CyberScient

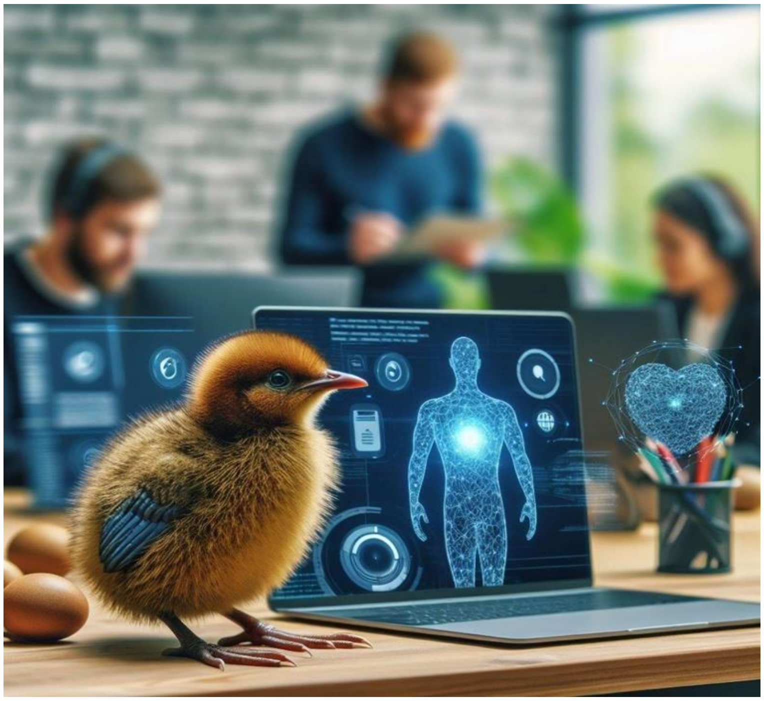
Crafting your Phishing Awareness Campaign: A Step-by-Step Guide

Table of Contents

About this guide

If you're looking to launch your own phishing awareness training instance for your organisation, you've come to the right place! This guide aims to help you launch your phishing awareness training instance locally from your own servers for your organisation.

We've made this as simple as possible so that little technical knowledge around phishing is required. Of course, some technical knowledge would come in handy rather than none. We will walk you through the entire process, from setting up a domain name and email server to running a successful campaign and conducting effective phishing training. Throughout this guide, we will use the example fictional company Kiwi Byte Solutions (kiwibytesolutions.com) to illustrate the steps involved.



What is Phishing?

Phishing is a type of social engineering attack that enables cybercriminals to launch attacks on unsuspecting victims by using fraudulent messages. Criminals use every trick in the book to persuade their targets into revealing confidential data, such as usernames and passwords, financial information, or other sensitive details. Anyone can be a victim, including cybersecurity professionals. Attackers use anything and everything at their disposal to create their master plan to cause maximum damage.

Phishing is the most experienced cyberattack by organisations in New Zealand. Training your employees on how to recognise these attacks and the typical formats that attackers use is a great way to keep your organisation safe.

However, sending phishing emails alone is not enough, so this guide will take you through the whole process of how to do phishing awareness training that's effective.

Prerequisites

Before you start, it's important to note that creating your own phishing awareness training campaign can be pretty complicated.
You will need the following.

A server:

You have two options for this -

A. You can either set up a local server on your own machine, but in this case, you will also need a static IP address from your Internet Service Provider (ISP).
B. Alternatively, you can use a Virtual Private Server (VPS) such as the one offered by Contabo: https://contabo.com/.
C.

If you don't have a server or a static IP address available to use, we recommend that you choose a VPS provider that doesn't block **port 25**. This is because our method involves setting up your own email server using Postfix, which requires port 25 to be open for the outbound sending of email (SMTP) messages. Most VPS providers like AWS, DigitalOcean, Linode, and Azure block messages coming from port 25 to prevent spam and phishing. This means that it will be very difficult to get an exception to conduct phishing awareness training using their services.

If you prefer to use a VPS from AWS, DigitalOcean, or Linode, you can use a cloud-based email service provider such as Sendgrid or Mailgun. However, it's important to note that phishing goes against these providers' terms of service, so we highly advise against choosing this option.

Server Requirements:

We recommend using Ubuntu LTS 22.04 as the OS for your system, as that is what this documentation is based on. This isn’t a computing heavy container, but the amount of power and storage will depend on the number of users you plan on testing. For a small number of users, under 500, we recommend having around 4GB of RAM, 2-4 CPU cores and 400GB of SSD.

A domain name

We’ll cover this in the next section, but a domain name is critical to a phishing attack. You can purchase a cheap domain name from https://www.ionos.com/. If you would like to create multiple types of phishing emails, you will need to purchase multiple domains.

A cloned copy of this GitHub repository.

We’ve included a few containers and some scripts to make the setup easier.
https://github.com/Hgarnell/AUTcyberscient23B

Picking and creating a domain name

How to pick a domain name

If you’ve configured and protected your domain name, an attacker can't use it. So, what do they do? They create convincing replicas of your company domain or popular companies like Amazon and Microsoft. You can employ the same tactics when picking a domain name to create a phishing campaign.

Character swapping
Attackers swap out the number 1 with either the letter "I" or "L" or vice versa to deceive or trick unsuspecting individuals.
e.g. k1w1bytesolut1ions.com, m1crosoft.com

International Alphabet character-swapping
Attackers may use characters from other languages that look like English letters. Examples often used are the Cyrillic є to replace e or the Greek to replace α and β to replace A and B.
e.g. kiwibytєsolutions.com, amazon.com

Typos
Another option is to use typos or misspellings of words to trick busy users who may not be attentional to detail.
e.g. kiwibitesoltuions.com, amozan.com

Subdomain impersonation
Attackers may also pose as fake subdomains or sections of your company, such as IT help support or accounting to create new domains that look realistic
e.g. Ithelpkiwibytesolutions.com, Helpmicrosoft.com

How to buy a domain name

You cannot just create and choose a domain name without registering with a domain registrar to connect your domain name to a DNS system, which allows you to know where your webpage is on the internet. There are many domain registrars to choose from, including Google Domains, GoDaddy, and more.

A full list of domain registers can be found here: List of Accredited Registrars (icann.org).

Depending on who you purchase from, the price can vary greatly. We decided to choose **Ionos** because their offer lets you purchase a domain name for a dollar for a year. You will want to use a different domain for every campaign or theme so that employees don't begin to recognise a test. Using the same domain wouldn't be realistic, as hackers will use a variety of domain names to pass by firewalls and manipulate their victims.

Connecting your server to the domain

After you purchase a domain, you'll need to connect it to your server instance so that when people visit the domain name, the DNS server can direct you to the right location.
To do that you will need to add 4 records into your DNS server.

This includes the following records:
Apex Domain (@) A Record: This record points your domain name to the ipv4 address of your server. It ensures that requests such as, yourdomain.com, go to the correct ipv4 address.
WWW Subdomain A Record: Like the Apex Domain A Record, this record helps ensure that your domain name points to your server, but also ensures that records with a subdomain, such as www.yourdomain.com or www.testing.yourdomain.com also go to the correct ipv4 address.
Apex Domain (@) AAAA Record: This has the same function as the Apex Domain A Record, but for your servers ipv6 address.
WWW Subdomain AAAA Record: This has the same function as the WWW Subdomain A Record, but for your servers ipv6 address.

Whitelisting domain name on your email servers

Fortunately, many email providers have implemented strong filters to weed out phishing emails. While this is good, it can pose a challenge when conducting phishing engagement tests. To ensure you can test your employees with your set-up, you will want to whitelist your phishing awareness domain in your corporate email settings. The goal of phishing awareness testing is not to test the strength of your firewalls and filters; instead, it is to test what your employees would do in the chance of firewall/filter failure.

Google
Allowlists, denylists, and approved senders - Google Workspace Admin Help

Microsoft

Manage allows and blocks in the Tenant Allow/Block List - Microsoft Defender for Office 365 | Microsoft Learn

Setting up the technology

Link to the GitHub: https://github.com/Hgarnell/AUTcyberscient23B

Before cloning into our instance, you'll want to ensure you have both git and make installed on your server. If your account is not in privileged mode, you may want to enter it to execute the following commands:

Enter privileged mode.

```
sudo -s
```

Update and install packages.

```
 apt-get update
 apt-get upgrade
```

You'll also want to update and install packages. Your server may already have **git** and **make** preinstalled, but if not, use the following commands.

```
apt install git
apt install make
```

Clone into our instance

First, you'll need to clone our GitHub instance.

```
git clone https://github.com/Hgarnell/AUTcyberscient23B.git
```

Then, change directories so that you are inside of it.

```
cd AUTcyberscient23B
```

Run the initiation script.

```
make init
```

Update the docker-compose file to reflect your domain name and IP address.

```
nano docker-compose.yml
```

Once inside the docker-compose file, replace the postfix container variables.
`SERVER_HOSTNAME=example.com` and `SERVER_IP=0.0.0.0/32`
And then the certbot container variables
`--email your_email@example.com` and `-d yourdomain.com`

to reflect your domain name, email and server IP.

Before:

```
certbot:
   image: certbot/certbot:latest
   command: certonly --webroot --webroot-path=/usr/share/nginx/html/letsencrypt --email your_email@example.com
--agree-tos --no-eff-email -d your_domain.com
   volumes:
     - ./certbot/conf/:/etc/letsencrypt
     - ./certbot/logs/:/var/log/letsencrypt
     - ./certbot/data:/usr/share/nginx/html/letsencrypt

 postfix:
    build:
      context: ./email-docker
      dockerfile: Dockerfile
    image: gophish_postfix
    environment:
     - SERVER_HOSTNAME=example.com
     - SERVER_IP=0.0.0.0/32
```

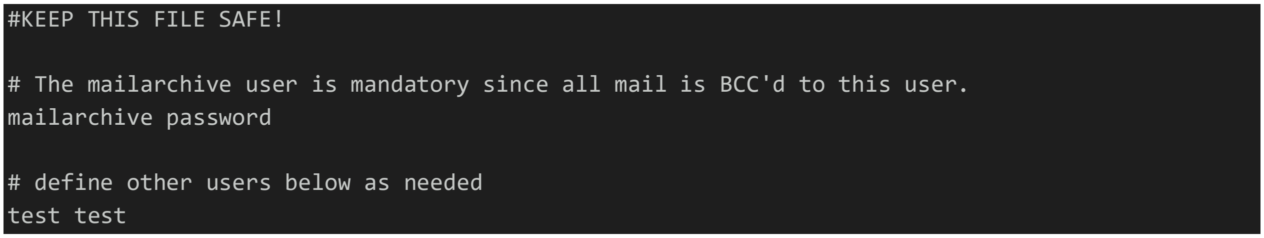
Example After:

```
certbot:
   image: certbot/certbot:latest
   command: certonly --webroot --webroot-path=/usr/share/nginx/html/letsencrypt --email
admin@kiwibytesolutions.info --agree-tos --no-eff-email -d kiwibytesolutions.info
   volumes:
     - ./certbot/conf/:/etc/letsencrypt
     - ./certbot/logs/:/var/log/letsencrypt
     - ./certbot/data:/usr/share/nginx/html/letsencrypt


postfix:
    build:
      context: ./email-docker
      dockerfile: Dockerfile
    image: gophish_postfix
    environment:
     - SERVER_HOSTNAME=kiwibytesolutions.info
     - SERVER_IP=11.111.111.111
```

Change email account logins

You will need to update the email account username and passwords from the default ones. You can keep the `mailarchive` account username, but we recommend changing the password to a more secure one.

