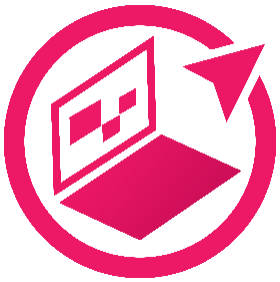


Simulated Email Phishing Attack

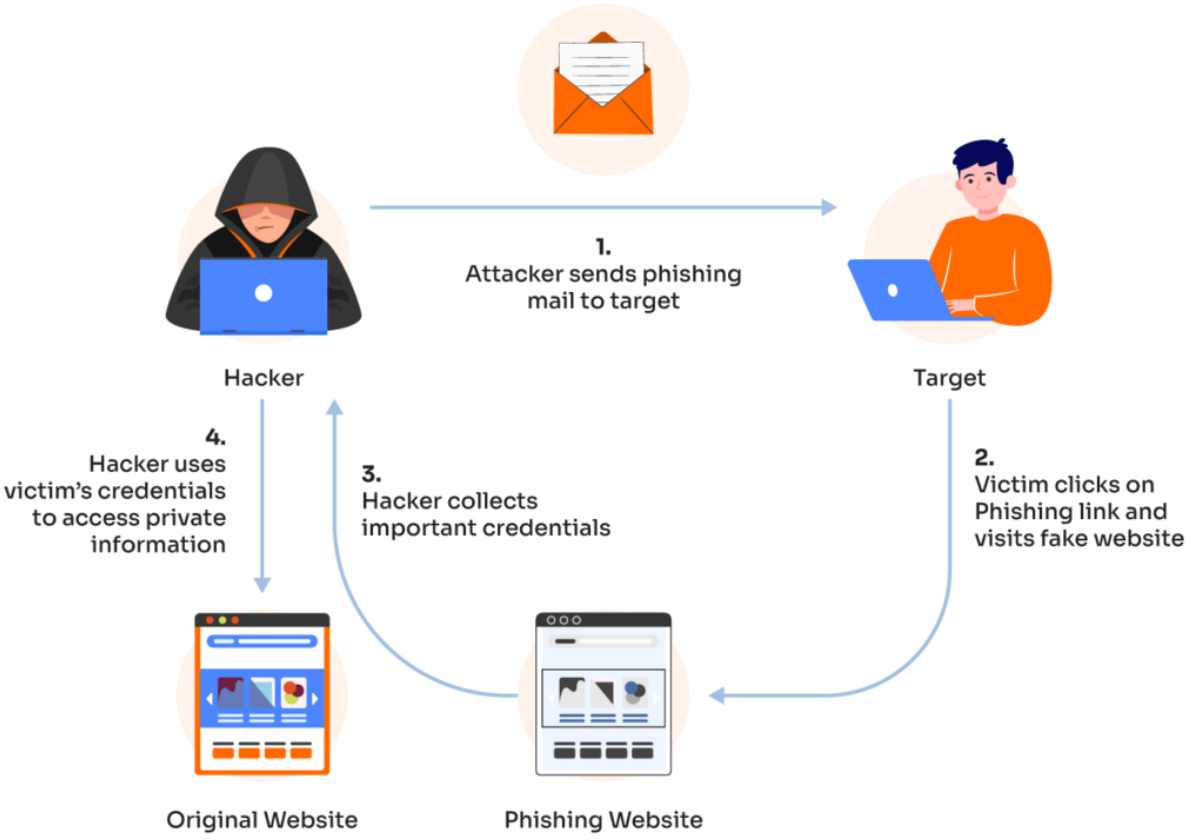
Perp: Khalid Ebn Elwleed Mohamed Ahmed

October 2025

Contents

Introduction

Phishing is a social engineering technique that, using various methodologies, aims to influence the target of the attack to reveal personal information, such as an email address, username, password, or financial information. This information is then used by the attacker to the detriment of the victim. **The Life cycle of Phishing Attack:**



This post simulates a common phishing attack (email phishing) to demonstrate the steps an attacker takes to achieve their objectives. The simulated test was performed in a controlled environment using the following tools**: Kali Linux** (a Debian-based distribution for penetration testing and security research), **VMware** (virtualization to run multiple operating systems safely), and several **Gmail accounts created specifically for testing the** scenario.

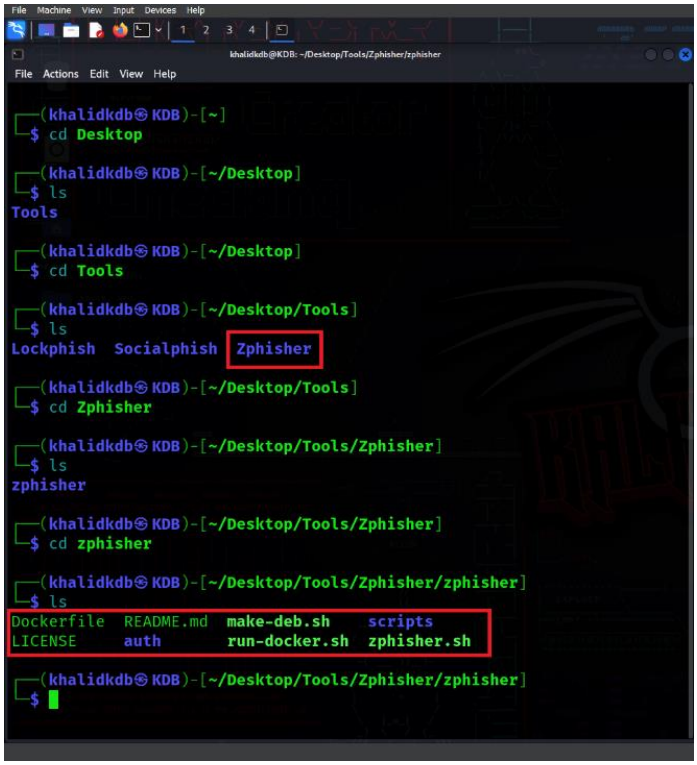
Note:

