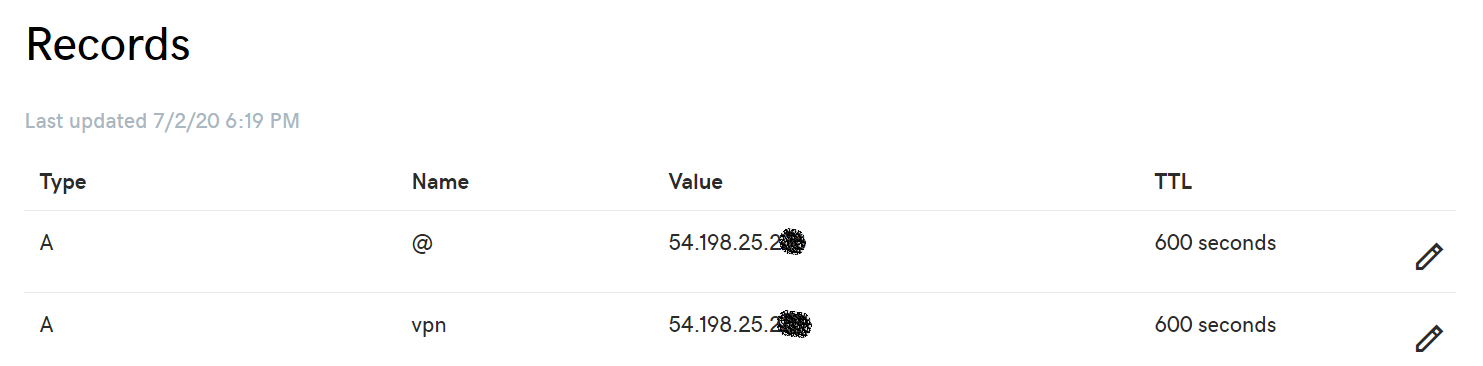
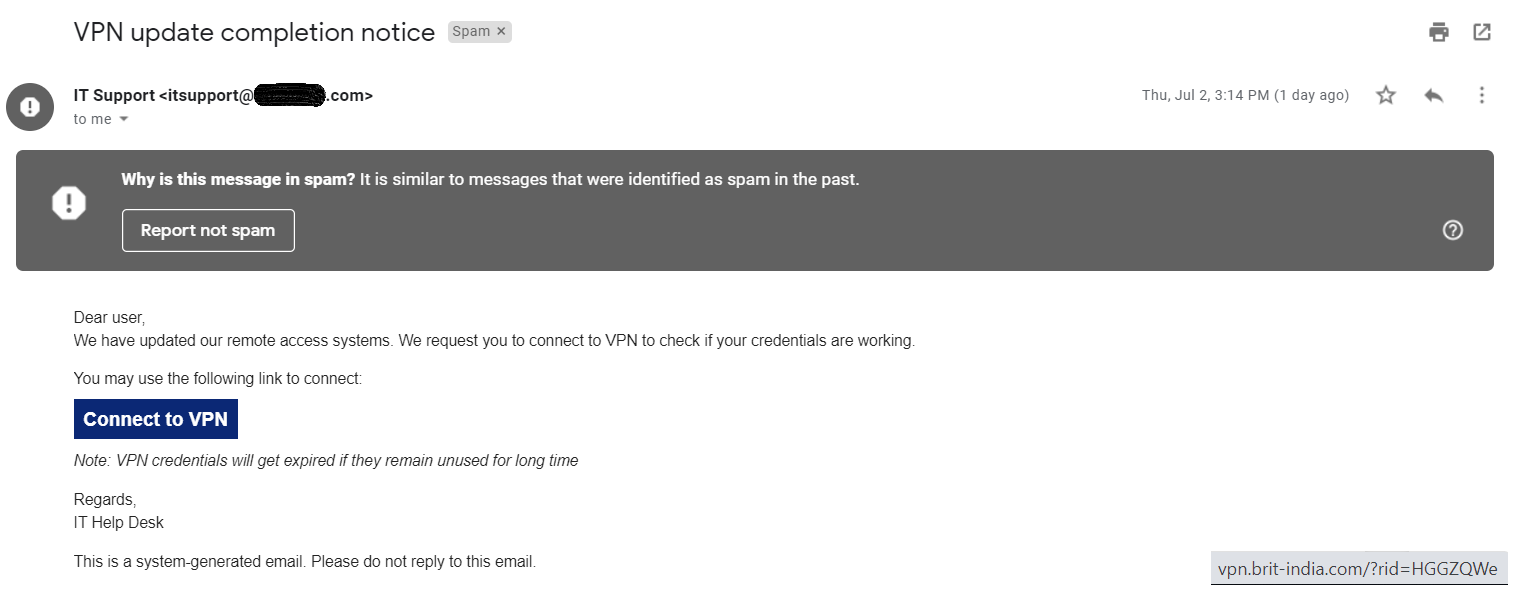
**Failures that led to success…**

