Safeguarding Against Phishing

In a Phishing attack, the attacker impersonates a trusted unit, and thereby is able to fool a user to divulge personal information including passwords, credit card details, or bank details. In this exercise, you will learn to configure Internet Explorer's built-in anti-phishing function called SmartScreen Filter.

Please refer to your course material or use your favorite search engine to research this topic in more detail.

Learning Outcomes

After completing this exercise, you will be able to:

- Use available tools to mitigate Phishing

Your Devices

You will be using the following devices in this lab. Please make sure these are powered on before proceeding.

- **PLABWIN10** (Workstation - Windows 10)

PLABWIN10
Workstation
192.168.0.5/24

Task 1 - Turn on the SmartScreen Filter

A SmartScreen Filter warns you of the website you are visiting is a potential phishing threat to your system. You can turn on the SmartScreen Filter for a browser by accessing a browser configuration. In this task, you will turn on the SmartScreen Filter on the Internet Explorer browser on the **PLABWIN10** device.

To do so, perform the following steps:

Step 1

Ensure that you have powered on the devices mentioned in the introduction section.

Connect to **PLABWIN10** device.

Click **Internet Explorer** on the taskbar.

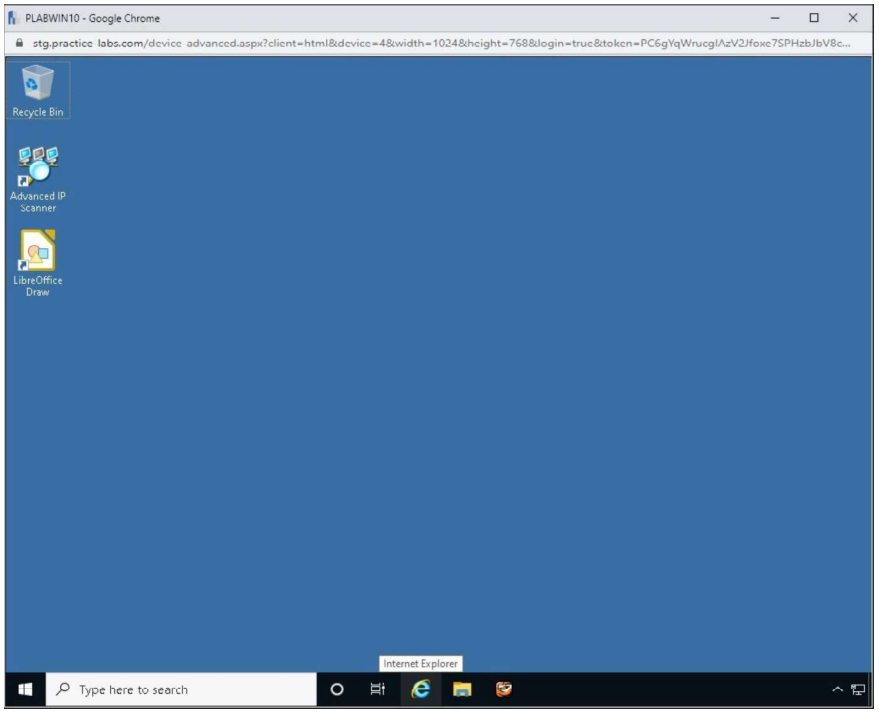

Figure 3.1 Screenshot of the PLABWIN10 desktop: Internet Explorer icon on the taskbar is highlighted on the PLABWIN10 Windows desktop.

Step 2

On the browser window, access the menu bar at the top.

Click the **Configuration** icon, select the **Safety** > **Turn on Windows Defender SmartScreen...**