This simulation was carried out for educational/testing purposes in a controlled environment—ensure all real-world tests have proper authorization and follow legal and ethical guidelines.

Create Malicious URL

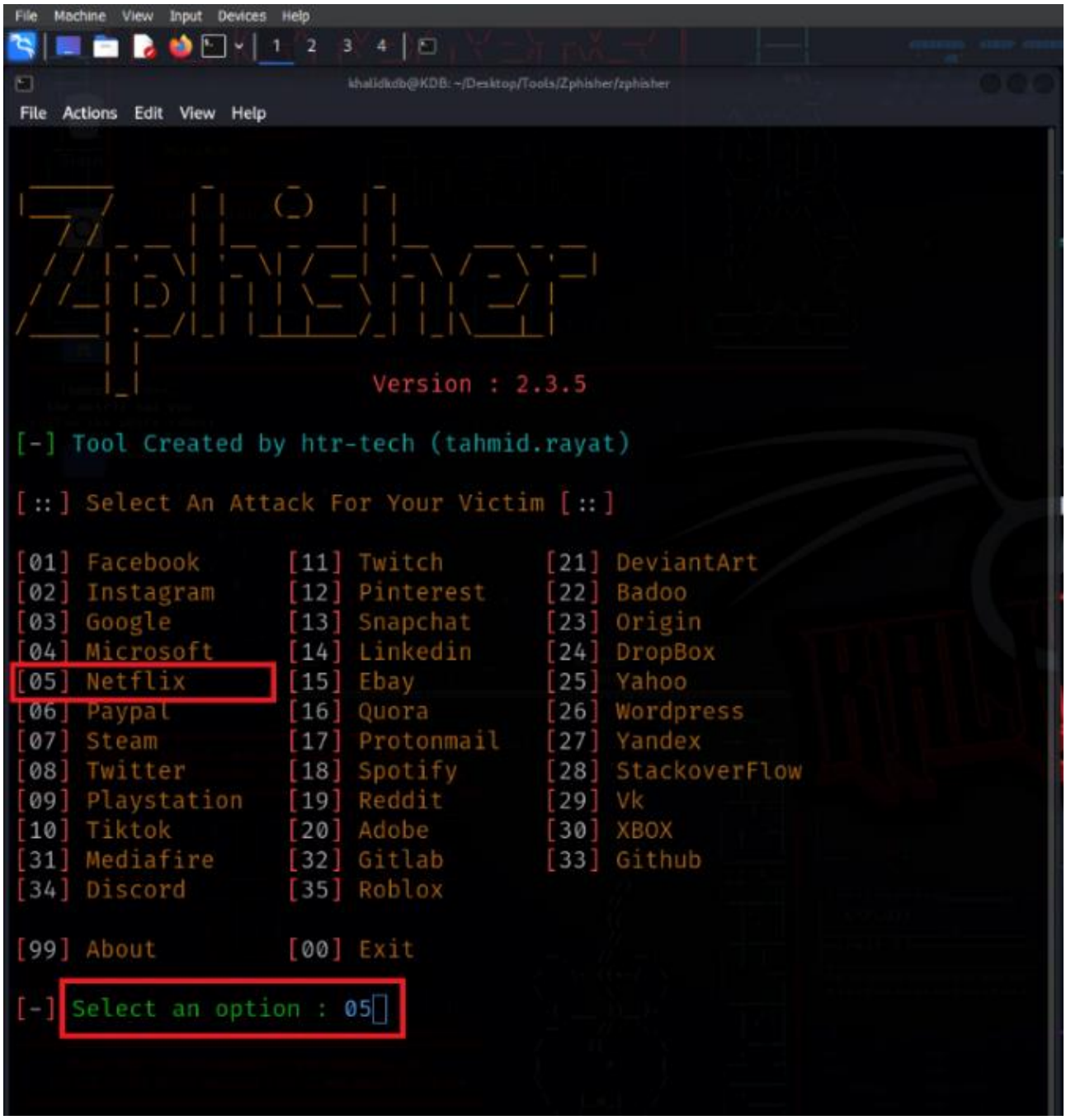
In any attempt to carry out a phishing attack, there are two stages to establishing, the first is **creating a malicious link** and the second is **creating a mail** with a malicious link inside it that looks like a familiar one.