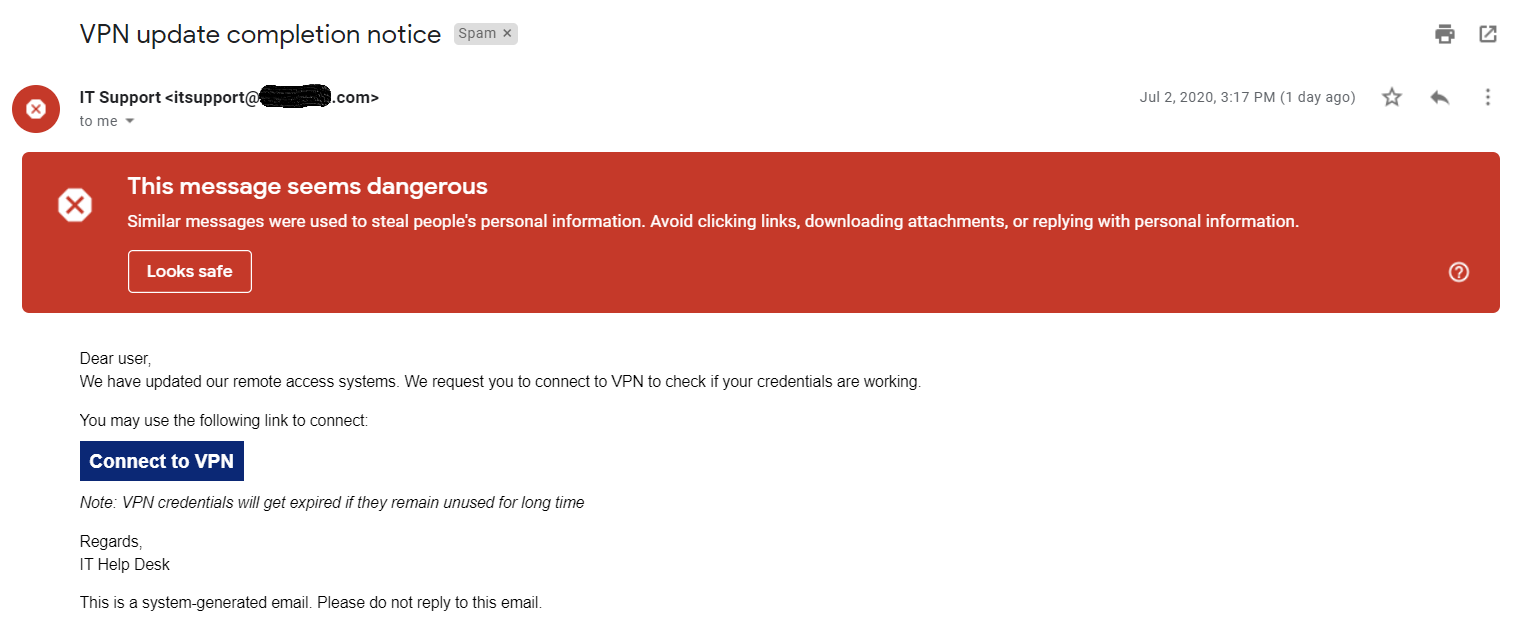
1. Bought domain client-sso.com
2. Bought G-Suite for client-sso.com (free for 14 days). Admin username is [itsupport@clientsso.com](mailto:itsupport@clientsso.com)
3. Set DNS (A record) for client-sso.com and vpn.client-sso.com to GoPhish server IP.