In the file we've identified one account with the username and password `test:test`



```
#KEEP THIS FILE SAFE!

# The mailarchive user is mandatory since all mail is BCC'd to this user.
mailarchive password

# define other users below as needed
test test
```

As these passwords are stored in plain text, we highly recommend keeping password stored hashed. This document won't go into further detail about that but further information can be found at the following link: https://doc.dovecot.org/configuration_manual/authentication/password_schemes/

However, to change the passwords and account names in file, use the following command.

```
nano email-docker/src/user.txt
```

Set GoPhish config file

We need to set the GoPhish configuration file before we build the containers to help with routing. Make sure to replace `YOUR_DOMAIN.COM` with your domain name.

```
 make runPhishing_config
./phishing_conf.sh YOUR_DOMAIN.COM
```

Set up containers

Build your containers with the make build command.

```
make build
```

Setting Up Nginx and SSL encryption

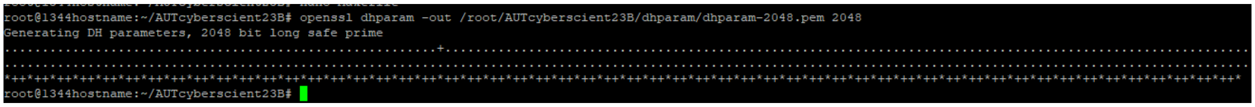
You may have come across a warning on your browser when you visit an “unsafe” site. These are sites that don’t have certifications. This happens when the website does not have a valid SSL/TLS certificate. To prevent that warning from happening we will be using the following tools to certify our phishing websites, Diffie-Hellman parameters, Nginx Image, CertBot and Let’s encrypt.

In the docker-compose file, we have two containers for web hosting and certifying. These containers ensure a secure HTTPS connection by automatically obtaining and renewing SSL/TLS certificates. Nginx plays a crucial role in routing requests and handling static and dynamic content, while CertBot ensures continuous HTTPS protection and certificate validity, enhancing the security, compliance, and trustworthiness of websites hosted on the server.

When you run the docker-compose file, it will start using Nginx to serve your website from `./public_html`. It will also set up CertBot to obtain SSL certificates you’re your domain using the webroot authentication method. The certificates will be stored in `./certbot/data` for Nginx to use.

First, we will need to generate Diffie-Hellman parameters of 2048 bits and save them to the specified file. Diffie-Hellman parameters are used in SSL/TLS communication to establish a secure session between a client (e.g., web browser) and a server (e.g., web server). These parameters are crucial for generating the shared secret key used to encrypt the data exchanged during the SSL/TLS handshake process.

```
make generateOpenSSL
```



```
root@1344hostname:~/AUTcyberscient23B# openssl dhparam -out /root/AUTcyberscient23B/dhparam/dhparam-2048.pem 2048
Generating DH parameters, 2048 bit long safe prime
.......................................................+.........................................................................................
.................................................................................................................................................
*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*++*
root@1344hostname:~/AUTcyberscient23B#
```

After running this command, you will have a file named `dhparam-2048.pem` containing the Diffie-Hellman parameters of 2048 bits, which can be used in your Nginx or other web server configurations to enhance SSL/TLS security.

Next, we will need to run the following commands to define the http configuration for the Nginx file. Make sure to replace `YOUR_DOMAIN.COM` with your domain name.

IMPORTANT: please make sure run http.sh command first NOT BOTH HTTP.sh and HTTPS.sh. If you receive an SSL file not found error in your web container, it will because of this error. If you encounter an error where the start command will not run, try make down then make start first.

```
 make runHttp
./http.sh YOUR_DOMAIN.COM
```

Run the command to the docker containers.

```
 make start
```

Then, run another script to define the HTTPS configuration for the Nginx file, ensuring that the `YOUR_DOMAIN.COM` reflects your domain name.

```
make runHttps
./http.sh YOUR_DOMAIN.COM
```

Run the command to the docker containers again.

```
 make start
```

Check that both containers are running.

```
 docker ps
```

The output should look like this if set up correctly.

```
root@1344hostname:~/AUTcyberscient23B# docker ps

CONTAINER ID   IMAGE                 COMMAND                  CREATED          STATUS          PORTS
NAMES

c38e79427ef5   nginx:1.14.2-alpine   "nginx -g 'daemon of…"   22 minutes ago   Up 19 minutes
0.0.0.0:80->80/tcp, 0.0.0.0:443->443/tcp                           autcyberscient23b_web_1

e7d5a0169d68   gophish_postfix       "/usr/local/bin/post…"   22 minutes ago   Up 21 minutes
0.0.0.0:25->25/tcp, 0.0.0.0:1587->587/tcp, 0.0.0.0:1993->993/tcp   autcyberscient23b_postfix_1

3fa618d0ec57   gophish/gophish       "./docker/run.sh"        22 minutes ago   Up 21 minutes
80/tcp, 8443/tcp, 0.0.0.0:3333->3333/tcp, 0.0.0.0:3380->8080/tcp   autcyberscient23b_gophish_1

root@1344hostname:~/AUTcyberscient23B#
```

Check that there aren’t any errors using the following command.

```
 docker-compose logs
```

If your certification ever expires and you start receiving a warning on your web browser, you can use the following command to restart CertBot.

```
docker compose run --rm certbot ren
```

Setting up DKIM, SPF, DMARC, MX

To set up DKIM, SPF, DMARC, and MX, we will need to update the configuration for both the container and our DNS server.

Luckily, we've set everything up in the container, so you just need to edit the entries in your DNS tables.

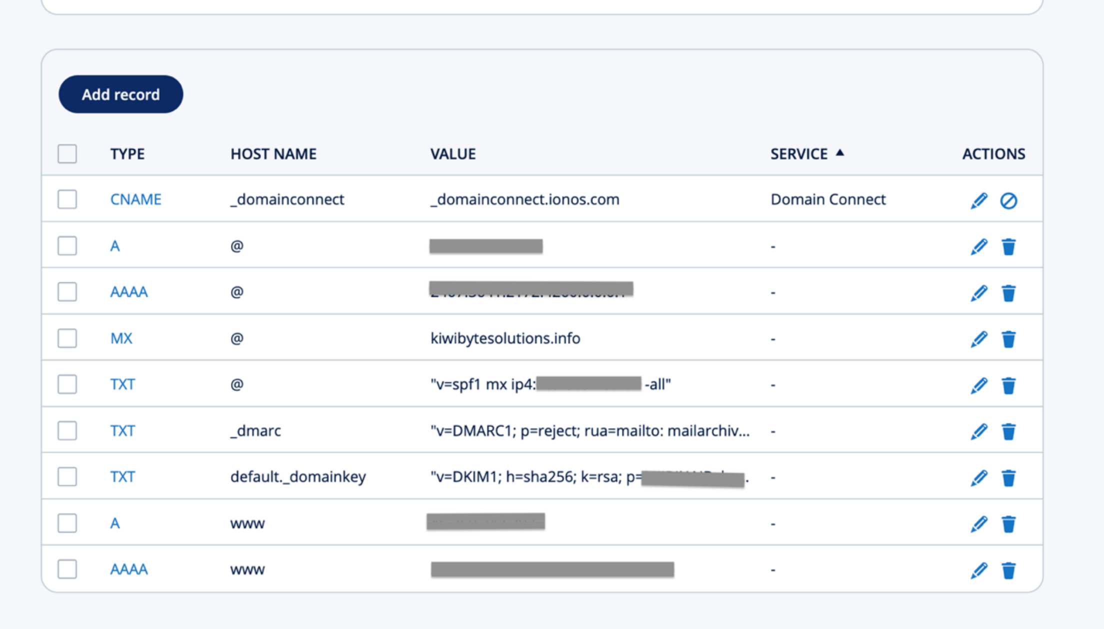
To view the entry items, enter the following command to view the logs from the postfix container.

```
 docker logs autcyberscient23b_postfix_1
```

The output should look something like the following.

```
 DKIM DNS entry:
 -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
 Place the following output as the DKIM key in your DNS server. Note that formatting may differ
depending on the DNS provider.

 Add this as a new TXT record where the Record name is default._domainkey.kiwibytesolutions.info


v=DKIM1;h=sha256;k=rsa;p=MIexamplekeydataFAAOCAQ8AMIIBCgKCAQEA7qMr8UbIWz+G+/laWzfg7PQbl46+syv+hx/KnW
UKijSlGwVaT0ZC93JvoE+zRYg2YR/examplekeydata/WMiSeDM+95Qkr7Y7Q9sVujQiPLP9W/00000sdfsdfsdgkasdjghakjsd
hfkj+8wDS8QM9syV1CP4rGyF4IRNv6hMwnO8R4H+tuhcJEE08tkcg5AxTCkfEPsUXx21s5XSd3JPq/QTrdUO2sDit6Y2Z59b1/Qv
a/lGGfDC01nhzxllai3vWGjvjUzIcwnFGP8xD examplekeydata8nrwG64WCfv/Wr1vApUYawIDAQAB

 File as is:
default._domainkey  IN        TXT       ( "v=DKIM1; h=sha256; k=rsa; "
"p=sdfsdfsdjfkadjsgexamplekeydata00+G+/laWzfg7PQbl46+syv+hx/examplekeydata+zRYg2YR/yZzfYJvEzsRMVMBjx
2fR/WMiSeDM+95Qkr7Y7Q9sVujQiPLP9W/8nvzexamplekeydataTFoE8n2evJTEYO5x23zrEY+8wDS8QM9syV1CP4rGyF4IRNv6
hMwnO8R4H+tu"
"hcJEE08tkcg5examplekeydatait6Y2Z59b1/Qva/lGGfDC01nhzxllai3vWGjvjUzIcwnFGP8xD6r0KPj1F9n+gClZ62Nf8nrw
G64WCfv/Wr1vApUYawIDAQAB" )  ; ----- DKIM key default for kiwibytesolutions.info
Place the following output as the DMARC key in your DNS server
v=DMARC1; p=reject; rua=mailto:mailarchive@kiwibytesolutions.info
Add this as a new TXT record where the Record name is _dmarc.kiwibytesolutions.info

 Place the following output as the MX (Mailserver) value in your DNS server
 10 kiwibytesolutions.info
 Add this as a new MX record where the Record name is kiwibytesolutions.info
 Add an SPF record
 v=spf1 mx ip4:11.111.111.111 -all
 Add this as a new TXT record where the Record name is kiwibytesolutions.info
 -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

In your DNS server, navigate to the section where you can edit DNS records. This will differ for every DNS provider but will look like the following.



Add record

□	TYPE	HOST NAME	VALUE	SERVICE ▲	ACTIONS
□	CNAME	_domainconnect	_domainconnect.ionos.com	Domain Connect	✎ ⊘
□	A	@	[redacted]	-	✎ 🗑
□	AAAA	@	[redacted]	-	✎ 🗑
□	MX	@	kiwibytesolutions.info	-	✎ 🗑
□	TXT	@	"v=spf1 mx ip4:[redacted] -all"	-	✎ 🗑
□	TXT	_dmarc	"v=DMARC1; p=reject; rua=mailto: mailarchiv...	-	✎ 🗑
□	TXT	default._domainkey	"v=DKIM1; h=sha256; k=rsa; p=[redacted].	-	✎ 🗑
□	A	www	[redacted]	-	✎ 🗑
□	AAAA	www	[redacted]	-	✎ 🗑

You will need to set up six records. The specific values are specified in the output from your container.

MX record: An MX record routes emails to your specific email server.

SPF record: SPF stands for secure policy framework and specifies which servers are authorised to send emails from a particular domain.

DMARC record: DMARC stands for Domain-based Message Authentication. It helps prevent attackers from spoofing your domain and also helps with email deliverability. Both Google and Yahoo now require email domains to have DMARC records.

DKIM record: DKIM stands for DomainKeys Identified Mail and helps the receiver know that the email came from an authenticated domain name. Enabling DKIM also helps with email delivery rates. Enter it into your DNS record with the value name of default._domainkey.example.com, or copy and paste the value specified in the output from your container. Copy and paste the key into your container; note that each DNS server has different formatting specifications, so we have also included the output from the file so you can easily adjust the formatting if the output we've given does not fit the requirements.

To check if you've set everything up correctly, you can visit `https://mxtoolbox.com/` and enter your domain name. Note that domain names that are less than a week old will be placed on blacklists to prevent spam. After a week, your domain name should be cleared.

Setting up a Phishing Container

Introduction to GoPhish

GoPhish is an open-source phishing framework that allows you to create phishing campaigns with ease. There are many in-depth tutorials on how to use it, so we won't be covering it in detail here. But we will cover the basics to get you through. For more in-depth guides and information, please check out the official GoPhish documentation https://docs.getgophish.com/user-guide

To log in, you'll first need to get the initial generated admin password. GoPhish used to use admin:admin as the username and password, but now they generate automatically after you launch the application.

To view the logs of the docker application, you'll need to find the name of the docker container. Assuming you haven't changed anything, it should be autcyberscient23b_gophish_1.

In your terminal, use the following command to view the logs.

