Setting Up Phishing Simulation with Gophish

The process of launching the phishing campaign is broken into 7 steps for the ease of understanding. Below are the steps,  
  
**Step 1: Setting up the server to host Gophish  
Step 2: Install and configure Gophish on the EC2 instance  
Step 3: Registering attacker domain name**

**Step 4: Hosting the phishing website & Configure SSL for the domain**

**Step 5: Test run of the phishing mail & Bypass google spam filter**

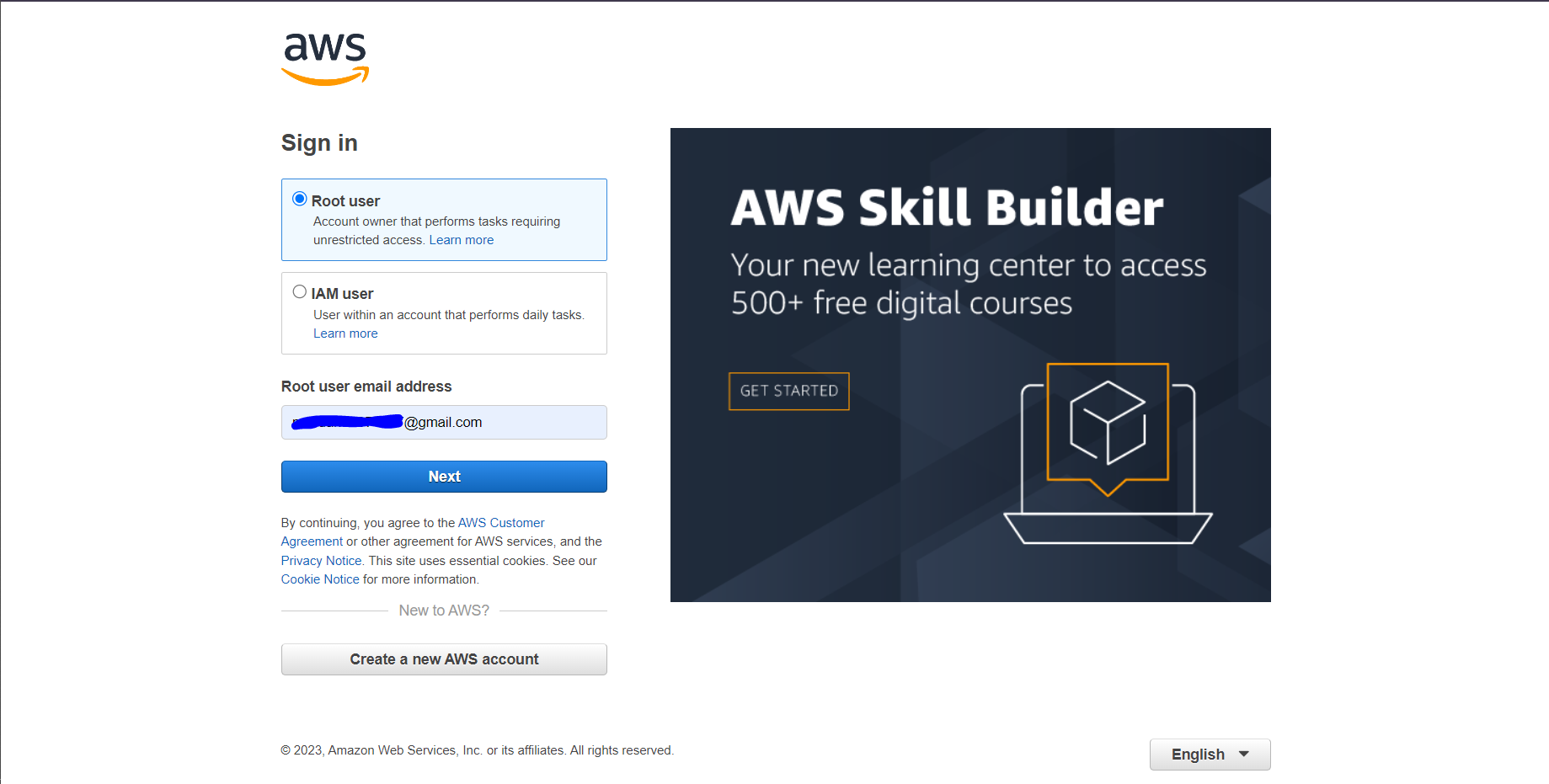
**Step 6: Configure the details of phishing campaign & Launch**

**Step 7: Collect results (Victim Data)**

Each of these steps are explained in detail below with diagrams.

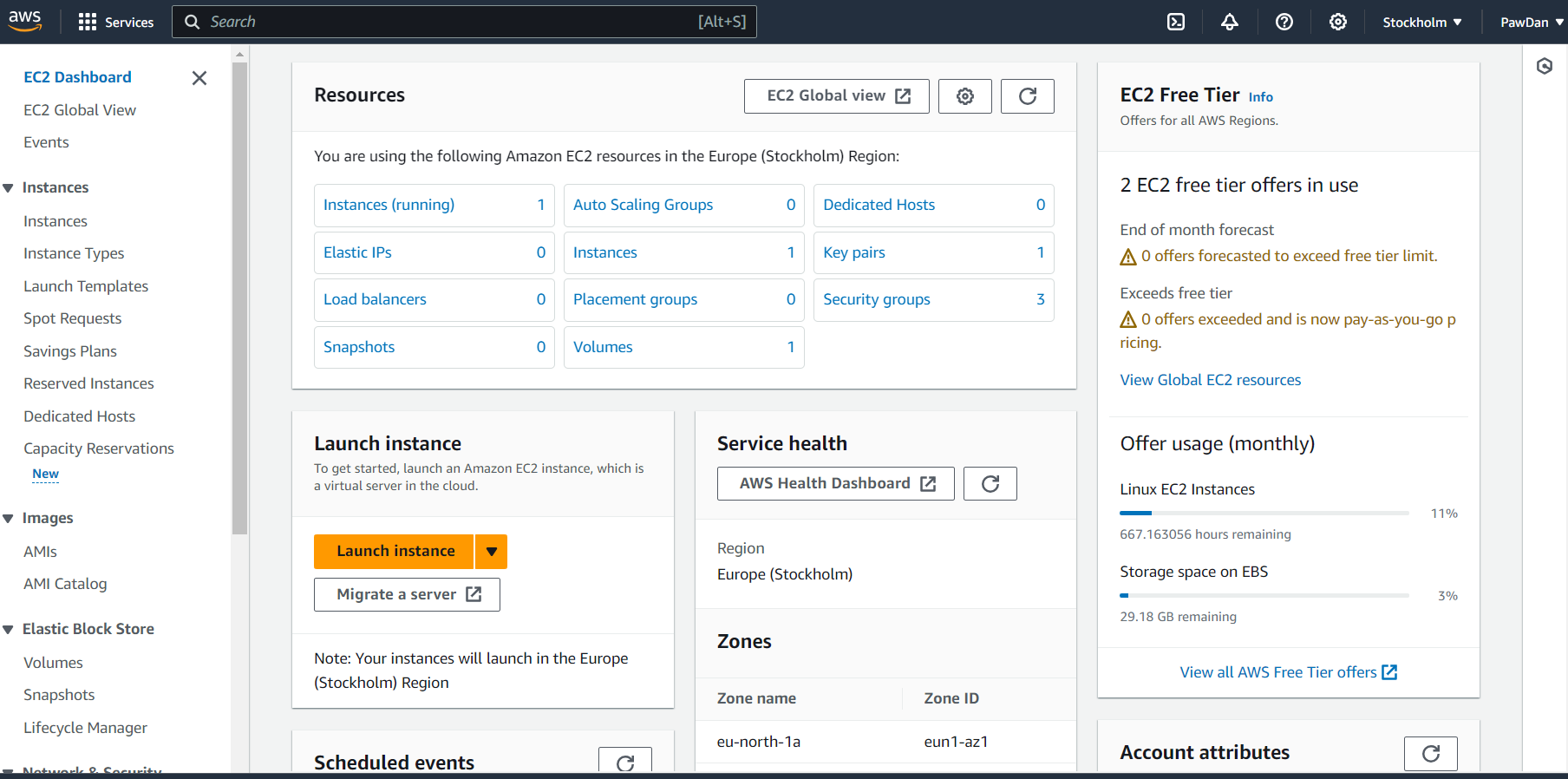
## Step 1: Setting up the server to host Gophish

**Setting up Amazon EC2 :** First, Login into AWS Console.

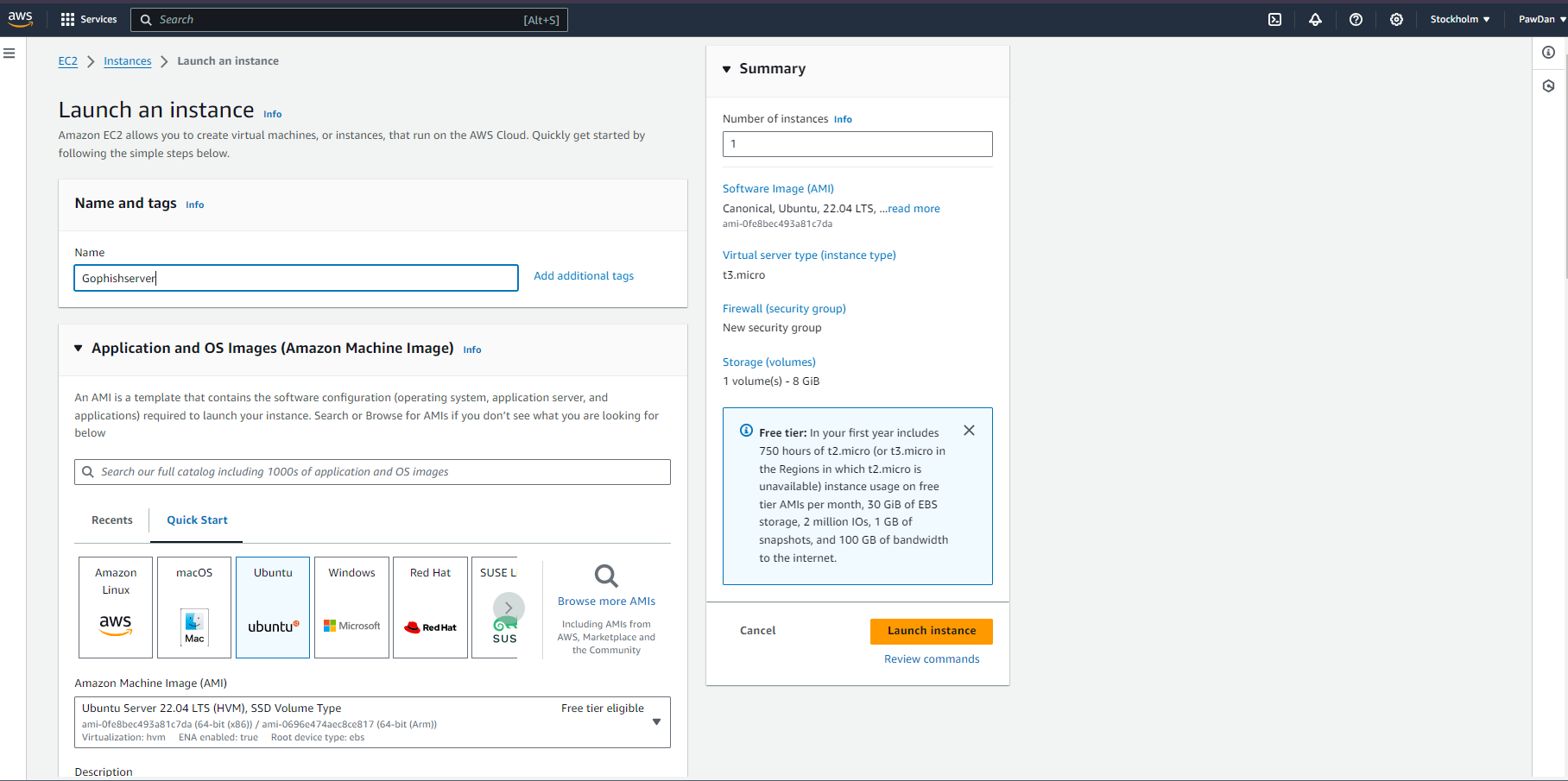


In the AWS Management Console, find the "Services" dropdown and select "EC2" under the "Compute" section.