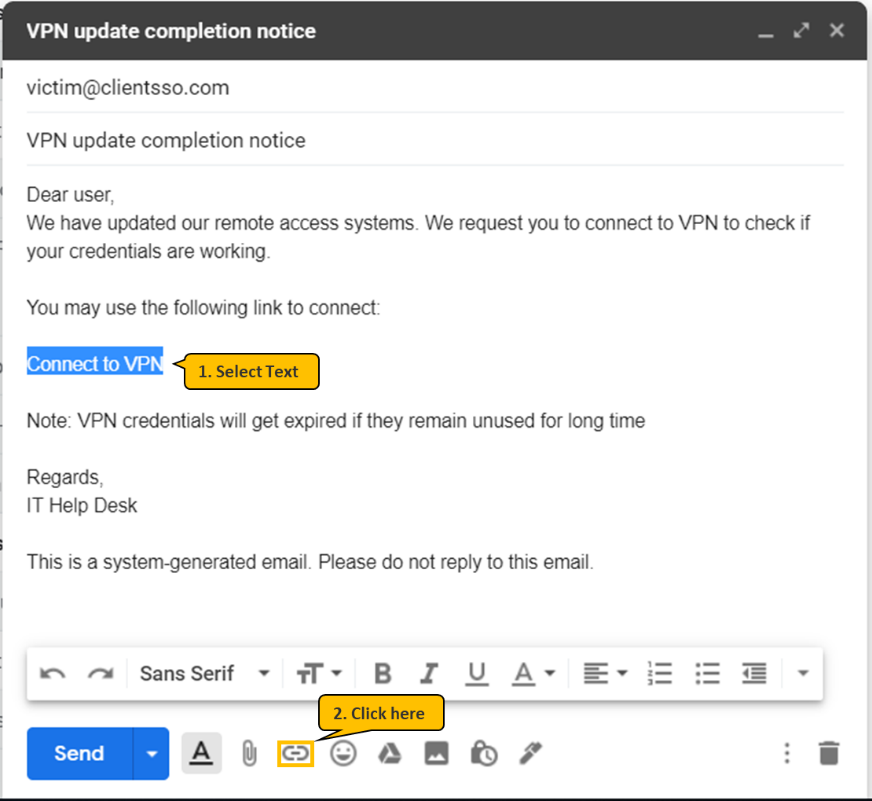
1. Used GoPhish to send mail with Gmail SMTP server.
2. The email template I tried to create with a button (“Connect to VPN”) for the landing page link and sending. It worked for first few tries.
3. Later on it didn’t work.

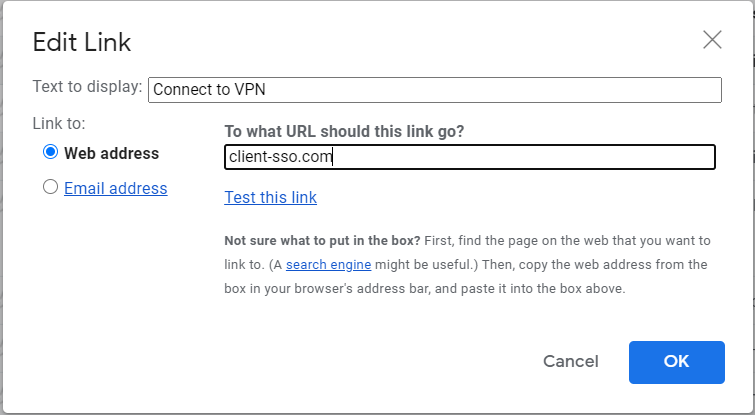


1. I tried changing the landing page link to real websites like google.com, facebook.com, vpn.clientsso.com. It worked (1 time this also didn’t).
2. I tried bit.ly to shorten the vpn.client-sso.com/rid=GoPhishID to bypass the filter. Gmail marked it as dangerous!