1. First, a malicious link will be created using **Zphisher tool**, a software application that is employed in phishing assaults (PhaaS), as we previously discussed.

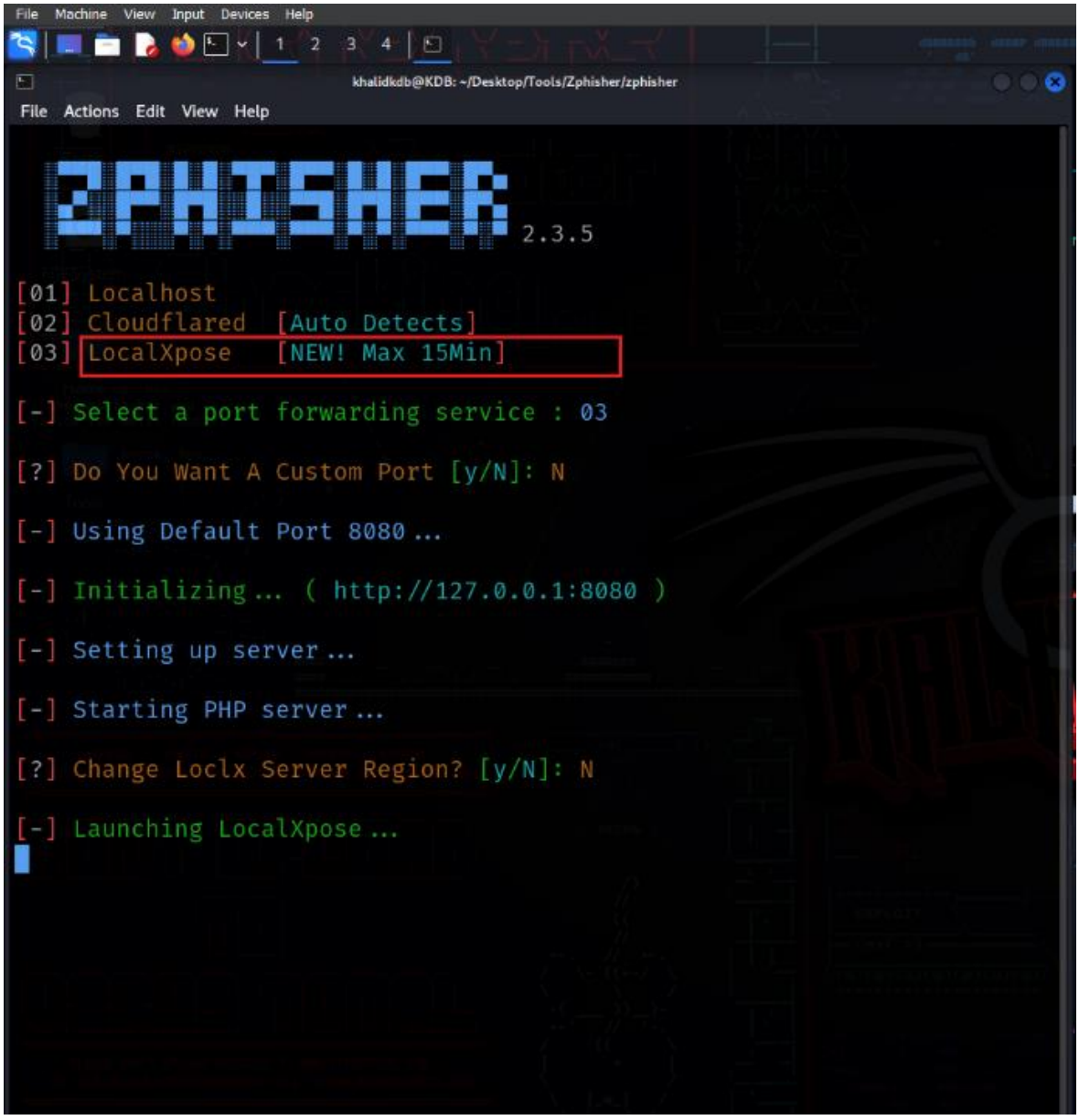


Based on the intended website or service, Zphisher's individual content files may change. But they often contain **JS, HTML and CSS code that mimics the interactive functionality and visual components of the authentic login page.** The phishing page's legitimacy may be improved by adding logos, pictures, and other assets to these files.

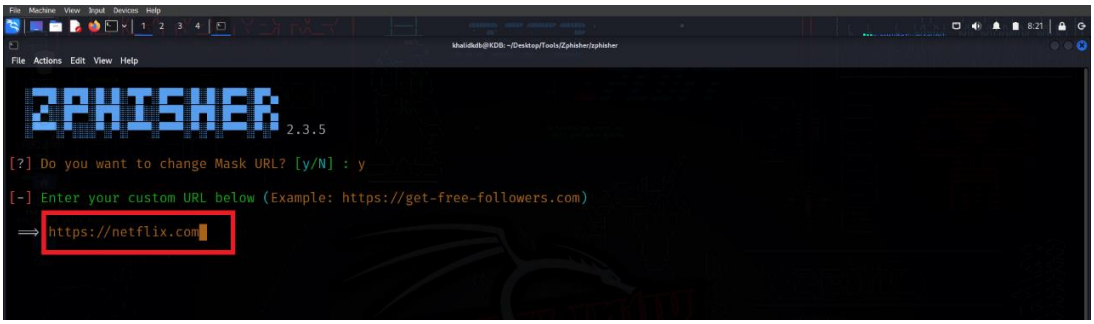
2. Next, bash Zphisher and choose the **Netflix platform** from among other options that appear to be authentic. You will find a lot of options for different platforms.