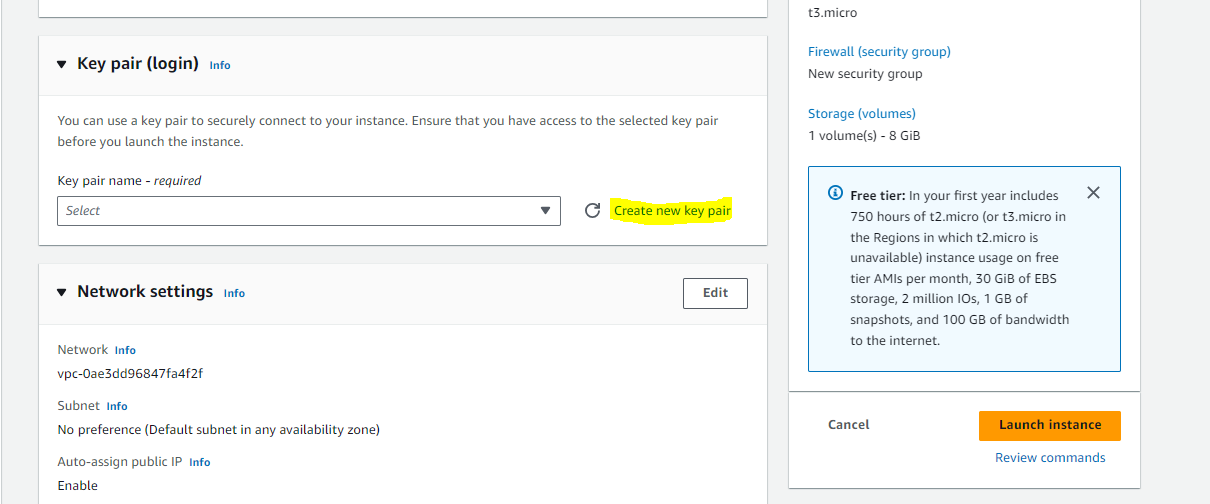
**Launch Instance:** In the EC2 dashboard, click the "Launch Instance" button.

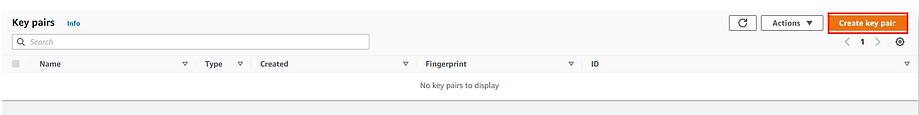


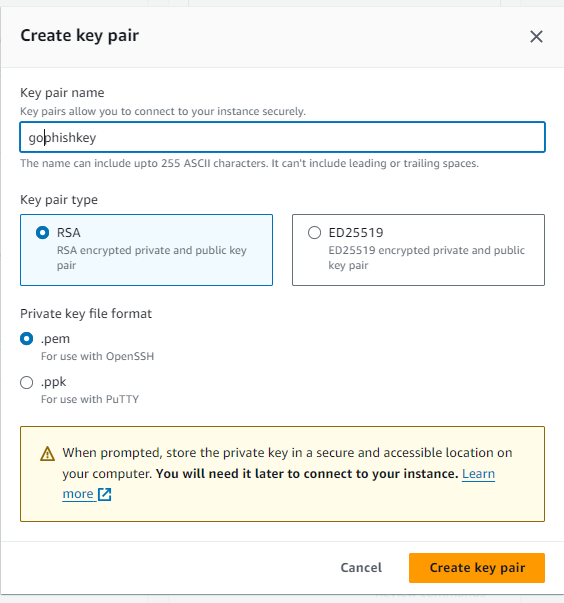
**Select Linux Server (Ubuntu) and continue as shown below.**



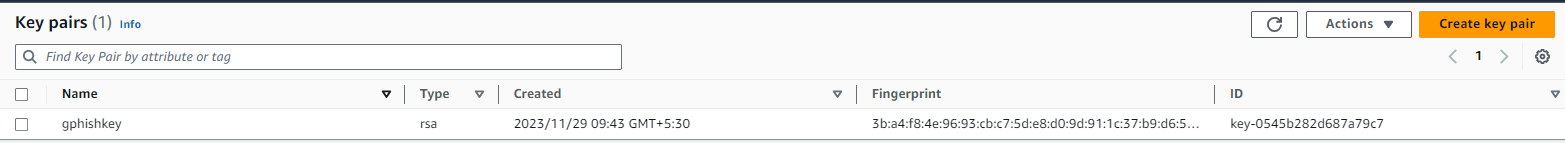
**Create a new key pair:** AWS uses public-key cryptography to secure the login information for EC2 instances. Since the Linux instance has no password; a key pair is used to log in to the instance securely. Users specify the name of the key pair when you launch your instance, then provide the private key when you log in using SSH.



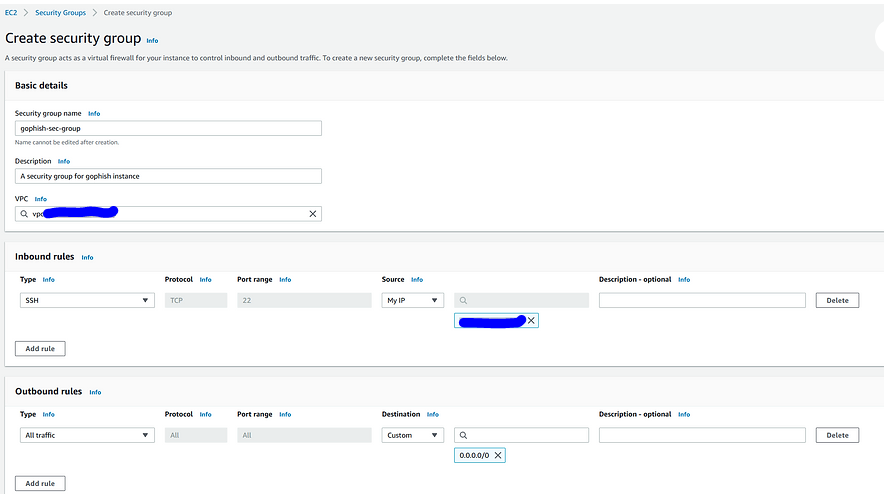




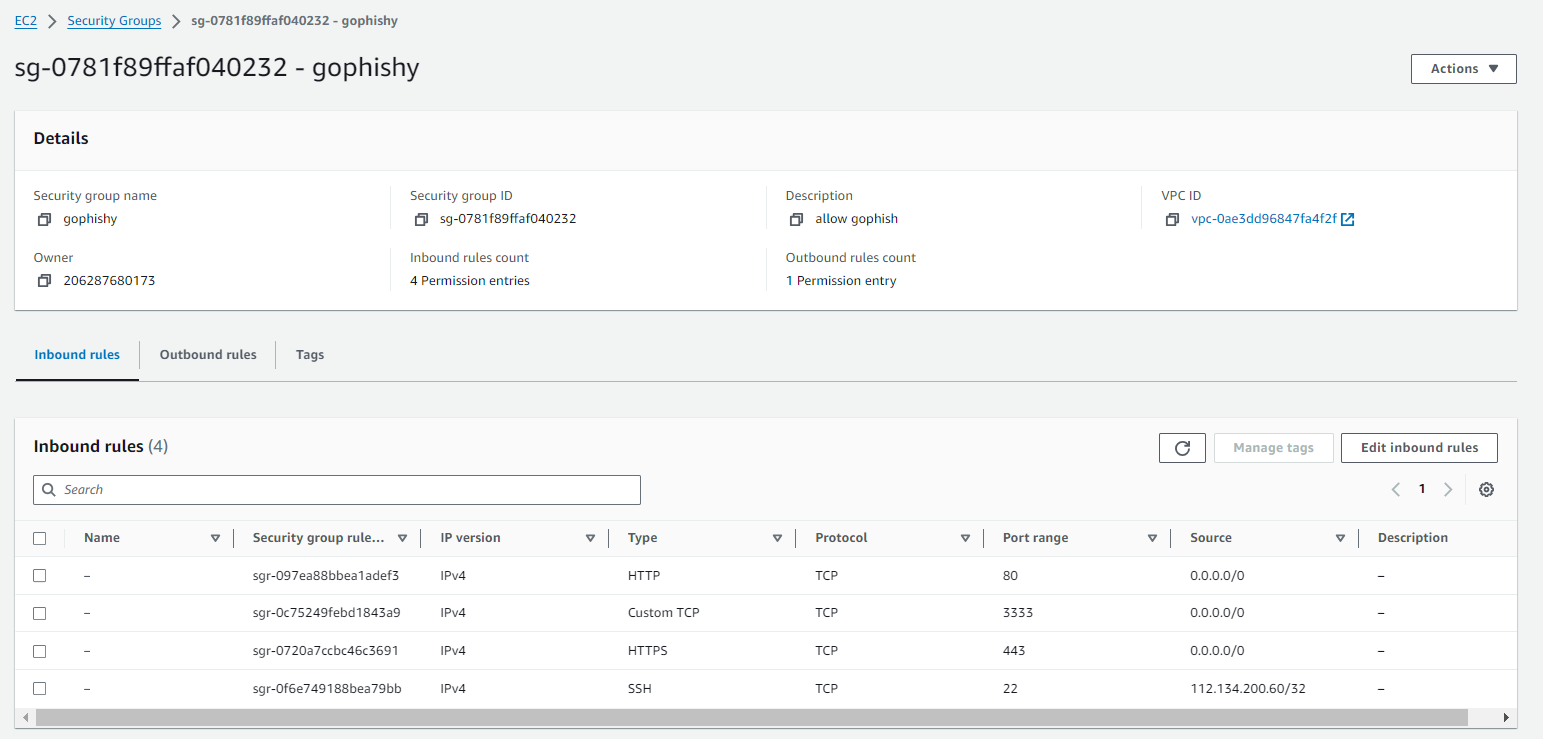
.pem file is used when connecting with the instance through OpenSSH.

