

Phishing

Diariamente milhares de ataques de phishing ocorrem em todo mundo! Alguns destes ataques são fáceis de detectar, porém muitos deles parecem tão confiáveis que acabam enganando suas vítimas



Vídeo aula



Tipos de Phishing

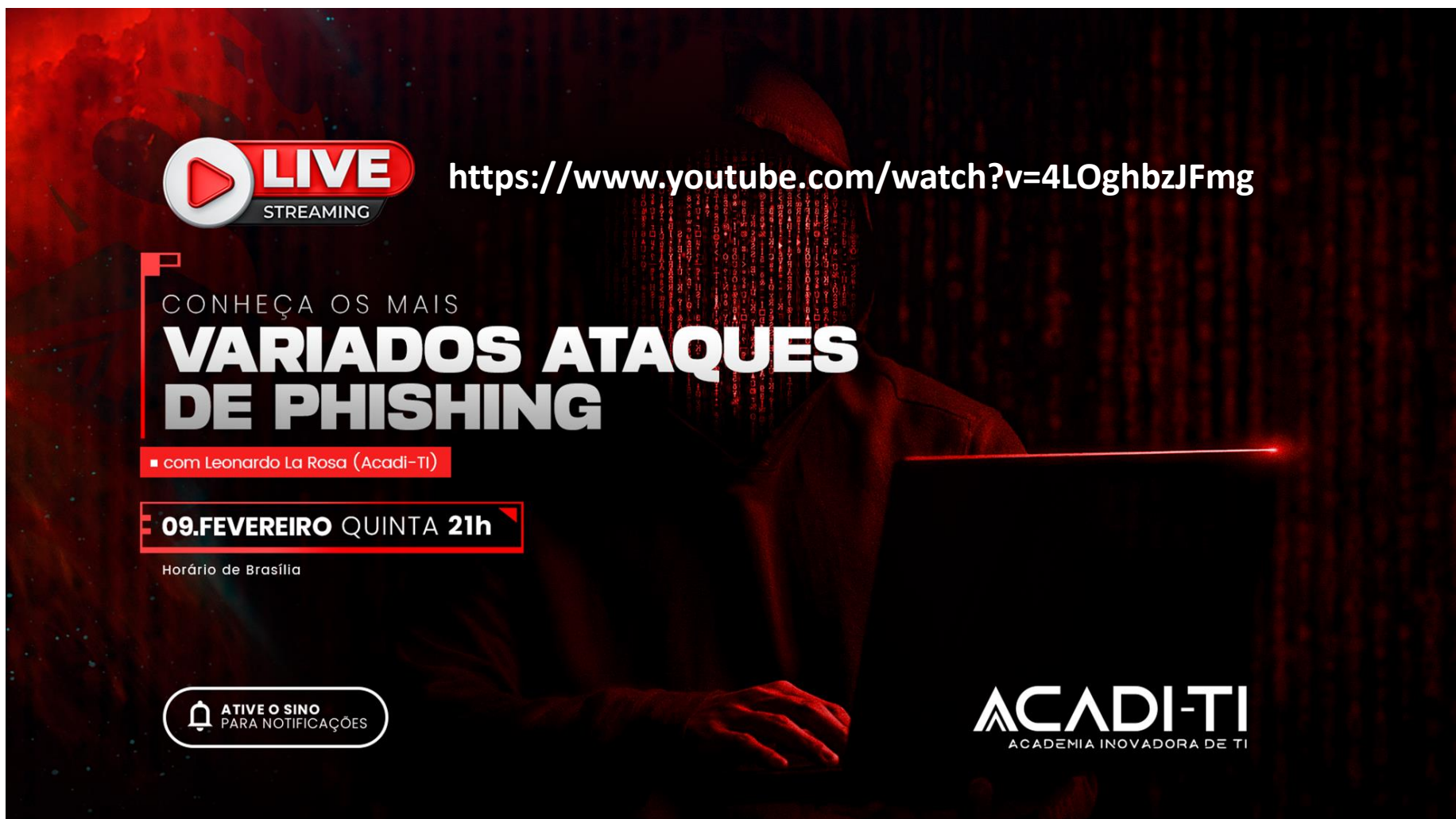


Como se Proteger



Testando nossos usuários

Vídeo



The image is a YouTube video player thumbnail. It features a dark background with a person's silhouette using a laptop, overlaid with a red digital rain effect. The text is primarily white and red.

LIVE
STREAMING

<https://www.youtube.com/watch?v=4LOghbzJFmg>

CONHEÇA OS MAIS
**VARIADOS ATAQUES
DE PHISHING**

■ com Leonardo La Rosa (Acadi-TI)