```
docker logs autcyberscient23b_gophish_1
```

Search for where the logs output the username admin and generated password.
It will look something like this.

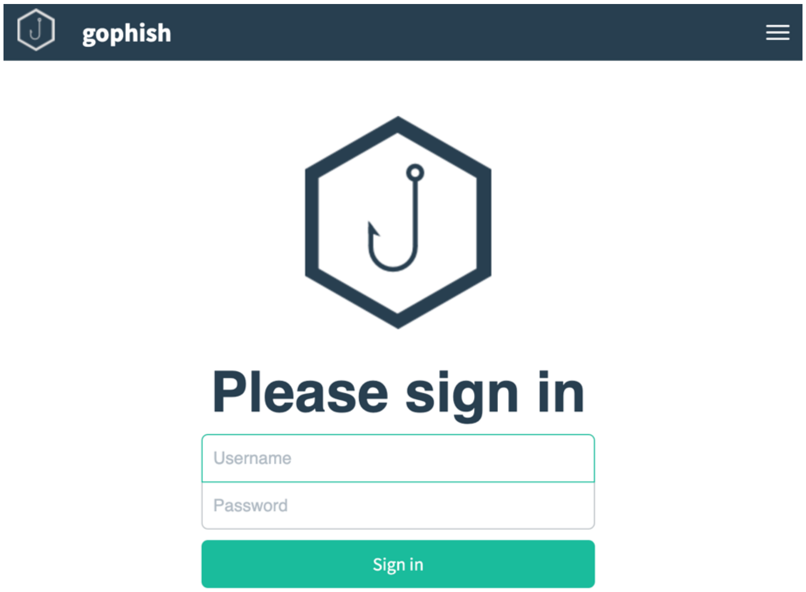
```
OK    20200914000000_0.11.0_last_login.sql
OK    20201201000000_0.11.0_account_locked.sql
OK    20220321133237_0.4.1_envelope_sender.sql
time="2024-04-04T00:17:29Z" level=info msg="Please login with the username admin and the password
e00000000000"
time="2024-04-04T00:17:29Z" level=info msg="Starting IMAP monitor manager"
time="2024-04-04T00:17:29Z" level=info msg="Creating new self-signed certificates for administration
interface"
time="2024-04-04T00:17:29Z" level=info msg="Background Worker Started Successfully - Waiting for
Campaigns"
time="2024-04-04T00:17:29Z" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2024-04-04T00:17:29Z" level=info msg="Starting new IMAP monitor for user admin"
time="2024-04-04T00:17:29Z" level=info msg="TLS Certificate Generation complete"
```

If you are having difficulty finding the username and password, you can use the command.

