# Фишинг с gophish

## Клонирование репозитория

```
ildar@debian:~/ZIS/Phishing$ git clone https://github.com/Ivanhahanov/InformationSecurityMethodsAndTools.git
Cloning into 'InformationSecurityMethodsAndTools'...
remote: Enumerating objects: 916, done.
remote: Counting objects: 100% (916/916), done.
remote: Compressing objects: 100% (723/723), done.
remote: Total 916 (delta 169), reused 876 (delta 136), pack-reused 0
Receiving objects: 100% (916/916), 40.39 MiB | 5.85 MiB/s, done.
Resolving deltas: 100% (169/169), done.
ildar@debian:~/ZIS/Phishing$
```

## Запуск контенейра

```
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing$ ls
docker-compose.yml  Gophish  MailServer  README.md
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing$ docker-compose up -d
Creating network "phishing_default" with the default driver
Creating volume "phishing_maildata" with default driver
Creating volume "phishing_mailstate" with default driver
Creating volume "phishing_maillogs" with default driver
Pulling mailserver (tvial/docker-mailserver:latest)...
latest: Pulling from tvial/docker-mailserver
a076a628af6f: Pull complete
b5afddf182ca: Pull complete
5ebe891e3bb9: Pull complete
6884ed77b465: Pull complete
a7f3ed9aa5e0: Pull complete
67f2c647b931: Pull complete
957fffd1ae7c: Pull complete
1c4b0df1cd9e: Pull complete
```

## Создание сертификатов

```