File Machine View Input Devices Help
1 2 3 4
khalidkdb@KDB: ~/Desktop/Tools/Zphisher/zphisher
File Actions Edit View Help
Version : 2.3.5
[-] Tool Created by htr-tech (tahmid.rayat)
[::] Select An Attack For Your Victim [::]
[01] Facebook [11] Twitch [21] DeviantArt
[02] Instagram [12] Pinterest [22] Badoo
[03] Google [13] Snapchat [23] Origin
[04] Microsoft [14] Linkedin [24] DropBox
[05] Netflix [15] Ebay [25] Yahoo
[06] Paypal [16] Quora [26] Wordpress
[07] Steam [17] Protonmail [27] Yandex
[08] Twitter [18] Spotify [28] StackoverFlow
[09] Playstation [19] Reddit [29] Vk
[10] Tiktok [20] Adobe [30] XBOX
[31] Mediafire [32] Gitlab [33] Github
[34] Discord [35] Roblox
[99] About [00] Exit
[-] Select an option : 05

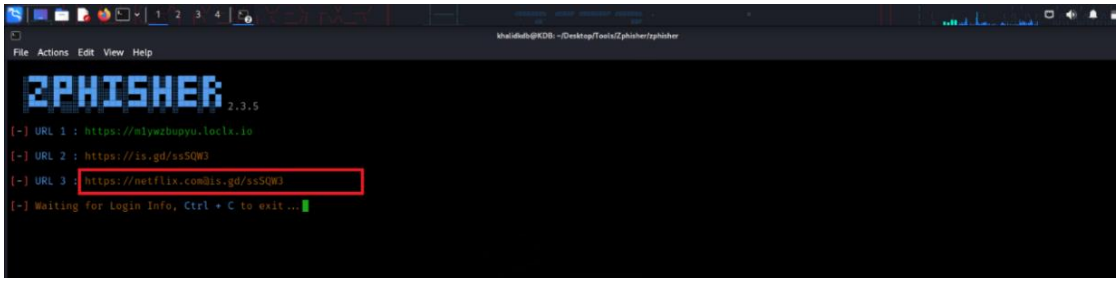
3. Choosing the port to establish a link between the phoney website and the injected link in the following email. Here, a reverse proxy called **LocalXpose** is utilised to allow you to expose your localhost to the internet to build a connection. This application has a lot of features that you may utilise, such changing the LocalXpose server area and connection port modification. However, in this case, accept the default settings for a better outcome.



4. In this part there is the option to let you **mask the link (URL) to be like an authorized**, that lured the victim to click on it.



5. The malicious link has finally been formed in the first phase. and proceed to the second stage of composing the email, inserting the link, and watching for the victim to click on it.