09.FEVEREIRO QUINTA **21h**

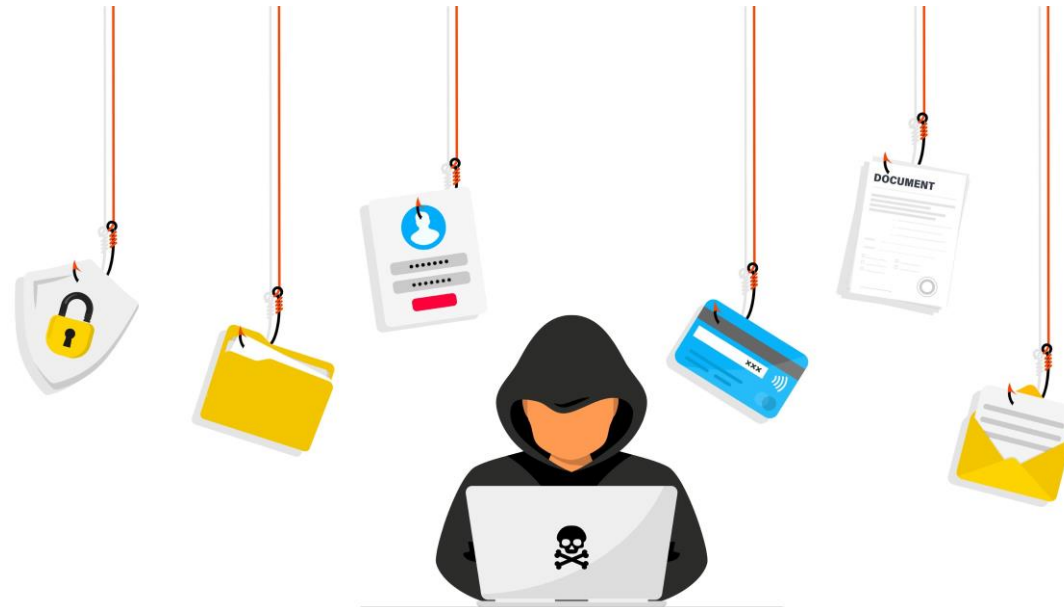
Horário de Brasília

ATIVE O SINO
PARA NOTIFICAÇÕES

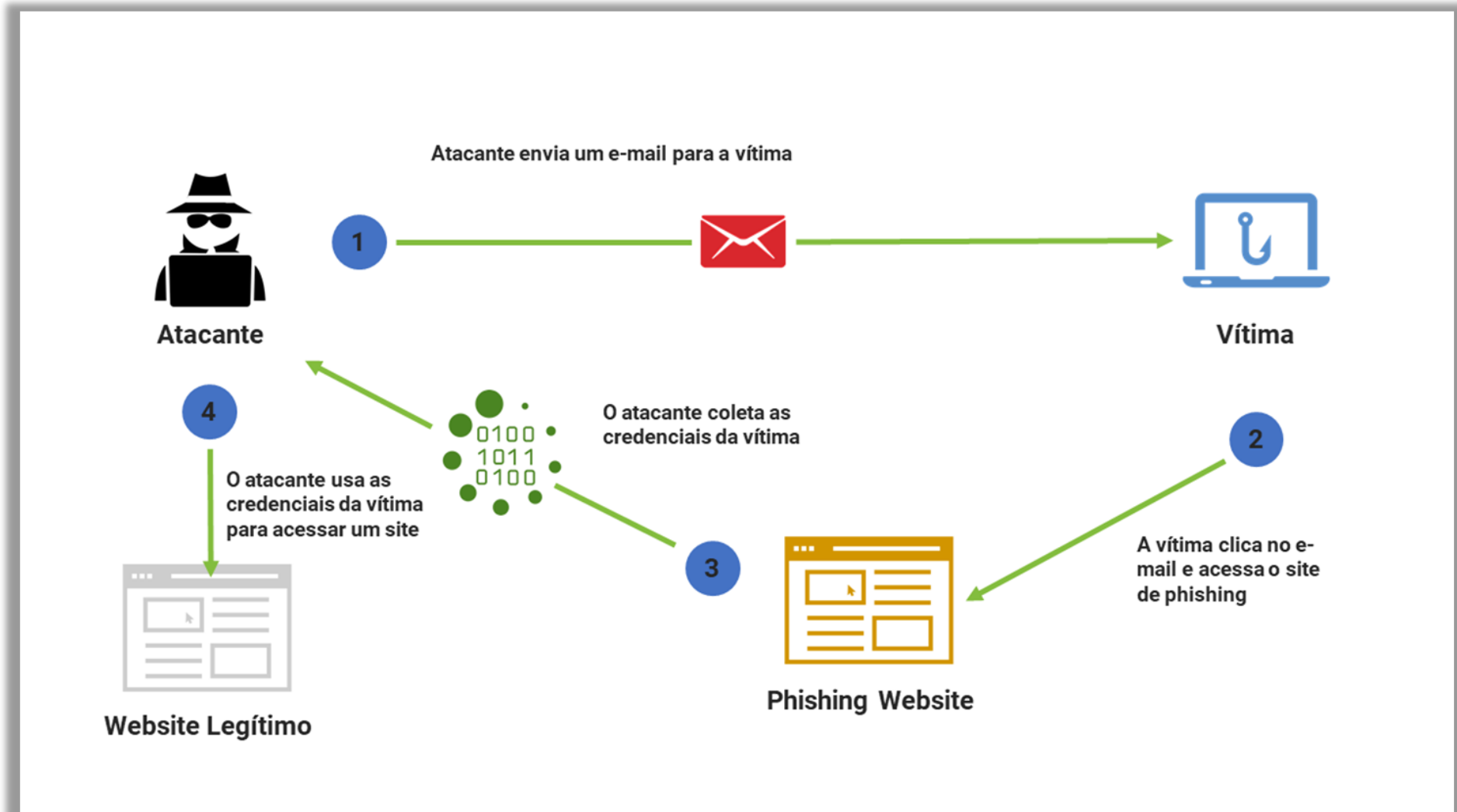
ACADI-TI
ACADEMIA INOVADORA DE TI

O que é Phishing?

“Phishing é uma das formas de fraude presente na internet onde os crackers e pessoas mal-intencionadas tentam obter informações pessoais das pessoas, como senhas de bancos, números de cartões de crédito, etc., por meio de armadilhas virtuais.”



Como Funciona um ataque de Phishing?



Tipos de Phishing

Smishing

É o phishing realizado por mensagens de SMS, normalmente envolvendo sorteios, resgate de pontos e mensagens bancárias.

Vishing

O phishing do tipo Scam busca conseguir dados das vítimas, simulando pessoas importantes, ou mesmo grandes instituições e entram em contato através de e-mail ou telefone.

Clone

O Clone Phishing é quando os golpistas criam uma versão muito semelhante de um grande site, tentando se passar como o verdadeiro. Dessa forma, as vítimas sentem que estão em um ambiente seguro, mesmo que seja exatamente o oposto.

Smishing



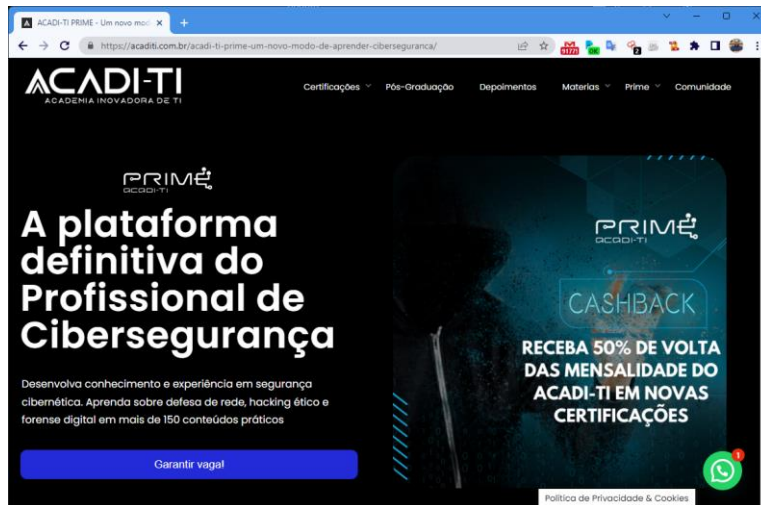
Vishing

https://www.youtube.com/watch?v=Vc6DxiKh_4w



Clone

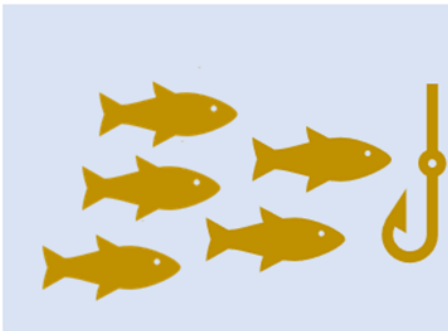
<https://www.ACADITI.com.br>



<https://www.ACADITI.com.br>

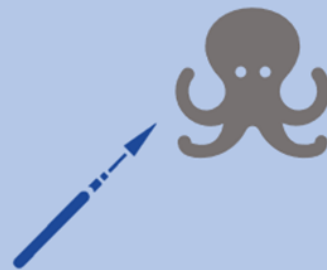


Classificação de Phishing



PHISHING EM ESCALA

Ataque onde os fraudadores lançam uma ampla rede de ataques que não são altamente visados



SPEAR PHISHING

Adaptado a uma vítima específica ou grupo de vítimas usando dados pessoais



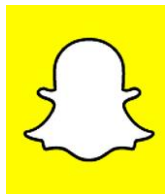
WHALING

Tipo especializado de phishing que tem como alvo uma vítima "grande" dentro de uma empresa, como executivos.

Impactos de um Whaling Phishing



Seagate: Um whaling attack bem sucedido levou ladrões a ter acesso a mais de 10.000 documentos fiscais de todos os funcionários.



Snapchat: Um funcionário abriu um e-mail personificando um pedido do CEO Evan Spiegel e comprometeu dados de folha de pagamento de 700 funcionários.