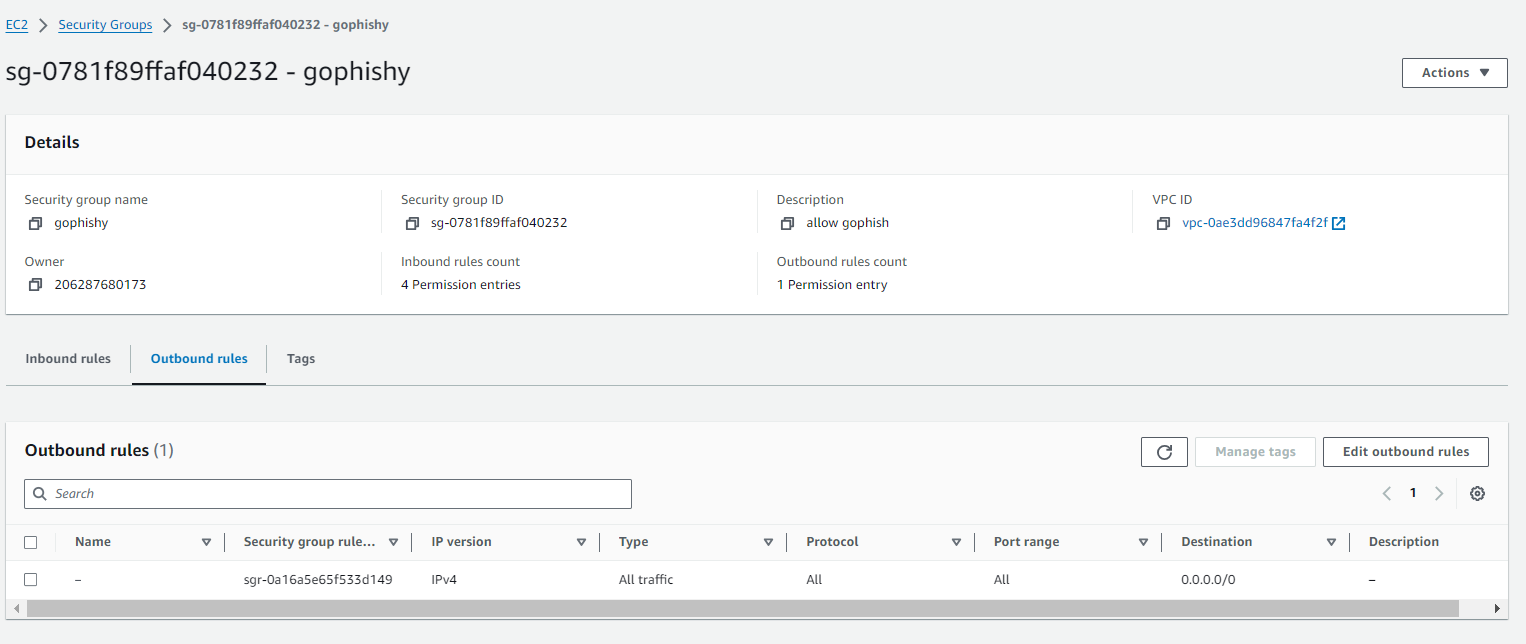


**Create Security group:** Security groups act as a firewall for EC2 instances, controlling both inbound and outbound traffic. The rules to a security group enable users to connect to their instance from their IP address using SSH. Also rules that allow inbound and outbound HTTP and HTTPS access from anywhere are added for Gophish to run properly.

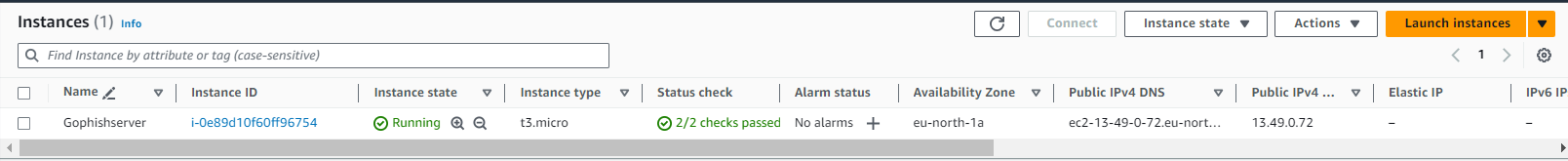


**Configure the security group:** Also rules that allow inbound and outbound HTTP and HTTPS access from anywhere as shown below are added for Gophish to run properly.

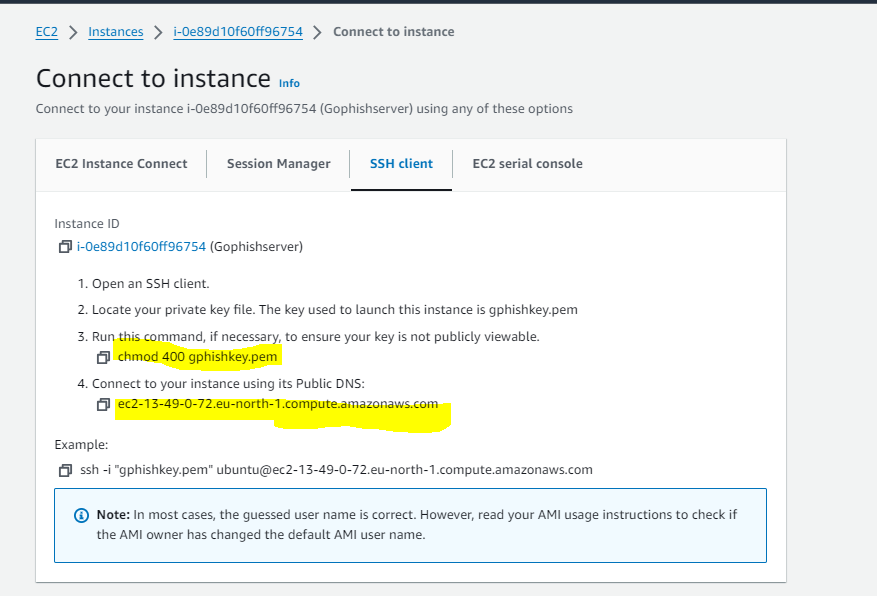


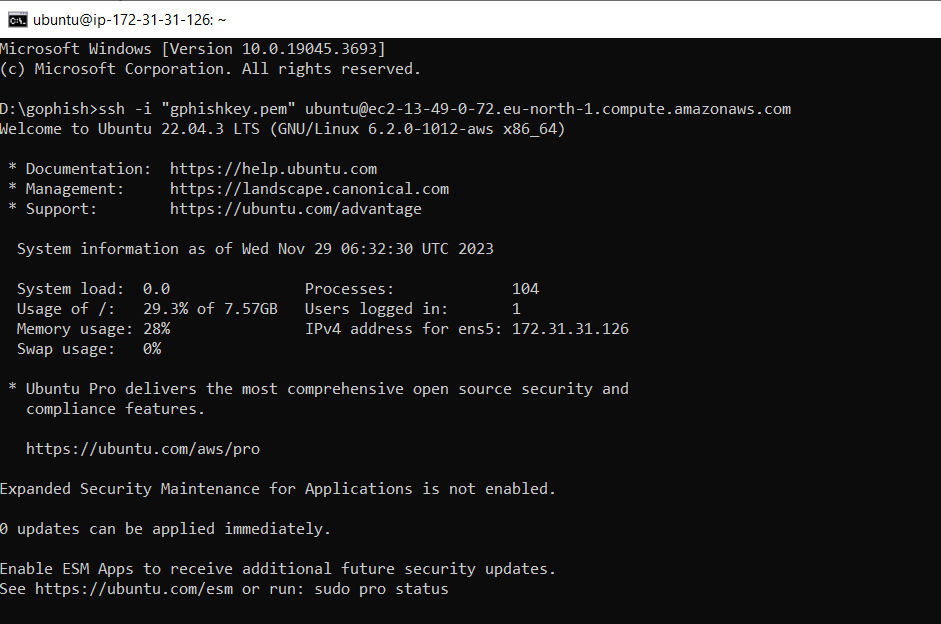


**Launch the EC2 instance:** Once the instance is initialized, user can connect into it through SSH.

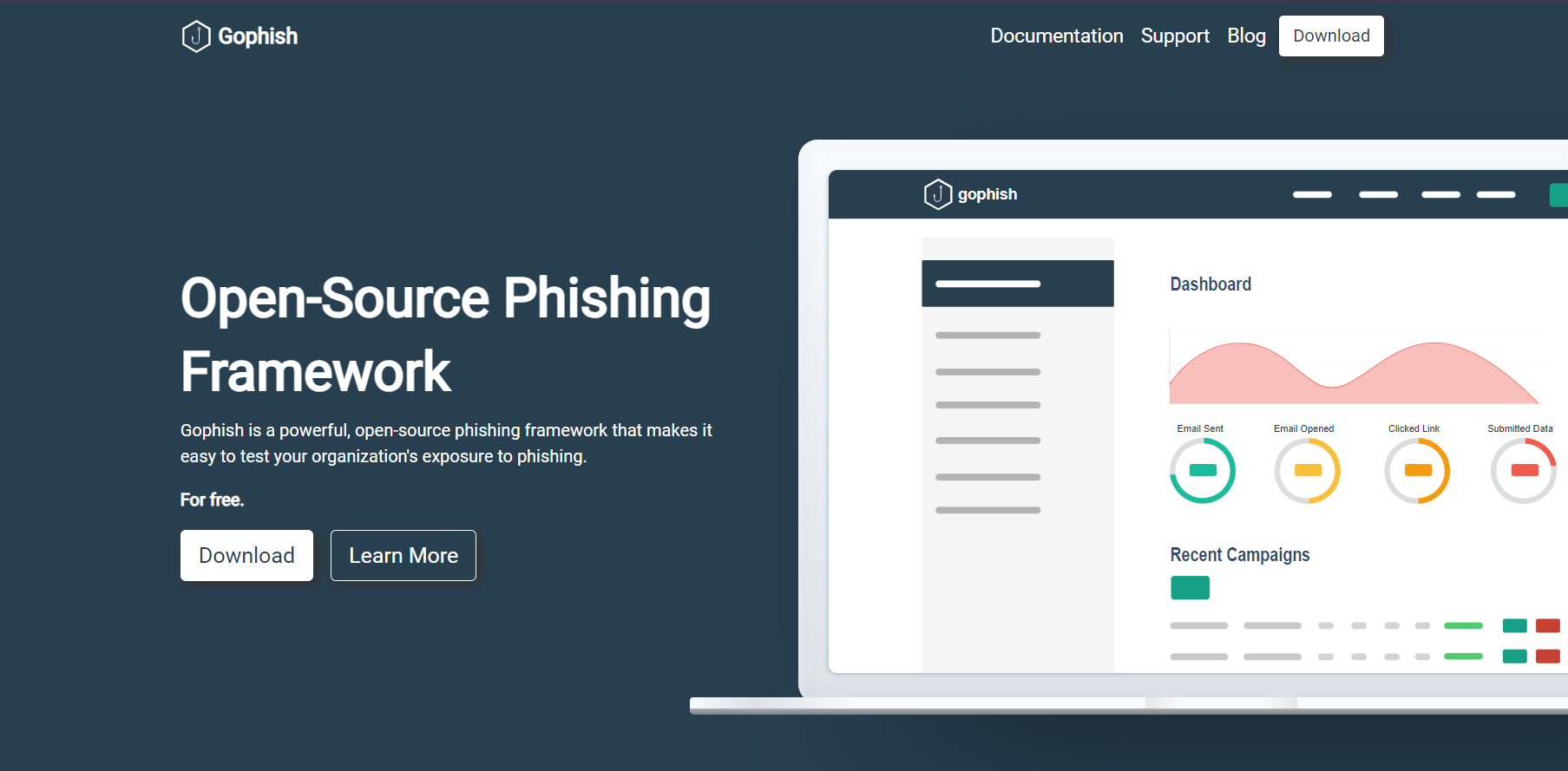


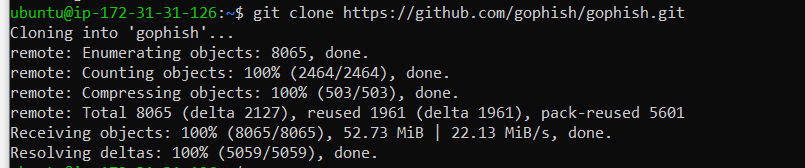
**Connect to the Ubuntu server:** Using the security key generated prior the user can access the server through SSH.