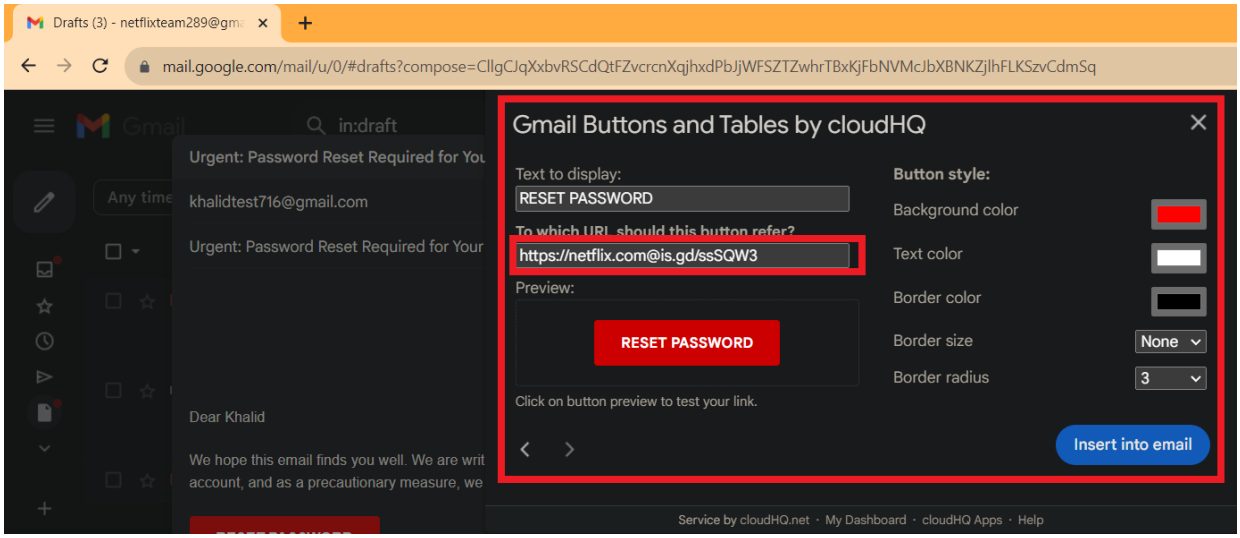


Creating Email

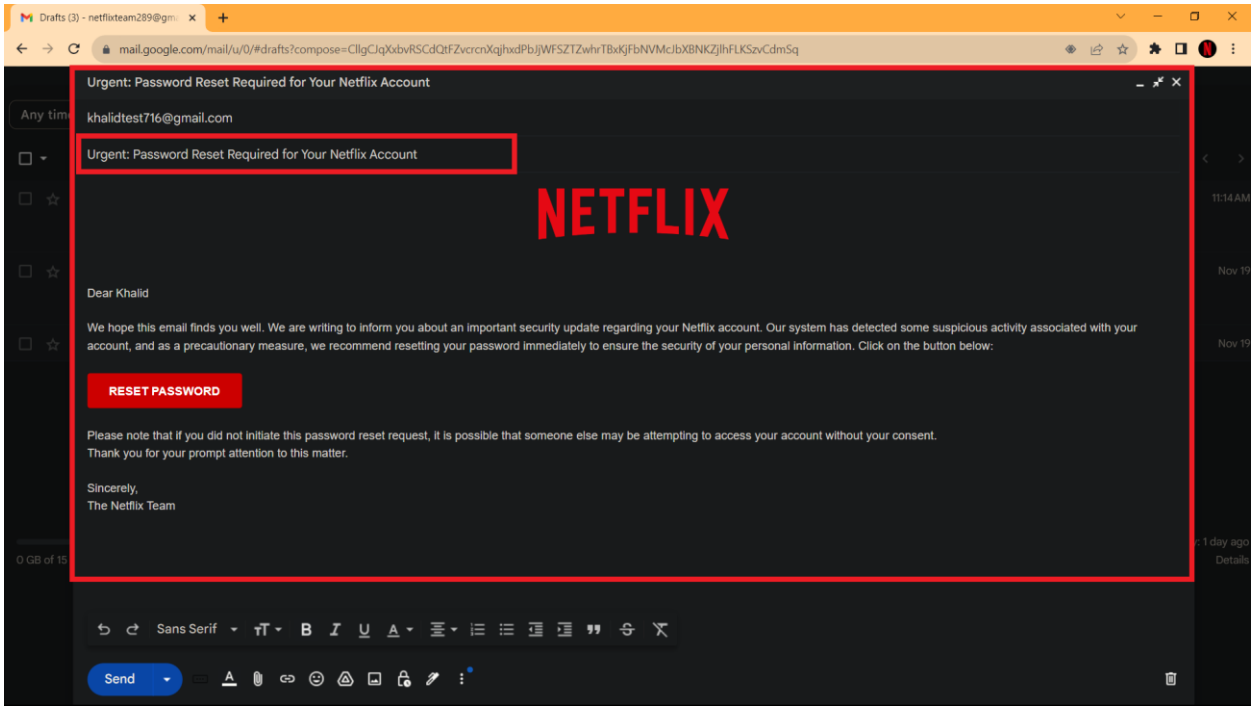
The second phase now is creating the mail to deceive the victim; you should make your domain name appear authentic; the attacker uses techniques such as:

- Establishing a Gmail account, such as the one used for this test, the real one: **info@members.netflix.com**, so the target will be able to trust it. and **netflixteam289@gmail.com**, the fake one. to look like correspondence from Netflix's support team.

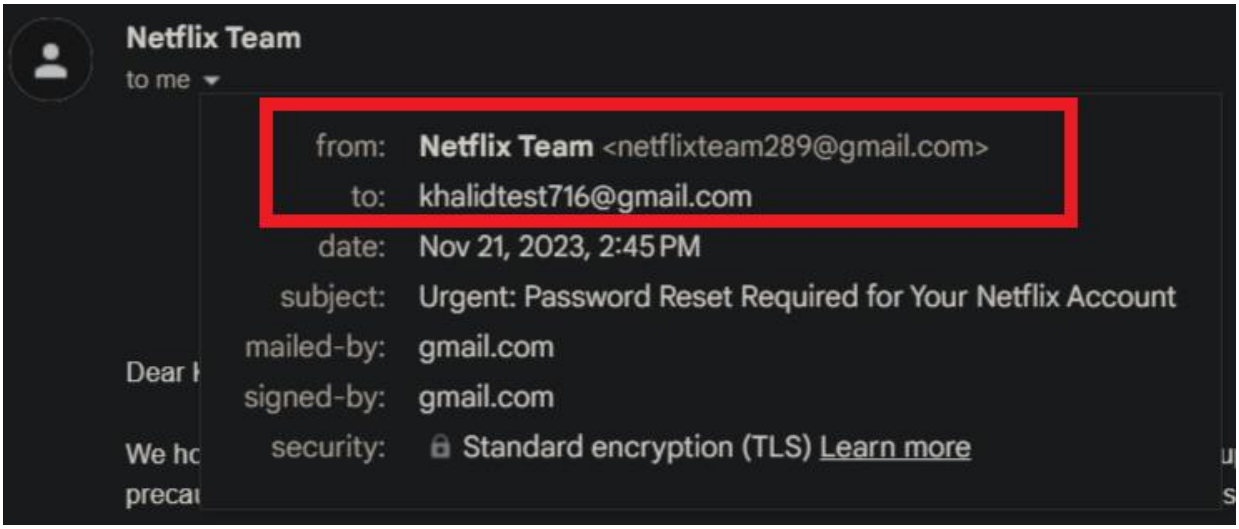
In the image below injected the malicious link in the button called **"RESET PASSWORD"**