Ubiquiti Networks: Esta empresa de tecnologia de rede sofreu uma perda de US\$ 41,1 milhões como resultado de um whaling attack.

Como se proteger?



Não abra e-mails de origem desconhecida e sempre desconfie de links e anexos de e-mails de fora da organização.



Os bancos nunca solicitam senhas ou dados de cartões aos seus clientes, portanto, cuidado com e-mails com este conteúdo.

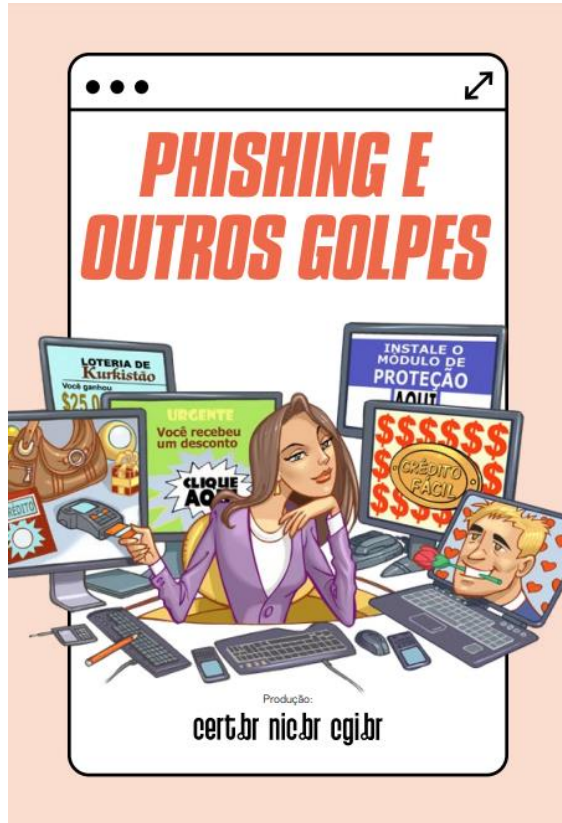


Não compartilhe dados pessoais em planilhas e emails.



Cuidado com links em mensagens de promoções “imperdíveis” e “sorteios”

Como se proteger?



O CertBR possui diversas apostilas para orientar os usuários quanto a segurança na internet, redes sociais, senhas e emails.

Possui um material voltado para Phishing que vale muito a leitura.

<https://cartilha.cert.br/fasciculos/#phishing-golpes>

Como avaliar se meus usuários estão protegidos contra Phishing

Utilizaremos um framework voltado para phishing para testarmos a segurança dos nossos usuários.

The image shows a dark-themed website for 'gótico' (Gophish) and a laptop displaying the Gophish dashboard. The website header includes the 'gótico' logo and navigation links: 'Documentação', 'Apoiar', 'blog', and a 'Download' button. The main content area features the title 'Estrutura de phishing de código aberto' (Open source phishing structure) and a description: 'Gophish é uma poderosa estrutura de phishing de código aberto que facilita o teste da exposição de sua organização a phishing.' (Gophish is a powerful open source phishing structure that facilitates testing the exposure of your organization to phishing). Below this is the text 'De graça.' (For free.) and two buttons: 'Download' and 'Saber mais' (Know more).

The laptop screen shows the Gophish dashboard. It has a 'gophish' logo in the top left. The dashboard includes a 'Dashboard' section with a red area chart showing a fluctuating trend. Below the chart are four circular progress indicators for 'Email Sent', 'Email Opened', 'Clicked Link', and 'Submitted Data'. The 'Email Sent' indicator is green, while the others are yellow. Below these is a 'Recent Campaigns' section with a table of campaign data, including columns for status (green/red) and completion (green/red).

Como avaliar se meus usuários estão protegidos contra Phishing

Em poucos minutos você consegue criar uma campanha de phishing e testar a segurança de seus usuários.

Lance uma campanha em 3 passos



Definir modelos e metas

O Gophish facilita a criação ou importação de modelos de phishing perfeitos para pixels .

Nossa IU da Web inclui um editor de HTML completo, facilitando a personalização de seus modelos diretamente no navegador.



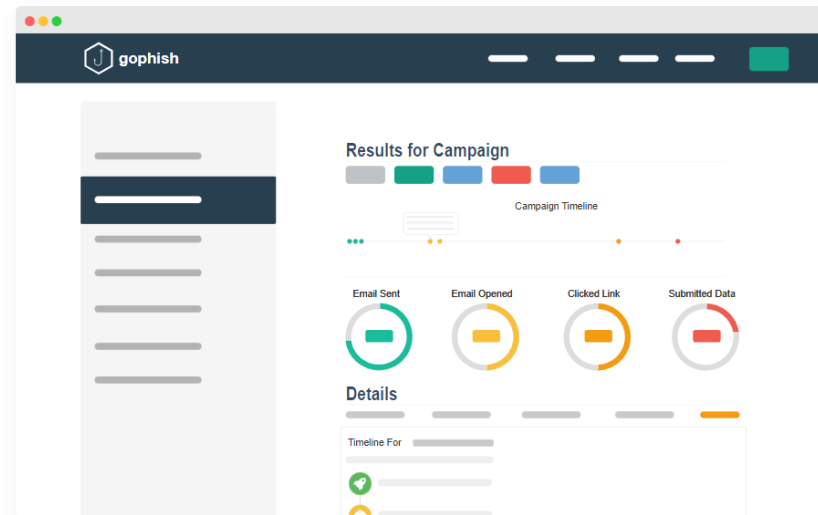
Lançar a campanha

Inicie a campanha e os e-mails de phishing são enviados em segundo plano. Você também pode agendar campanhas para lançar quando quiser.



Rastrear resultados

Resultados detalhados são entregues quase em tempo real. Os resultados podem ser exportados para uso em relatórios.



Atenção!!!








O conteúdo prático demonstrado a seguir tem como objetivo alertar aos usuários sobre os perigos dos ataques de phishing e não recomendamos o uso das ferramentas para realização de ataques. Todos os testes realizados ocorreram em ambiente controlado com a ciência de todos os usuários envolvidos.

Realizando o Download do Go Phishing

Como o go phishing é uma solução cross plataforma você pode selecionar a versão que melhor se adeque ao sistema operacional que estiver utilizando.