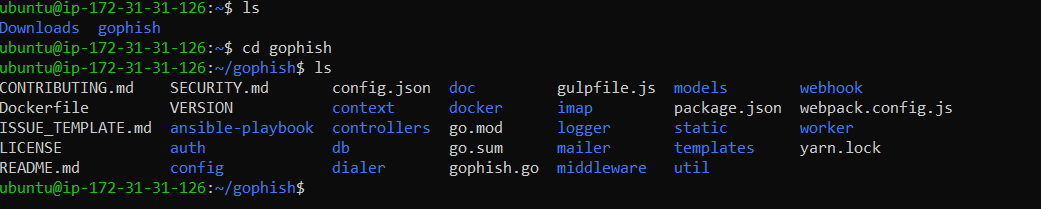




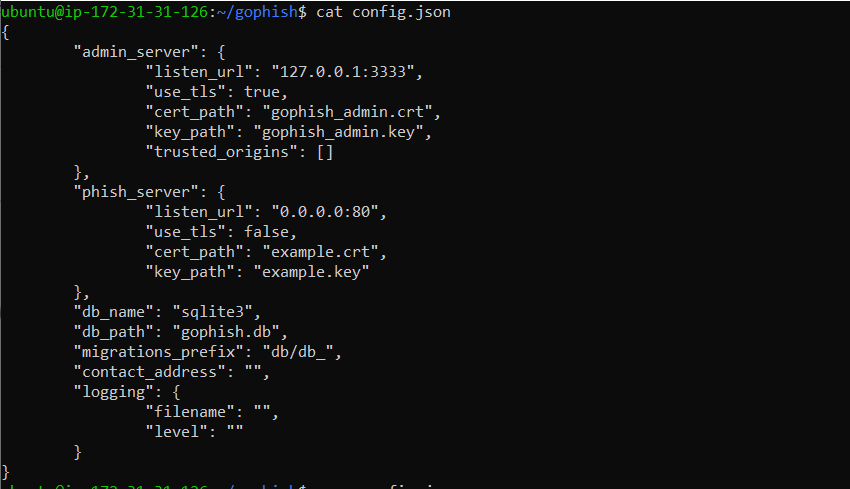
## Step 2: Install and configure Gophish on the EC2 instance

**Downloading Gophish framework:** Once the server is upgraded and updated, users can download the Gophish Framework and install it on the machine. 



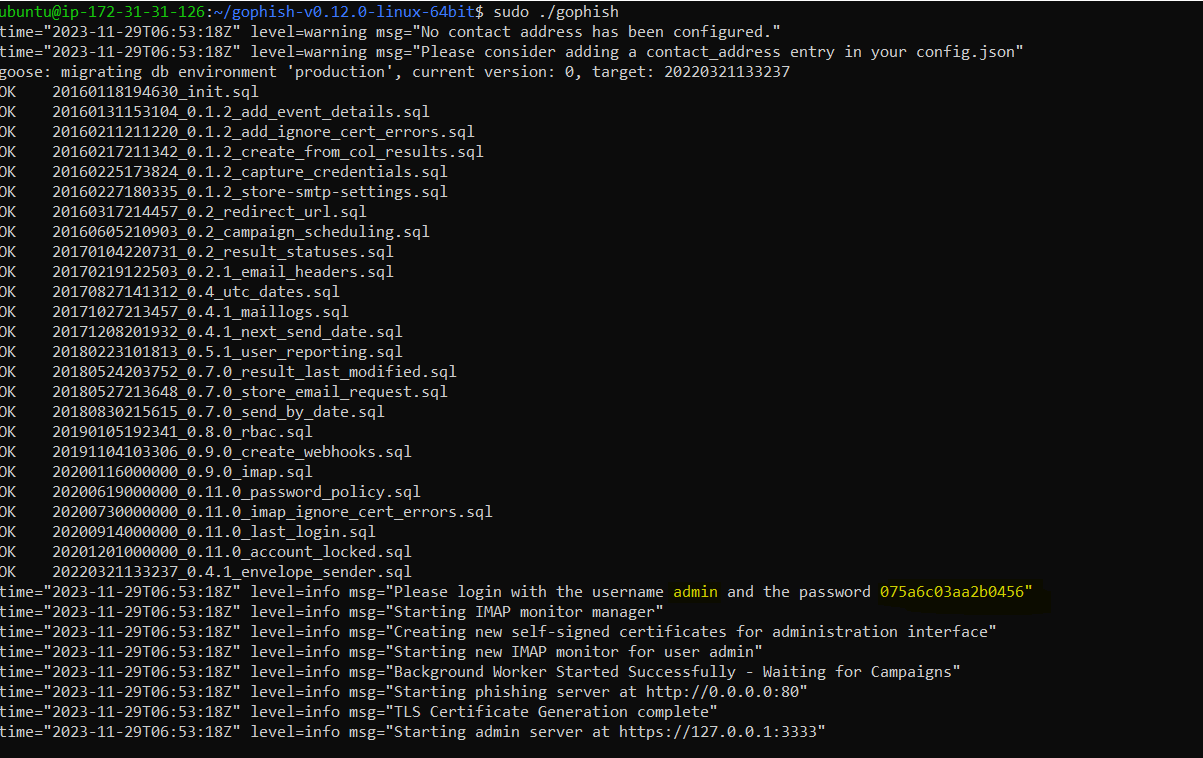


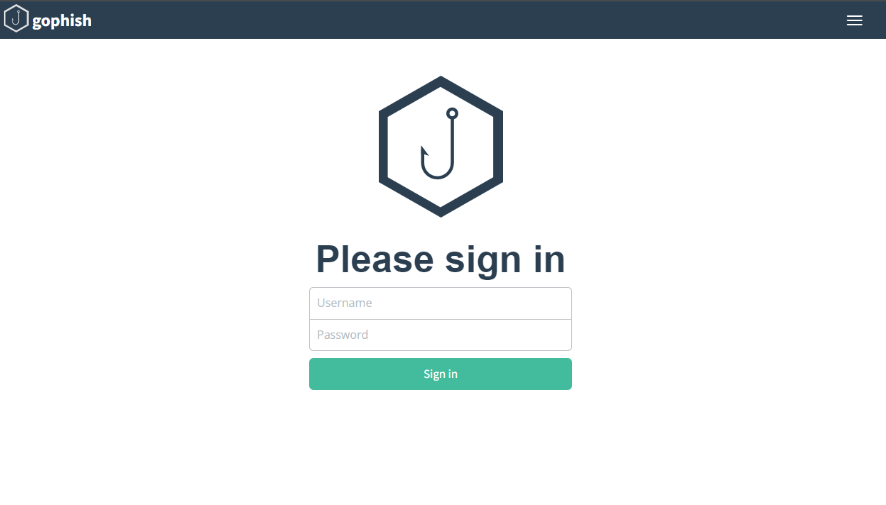
**Configure the config.json file:** The config.json is the configuration file of gophish framework. The admin\_server.listen\_url is IP/Port of gophish admin server, and phish\_server.listen\_url is IP/Port of the phishing server where landing pages will be hosted. The IP address in admin\_server.listen\_url has to be changed from 127.0.0.1 to 0.0.0.0 in order for the admin server to be accessible over the Internet.



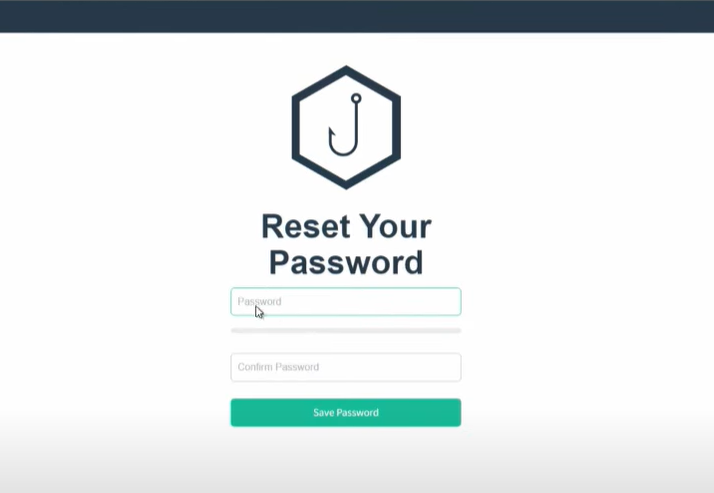


Execute the gophish server: Now the gophish server is started at [http://0.0.0.0:3333](https://0.0.0.0:3333), to access it, go to the EC2 instances public ip through port 3333. The temporary administrator credentials are printed in the logs when you first execute the GoPhish binary.





**Change credentials:** Once the user has logged in for the first time, they will be prompted to change the default password into a more secure one.



**Access the Dashboard:** Now the user has access to the dashboard where the details of the phishing campaign are fine tuned.