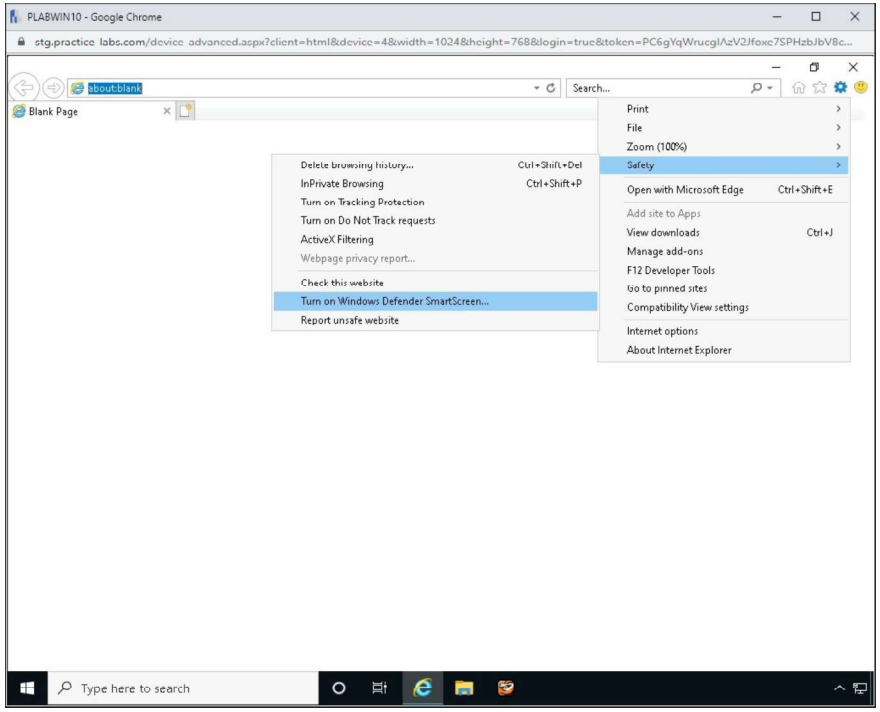

Figure 3.2 Screenshot of the PLABWIN10 desktop: Configuration icon > Safety > Turn on Windows Defender SmartScreen... menu-items are highlighted on the Internet Explorer window.

Step 3

The **Microsoft Windows Defender SmartScreen** dialog box appears.

Read what this feature was designed to do and verify that it is turned on.

Click **OK**.

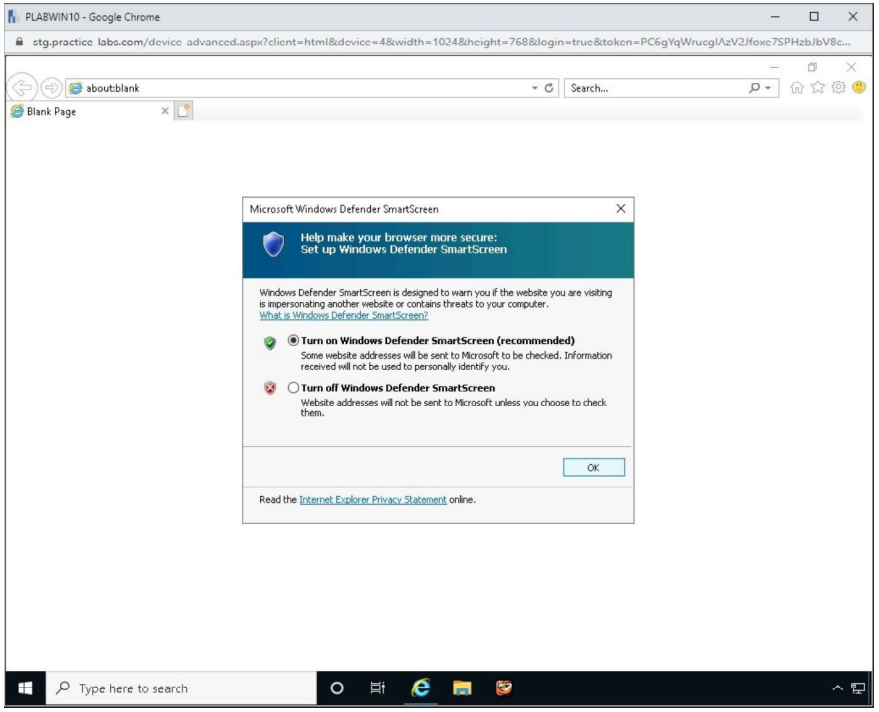

Figure 3.3 Screenshot of the PLABWIN10 desktop: Microsoft Windows Defender SmartScreen dialog box is displayed showing the required settings performed and the OK button available.