<https://github.com/gophish/gophish/releases>

 gophish-v0.12.1-linux-32bit.zip	31.4 MB	Sep 14, 2022
 gophish-v0.12.1-linux-64bit.zip	31.8 MB	Sep 14, 2022
 gophish-v0.12.1-osx-64bit.zip	33.2 MB	Sep 14, 2022
 gophish-v0.12.1-windows-64bit.zip	32.1 MB	Sep 14, 2022
 Source code (zip)		Sep 14, 2022
 Source code (tar.gz)		Sep 14, 2022

Definindo o Sistema Operacional

Em nosso exemplo, utilizaremos o Ubuntu Linux em Cloud na Digital Ocean como máquina host para nosso laboratório



Link de acesso: <https://m.do.co/c/dd62f5ff6b51>

Configurando o Go Phishing

Utilizando o usuário root, criaremos uma pasta em /opt com o nome gophish e realizaremos o download do arquivo compactado do site do go phish.

```
cd /opt  
mkdir gophish  
cd gophish  
wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip
```

Configurando o Go Phishing

Após a conclusão do Download, descompactaremos o arquivo zip e daremos permissão de execução ao binário gophish

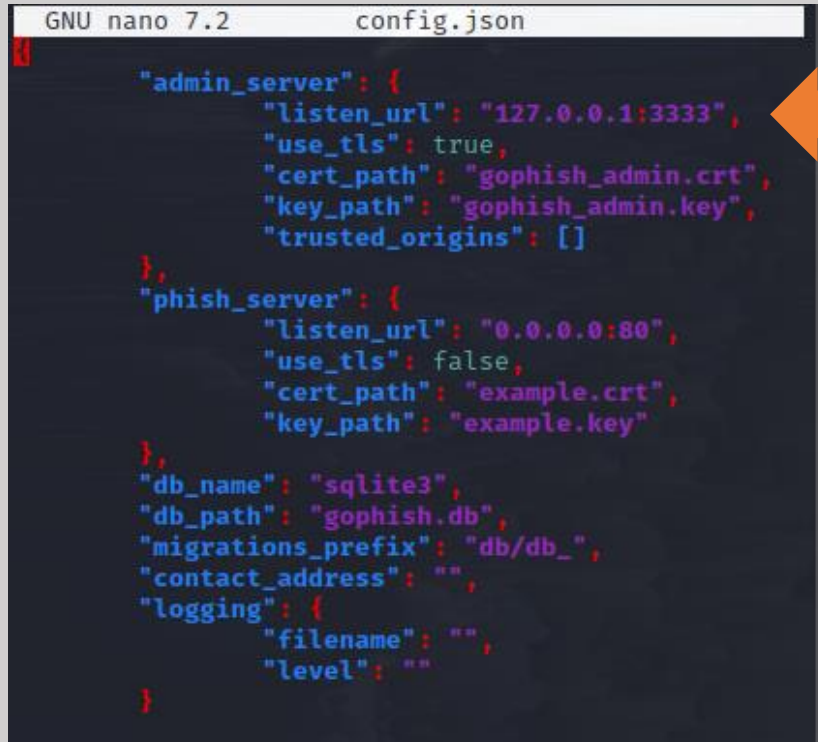
```
unzip gophish-v0.12.1-linux-64bit.zip  
chmod +x gophish
```

Configurando o Go Phishing

Antes de executar o gophish, edite o arquivo de configuração config.json e altere o endereço ip que está em "listen_url": para seu endereço IP Público

```
GNU nano 7.2  config.json

{
  "admin_server": {
    "listen_url": "127.0.0.1:3333",
    "use_tls": true,
    "cert_path": "gophish_admin.crt",
    "key_path": "gophish_admin.key",
    "trusted_origins": []
  },
  "phish_server": {
    "listen_url": "0.0.0.0:80",
    "use_tls": false,
    "cert_path": "example.crt",
    "key_path": "example.key"
  },
  "db_name": "sqlite3",
  "db_path": "gophish.db",
  "migrations_prefix": "db/db_",
  "contact_address": "",
  "logging": {
    "filename": "",
    "level": ""
  }
}
```



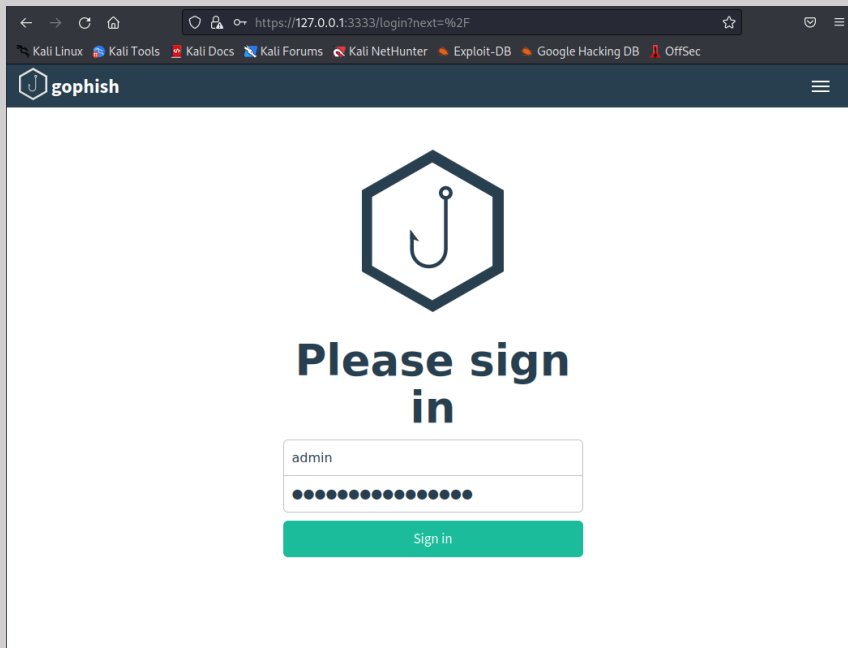
Configurando o Go Phishing

Para executarmos nossa aplicação, basta digitar o comando `./gophish`.

Você verá as credenciais para se conectar à plataforma e o endereço para inserir em seu browser: `https://<seu IP>:3333`

```
./gophish
```

Acessando o Go Phishing

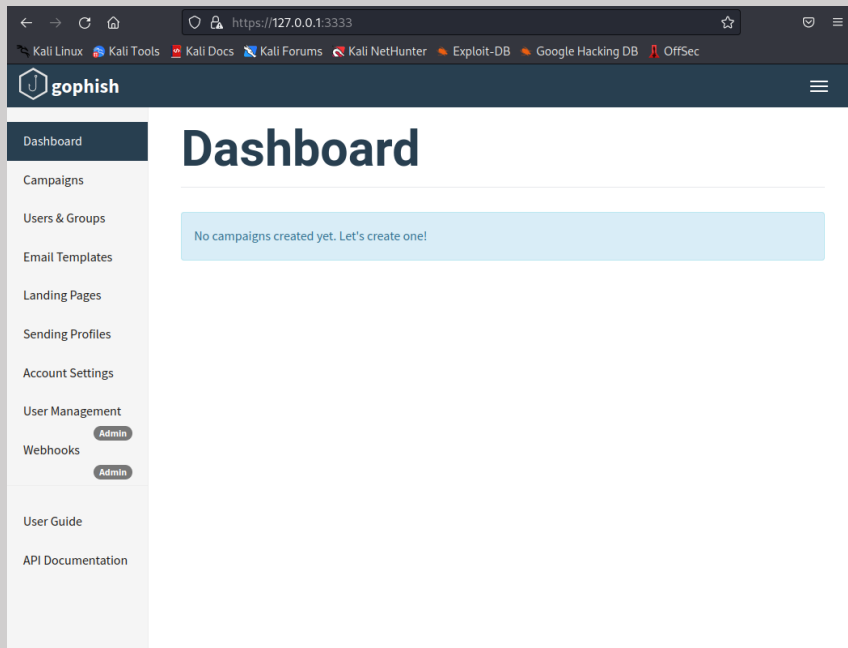


Ao digitar o endereço <https://127.0.0.1:3333> em seu browser, você será direcionado para a tela de login. Informe o login admin e a senha que aparece em seu terminal.

