PhishMyTeam

User Guide

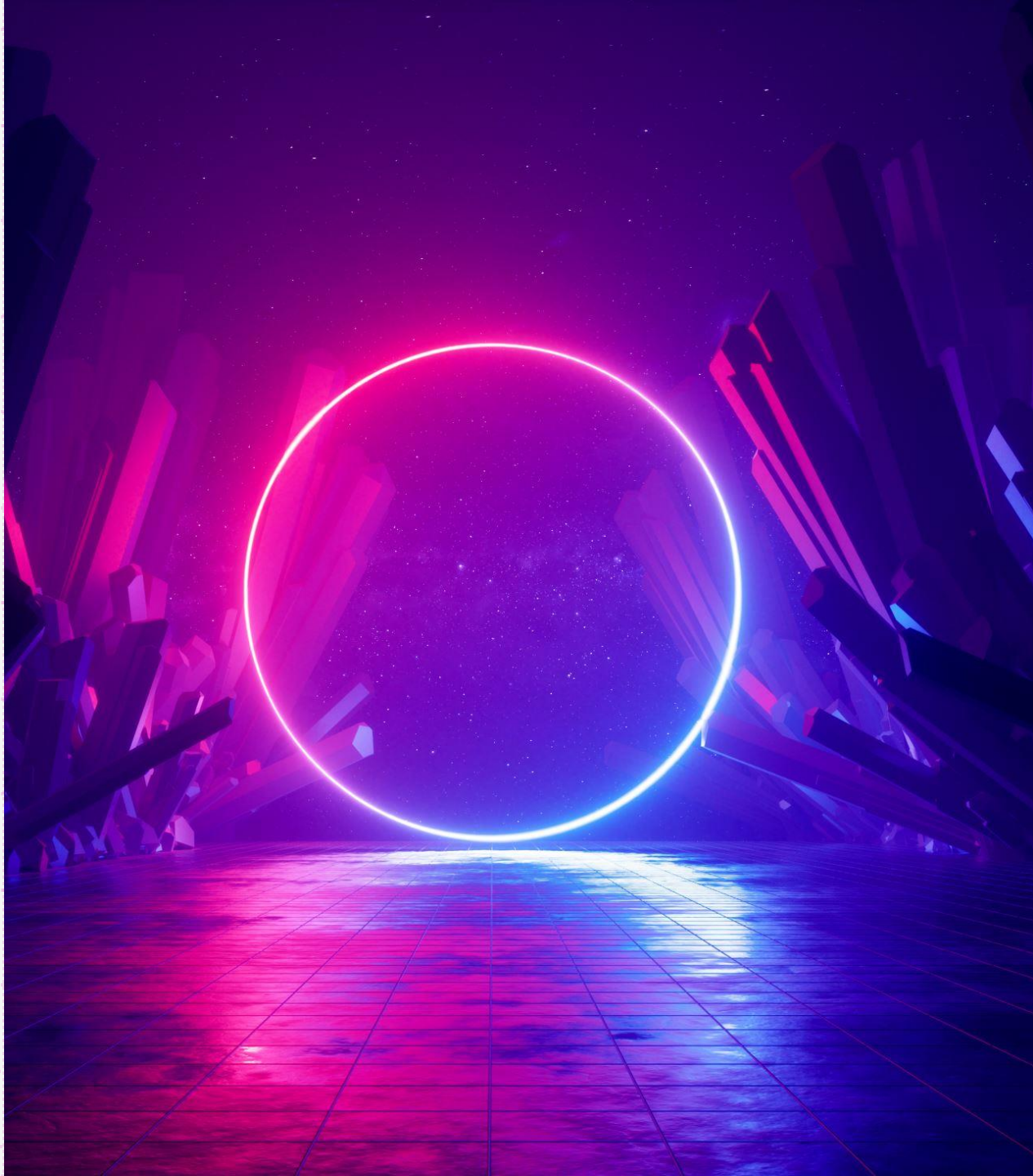


Table of Contents:

Overview:

- Phishing awareness is critical because it empowers employees to be the first line of defense against cyberattacks. Phishing emails are designed to trick users into clicking malicious links or surrendering sensitive information. By educating employees on how to recognize phishing attempts, you can significantly reduce the risk of falling victim to these ever-evolving scam.

- Phishmyteam is a phishing simulation solution that’s uses latest attack trends and templates leading to data harvesting and establishment of C2 Connection with the victim. You can use it to identify organization hotspot to such attack and getting insights into how can an attacker exfiltrate the organization assets.

- Identify who are all alert when it comes to identify the phishing email and its also easy to do the phishing campaign in bulk within few seconds.

Account Creation:

- 1- Signup:
  - User must first create an account with fields such as :
    - Email address
    - Username
    - Password
    - Confirm Password
    - Contact Number
- Note : Once successful creation account, you will receive an qrcode on your email which you need to scanned with Microsoft authenticator for otp verification during login process.
- 2- Login:
- Entered your username, password and authenticator code to access the phishmyteam application and moved to further instruction.

User Settings:

- Once logged, moved to settings tab and scroll over to Gmail and Outlook settings window, after that enter the email address and credentials for the email client which you are going to use.

- You can enter the email address and credential for both gmail and outlook and based upon your needs you can specify which one to use on sending profiles windows host option (Gmail or outlook)

- You can also view other information on the settings window such as username, validity, status of two factor (enabled, disabled), api and email address.

Getting Started: Email Templates

Once you have done the user settings, it's time to start designing the phishing campaign, but before proceeding any further you have to decide an important thing i.e what is the goal of this campaign , let me help you out what I mean by that.

