as a phishing website, what message will Netcraft display on the user's web browser?