```
docker logs autcyberscient23b_gophish_1 | grep --color=always "Please login with the username"
```

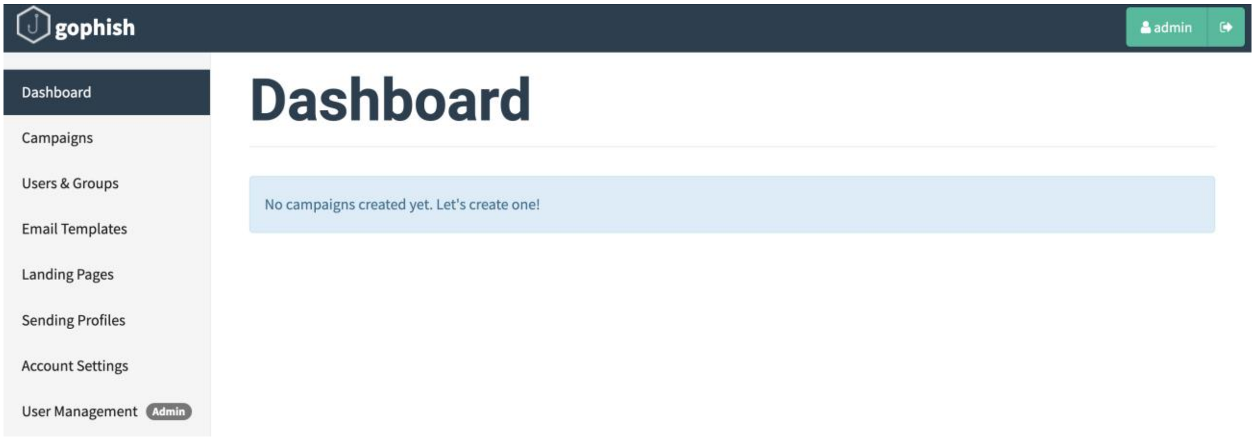
Navigate to the admin webpage at

https://yourdomainname.com:3333.



After logging in, you'll be prompted to change your password. Choose a strong password with unique, mixed characters and longer than 12 characters. Keep it safe, as you'll need to restart the container if you forget it. You will lose all your data if you forget this password.

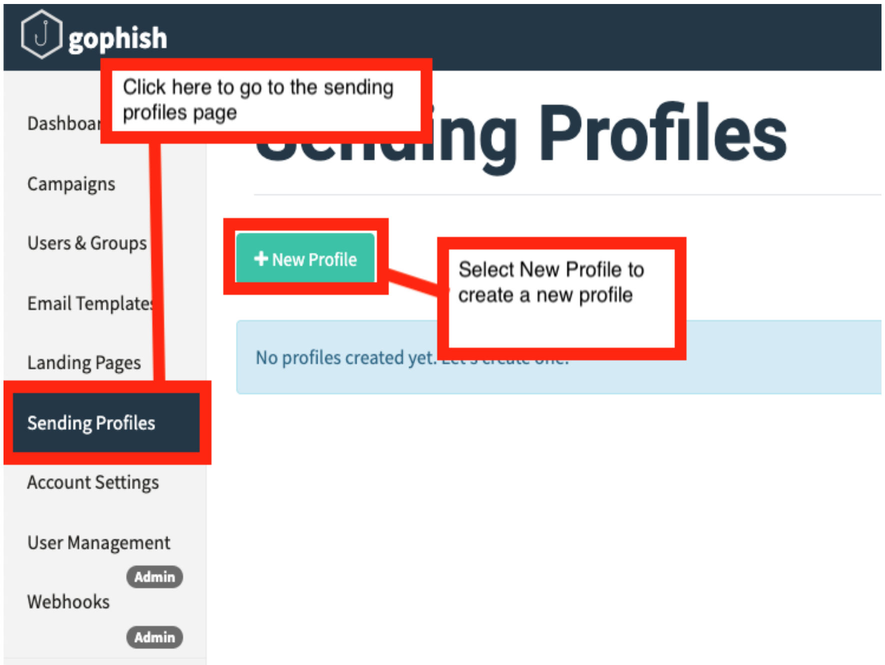
Congrats! You should now be logged in!



No campaigns created yet. Let's create one!

Setting up Sending Profiles

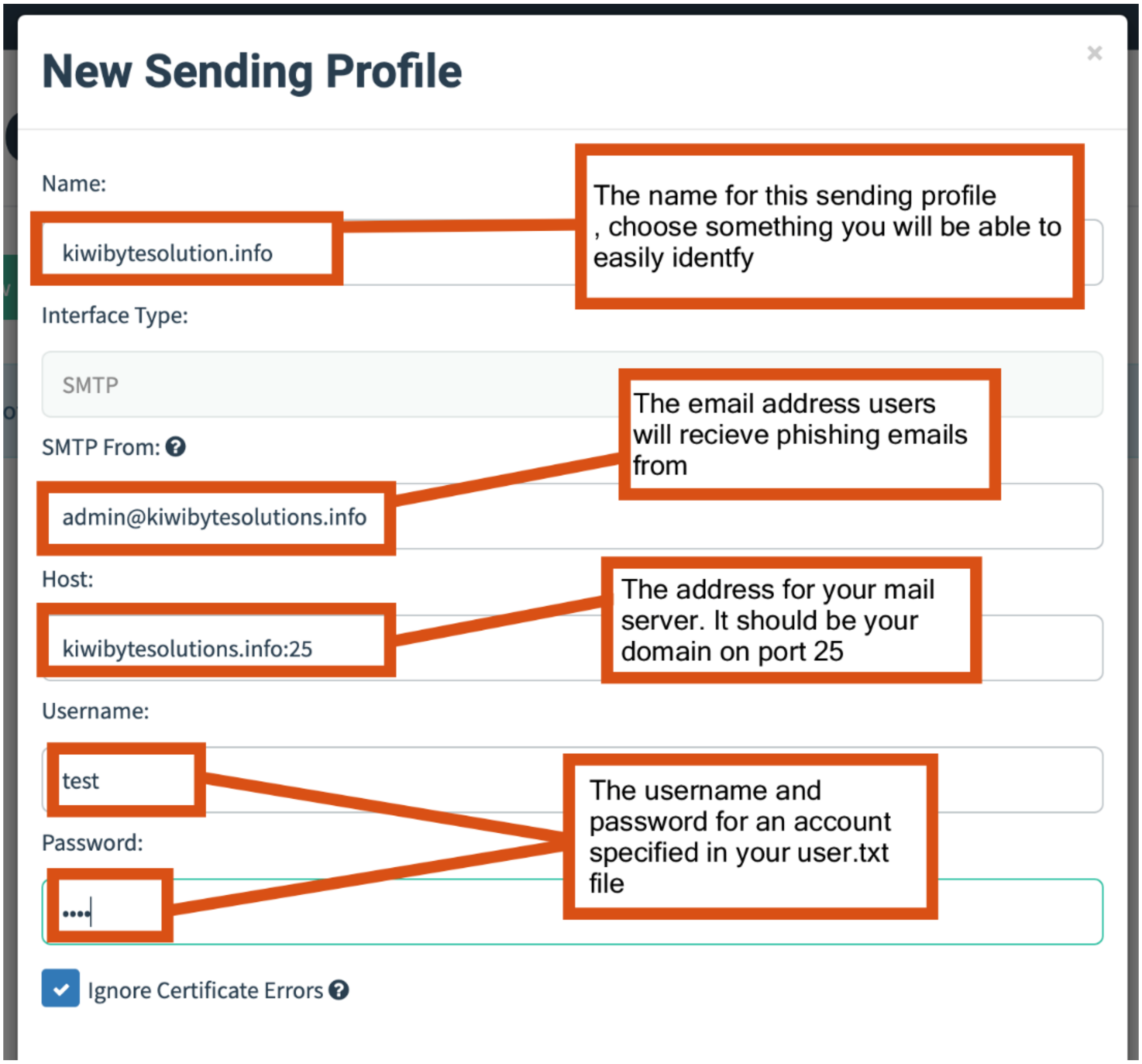
If you have correctly set up your Postfix server, you should be able to set up a sending profile. These will be the accounts to which you send the phishing emails. If you have multiple domain names and email servers up and running, you can manage them all from here. Firstly, go to the sending profile page and create a new profile.



Click here to go to the sending profiles page

Select New Profile to create a new profile

Assign a name to the sending profile that's easily recognisable when you create your campaign. You'll also need to login to your postfix server in which you've just created. The hostname should be your domain at port 25, and the username and password should be specified, and account specified the `/emaildocker/src/user.txt` file.



New Sending Profile

Name: kiwibytesolution.info

The name for this sending profile , choose something you will be able to easily identfy

Interface Type: SMTP

SMTP From: admin@kiwibytesolutions.info

The email address users will recieve phishing emails from

Host: kiwibytesolutions.info:25

The address for your mail server. It should be your domain on port 25

Username: test

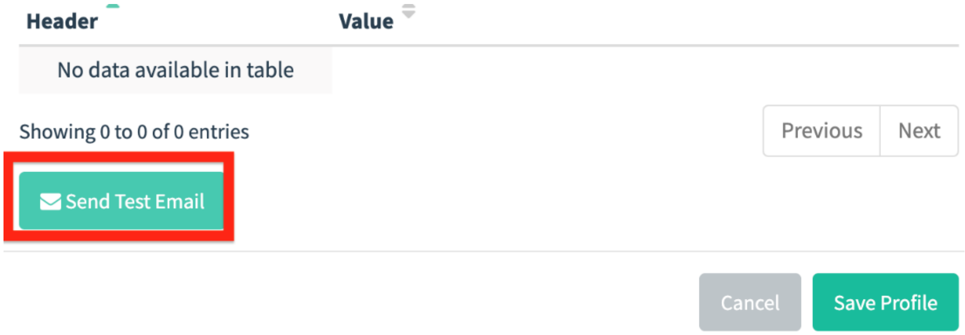
Password: ••••

The username and password for an account specified in your user.txt file

☑ Ignore Certificate Errors

Testing Sender Profiles

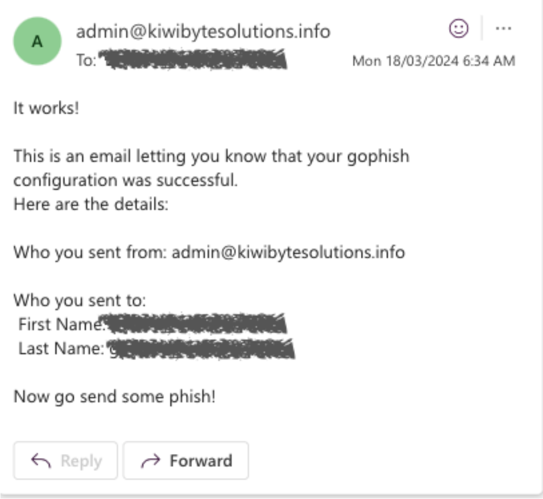
Send a test email to an email address you own to test that the sending domain works.



Header	Value
No data available in table	

Showing 0 to 0 of 0 entries

If you set everything up correctly, you should receive an email like the one below.



A admin@kiwibytesolutions.info
To: [redacted]
Mon 18/03/2024 6:34 AM

It works!

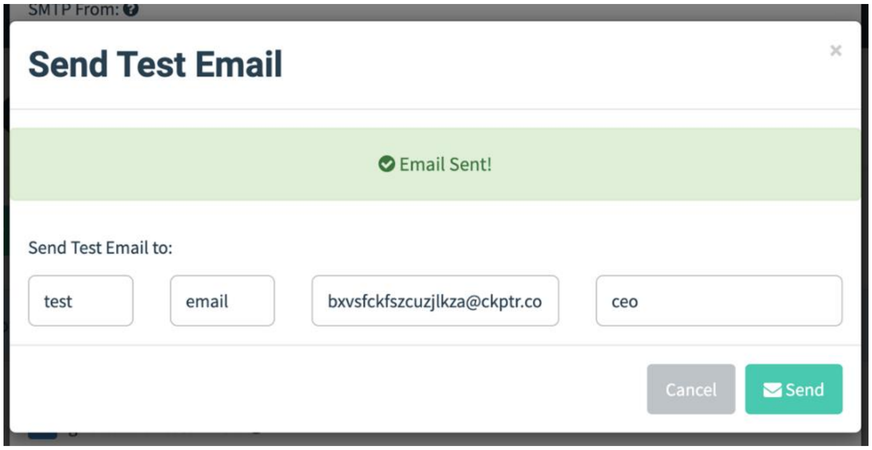
This is an email letting you know that your gophish configuration was successful.
Here are the details:

Who you sent from: admin@kiwibytesolutions.info

Who you sent to:
First Name: [redacted]
Last Name: [redacted]

Now go send some phish!

Note that it may be in your spam inbox if you have yet to whitelist your domain name.



Send Test Email

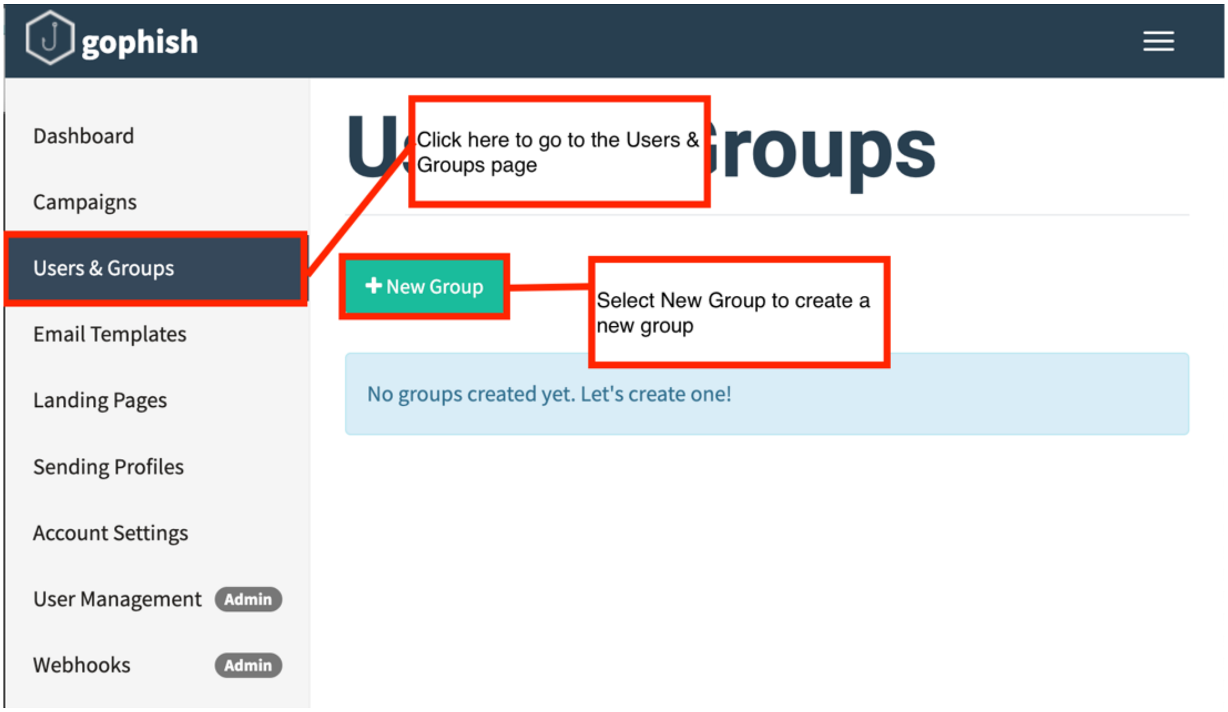
Email Sent!

Send Test Email to:

test	email	bxvsfckfszcuzjlkza@ckptr.co	ceo

Setting up User Profiles

You'll want to create a list of all the users for whom you want to run a phishing awareness training campaign. Select the user & groups page from the side bar.



Click here to go to the Users & Groups page

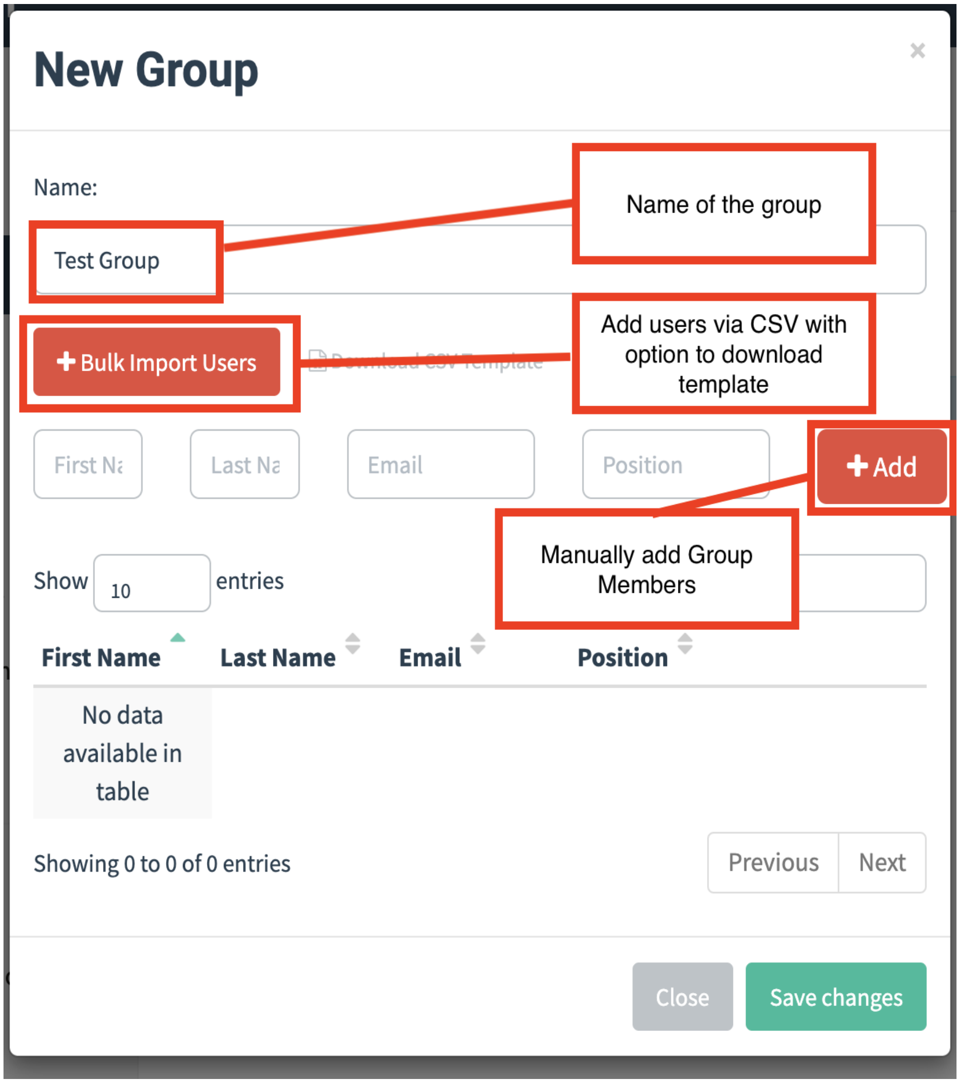
Select New Group to create a new group

No groups created yet. Let's create one!

To do that, we'll create a new user group. You'll need to give the user group an identifiable name which you can recognize when creating a campaign. You can select multiple groups in a campaign, so you may want to organise the groups based on company department or office location.

You can add each user individually or import a CSV file with a list of all the users.

Please make sure to include the headers, First Name, Last Name, Email, and Position so that GoPhish knows what the specific sections are.



New Group

Name: Test Group

Name of the group

Add users via CSV with option to download template

Manually add Group Members

Show 10 entries

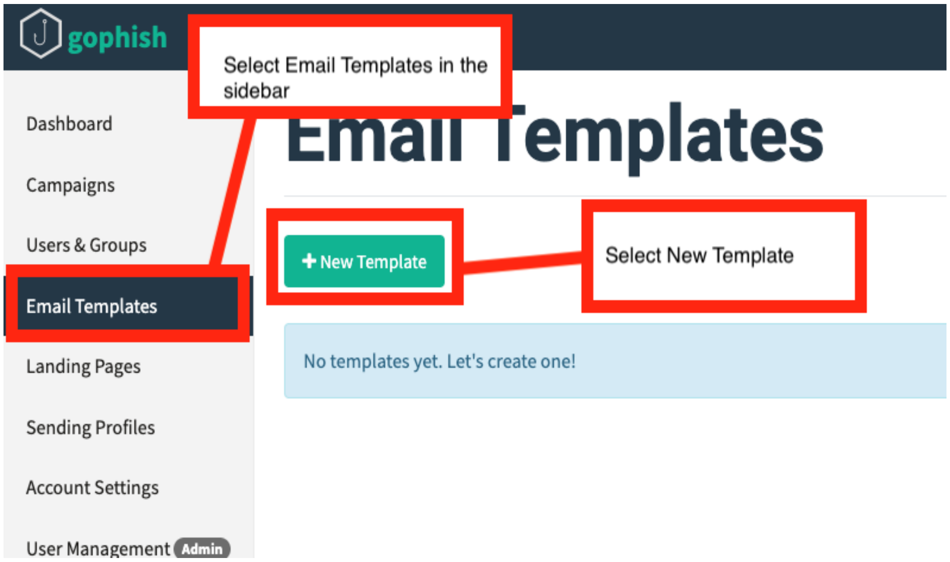
First Name	Last Name	Email	Position
No data available in table			

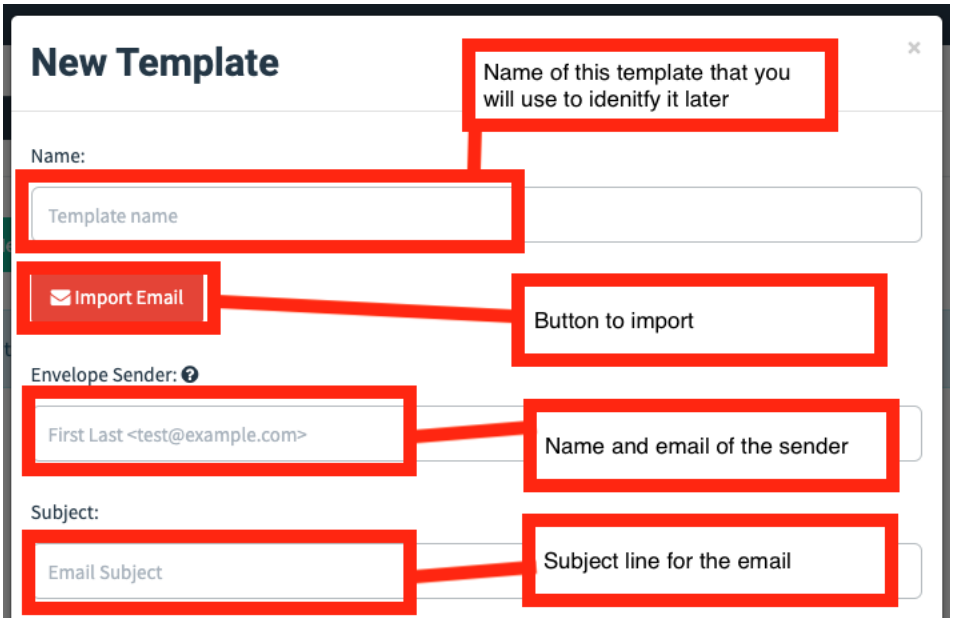
Showing 0 to 0 of 0 entries

Importing email templates

How you set up your email templates is important to the success of the phishing campaign. The more sophisticated the email, the harder it is for users to identify whether it is a phishing attempt. Your emails need to be realistic but not too complex so that your employees get experience with real-world attacks and can apply their learnings.

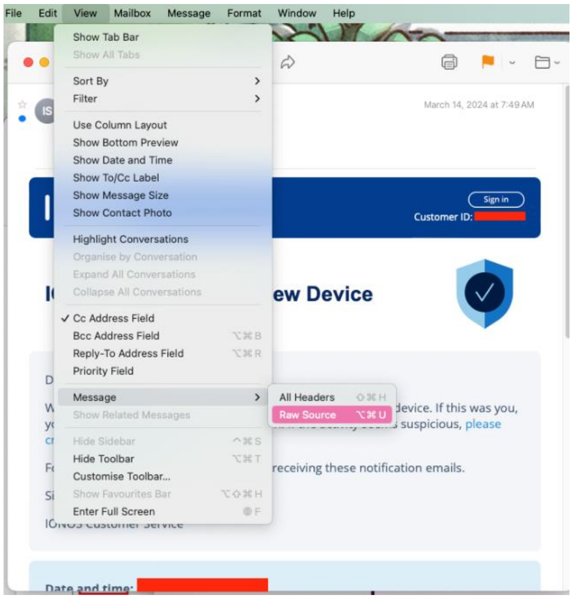
Select Email Template from the sidebar and click New Template to create a new email template.

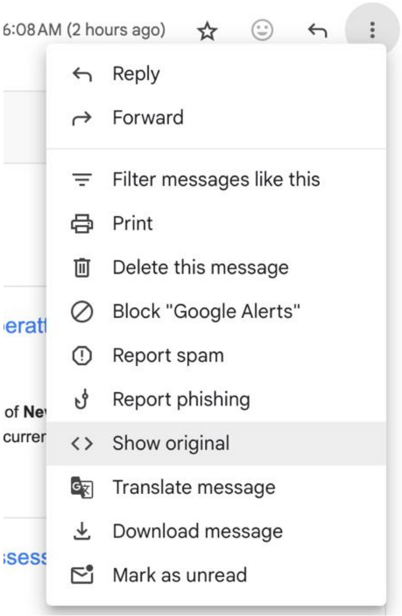


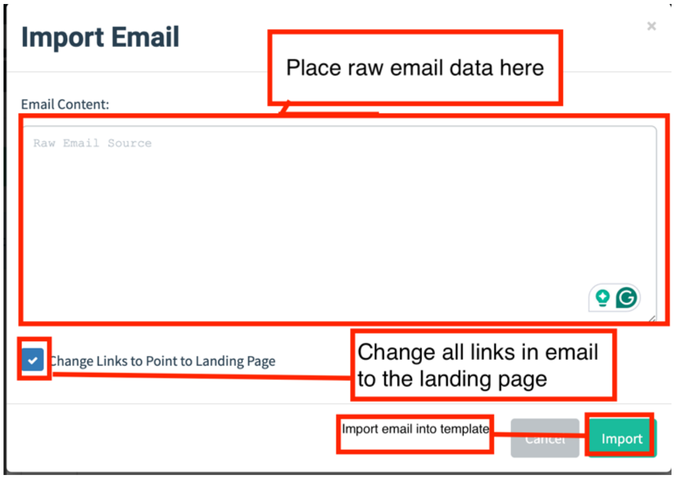

New Template
Name of this template that you will use to idenitfy it later
Name:
Template name
Import Email
Button to import
Envelope Sender:
First Last <test@example.com>
Name and email of the sender
Subject:
Email Subject
Subject line for the email