1. I finally put the link as it is (along with the plaintext for the mail) and sent it. It worked without any problem!
2. I later realized that Gmail has option to create links while composing mails. So I tried that option while manually sending the mails using [itsupport@client-sso.com’s](mailto:itsupport@client-sso.com's) gmail. (Press compose. Press create link on bottom. Enter name to be displayed (eg. Connect to VPN). Enter the link (vpn.client-sso.com)). It worked well.



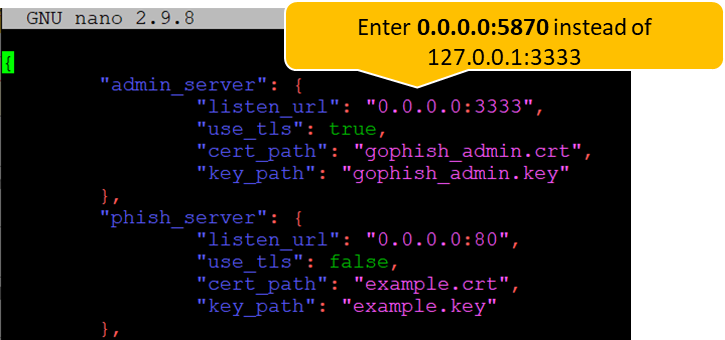


1. I was sending individual mails from GoPhish to itsupport to generate the tracking URLs and then sending manually from itsupport’s mail ID to targets using link creation as mentioned in step 10. This worked well. Tracking image also was used, which didn’t cause any issue. (I had done directly from GoPhish to targets first couple of times **using button**, which worked fine in the beginning but later went to spam).
2. Finally I tried directly from GoPhish to send the mail to the targets (In email template I used <p><a href=”{{.URL}}”>Connect to VPN</a></p> as in steps 10 and 11). This also worked well and it went to inbox.

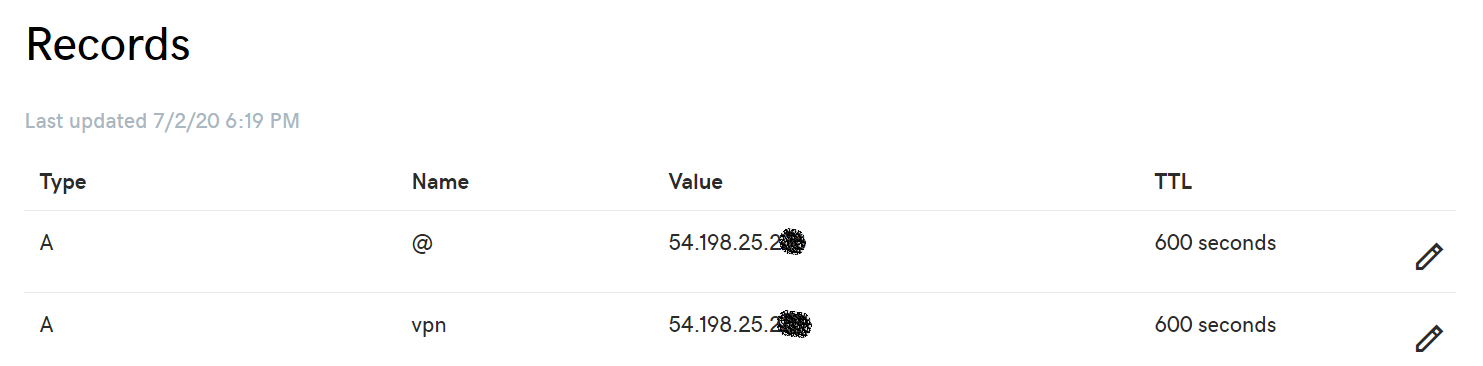
**G-Phish Configuration**

**GoDaddy and G-Suite**

1. Buy domain client-sso.com
2. Buy G-Suite for client-sso.com (free for 14 days). Admin username is [itsupport@clientsso.com](mailto:itsupport@clientsso.com)
3. Instantiate EC2 server in AWS
4. Make appropriate firewall inbound rules (admin port – random port (say, 5870), better not to put 3333, port 80, port 22)
5. SSH to server
6. Install GoPhish in server
7. Configure config.json:
   1. Change 127.0.0.1 to 0.0.0.0 in admin server side
   2. Change port 3333 to any other random port (say, 5870) in admin server side (to prevent compromise)