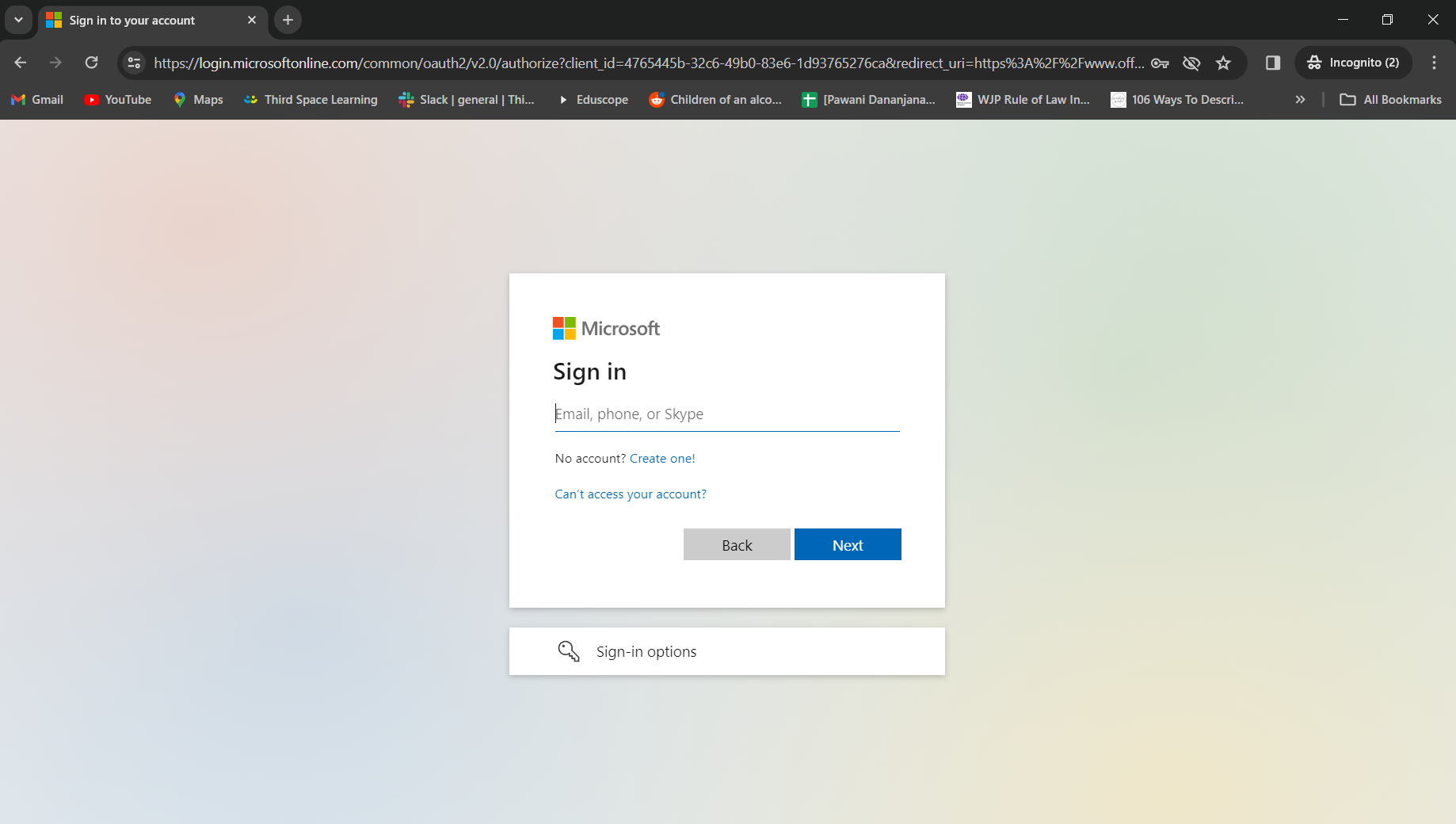


## Step 3: Registering attacker domain name

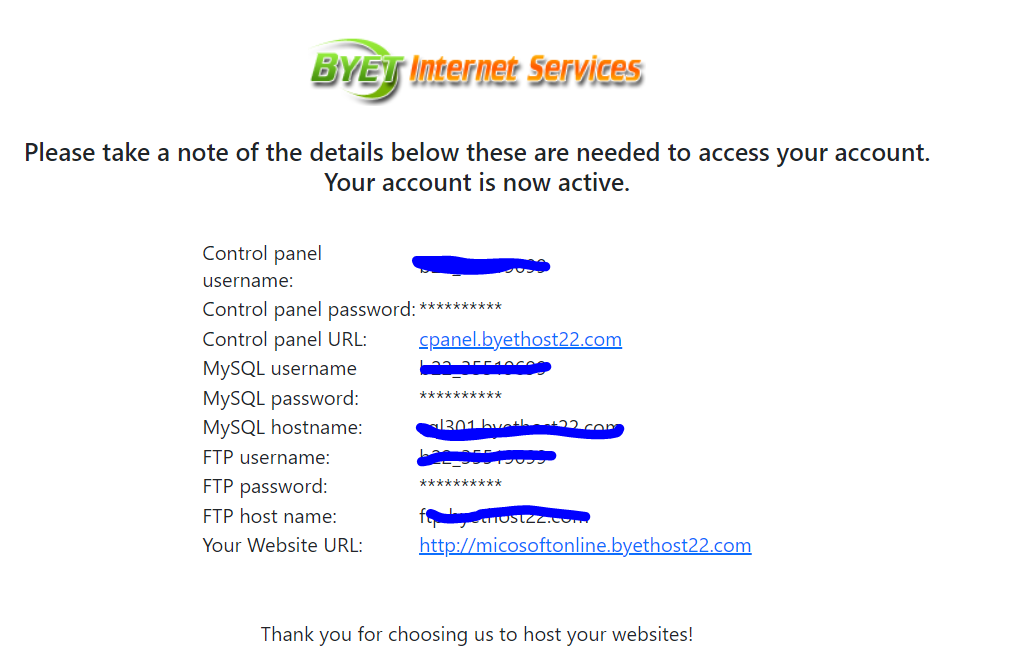
**Choosing the cover story:** The domain name depends on your phishing strategy and “cover story”. Which is one of the social engineering portions of the phishing campaign. Since most users do not pay attention to the URL in the browser, the domain should be at least convincing at a first glance to be legit.

In this instance the strategy is to tell the user that their O365 credentials have expired and for them to sign in again.

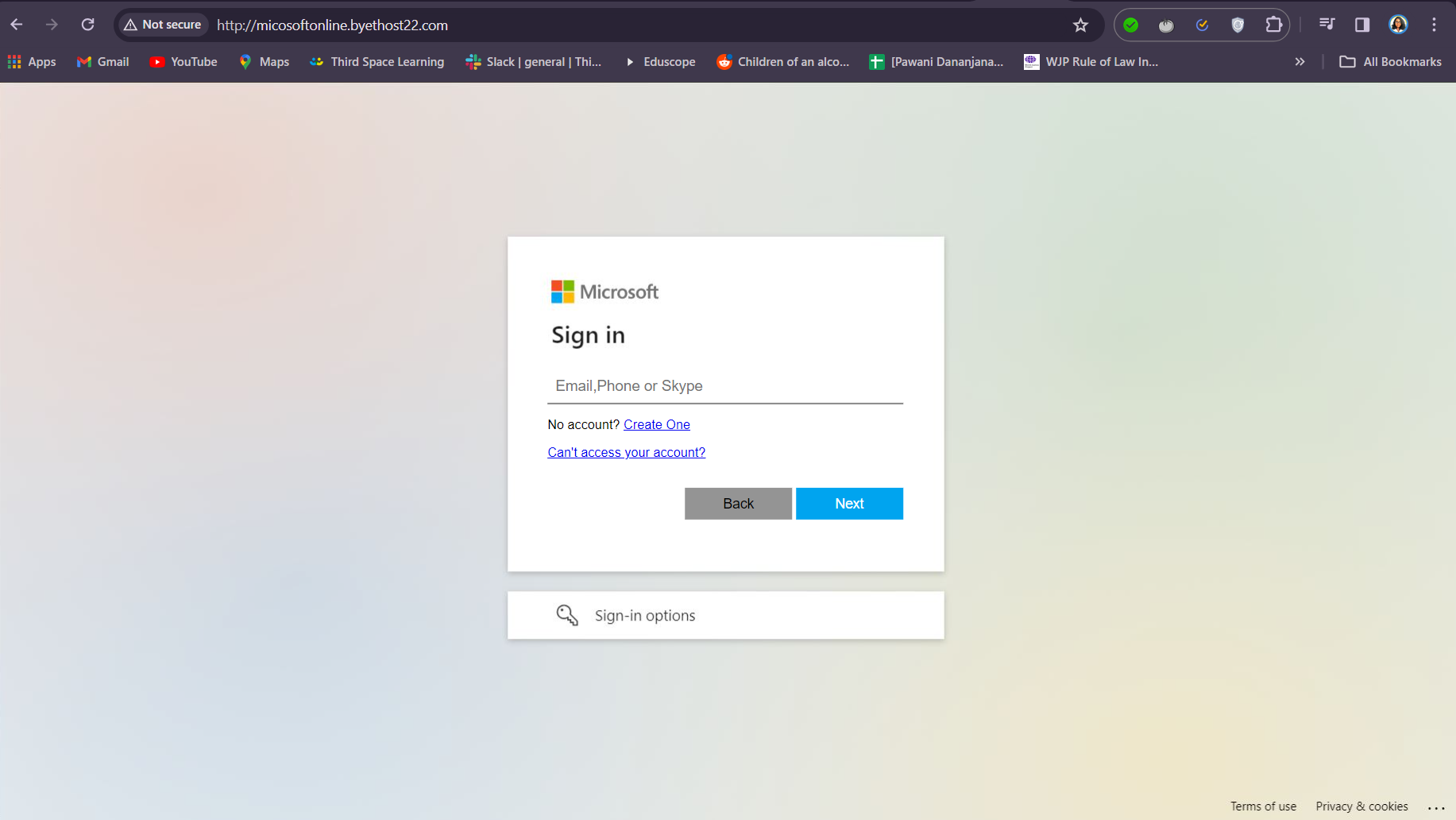
Therefore the domain has to be close enough to the actual O365 sign in page. Following is how the legitimate page looks like.



**Creating the domain:** A free domain named **“**[**http://micosoftonline.byethost22.com**](http://micosoftonline.byethost22.com/)**”** was created through ByteHost for the purpose of this test. At a first glance most users wouldn’t recognize a difference between the legit O365 site vs the attack domain.

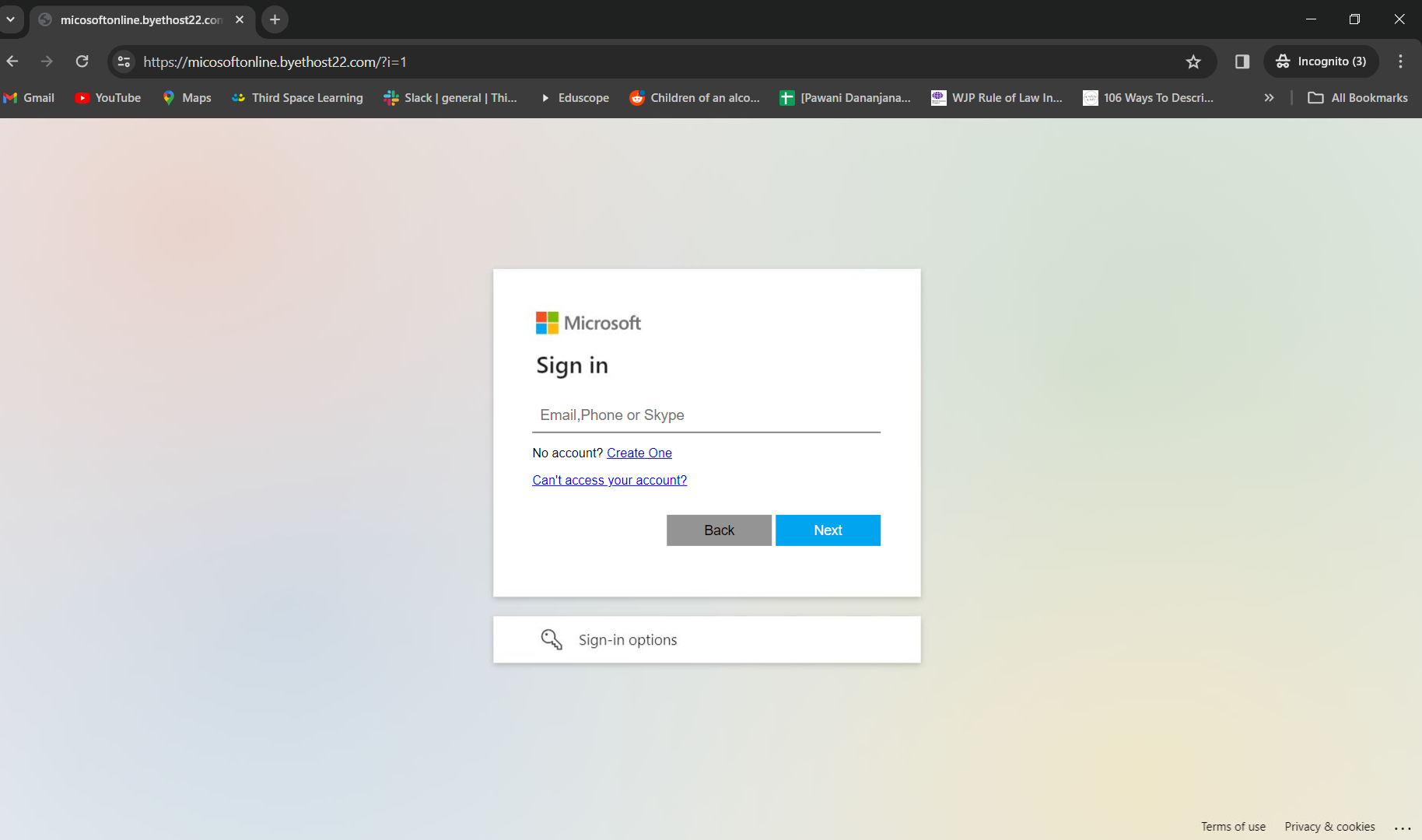
  
Through the Cpanel some other changes have to be made in order to run the campaign smoothly, which will be discussed later.