Em seguida surgirá uma mensagem para você alterar a senha padrão.

```
time="2023-02-09T09:13:20-05:00" level=info msg="Please login with the username admin and the password b03219a3756780a9"
```


Acessando o Go Phishing



Pronto! Você já está no dashboard da aplicação.

Navegue entre as abas para se familiarizar e em seguida criaremos nossos templates para darmos início às nossas campanhas

Definindo a lista de usuários

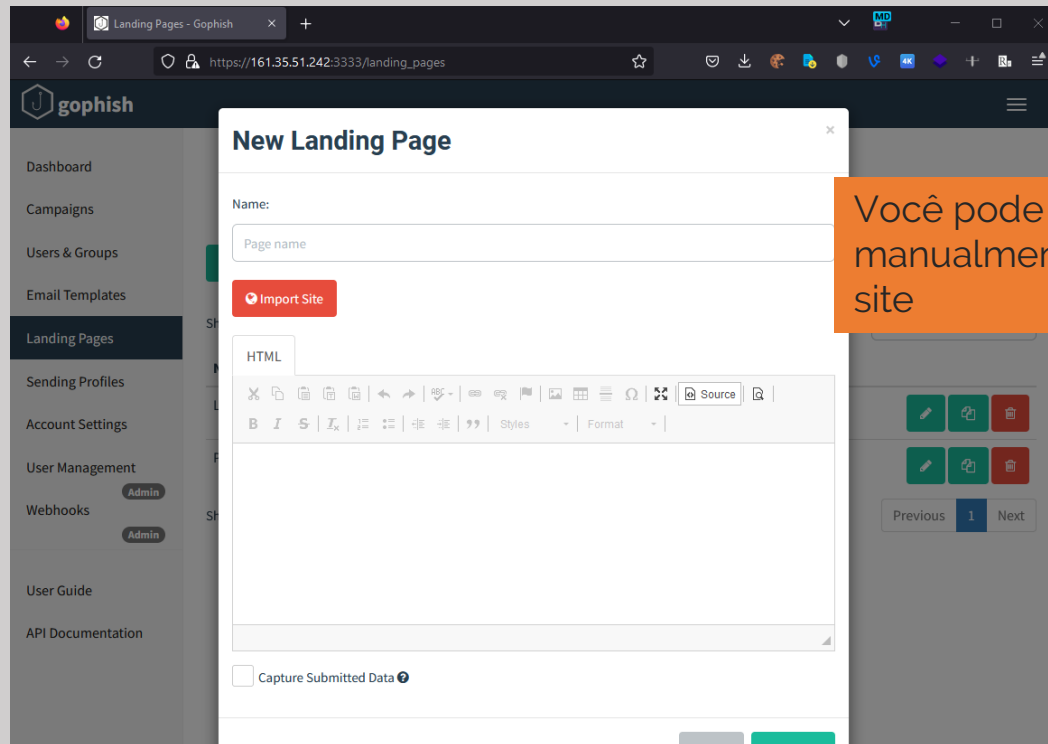
O primeiro passo para nosso teste é definir os usuários que receberão nosso “ataque” para avaliar seu comportamento ao receber e-mail.

The screenshot shows the Gophish web interface with the 'New Group' modal open. The modal has a sidebar on the left with navigation links: Dashboard, Campaigns, Users & Groups (active), Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management, Webhooks, and User Guide. The main content area of the modal includes a 'Name' field with a placeholder 'Group name', a red '+ Bulk Import Users' button, and a 'Download CSV Template' link. Below these are input fields for 'First Name', 'Last Name', 'Email', and 'Position', followed by a red '+ Add' button. A table below shows columns for 'First Name', 'Last Name', 'Email', and 'Position', with a message 'No data available in table' and 'Showing 0 to 0 of 0 entries'. At the bottom are 'Close' and 'Save changes' buttons. An orange callout box with an arrow points to the 'Bulk Import Users' button.

Caso queira carregar vários usuários, utilize o arquivo de template.

Criando a Landing Page

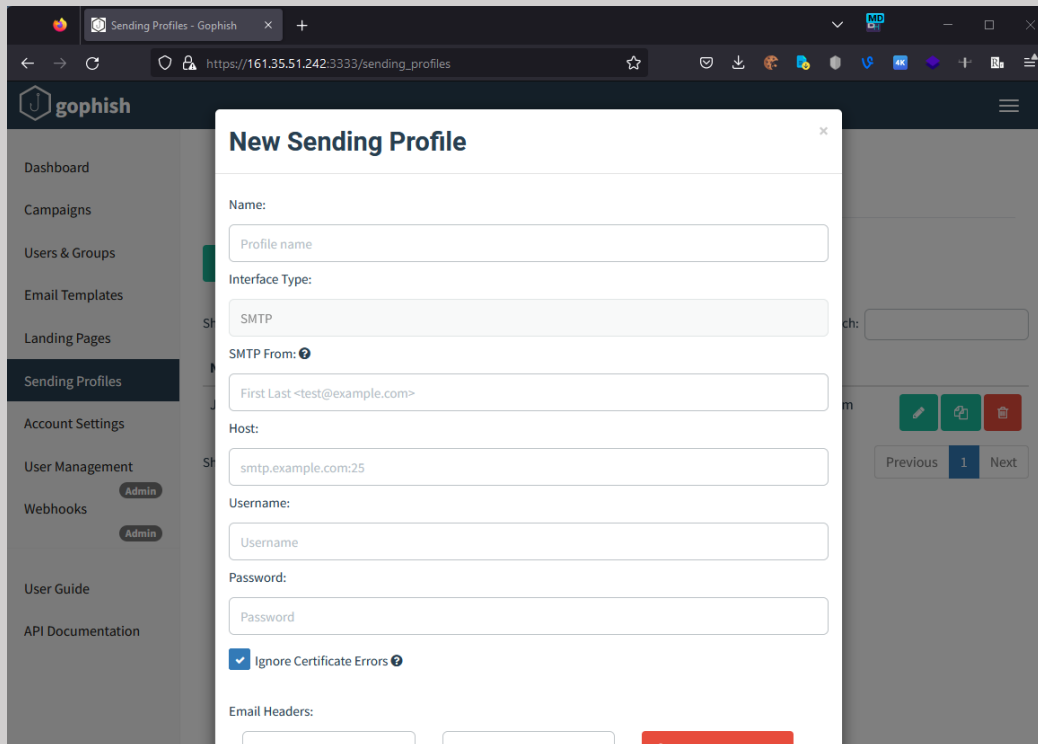
Agora vamos criar uma Landing Page onde o usuário informará os dados que queremos.



Você pode criar uma landing page manualmente ou importar de algum site

Configurando o Perfil de Envio dos e-mails

Precisaremos criar o perfil para envio de mensagens. Você pode utilizar uma conta no google ou qualquer outro provedor.