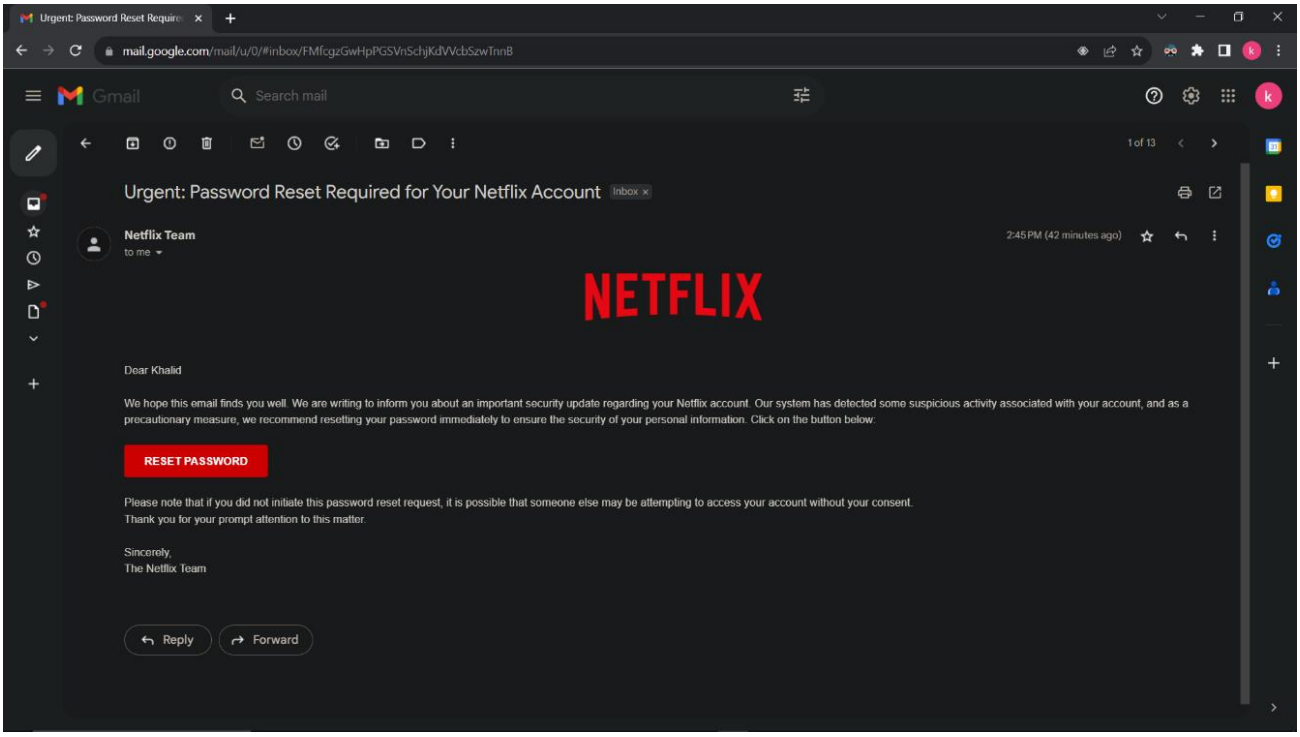
6. Using the phrase "**Urgent: Password Reset Required**" in the subject line to convey a sense of urgency may cause the recipient to experience a psychological reaction that will push him to click the "**RESET PASSWORD**" button. The final component should be conscious of it, creating the email form to resemble one that was sent from the actual Netflix Gmail account, as the example below.