1- If you just wanted to send a normal email with a phishing link in it, then your option:

a) Email Templates window– click on **WITH TEXT** button

2- If you wanted the fool the victim and harvest their credential for website, then your option would be :

a) Email Templates window- click on **WITH TEMPLATES** button

3- If you wanted the victim download some attachment, then your option would be:

a) Email Templates window- click on **WITH TEXT & ATTACHMENT** button

Now go to email templates window and based upon your goal click on appropriate button and design your email template which will be send to victim.

Note : **With Templates** button, Email Source inbox accept HTML Codes only.

Getting Started: User And Group

Next comes **user and group** window, where you specify the victim information which will be used later on to send the phishing campaign to victim falling to specific group, currently there are only 6 group i.e :

Product and Service Department

Finance and Accounting Department

Information Technology Department

Sales and Marketing Department

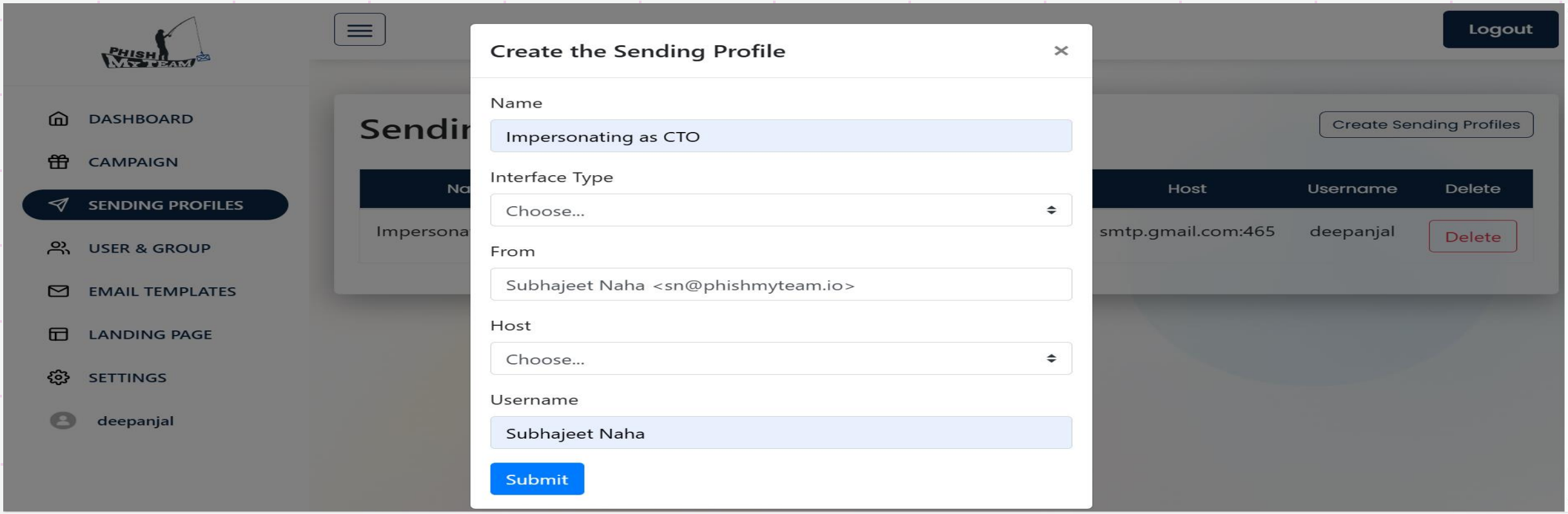
Administrative Department

Human resource Department

Note : Victim should fall under any one group when you define the victim details.

Getting Started: Sending Profiles

Next comes **sending profiles** window, where you specify the sender information which will be used to send emails to victim. Note if you are using Gmail as an email client you can spoof the email address of the sender by defining your desired Named in the From input box.



Start Campaign

Now we will start the campaign, when you visited the **Campaign** window, first select the tab for which email client you want to use whether its Gmail or Outlook.

Once you have selected all the options the last option will be enabled tracker, i.e if you select this option as yes, you will be able to track when a particular victim has opened your phishing email with other relevant information such as user agent, ip address, time.

When you will hit the submit button, phishmyteam will start sending the phishing campaign to the target group and for any reason if it fails to send an email to particular victim, it will give detail information for that victim.

Dashboard view

Once you have sent your first phishing campaign you can look at the statistics for all campaign i.e:

1- Total number of sending profiles.

2- Total number of user and group

3- Total number of email templates

4- Email statistics:

Total created, sent, received, opened and others.

5- All campaign views

Campaign Details:

When you clicked on details button on **dashboard** window, you will receive detailed information for that particular campaign.

1- Campaign information's
2- Victim who opened the email information's
3- Victim who didn't receive the email information's
4- Victim who clicked on the phishing link information's
5- Data harvested from phishing websites

Notification and Alert:

As soon as the victim clicked on the phishing link , the user will be notified that victim has fallen for phishing campaign on his email address.

This is how notification email will look like:

Hi there user deepanjal@phishmyteam.com got phished for campaign ID:e5791718-7b9a-43a2-965e-e0a831eb64ba
Details :
Campaign ID : e5791718-7b9a-43a2-965e-e0a831eb64ba
User : deepanjal
Email : deepanjal@phishmyteam.com
Position :Product Head
Department :productandservicedepartment

Please sent them for training

Training and Assessment:

Once the phishing campaign is over the victim will be sent training module as to how identify and stay protected against modern day phishing attacks.

For personalized phishing training you can contact us at support@protecte.io or visit us at www.phishmyteam.com