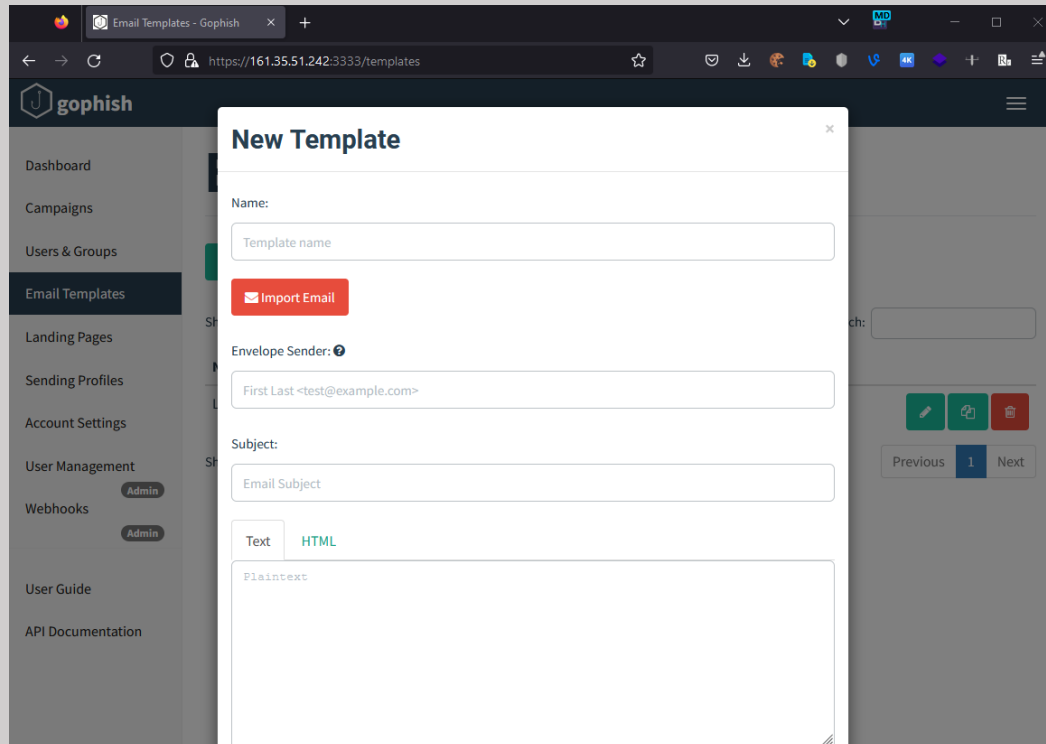
The screenshot displays the Gophish web application interface. On the left, a sidebar menu lists various sections: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles (highlighted), Account Settings, User Management, Webhooks, User Guide, and API Documentation. The main content area shows a modal window titled 'New Sending Profile'. This form includes the following fields and options:

- Name:** A text input field with the placeholder 'Profile name'.
- Interface Type:** A dropdown menu currently set to 'SMTP'.
- SMTP From:** A text input field with the placeholder 'First Last <test@example.com>'.
- Host:** A text input field with the placeholder 'smtp.example.com:25'.
- Username:** A text input field with the placeholder 'Username'.
- Password:** A text input field with the placeholder 'Password'.
- Ignore Certificate Errors:** A checked checkbox with a label and a help icon.
- Email Headers:** A section with two text input fields and a red 'Add New Header' button.

The browser's address bar shows the URL 'https://161.35.51.242:3333/sending_profiles'. The Gophish logo is visible in the top left of the interface.

Criando o template de mensagens

Por fim, criaremos o e-mail que será enviado para todos os usuários.



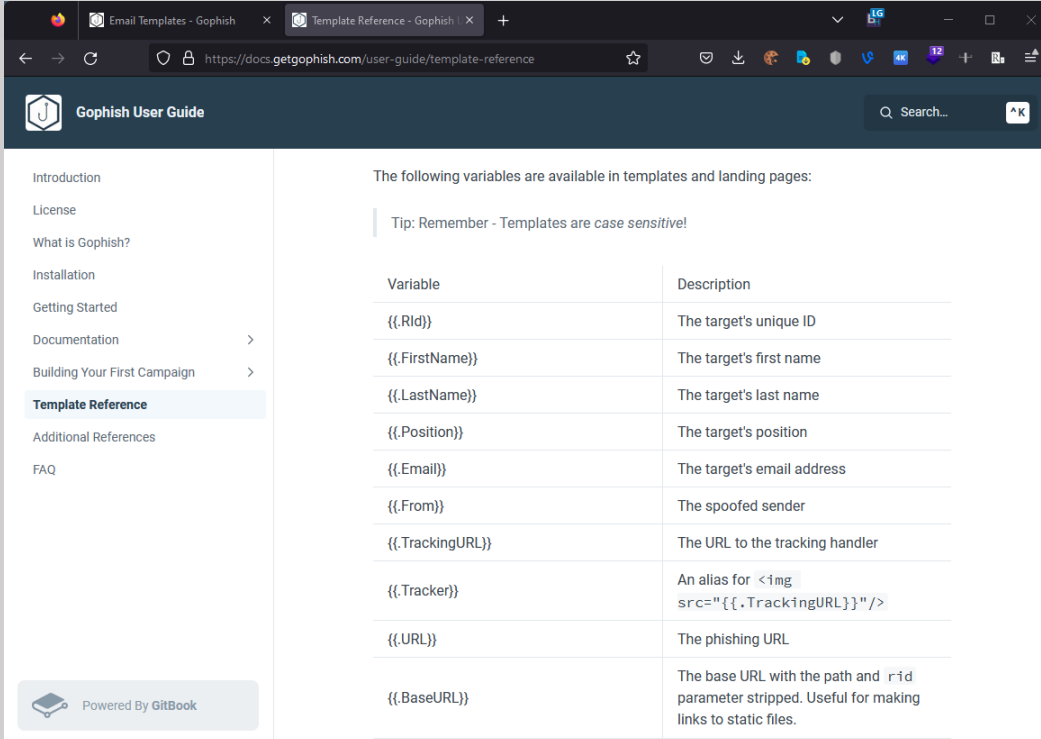
The screenshot shows a web browser window with the Gophish interface. The address bar displays the URL `https://161.35.51.242:3333/templates`. The left sidebar contains a navigation menu with the following items: Dashboard, Campaigns, Users & Groups, Email Templates (highlighted), Landing Pages, Sending Profiles, Account Settings, User Management (with an 'Admin' button), Webhooks (with an 'Admin' button), User Guide, and API Documentation. The main content area features a 'New Template' modal form. The form includes the following fields and elements:

- Name:** A text input field with the placeholder 'Template name'.
- Import Email:** A red button with a white envelope icon and the text 'Import Email'.
- Envelope Sender:** A text input field with the placeholder 'First Last <test@example.com>'.
- Subject:** A text input field with the placeholder 'Email Subject'.
- Format:** Two tabs, 'Text' and 'HTML' (which is selected and highlighted in green).
- Plaintext:** A large text area for entering the email content.

In the background, partially obscured by the modal, there is a search bar and a pagination control showing 'Previous', '1' (the current page), and 'Next'.