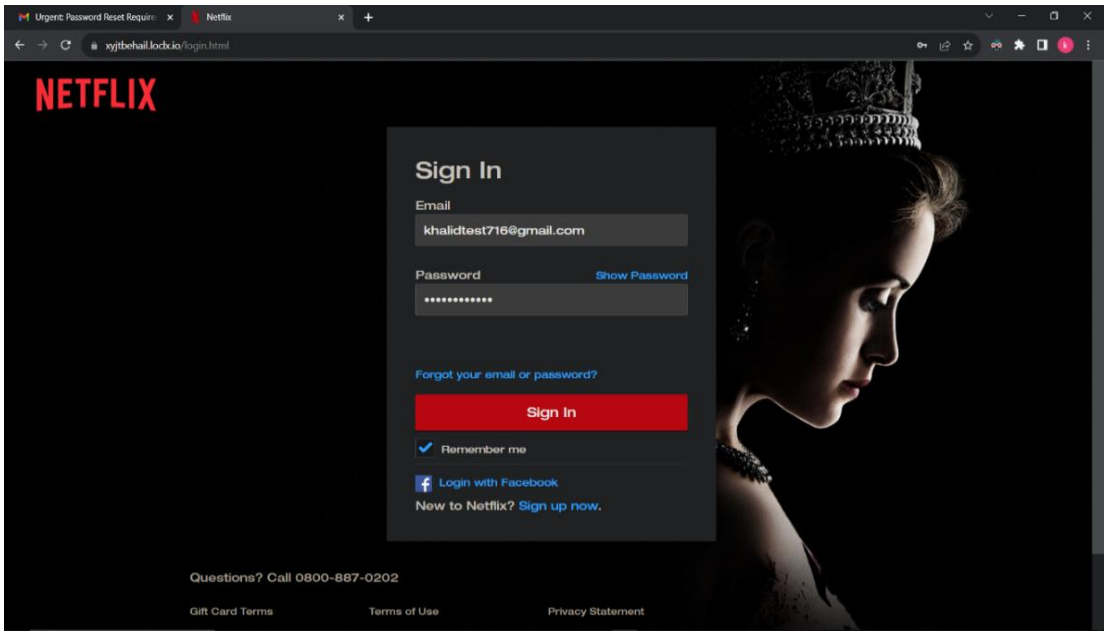
7. The victim will then get the message at **khalidtest716@gmail.com**, which is the email address that will be used.



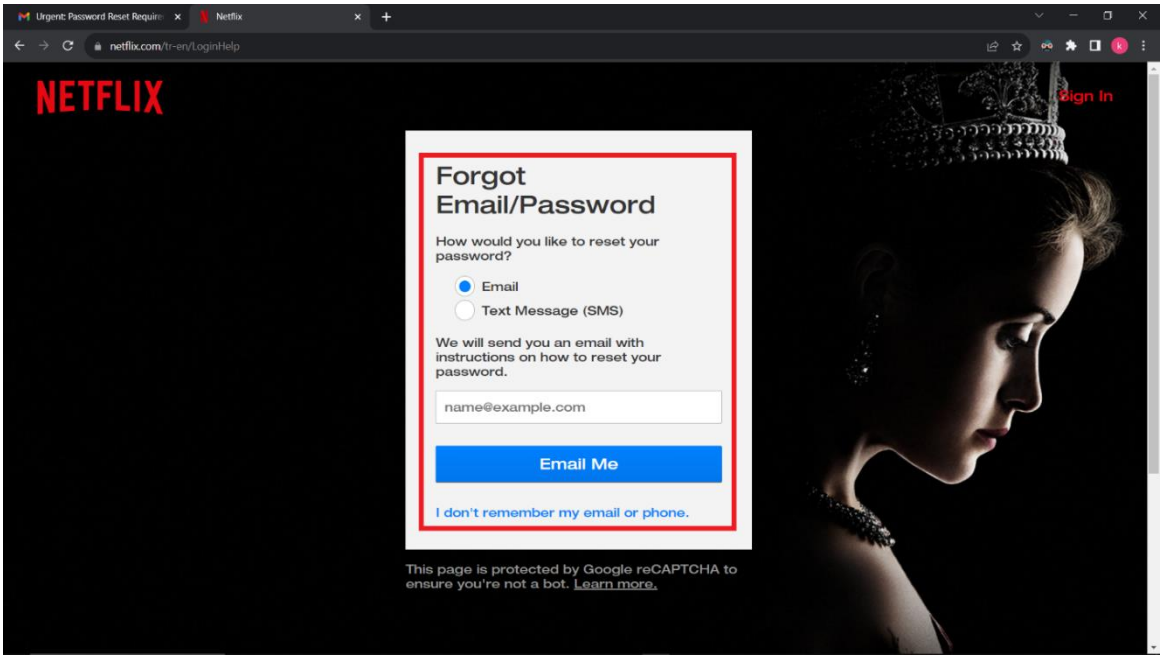
8. Now that the victim has received the phishing email, and this is the version that includes every element of the techniques the scammer may employ to trick the victim into clicking on the link.



9. The user will get a new tab in the browser that looks like the original one after clicking the password reset button. **The victim will then enter his credentials so that the attacker may obtain them**.