Task 2 - Verify the Phishing Filter is Working

Once the SmartScreen Filter activated, it should block any potential phishing websites that the browser might try to access. In this task, you will try to access one such website listed on http :// www . phishtank . com and watch the browser response on the **PLABWIN10** device.

> *Note: Various databases are available that list of websites that indulge in phishing. Examples of such databases include* http :// www . phishtank . com, http :// www . phishbank . com, *and many more.*

To find out if the phishing filter activated on the browser is working, follow these steps:

Step 1

Connect to **PLABWIN10**.

Access the website http :// www . phishtank . com.

Highlight any of the listed websites, right-click and select **Copy**.

Please note that this website is dynamically updated and will have different results than what you see below.

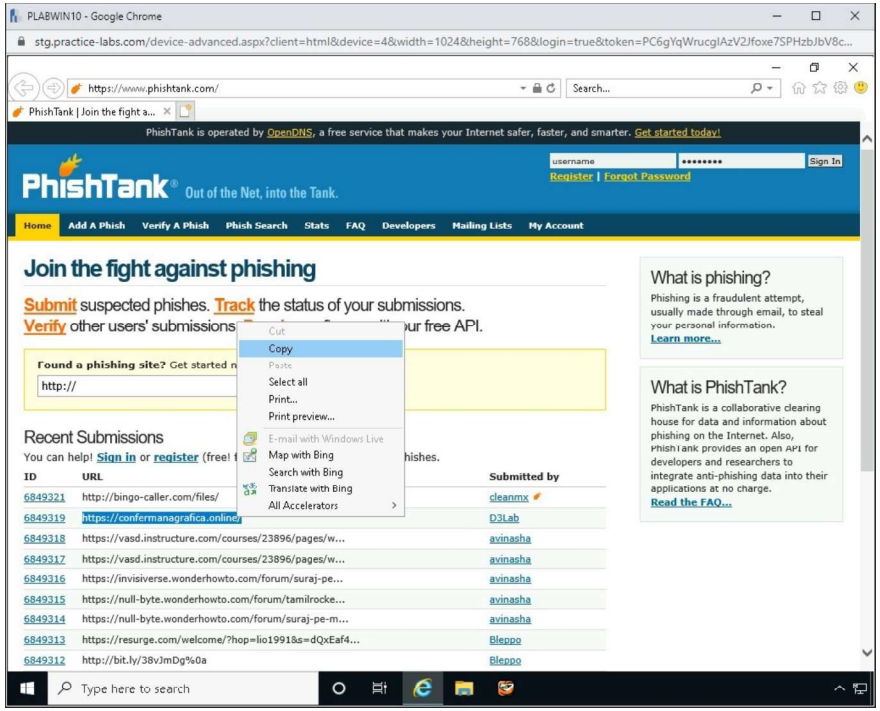

Figure 3.4 Screenshot of the PLABWIN10 desktop: Context menu (that appears on right-clicking selected content) > Copy menu-options are displayed on the PhishTank website.

Step 2

Open a new tab on the web browser.

Paste the copied website name in the address bar and press **Enter**.