Dicas importantes

Para deixar o template de e-mail personalizado para cada usuário, você pode utilizar algumas variáveis definidas no Go Phishing



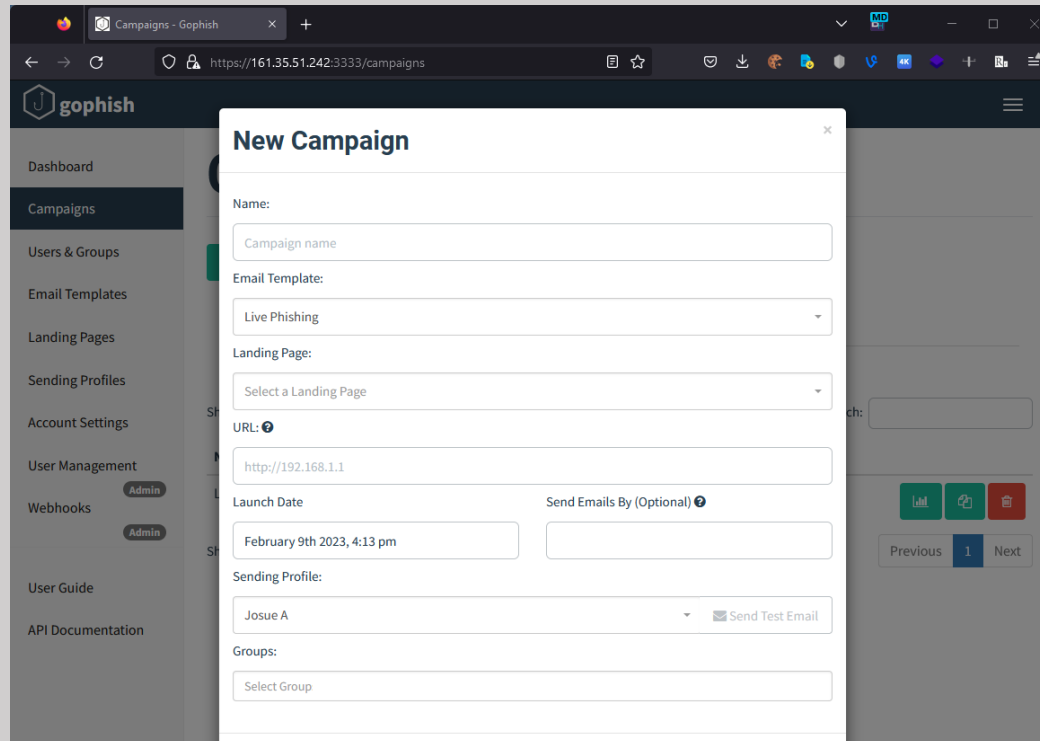
The screenshot shows a web browser window displaying the Gophish User Guide. The left sidebar contains a navigation menu with the following items: Introduction, License, What is Gophish?, Installation, Getting Started, Documentation, Building Your First Campaign, **Template Reference** (highlighted), Additional References, and FAQ. The main content area is titled "The following variables are available in templates and landing pages:" and includes a tip: "Tip: Remember - Templates are case sensitive!". Below the tip is a table with two columns: Variable and Description.

Variable	Description
{{.Rid}}	The target's unique ID
{{.FirstName}}	The target's first name
{{.LastName}}	The target's last name
{{.Position}}	The target's position
{{.Email}}	The target's email address
{{.From}}	The spoofed sender
{{.TrackingURL}}	The URL to the tracking handler
{{.Tracker}}	An alias for <code></code>
{{.URL}}	The phishing URL
{{.BaseURL}}	The base URL with the path and <code>rid</code> parameter stripped. Useful for making links to static files.

At the bottom left of the page, there is a "Powered By GitBook" logo.

Criando uma campanha

Agora que todas as configurações já foram feitas, é hora de criarmos nossa campanha e acompanhar o resultado.



The screenshot displays the Gophish web application interface. On the left is a sidebar menu with options: Dashboard, Campaigns (selected), Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management, Webhooks, User Guide, and API Documentation. The main content area shows the 'New Campaign' form with the following fields:

- Name:** A text input field with the placeholder 'Campaign name'.
- Email Template:** A dropdown menu currently showing 'Live Phishing'.
- Landing Page:** A dropdown menu with the option 'Select a Landing Page'.
- URL:** A text input field containing 'http://192.168.1.1'.
- Launch Date:** A date and time picker set to 'February 9th 2023, 4:13 pm'.
- Send Emails By (Optional):** An empty text input field.
- Sending Profile:** A dropdown menu showing 'Josue A' with a 'Send Test Email' button next to it.
- Groups:** A dropdown menu with the option 'Select Group'.

At the bottom right of the interface, there are navigation buttons: 'Previous', '1' (the active page), and 'Next'.

Resultado

Agora é só acompanhar o resultado da campanha

Live Phishing - Gophish

https://161.35.51.242:3333/campaigns/11

gophish

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User Management

Webhooks

User Guide

API Documentation

Details

Show entries

Search:

First Name	Last Name	Email	Position	Status	Reported
▶				Clicked Link	✖
▶				Email Opened	✖
▶				Email Sent	✖
▶				Email Sent	✖
▶				Email Sent	✖
▶				Email Sent	✖
▶				Email Sent	✖
▶				Email Sent	✖
▶				Email Sent	✖
▶				Email Sent	✖

Showing 1 to 10 of 15 entries

Previous12Next

Utilizando uma outra solução para Campanha de Phishing

Já vimos como funciona um ataque de phishing por e-mail e como ele pode ser muito bem sucedido caso os usuários não se atentem a alguns detalhes.

Agora realizaremos simulações baseadas em ataques a redes sociais. Para isso utilizaremos a ferramenta zphisher.

<https://github.com/htr-tech/zphisher>

Definindo o Sistema Operacional

Para este exemplo utilizaremos o Kali Linux local como máquina host para nosso laboratório



Link de acesso: <https://www.kali.org/get-kali/#kali-virtual-machines>

Realizando o download do zphisher

Utilizando o usuário root, entraremos na pasta /opt/ e baixaremos os arquivos de instalação do zphisher

```
cd /opt  
git clone https://github.com/htr-tech/zphisher.git
```

Para instalar os componentes e executar o zphisher entre na pasta zphisher e execute o comando de mesmo nome:

```
cd zphisher  
./zphisher.sh
```

Instalando componentes

Após a configuração de todos os componentes, você verá uma tela com as opções de utilização



```
root@kali: /opt/zphisher
File Actions Edit View Help

Zphisher
Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

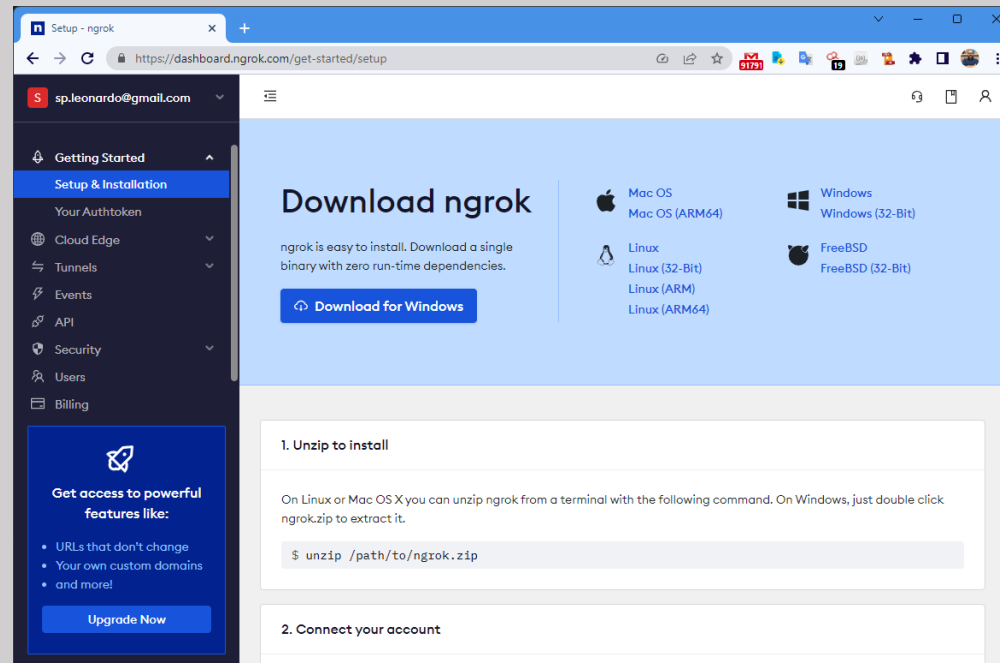
[01] Facebook      [11] Twitch          [21] DeviantArt
[02] Instagram     [12] Pinterest       [22] Badoo
[03] Google        [13] Snapchat        [23] Origin
[04] Microsoft     [14] LinkedIn        [24] DropBox
[05] Netflix       [15] Ebay            [25] Yahoo
[06] Paypal        [16] Quora           [26] Wordpress
[07] Steam         [17] Protonmail      [27] Yandex
[08] Twitter       [18] Spotify         [28] StackoverFlow
[09] Playstation  [19] Reddit          [29] Vk
[10] Tiktok        [20] Adobe           [30] XBOX
[31] Mediafire     [32] Gitlab          [33] Github
[34] Discord      [35] Roblox

[99] About         [00] Exit

[-] Select an option : █
```