When designing your email template in Gophish, you have several options to create a compelling message. You can use plaintext for simple messages or start by choosing the "HTML" editor option, allowing you to craft a custom HTML email tailored to your campaign. You can utilize the built-in tools provided by Gophish or external HTML editors for more advanced customization. You can also import an HTML template from repositories like the one below.
https://github.com/criggs626/PhishingTemplates/tree/master/emails

We recommend importing from emails you've already received as this is the most realistic and easiest way to import emails. To import you will need to capture the raw source of the email, which will look like the following: Different email providers have different methods of retrieving the raw source, so it is best to Google how.





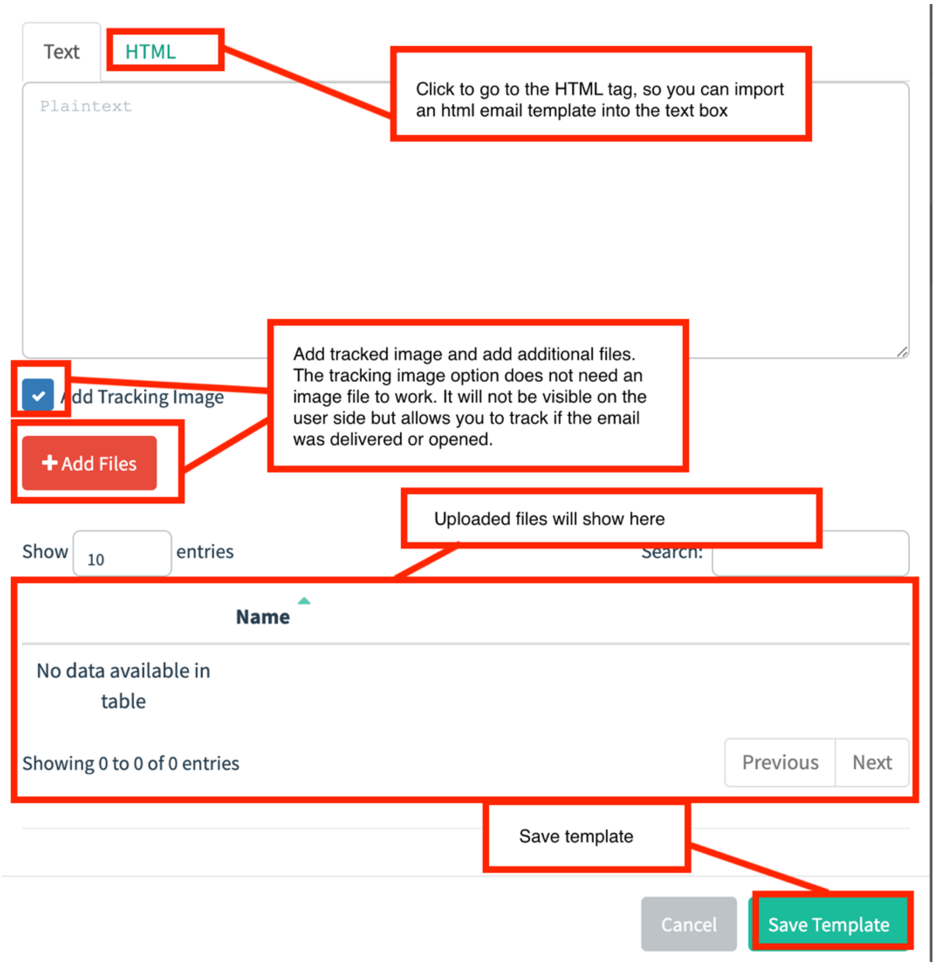


Place raw email data here

Change all links in email to the landing page

Import email into template

GoPhish also allows you to add attachments to the email. You can attach PNG, PDF, Word, etc., to track user data and input. This is still an experimental feature, but more information about how to do it can be found on the GoPhish Docs.https://docs.getgophish.com/user-guide/documentation/attachments



Click to go to the HTML tag, so you can import an html email template into the text box

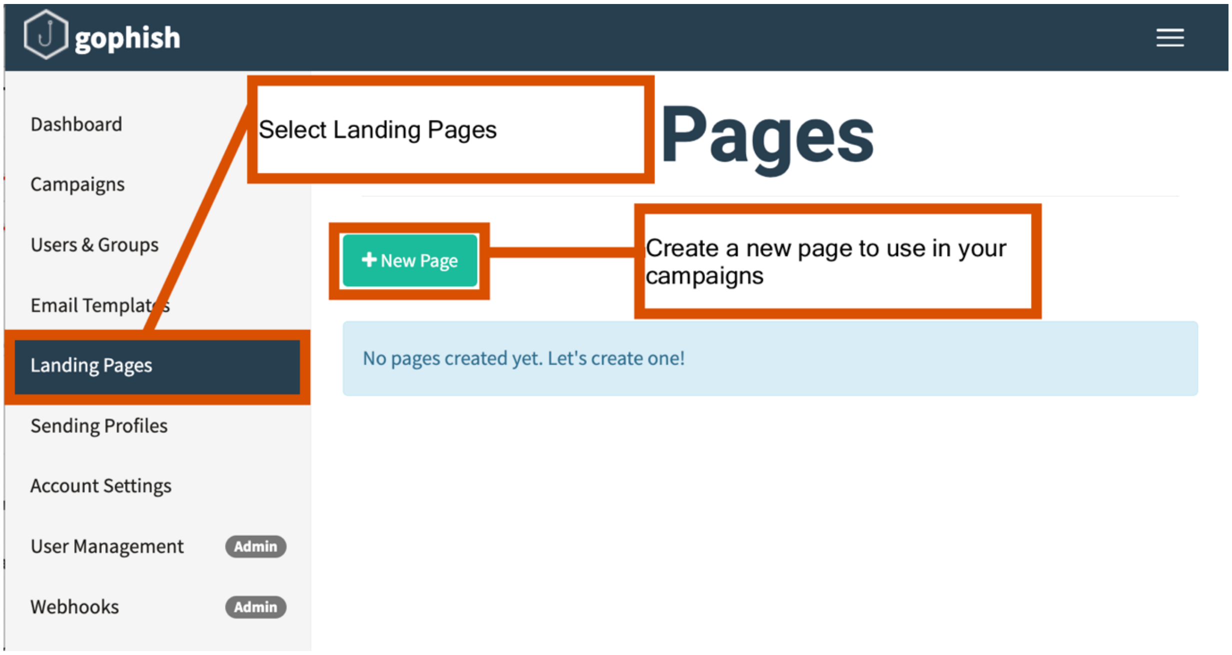
Add tracked image and add additional files. The tracking image option does not need an image file to work. It will not be visible on the user side but allows you to track if the email was delivered or opened.

Uploaded files will show here

Save template

Setting up Landing Pages

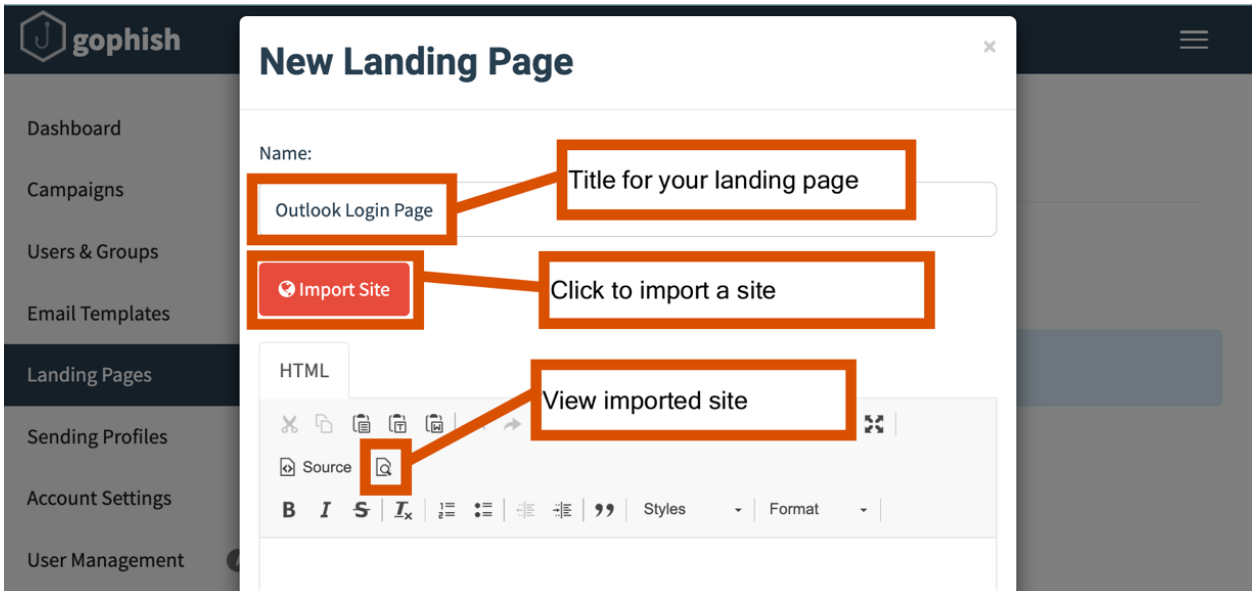
The landing page is when user click into your link, this is where you want them to be directed to. Select Landing Pages in the side panel and select the new page button.



Select Landing Pages

Create a new page to use in your campaigns

You need to set up a name for your landing page, we recommend choosing something that can be easily identified.



Name: Outlook Login Page

Import Site

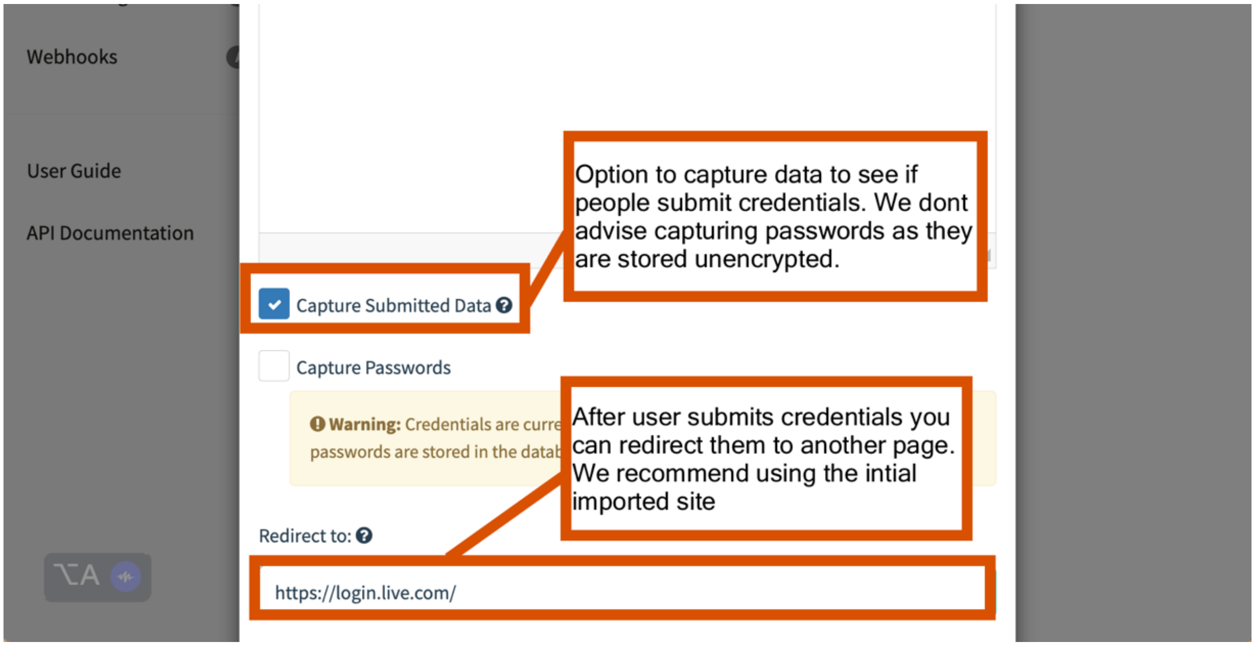
Title for your landing page

Click to import a site

View imported site

You have two options for the creation of the landing page. You can import any website on the Internet, this will be depending on the nature of the phishing campaign, a website that more relevant to the campaign will be more effective. You can also import site via HTML. With HTML, it is highly customizable to fit with your demand and campaign.

With GoPhish, you can also capture submitted data, if the landing has a form, every input data will be captured except password. You can also redirect user to another landing page once their credential is submitted. These are useful in a campaign as you can automatically redirect user to awareness docs if they fall for the phishing.



☑ Capture Submitted Data

□ Capture Passwords

Warning: Credentials are curre
passwords are stored in the datab

Redirect to:

https://login.live.com/

Option to capture data to see if people submit credentials. We dont advise capturing passwords as they are stored unencrypted.

After user submits credentials you can redirect them to another page. We recommend using the intial imported site

Launching your phishing campaign

Planning

So you have your phishing instance and are ready to start phishing! But wait, there are a number of things to consider before you begin testing your employees.

Notification:

It is unfair to send a phishing email to your employees without educating them about what phishing is. If employees receive such an email from their local IT team without prior knowledge, they may feel tricked or deceived. Although you may choose to keep the phishing engagement a secret to gather more accurate results, it is essential to note that employees may feel misled if not alerted prior.

You will want to clearly communicate to staff the process of reporting phishing emails and how to do it. In addition, it is crucial to emphasise that even if they are unsure, they should still flag emails as potential phishing attempts. False positives are better than missing a phishing email altogether. It is also important to educate employees on the signs of phishing and how to distinguish a phishing email from a legitimate one. You'll want to stress the purpose of this training, which is to protect customers, the company, and most importantly, the staff from cyber criminals.

Education

You'll want to educate employees on the signs of phishing regularly. Once a year or a few times, employees will likely forget how to recognise phishing in their active recall. Repeating education monthly lets employees pick up on the signs of phishing without causing an additional burden on their memory, alongside their daily work priorities. It's essential to make the training engaging and sustainable so that employees not only retain the information but are also entertained while learning. Failure to do so can lead to cybersecurity fatigue, where employees become overwhelmed by new information and fall into bad security practices for convenience.

Creating Training modules