**Creating a convincing landing page:** If the phishing victim will click a link or any applicable object, Redirecting to a real domain landing page will Strengthen the “Cover story” and will raise the odds for the victim to fall for the trick. Given below is the fake landing page created for this phishing campaign.

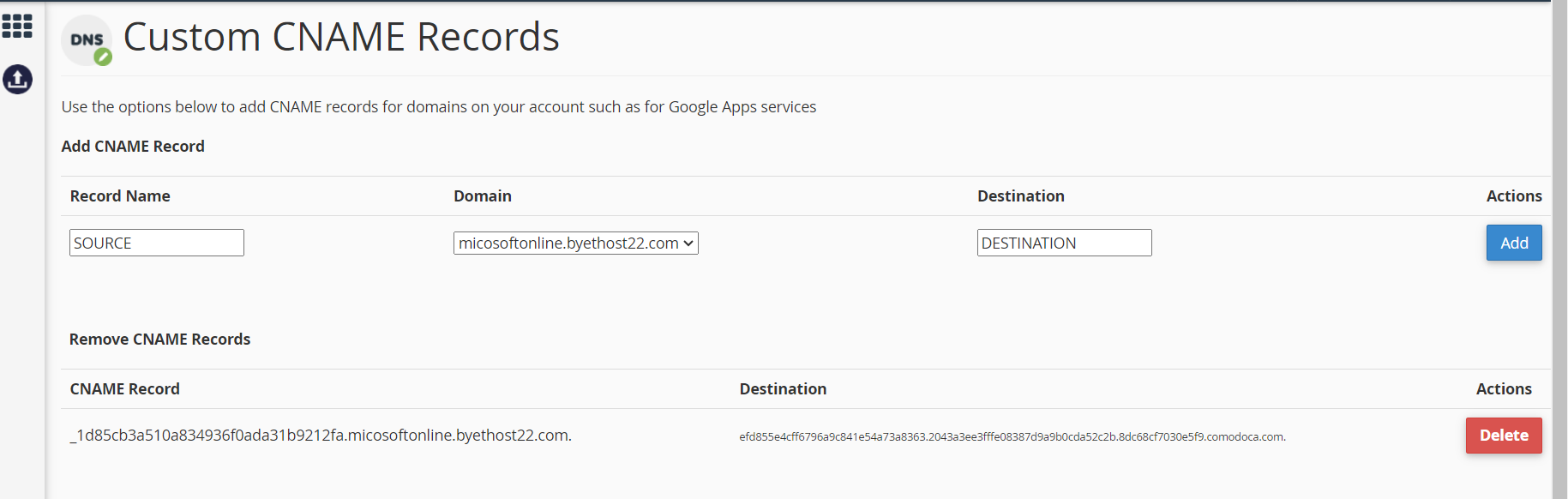
****

## Step 4: Hosting the phishing website Hosting the phishing website & Configure SSL for the domain

**Hosting the webpages:** The phishing website is hosted on bytehost platform, which gives the user the freedom to manipulate the content as needed.



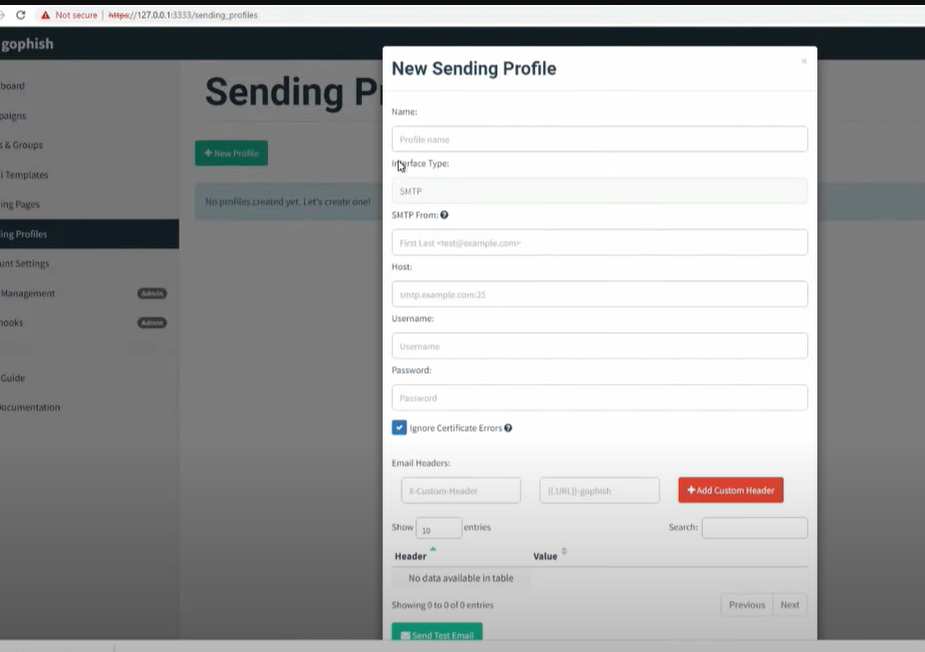
**SSL certificate obtaining:** Obtaining the SSL certificate will make it more convincing about the safety of the website the user is visiting. Which can be easily done through services like ZeroSSl

****

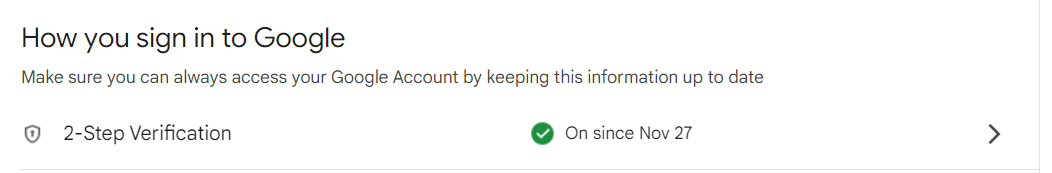
## Step 5: Test run of the phishing mail & Bypass google spam filter

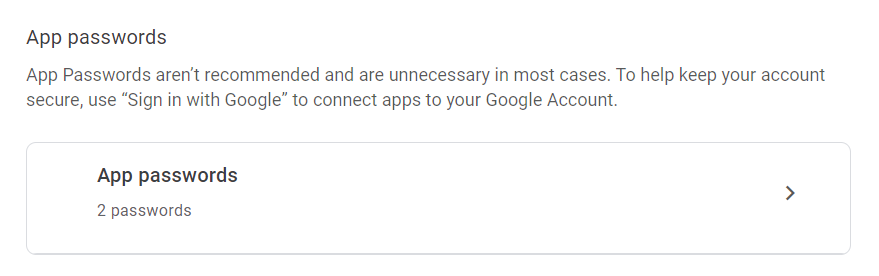
Now with everything in place a test campaign can be run to check if the phishing server is configured correctly.

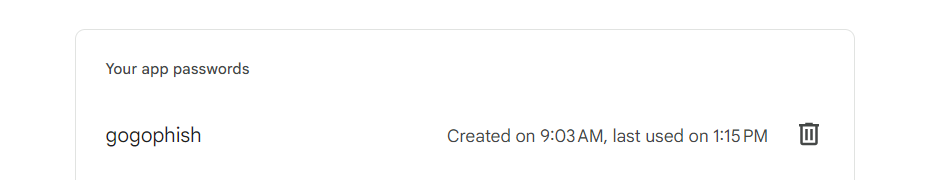
**Create a new sending profile:** here you set up the test Sender’s profile. Since the google SMTP is used here in order to bypass spam, an app password must be created, it should be the input in the password field and not the Gmail account login password.

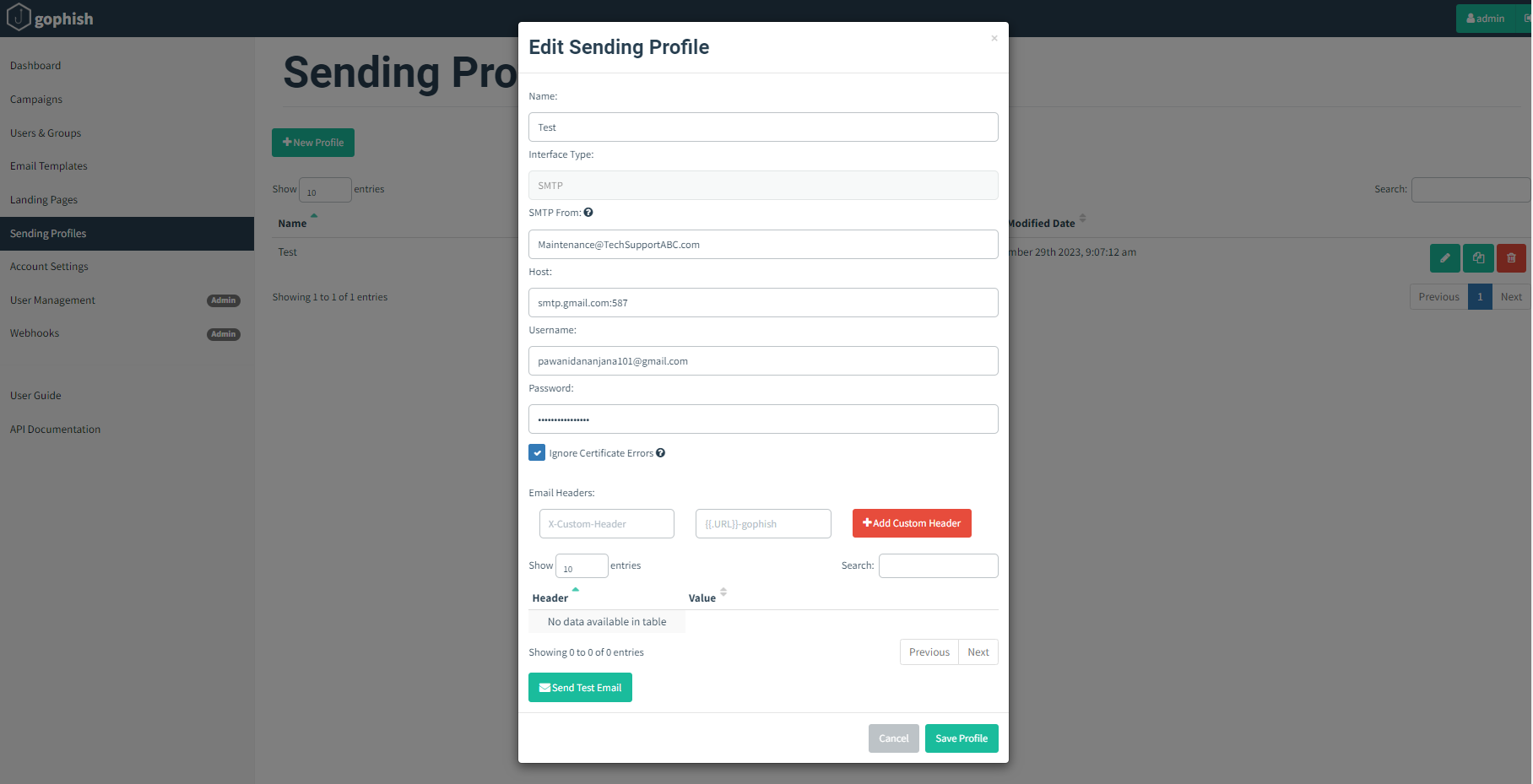


**Generate gmail app password:** An app password can be created for gophish by going through the 2-step verification in google.