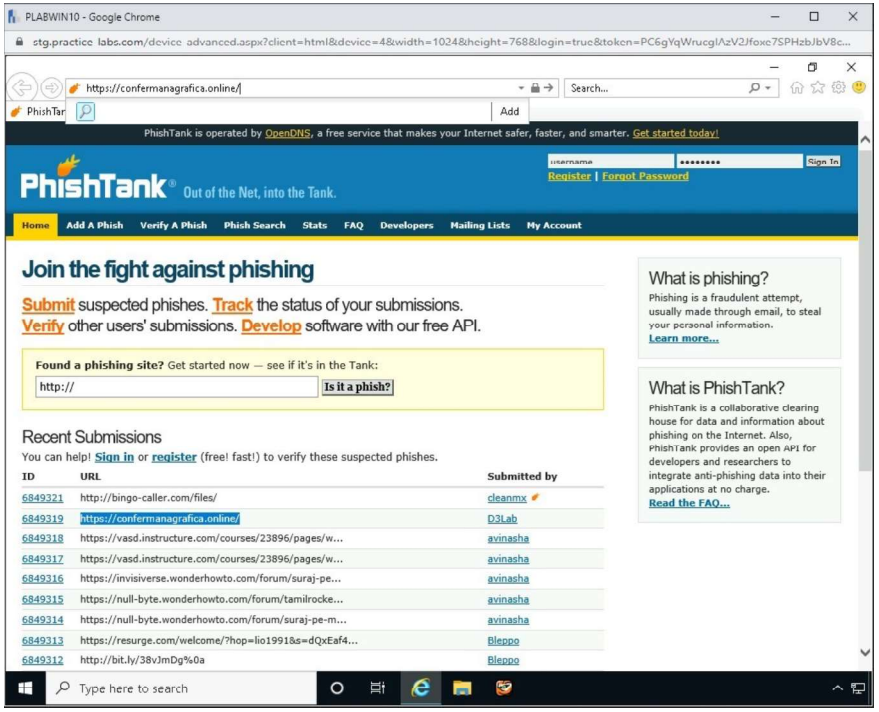

Figure 3.5 Screenshot of the PLABWIN10 desktop: Required URL is copied into the address bar at the top on the Internet Explorer window.

Step 3

Note the message from the activated filter flagging the website as a potential threat.

You might also sometimes get a message that the webpage is blocked.

It is important to understand that the maintenance of an updated list of dangerous and malicious sites is a dynamic process. There may be sites that have been identified as phishing sites by databases such as www.phishtank.com. However, these sites may yet have to be classified as potential threats by Microsoft's listing. For this reason, you may find that some or even many of the sites you test will not be blocked by the filter. In order to get the results shown here, you may need to test several sites.

You may find that some of the sites in the phishing list may be blocked by the proxy server of the Practice Labs topology and you may get an error message

stating something like "Web Page Blocked." Try several different sites in the list until you get a result similar to that in the screenshot.

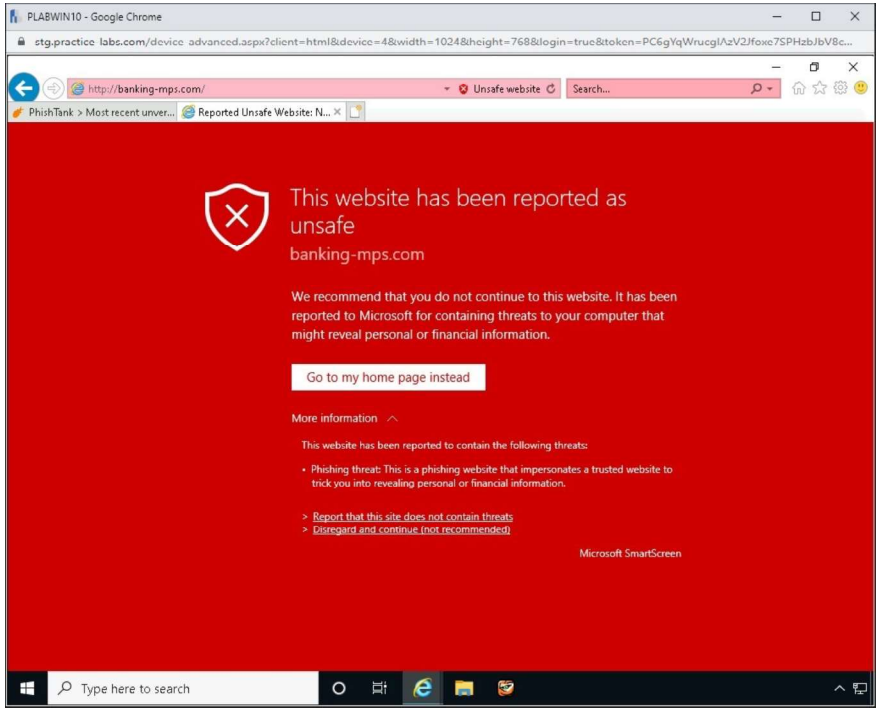

Figure 3.6 Screenshot of the PLABWIN10 desktop: Warning dialog box is displayed in the Internet Explorer window.

Keep all devices that you have powered on in their current state and proceed to the next exercise.