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing$ docker run -it --rm -v "$(pwd)"/config/ssl:/tmp/docker-mailser
te-ssl-certificate
CA certificate filename (or enter to create)

Making CA certificate ...
====
openssl req  -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
..............................+++++
.................................+++++
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:Moscow
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MIREA
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:domain.com
Email Address []:admin@domain.com
```

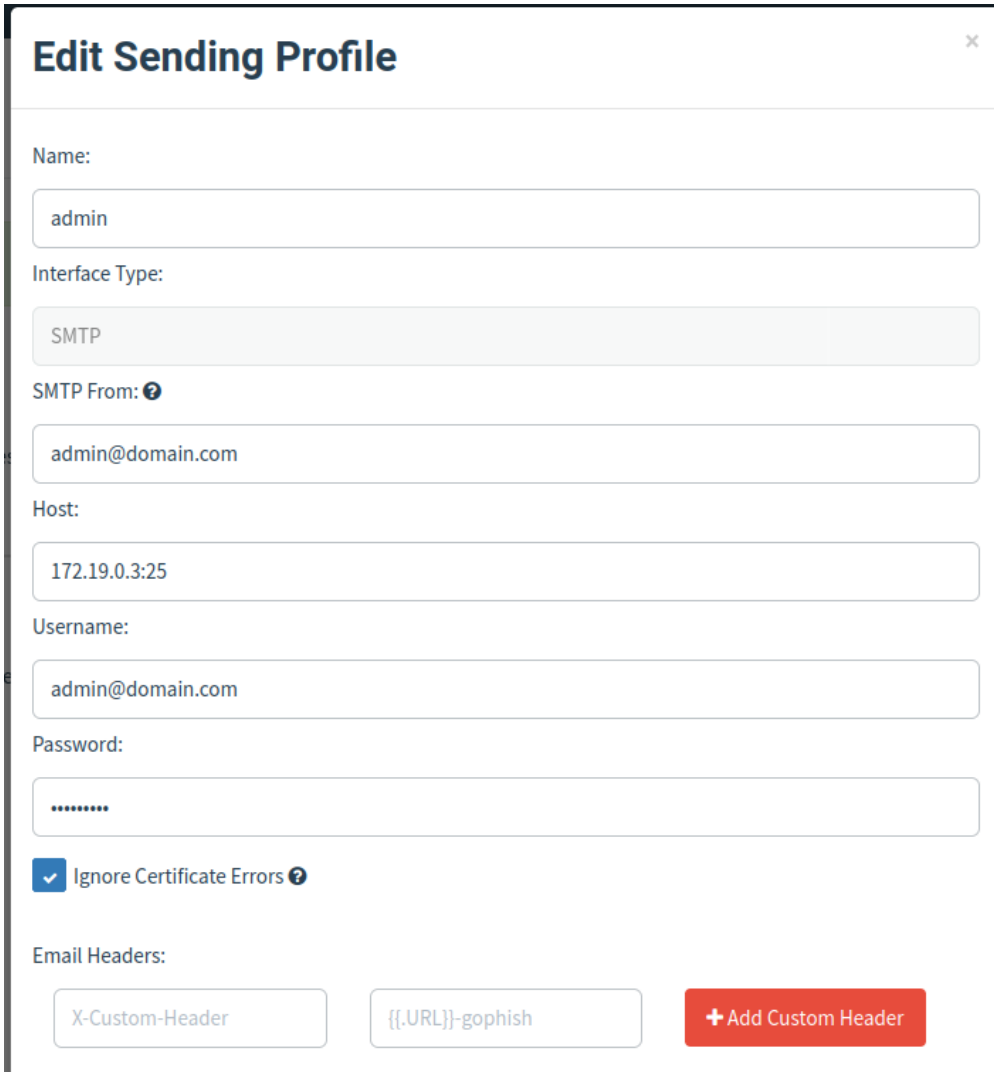
## Создание пользователей с пересборкой контейнера

```
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ ls
config  mailserver.env  setup.sh
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ chmod +x setup.sh
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ ./setup.sh -i tvial/docker-mailserver:latest email add
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ ./setup.sh -i tvial/docker-mailserver:latest email add
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ ./setup.sh -i tvial/docker-mailserver:latest email list
admin@domain.com
user@domain.com
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ docker-compose up --build -d
Starting mail    ... done
Starting gophish ... done
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$
```