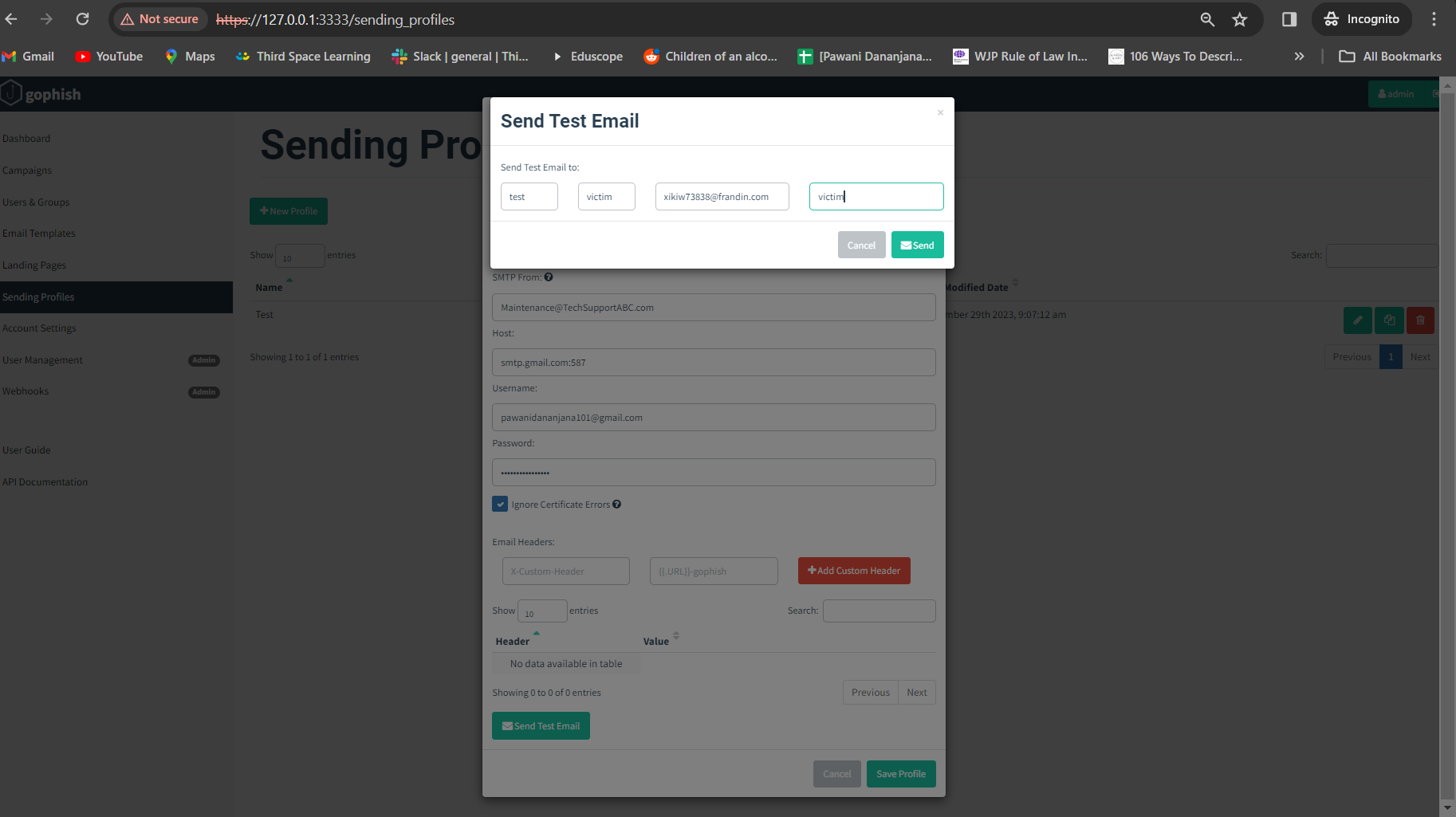
****

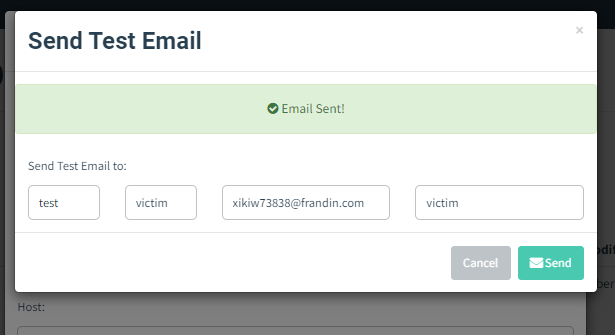
****

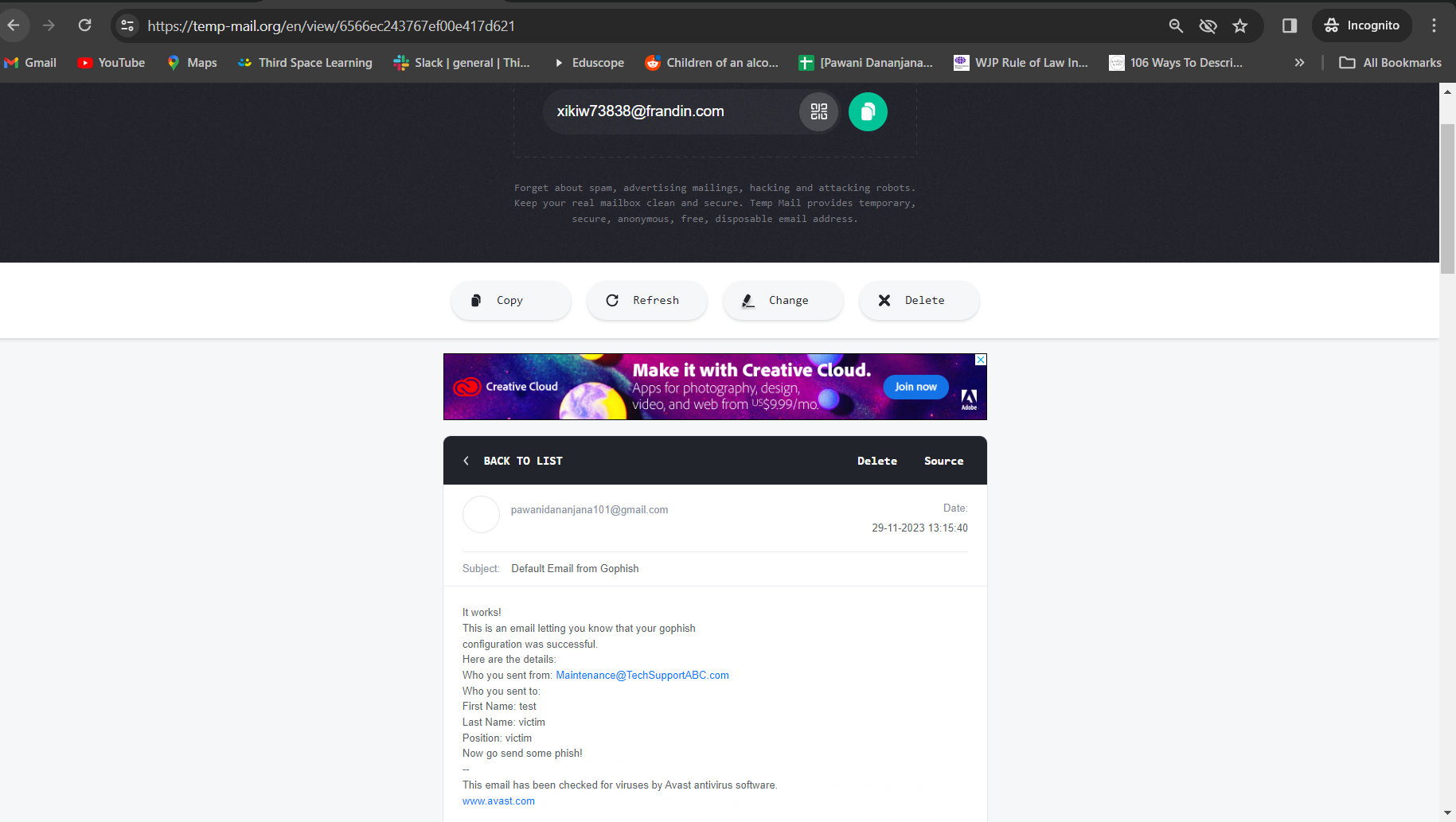
****



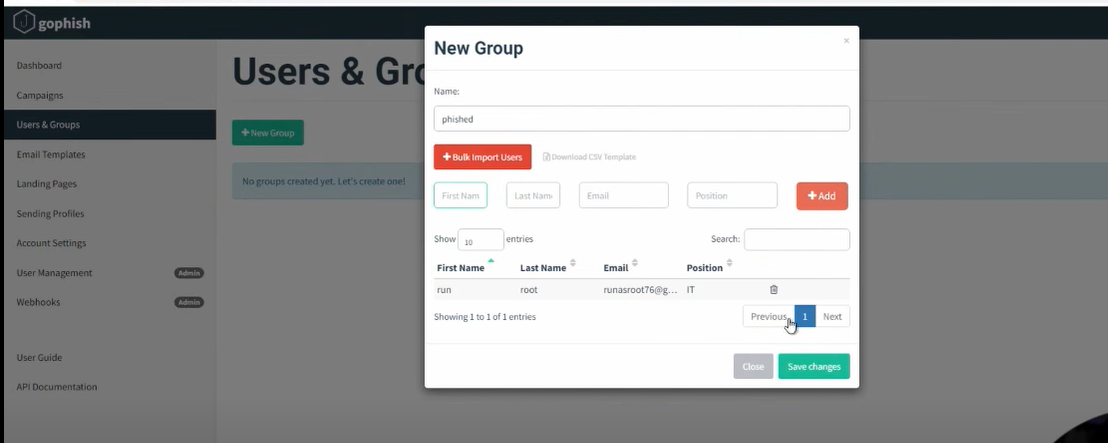
**Send test email:** In here a temporary email address is used to check if the server functions correctly. Once the email is received we can determine that it is ready for the phishing campaign.