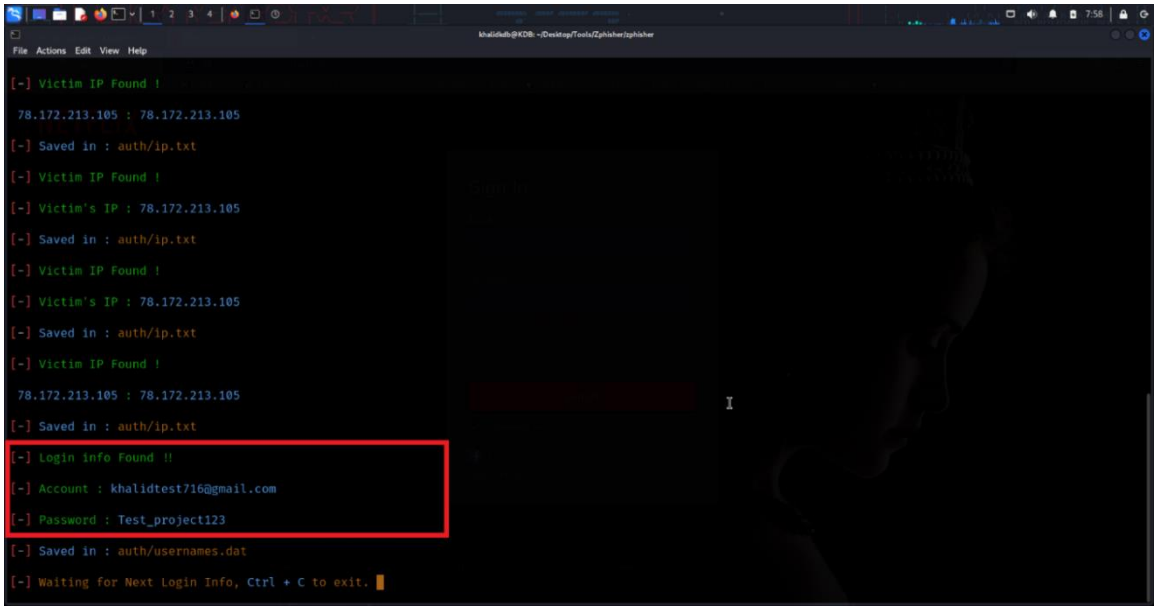


10. The screen that appears after the victim enters their credentials in the email and password areas and clicks "**Sing In**" will indicate that there is a problem with the entry and that they should try again with a valid email address or by sending a text message (SMS) or email to reset their password, as seen in the image below. **However, that's all phoney; even if the user types again, his email will remain blank, and the attacker has already harvested the victim's data**.

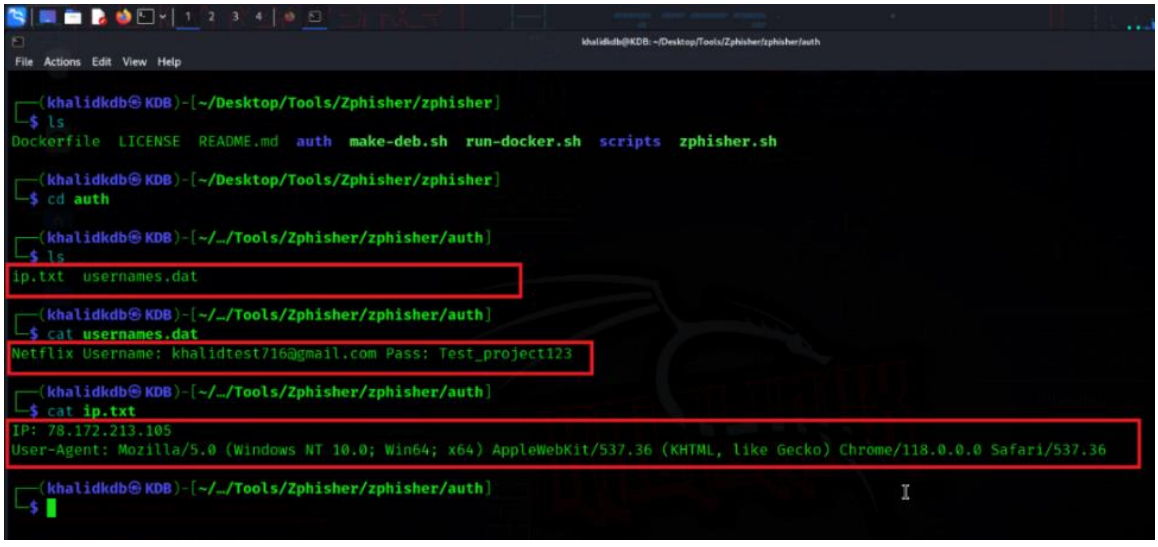


NOTE: This time, the **attacker obtained the user's credentials and displayed additional information** on his screen, as seen in the figure below. A wealth of information about the victim, including their **IP address, account, and password**, could be utilised by the attacker to **access their Netflix account, sell it to a third party**, and do a variety of other things.

11. By the time this scenario ends, the user's account name and password have been made public. Additionally, **this tool allows the attacker to save the victim's login information** (password, account, and IP address) on **file for later use**.



12. As can be seen in the figure below, there is a folder called **auth**. Inside this folder, there are two files with different extensions. The first file, called **ip.txt**, contains the victim's IP address, and the second file, called **usernames.dat**, contains the website name, username, and password.



13. As well as the result, as shown in the instance above. The email phishing operation was successful, and the victim's password (**Test_project123**) could be obtained by the phisher. We'll talk about strategies and tactics in the discussion chapter to guard against, stop, and mitigate the impact of phishing attacks.

Conclusion

In the end, this blog demonstrates how an attacker might think of luring a victim into clicking on malicious links and entering their login credentials in order to be harvested without the user's knowledge, The simulation test in real work using some of the phisher's methods to generate the malicious link that guide to fake website.

The type of phishing attacks has been used in the simulation section is Email phishing one of the five common phishing assault, have been target the victim by chose one of the most famous platform website Netflix to creating a phishing email looking like coming from trustworthy sender.