Recent studies have found that short-form videos with quizzes for education gamification led to better employee engagement. Traditional methods such as webinars or PowerPoint slides may not be as effective as they can be boring and lead to a loss of interest among the employees.

Using phishing awareness posters around the office
One effective way to create awareness about phishing is by using eye-catching posters around the office. These posters can include relevant designs and provide a friendly reminder to employees about the signs to look out for in phishing attacks. These posters help to create a security-focused culture in the office by subconsciously reminding employees of what to do in case of a phishing attack.

Informative emails
Emails can also be an informative way to educate employees about phishing attacks. It's particularly important to send out such emails after an employee has fallen for a phishing attack. This helps them understand what happened and what they should look out for in the future.

Other considerations:

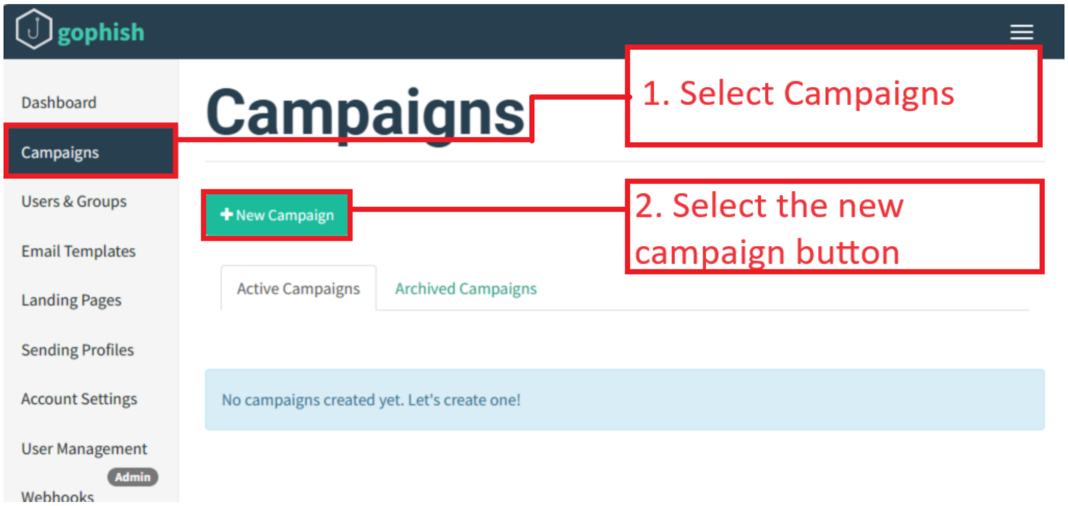
Get approval from upper management
The goal of a phishing awareness campaign is to improve a company's security culture. However, your efforts will not be successful without the support and approval of the upper management. It is crucial for them to encourage and educate employees about the importance of security actively. This will help create a security culture where everyone in the company is aware of the risks and consequences of a security breach. It will also ensure that employees know where to seek help. By doing so, security will not just be perceived as "something the IT guys do", but everyone on board will understand and take responsibility for it.

Bringing everything together

Now it's time to bring everything together!

Launching a Campaign

In the GoPhish dashboard, select Campaign and then select the new campaign button.

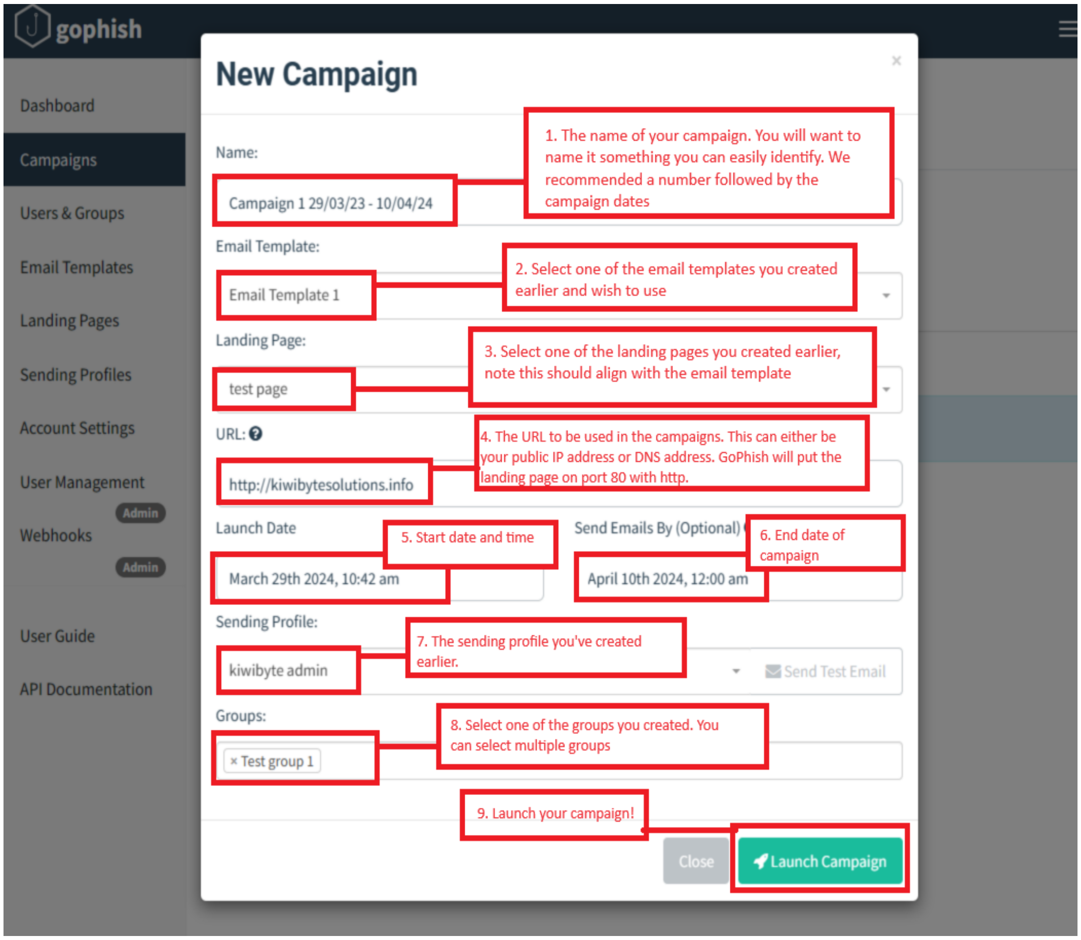


1. Select Campaigns

2. Select the new campaign button

No campaigns created yet. Let's create one!

You'll be prompted to fill out the campaign details using the emails, landing, sending, and group template you created earlier.



Name: Campaign 1 29/03/23 - 10/04/24

1. The name of your campaign. You will want to name it something you can easily identify. We recommended a number followed by the campaign dates

Email Template: Email Template 1

2. Select one of the email templates you created earlier and wish to use

Landing Page: test page

3. Select one of the landing pages you created earlier, note this should align with the email template

URL: http://kiwibytesolutions.info

4. The URL to be used in the campaigns. This can either be your public IP address or DNS address. GoPhish will put the landing page on port 80 with http.

Launch Date: March 29th 2024, 10:42 am

5. Start date and time

Send Emails By (Optional): April 10th 2024, 12:00 am

6. End date of campaign

Sending Profile: kiwibyte admin

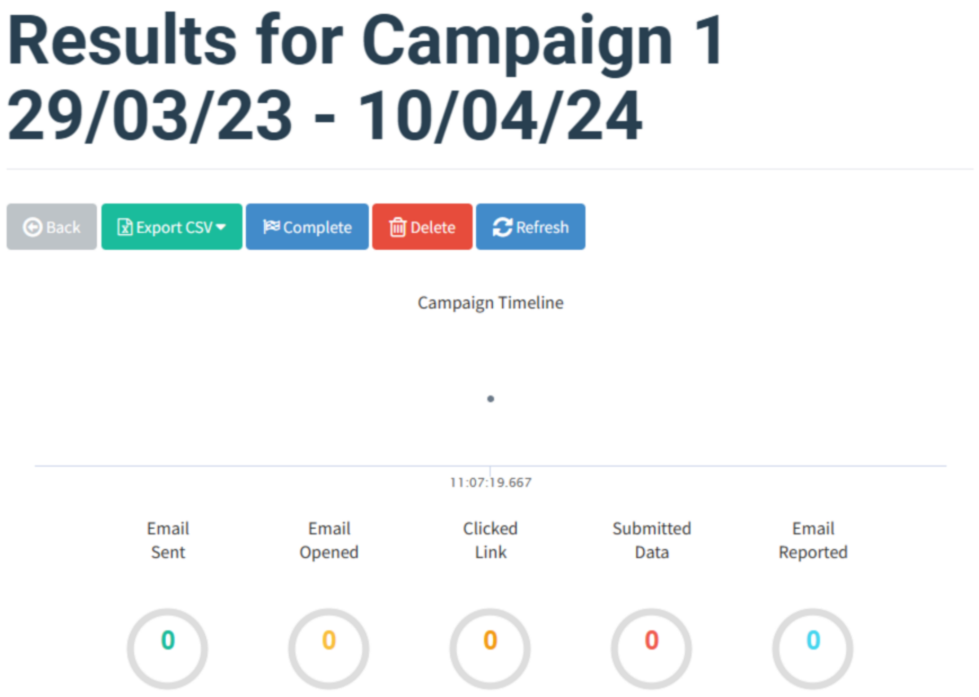
7. The sending profile you've created earlier.

Groups: × Test group 1

8. Select one of the groups you created. You can select multiple groups

9. Launch your campaign!

After you launch the campaign, you’ll be taken to the campaign results page.



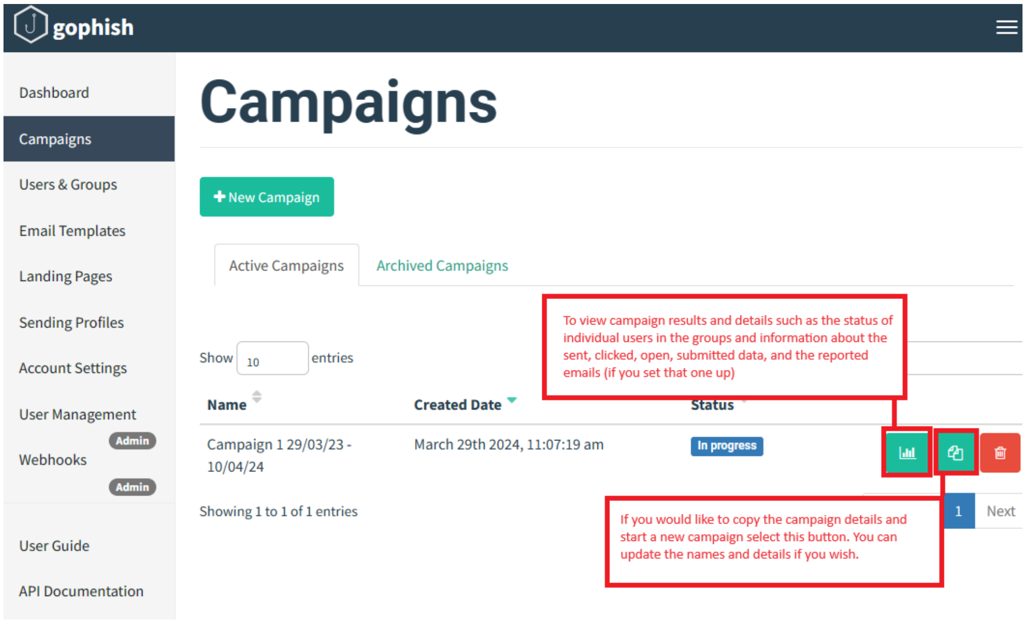
Results for Campaign 1
29/03/23 - 10/04/24

Email Sent 0
Email Opened 0
Clicked Link 0
Submitted Data 0
Email Reported 0

The report page is an important page that allows you to get insights into your campaign's progress and the status of everyone as emails are sent.

Open rate: How many users opened the email?
Click rate: How many users clicked on the email?
Submitted Data Rate: How many users submitted data after clicking on the link?
Report Rate: How many users report the received email as phishing?

If you haven't conducted a phishing awareness campaign before, it's important to conduct an initial baseline assessment to identify the current vulnerabilities and behaviours of your staff. Based on the assessment, you can tailor education to focus on the indicators of phishing that most employees struggle with. The focus should be on increasing the report rate to ensure that users report any suspicious emails. Users who click on the link in the email or submit data require immediate retraining.



Name	Created Date	Status
Campaign 1 29/03/23 - 10/04/24	March 29th 2024, 11:07:19 am	In progress

To view campaign results and details such as the status of individual users in the groups and information about the sent, clicked, open, submitted data, and the reported emails (if you set that one up)

If you would like to copy the campaign details and start a new campaign select this button. You can update the names and details if you wish.

Learnings and Reporting

After a phishing awareness campaign, it is essential to analyse the metrics received and use them to improve the current training. The focus could be on specific factors that employees struggled to recognise as phishing or adjust it to more relevant topics or increase the difficulty level. It is imperative to understand why employees fail. It could be due to insufficient education or not covering a specific topic. A report should be made on the findings and shared with the wider business.