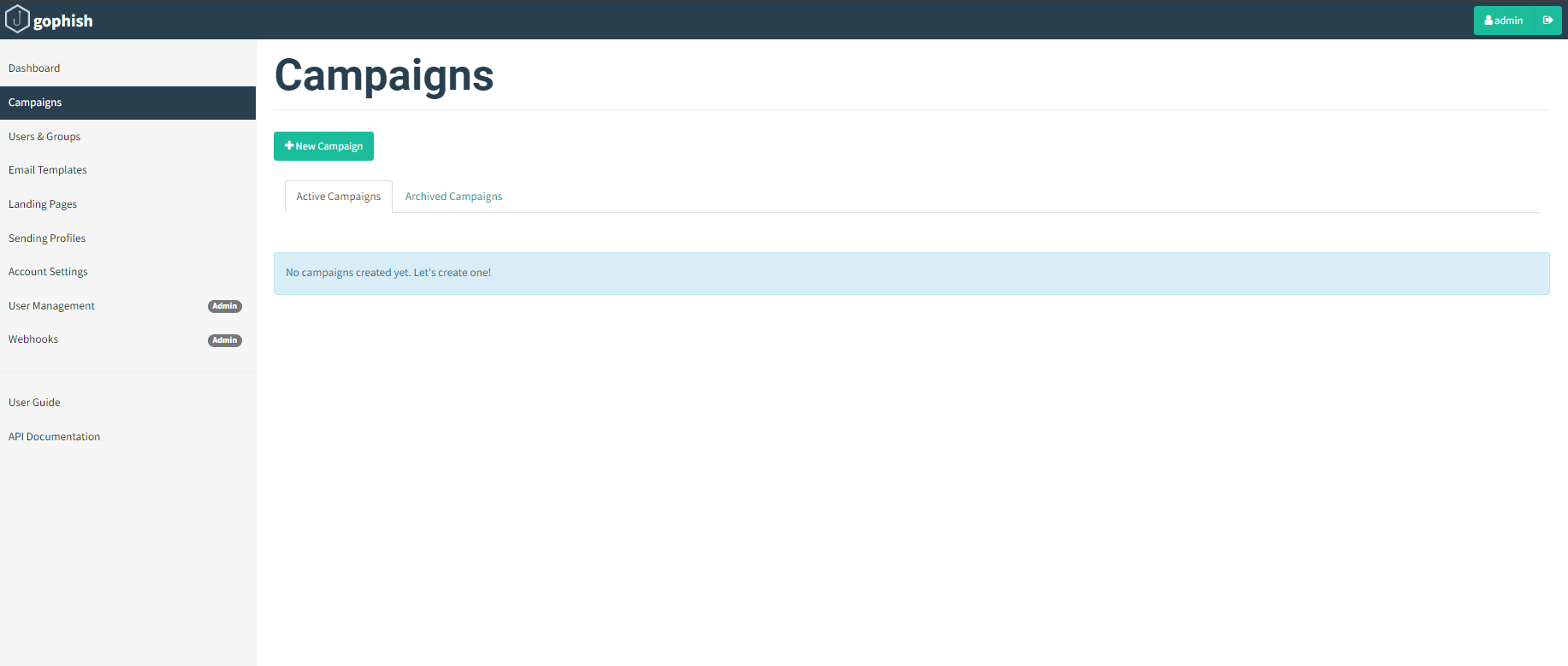




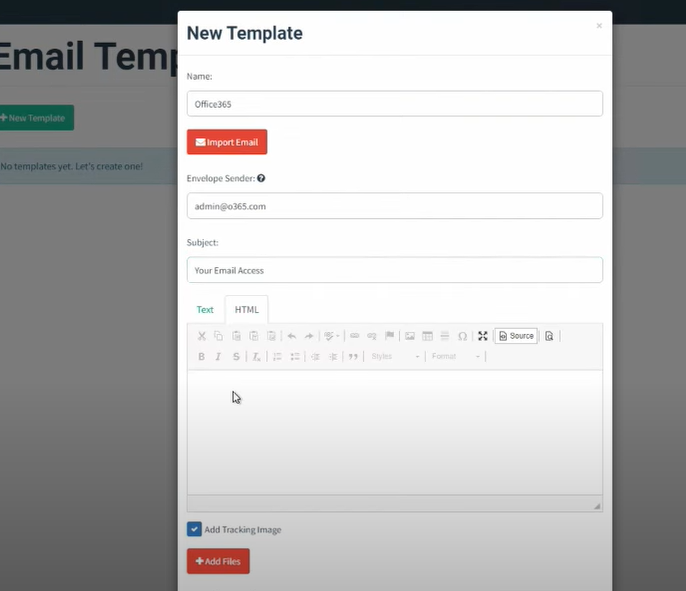
## Step 6: Configure the details of phishing campaign & Launch

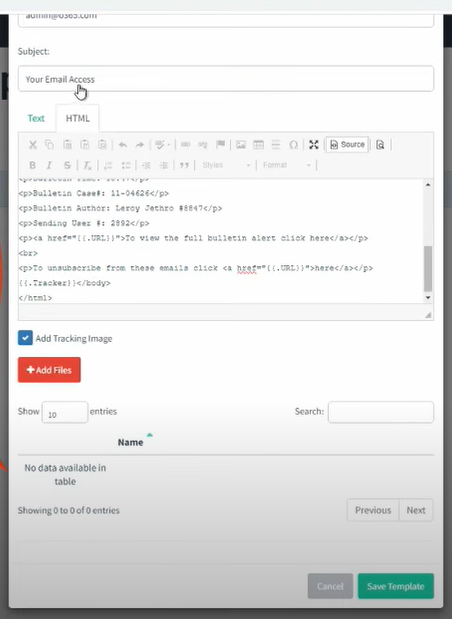
****

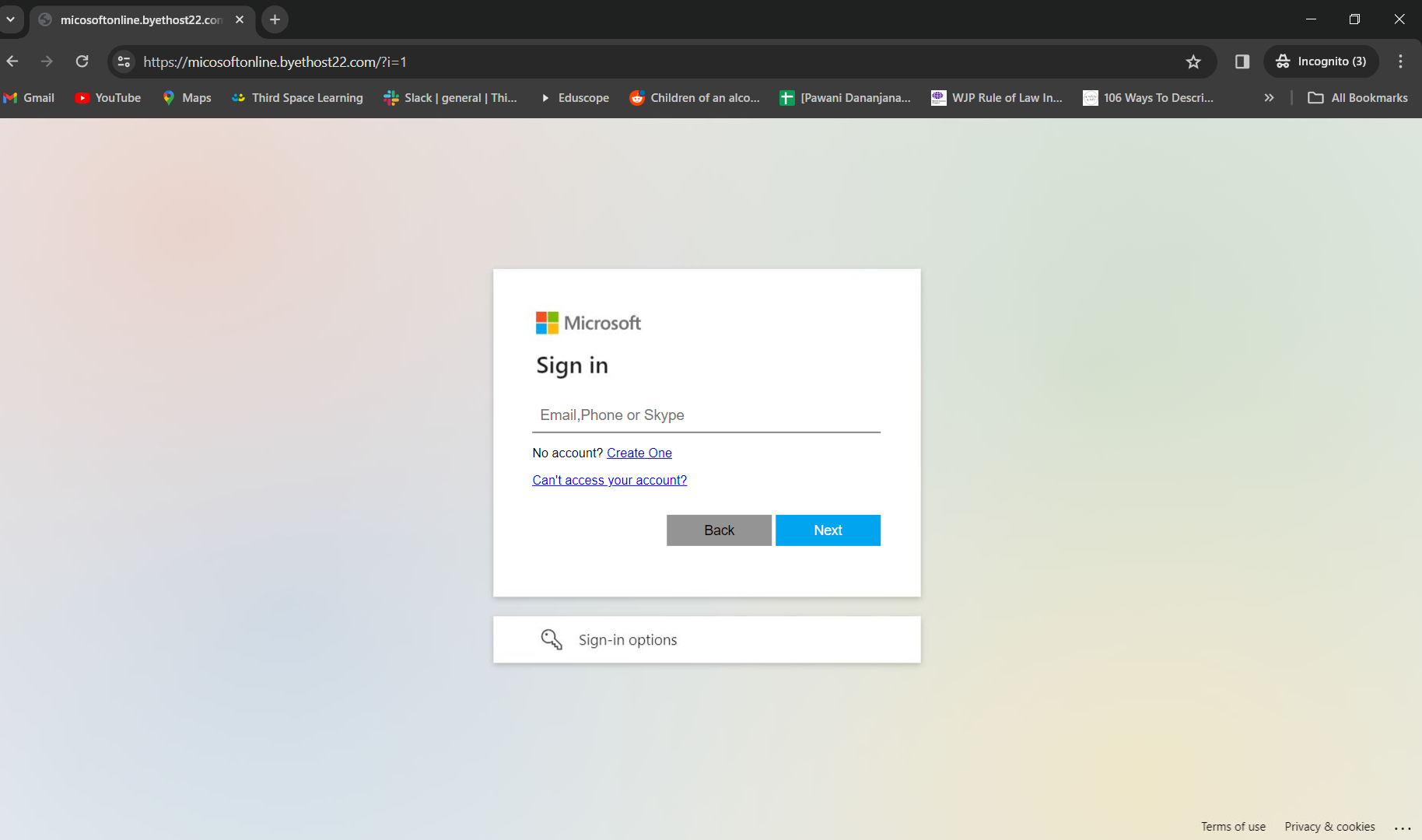
**Start the campaign:** Just like in the test round a new campaign will be started, after the relevant email templates and landing pages are created and the victims are added to the user group

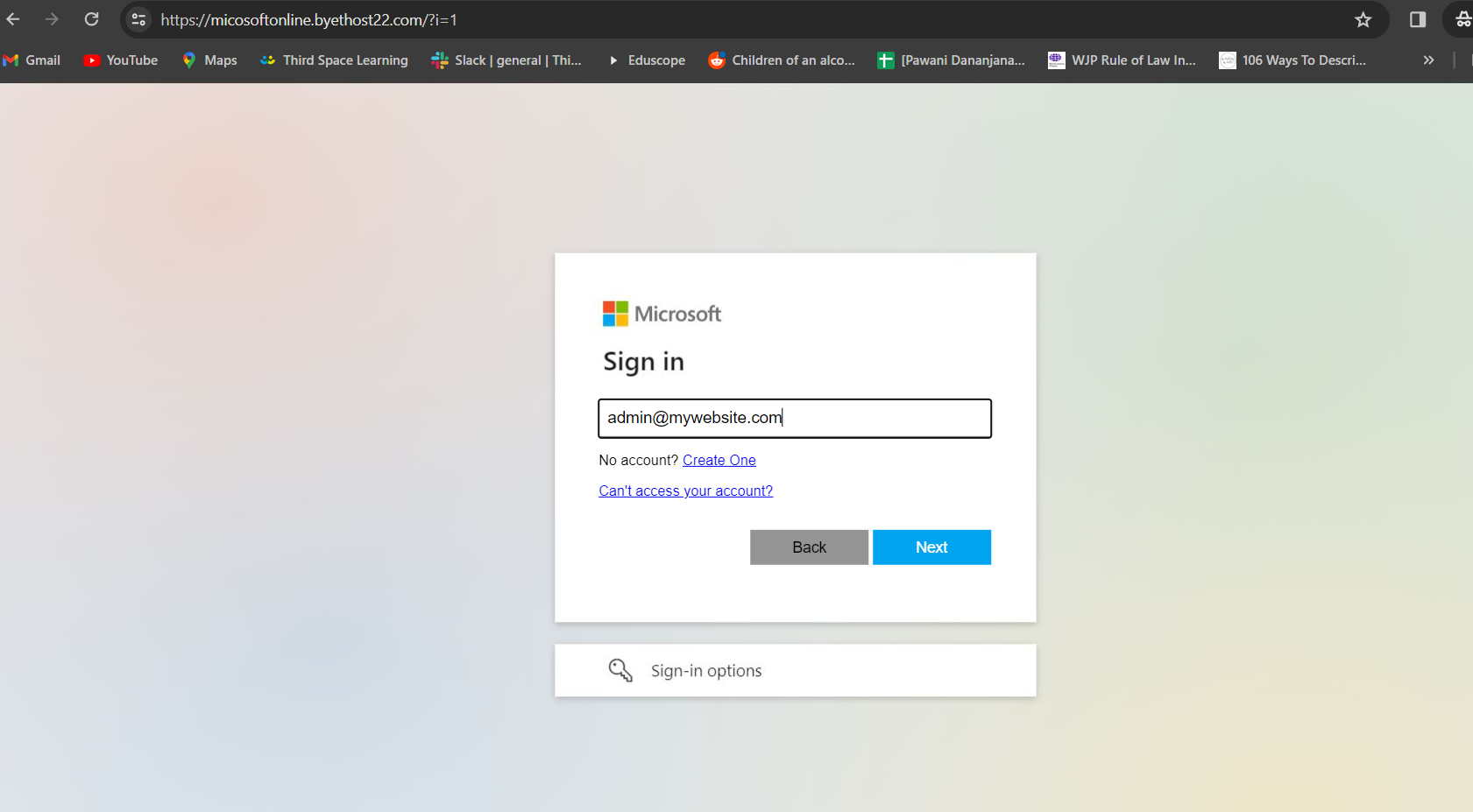


**Create the phishing email:**









## Step 7: Collect results (Victim Data)