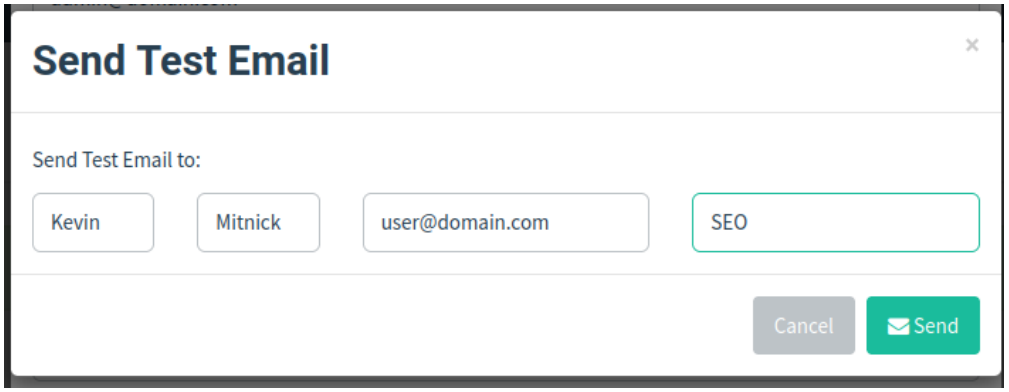
## Тестирование SMTP с помощью swaks

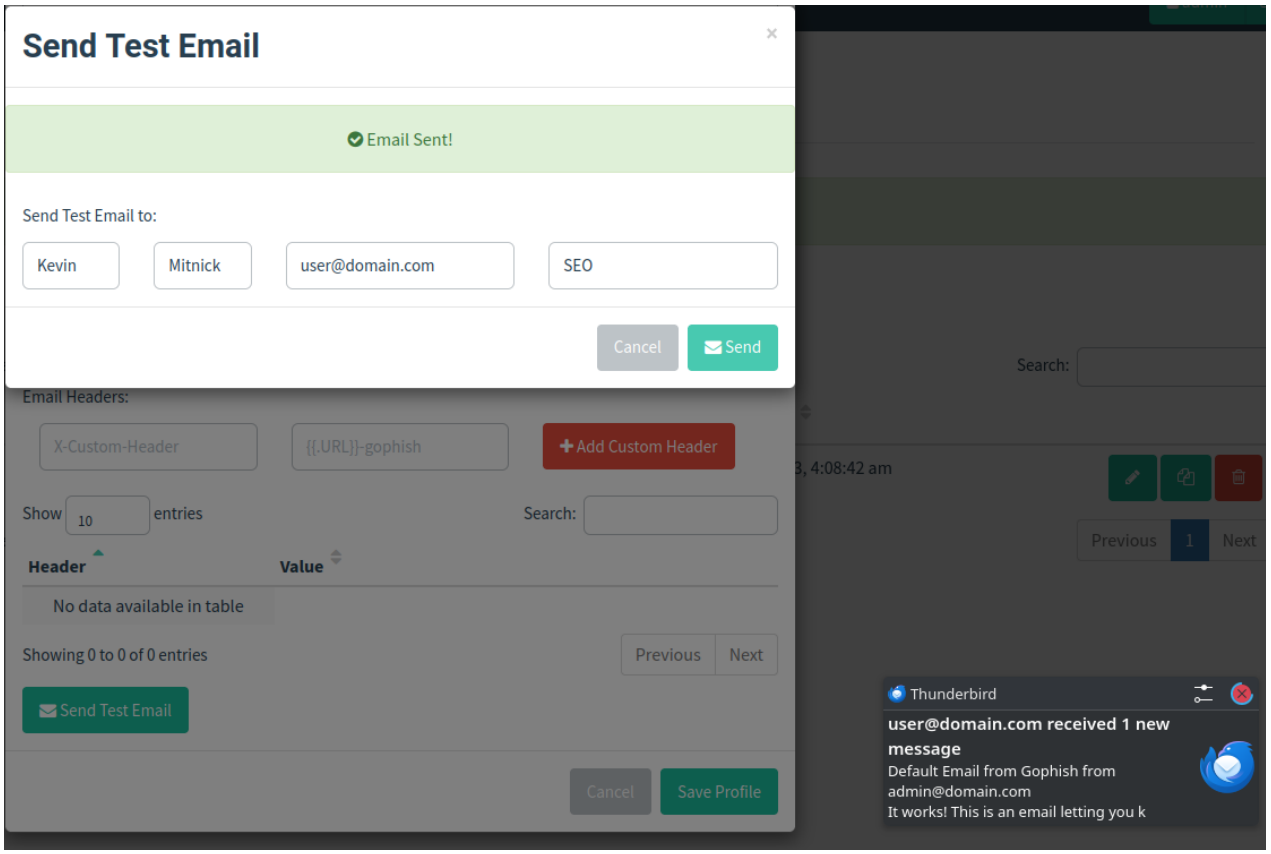
```
ildar@debian:~/ZIS/Phishing/InformationSecurityMethodsAndTools/Phishing/MailServer$ swaks --from admin@domain.com --to user@
23 --header "Subject: test from admin" --body "testing 123"
=== Trying 127.0.0.1:587...
=== Connected to 127.0.0.1.
<-  220 mail.domain.com ESMTP
 -> EHLO debian
<-  250-mail.domain.com
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-ETRN
<-  250-STARTTLS
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
```