1. Set DNS (A record) for client-sso.com and vpn.client-sso.com to GoPhish server IP.



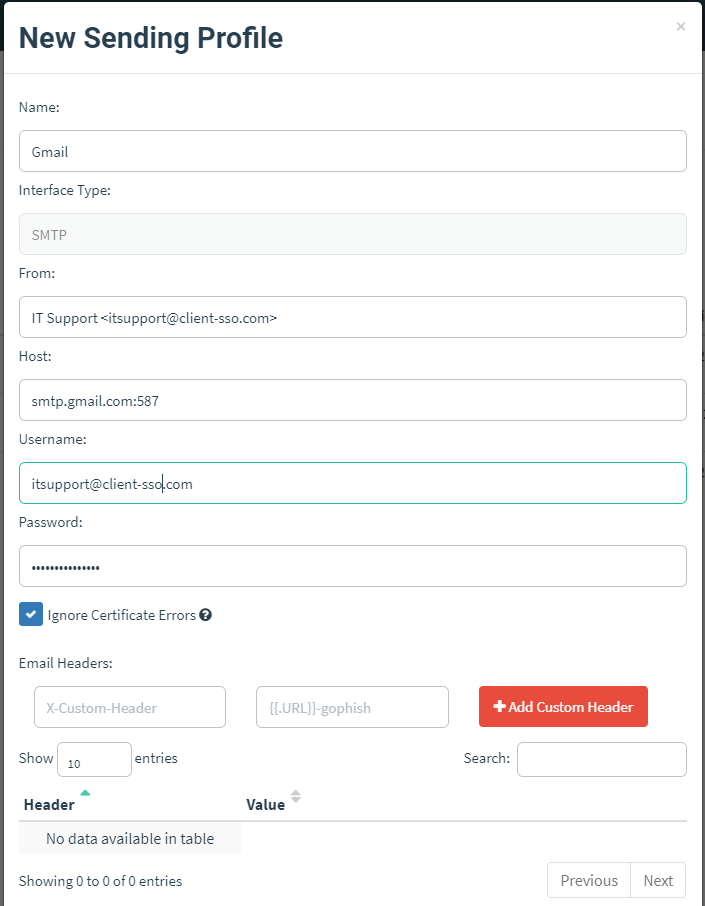
**GoPhish**

Log in with GoPhish’s default credentials (admin:gophish). It is better to change password and admin port.

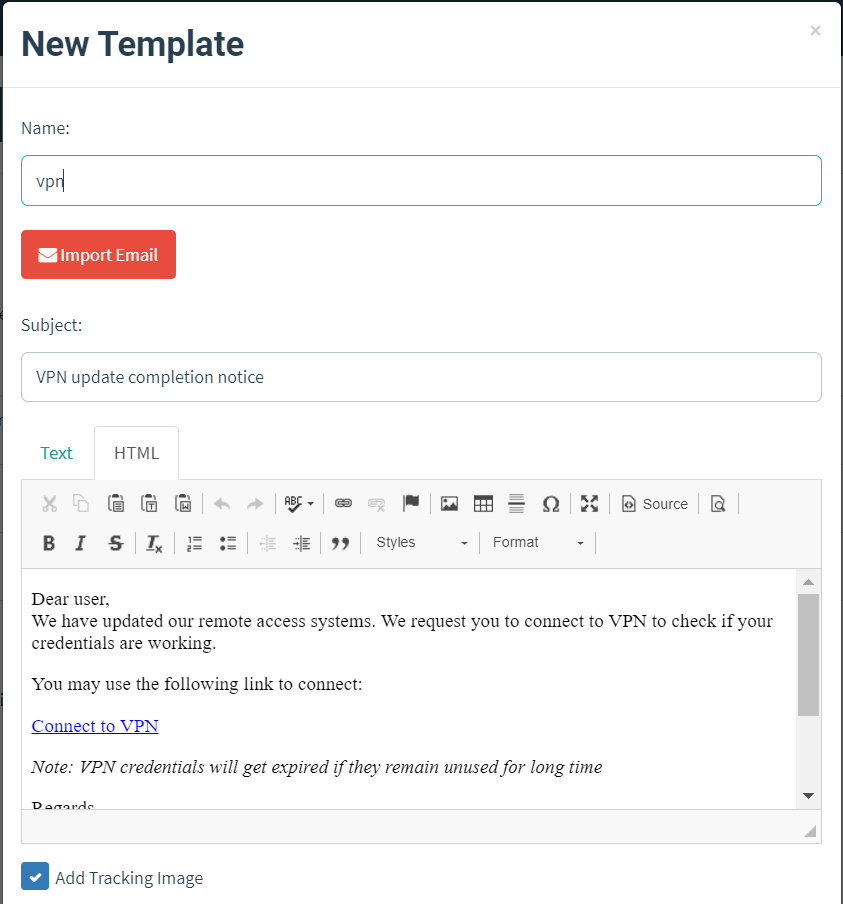
1. Password can be changed in web console.
2. Admin port can be changed in config.json file in server.