Rinse and Repeat

Congratulations on completing your first phishing campaign! Remember, security is an ongoing process that requires continuous education and improvement. Over time, you hope to see key metrics improve, such as increased reporting rates and decreased compromised credential rates.

Timeframe:
How often do you send phishing emails? Once a month? Once a quarter? Once a year? This is actually a topic that’s heavily debated. But many sources agree between 1 to 3 months is the sweet spot. Having too far of an interval between phishing awareness training means employees may forget what they've learned, while too little won't allow them to learn and improve from past phishing attempts. We recommend a timeframe between 2-3 months to allow for sufficient re-education and for procedures and policies to be built off the previous campaign.

Note:

Positive Reinforcement:
Being told that you are doing badly all the time will make anyone feel frustrated or demotivated. Studies have shown that rewarding employees for good behaviour leads to better outcomes in phishing reporting. If employees are only reprimanded when they fall for a phishing email, they may become hesitant to report suspicious emails altogether. This is not the outcome we want. Instead, encourage employees to report any email that they suspect is a phishing attempt.

One effective approach is to recognise and reward those who identify and report phishing emails each month or those who share details from a recent phishing campaign with their team. You could even create challenges to incentivise teams to report the most phishing emails. It's important not to single out or punish specific users or departments who fail phishing simulations. Instead, we should focus on sharing the percentage of employees who avoid phishing attacks and reporting metrics.

Remediation

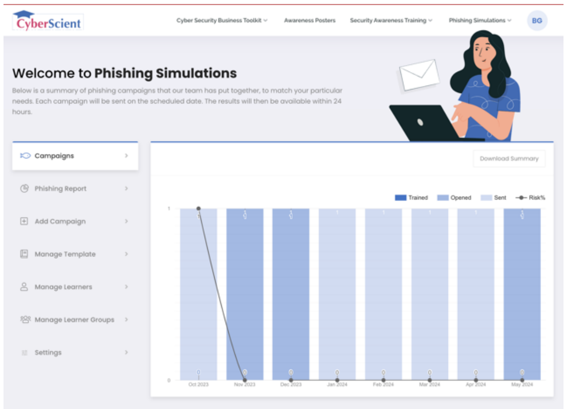
Instant feedback
If you have an employee that fails a phishing engagement test, you should let them know as soon as possible and provide them with feedback and further educational material on how to avoid phishing in the future.
Employees who didn’t pass the phishing engagement should have instant feedback on what went wrong. However, it's equally important to avoid shaming or embarrassing them for their failure. Instead, kindly inform them that they clicked on a phishing email link,

explain how to recognise, and report it in the future, and guide them towards training modules.

Consistent failures.
If an employee consistently fails phishing tests, it's a red flag that should be brought to the attention of upper management and HR. You may want to consider options like reducing their access permissions, isolating their actions, and understanding why they become repeat offenders. If the problem persists, it might be necessary to work with HR and legal teams to implement appropriate policies and remediation measures.

Conclusion

We hope this guide has been an informative and easy-to-use document on how to set up your own phishing campaigns on your own network. It's important to understand that setting up a phishing campaign for phishing awareness for your staff is complex. From configuring your domain name and DNS settings and email server to designing a campaign that effectively educates your employees about phishing, significant effort and time will be required. The initial setup of the baseline technologies is just the beginning, and we've strived to simplify this process for you.

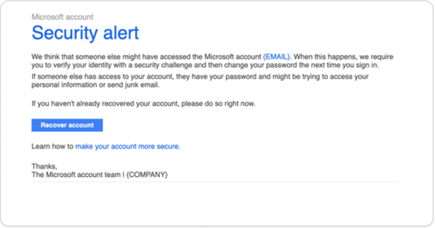


Welcome to **Phishing Simulations**

Below is a summary of phishing campaigns that our team has put together, to match your particular needs. Each campaign will be sent on the scheduled date. The results will then be available within 24 hours.

If you've read this document and feel a bit in over your head or know this is different from the amount of effort you would like to put in, consider CyberScient Pro plan. Similar to GoPhish, CyberScient's Pro plan allows you to create custom phishing awareness training campaigns to your organisation without the technical setup.
CyberScient user-friendly interface and intuitive design make it easy for anyone to operate, regardless of their technical skills. The platform offers more than 100 email templates with varying levels of difficulty to expose your staff to different types of phishing campaigns. With automated scheduling of phishing awareness training, you won't have to worry about timing or re-educating users if they fail a phishing

assessment.



Microsoft account

Security alert

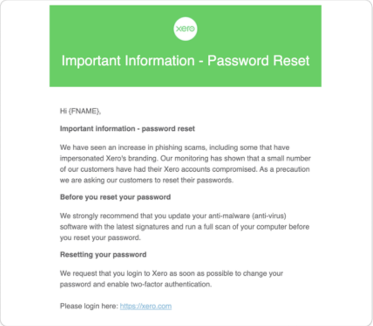
We think that someone else might have accessed the Microsoft account {EMAIL}. When this happens, we require you to verify your identity with a security challenge and then change your password the next time you sign in.