## Sending profile

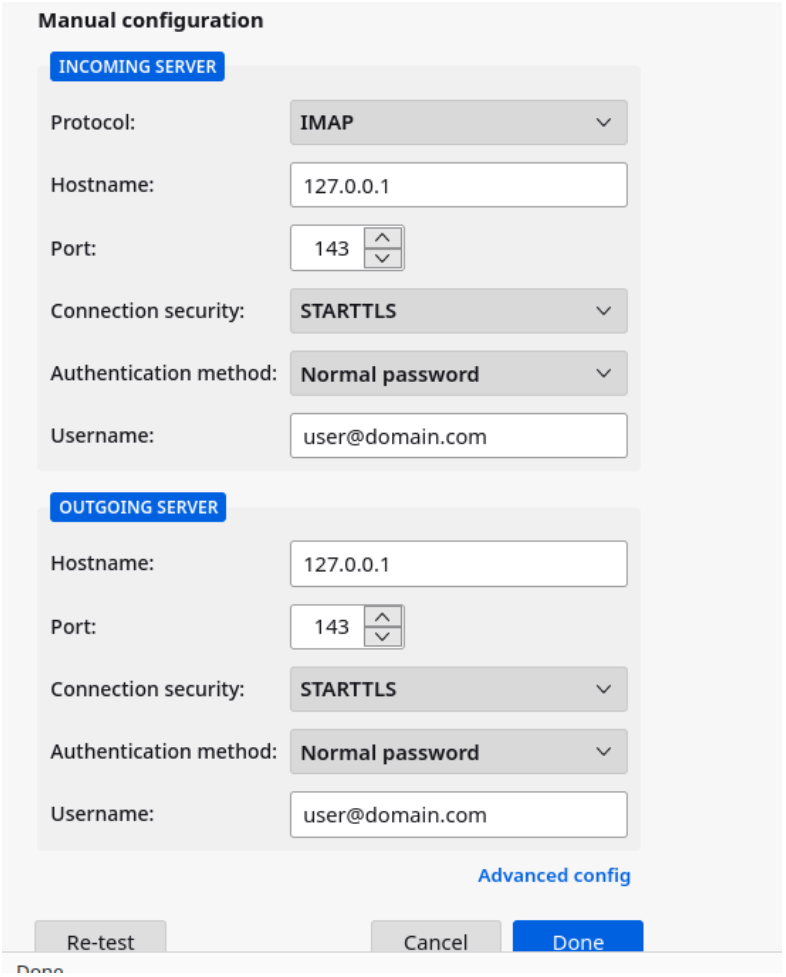



## Тестовое сообщение

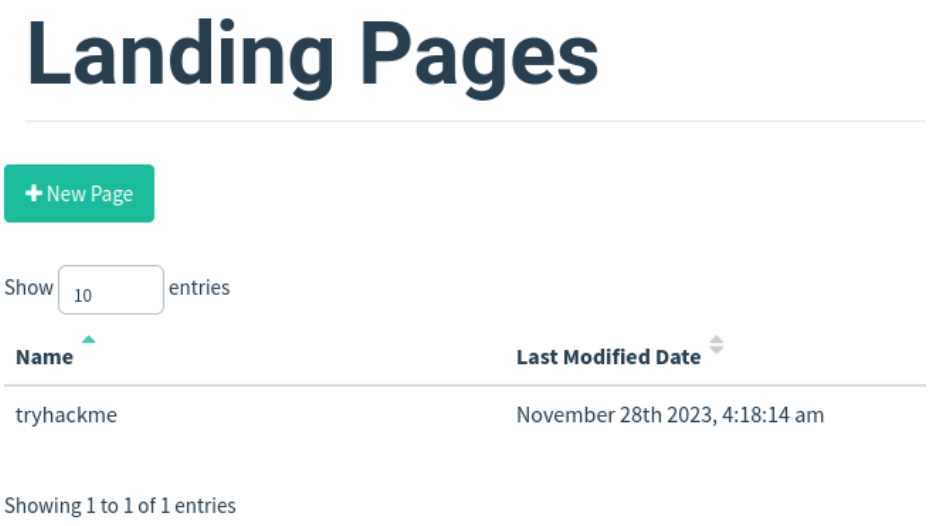


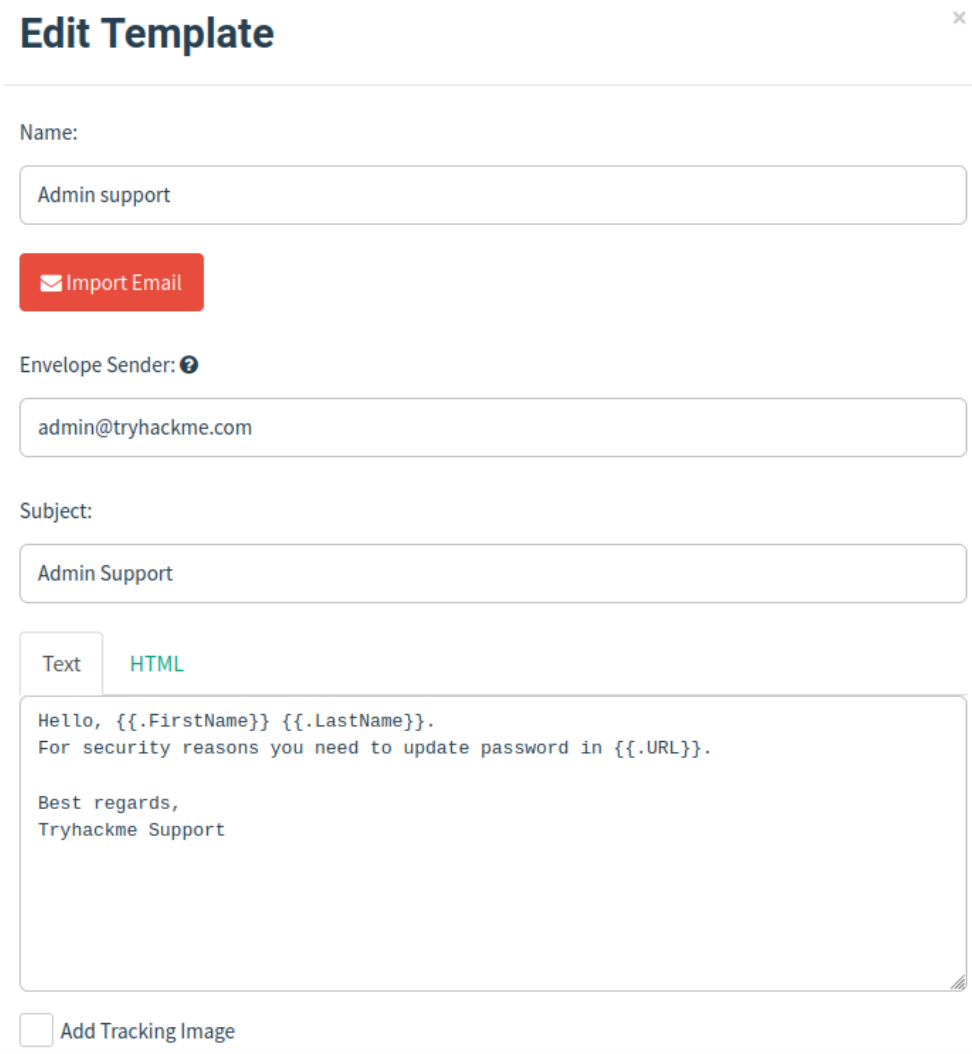