The following configurations can be made to set up GoPhish to send Phishing mails:

**Sending profile**



**Email Template**



Subject: VPN update completion notice

HTML Source:

<html>

<head>

<title></title>

</head>

<body>

<p>Dear user,<br />

We have updated our remote access systems. We request you to connect to VPN to check if your credentials are working.</p>

<p>You may use the following link to connect:</p>

<p><a href="{{.URL}}">Connect to VPN </a></p>

<p><i>Note: VPN credentials will get expired if they remain unused for long time</i></p>

<p>Regards,<br />

IT Help Desk</p>

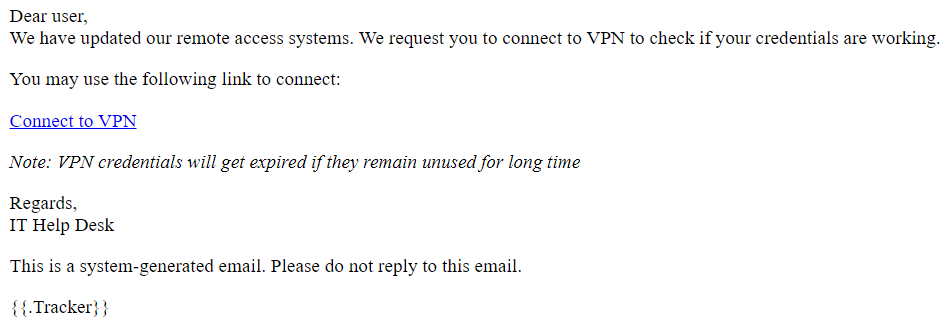
<p>This is a system-generated email. Please do not reply to this email.</p>