If someone else has access to your account, they have your password and might be trying to access your personal information or send junk email.

If you haven't already recovered your account, please do so right now.

Learn how to make your account more secure.

Thanks,
The Microsoft account team I {COMPANY}



Important Information - Password Reset

Hi {FNAME},

Important information - password reset

We have seen an increase in phishing scams, including some that have impersonated Xero's branding. Our monitoring has shown that a small number of our customers have had their Xero accounts compromised. As a precaution we are asking our customers to reset their passwords.

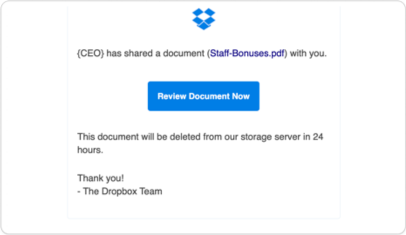
Before you reset your password

We strongly recommend that you update your anti-malware (anti-virus) software with the latest signatures and run a full scan of your computer before you reset your password.

Resetting your password

We request that you login to Xero as soon as possible to change your password and enable two-factor authentication.

Please login here: https://xero.com



{CEO} has shared a document (Staff-Bonuses.pdf) with you.

This document will be deleted from our storage server in 24 hours.

Thank you!
- The Dropbox Team

Combined with the rest of the CyberScient platform, such as the Security awareness training videos and posters, it will help ensure your cybersecurity awareness training is all-encompassing. While this document is here, if you would still like to set things up yourself, it may be more valuable for your time and organisation to use a service like CyberScient.

Future Improvements

This document provides the basics on how to start a phishing awareness campaign for your organisation. However, further improvements could be made regarding the security and functionality of the document and container.

This includes the following suggestions:
- Adding examples of email templates into the code base.
- Adding examples of relevant landing pages into the code base.
- Improving security by using asynchronous keys.
- Enhancing security by implementing hashed passwords in the mail server.
- Providing information on how to use tracked file types using GoPhish.
- Cleaning up code base with comments.

Thanks

We would like to thank CyberScient and AUT for their support throughout producing this documentation and project. We would also like the reference the following resources that were used to develop this documentation and our container.

References

Abdo, M. (2022, September 4). *itsmostafa/gophish-prod*. GitHub. https://github.com/itsmostafa/gophish-prod

Adlani, A. (2024, January 11). *Top ten impersonation techniques used in phishing domains*. EBRAND. https://ebrand.com/blog/top-ten-impersonation-techniques-used-in-phishing-domains/

Badman, A. (2023, August 9). *What is a phishing simulation?* IBM Blog. https://www.ibm.com/blog/phishing-simulation/

CERT NZ. (n.d.). *Phishing email scams*. Own Your Online. Retrieved May 8, 2024, from https://www.ownyouronline.govt.nz/personal/know-the-risks/common-risks-and-threats/phishing-email-scams/

CISA USA. (2024, April 4). *cisagov/postfix-docker*. GitHub. https://github.com/cisagov/postfix-docker

Contributor, I. H. (2020, March 11). *Install Let's Encrypt SSL on Ubuntu with Certbot | InMotion Hosting*. InMotion Hosting Support Center. https://www.inmotionhosting.com/support/website/ssl/lets-encrypt-ssl-ubuntu-with-certbot/

DigitalOcean. (n.d.). *How To Install Nginx on Ubuntu 20.04 | DigitalOcean*. Www.digitalocean.com. https://www.digitalocean.com/community/tutorials/how-to-install-nginx-on-ubuntu-20-04

Guoan (Admin), X. (2016, August 9). *How to Set up SPF and DKIM with Postfix on Ubuntu Server*. LinuxBabe. https://www.linuxbabe.com/mail-server/setting-up-dkim-and-spf

McDonough, B. (2022, December 15). *MFA Fatigue & Social Engineering Threaten Your Environment*. Agio.com. https://agio.com/how-mfa-fatigue-and-social-engineering-threaten-your-environment/

MxToolbox. (n.d.). *How to Setup DKIM*. MxToolbox. https://mxtoolbox.com/dmarc/dkim/setup/how-to-setup-dkim

Postfix. (n.d.). *Postfix Basic Configuration*. Www.postfix.org. https://www.postfix.org/BASIC_CONFIGURATION_README.html

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Landesberger, V., Volkamer, M., Lofthouse, B., Von Landesberger, T., & Niedersachsen, L. (2020). *An investigation of phishing awareness and education over time: When and how to best remind users An investigation of phishing awareness and education over time: When and how to best remind users*. https://www.usenix.org/system/files/soups2020-reinheimer_0.pdf

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. *DIGITAL HEALTH*, *8*, 205520762210817. https://doi.org/10.1177/20552076221081716

Tecadmin. (2022, December 1). *Setup DKIM (DomainKeys) with Postfix on Ubuntu & Debian*. Tecadmin. https://tecadmin.net/setup-dkim-with-postfix-on-ubuntu-debian/

Ubuntu. (2024). *Install and Configure Postfix*. Ubuntu.com. https://ubuntu.com/server/docs/install-and-configure-postfix