## Настройка почтового клиента ThunderBird



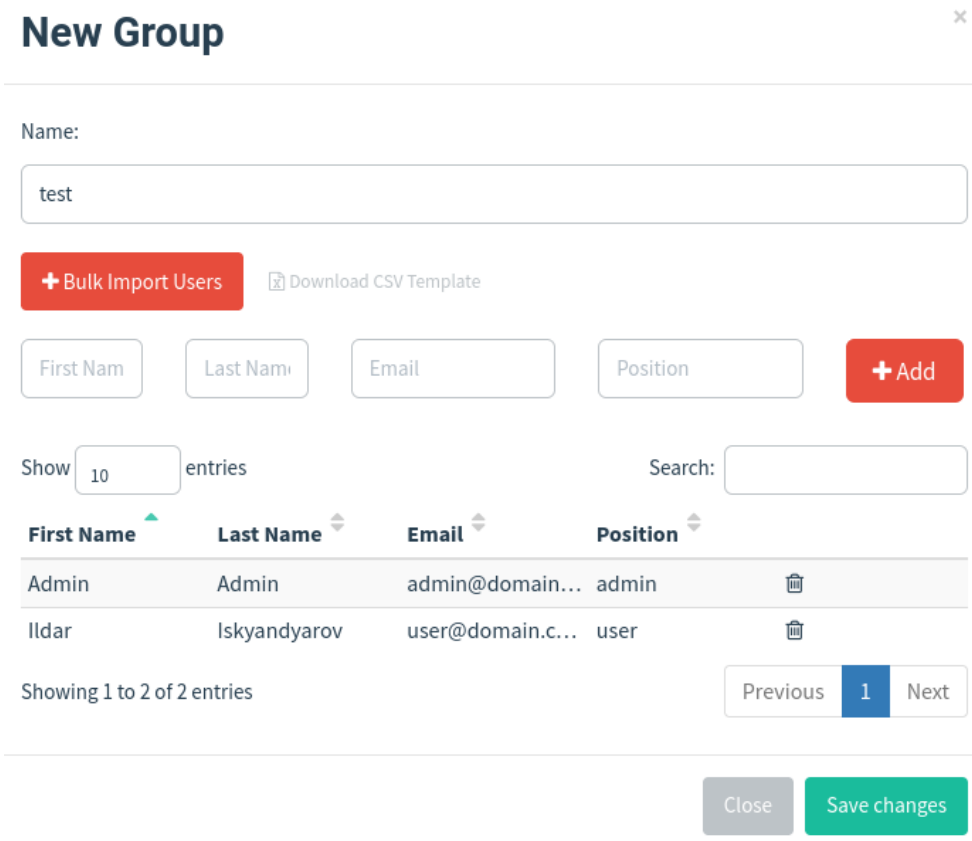

## Настройка фишинговой страницы



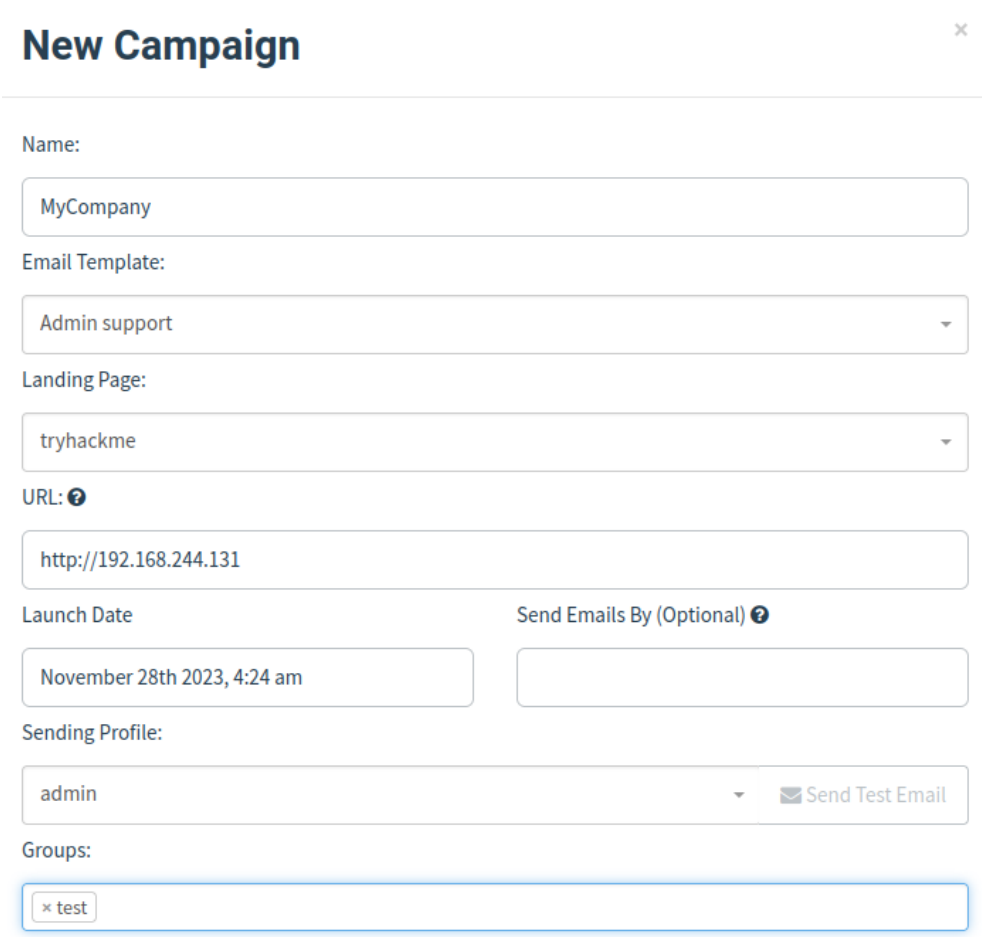

## Настройка шаблона фишингового письма



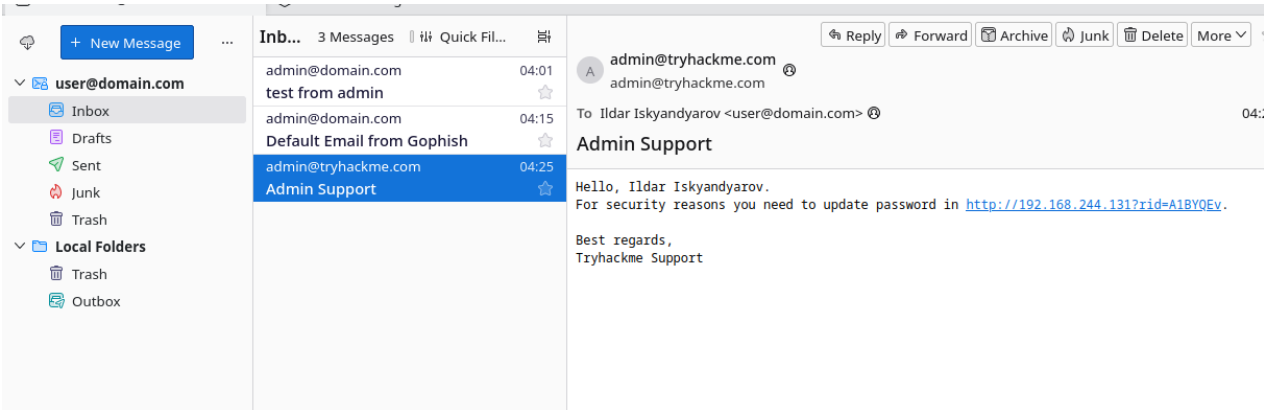