<p>{{.Tracker}}</p>

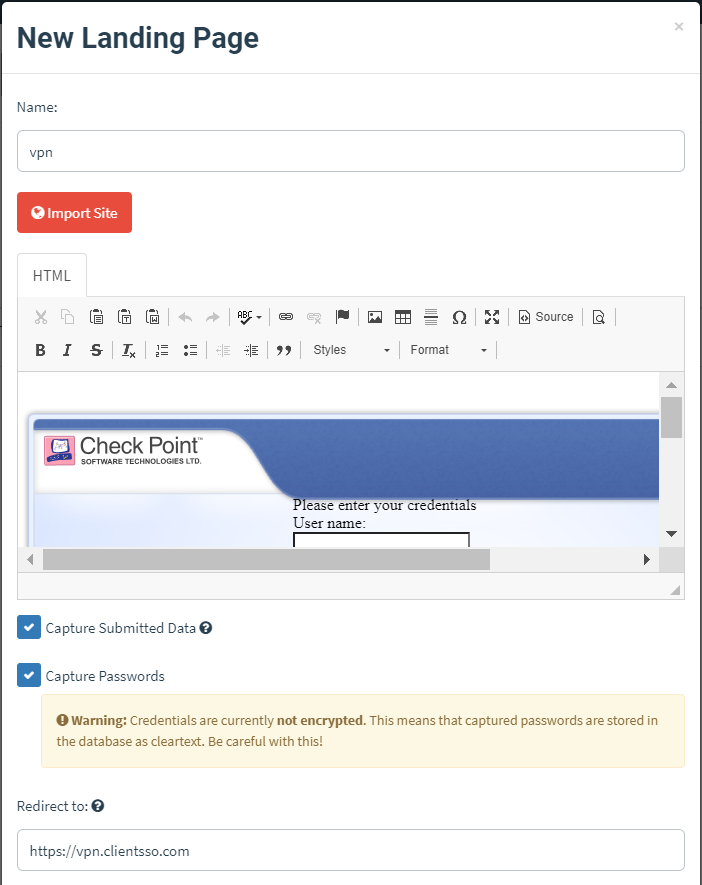
</body>

</html>

HTML Render



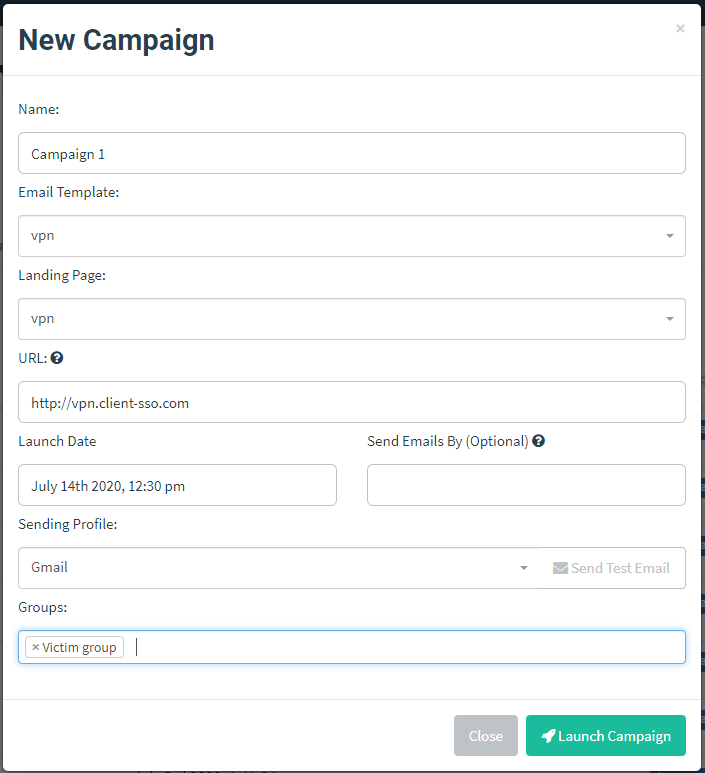
**Landing Page**



Copy from company’s SSO. If images don’t load (because of certificate issue or directory not accessible), you can:

1. Download the images (from SSO page or elsewhere),
2. Put it into a server (same server maybe?) in /var/www/html (eg. /var/www/html/vpn/CompanyLogo.png).
3. Use this link instead of the one used by the SSO. (http://<Server\_IP>/vpn/CompanyLogo.png)

**New Campaign Configuration**



Here, you can put URL as vpn.client-sso.com if you’re using a subdomain. Make sure that vpn.client-sso.com has A record to GoPhish IP in your Domain DNS (eg. GoDaddy)

**Precautions**

1. Try not to test the setup in EY laptop. My domain was marked in opendns as phishing after 1st few tries. (DNS resolution to client-sso.com resolves to opendns IP). Later on it was removed.
2. Try not to use bit.ly and also hi-fi stuff like buttons and images to hide the landing page links. Gmail might mark it as spam. (Note: Gmail will not mark a new clean mail as spam if it had marked a previous suspicious mail as spam, which is good for us! This allows us to test multiple mails, even if some got spammed)
3. Try not to get blacklisted. You could lose your domain (You can check domain health in mxtoolbox)
4. Gmail mainly doesn’t like hiding links. Even if you put google.com in the landing page, it may happen that Gmail spams it if it is covered in a button.