## Настройка получателей рассылки



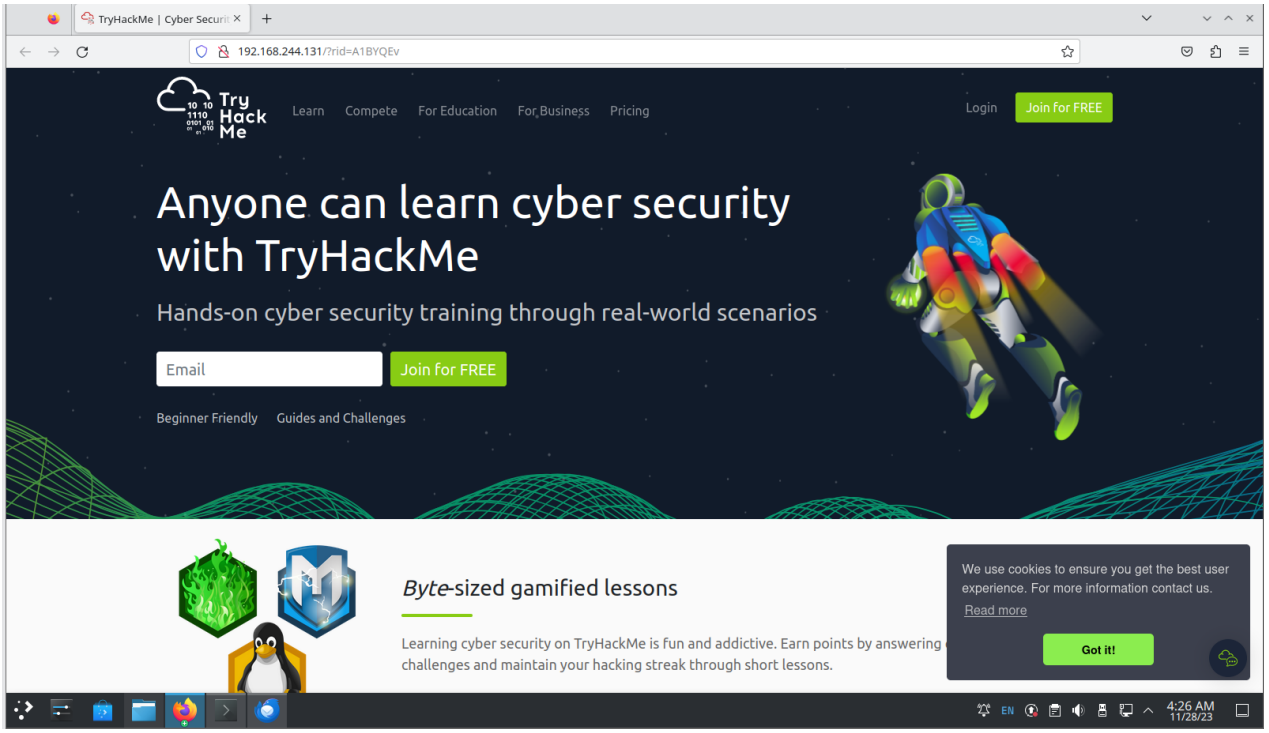
## Запуск фишинговой кампании



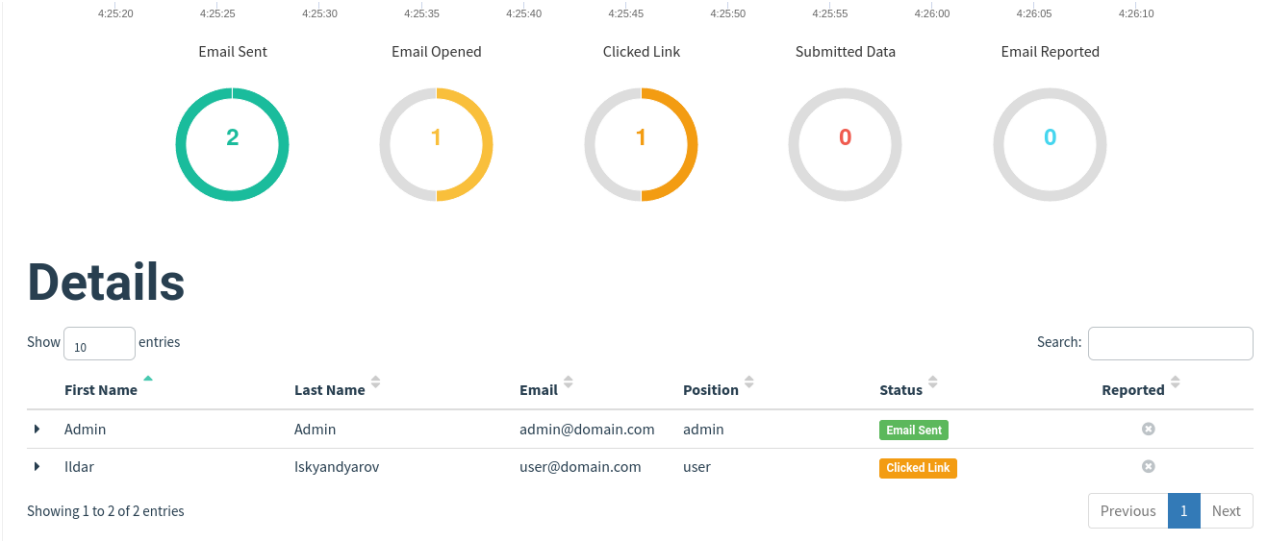

## Полученное сообщение




## Переход по ссылке из письма




## Статистика запущенной кампании




# Details

Show 10 entries

Search:

| | First Name | Last Name | Email | Position | Status | Reported |
|---|---|---|---|---|---|---|
| ▸ | Admin | Admin | admin@domain.com | admin | Email Sent | |
| ▸ | Ildar | Iskyandyarov | user@domain.com | user | Clicked Link | |

Showing 1 to 2 of 2 entries

Previous 1 Next