Configurando o ngrok

Como configuramos nossa aplicação em uma máquina virtual, precisaremos fazer um redirect do nosso endereço local para um endereço de internet. Para isso utilizaremos o ngrok



Configurando o ngrok

Realize um cadastro gratuito no site <https://ngrok.com/> e faça o download do arquivo compactado.

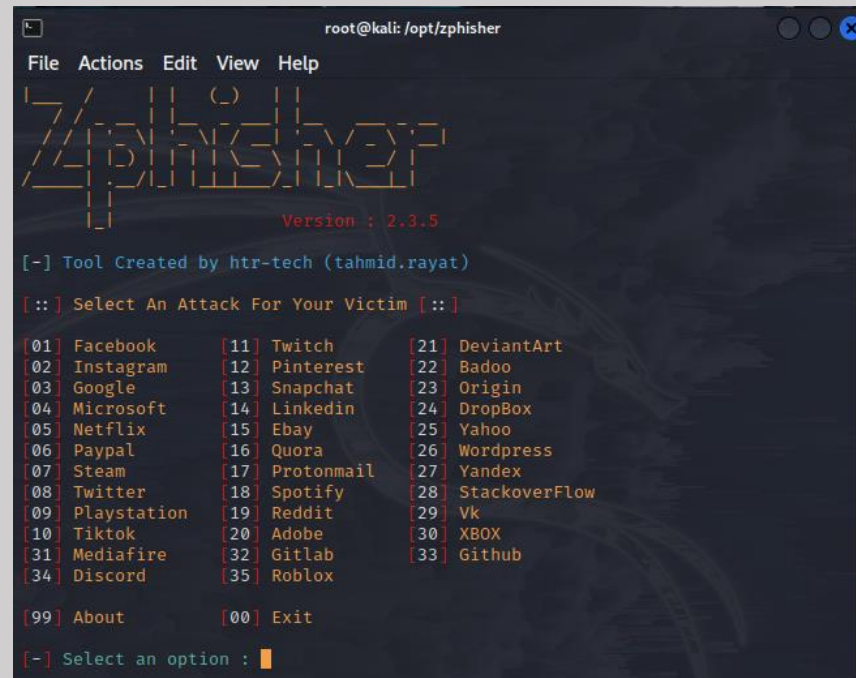
```
wget https://bin.equinox.io/c/bNyj1mQVY4c/ngrok-v3-stable-linux-amd64.tgz
```

Para o primeiro acesso é necessário criar o arquivo de configuração com seu token.

```
ngrok config add-authtoken <SEU TOKEN>
```


Acessando o zphisher

Retornando agora ao zphisher, podemos simular nosso ataque.



```
root@kali: /opt/zphisher
File Actions Edit View Help

Zphisher
Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

01] Facebook      11] Twitch        21] DeviantArt
02] Instagram    12] Pinterest    22] Badoo
03] Google       13] Snapchat     23] Origin
04] Microsoft    14] LinkedIn    24] DropBox
05] Netflix      15] Ebay        25] Yahoo
06] Paypal       16] Quora       26] Wordpress
07] Steam        17] Protonmail  27] Yandex
08] Twitter      18] Spotify     28] StackoverFlow
09] Playstation  19] Reddit      29] Vk
10] Tiktok       20] Adobe       30] XBOX
31] Mediafire    32] Gitlab      33] Github
34] Discord      35] Roblox

99] About        00] Exit

[-] Select an option : █
```

Acessando o zphisher

Phishing com Facebook

```
root@kali: /opt/zphisher
File Actions Edit View Help

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

01| Facebook      11| Twitch          21| DeviantArt
02| Instagram    12| Pinterest      22| Badoo
03| Google       13| Snapchat       23| Origin
04| Microsoft    14| LinkedIn       24| DropBox
05| Netflix      15| Ebay           25| Yahoo
06| PayPal       16| Quora          26| Wordpress
07| Steam        17| Protonmail     27| Yandex
08| Twitter      18| Spotify        28| StackoverFlow
09| Playstation 19| Reddit         29| Vk
10| Tiktok       20| Adobe          30| XBOX
31| Mediafire    32| Gitlab         33| Github
34| Discord      35| Roblox

[99] About      [00] Exit

[-] Select an option : 01

01| Traditional Login Page
02| Advanced Voting Poll Login Page
03| Fake Security Login Page
04| Facebook Messenger Login Page

[-] Select an option : 01
```

```
root@kali: /opt/zphisher
File Actions Edit View Help

ZPHISHER 2.3.5

01| Localhost      [Account Needed]
02| Ngrok.io       [Auto Detects]
03| Cloudflared    [NEW! Max 15Min]
04| LocalXpose

[-] Select a port forwarding service : 01
```

```
root@kali: /opt/zphisher
File Actions Edit View Help

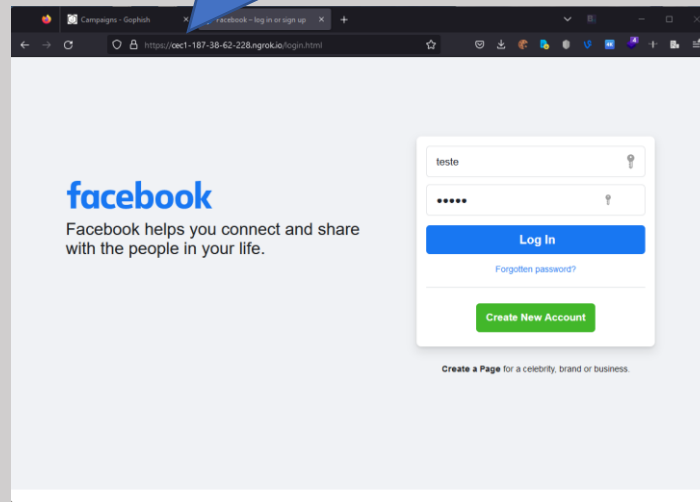
ZPHISHER 2.3.5

[-] URL 1 : https://cec1-187-38-62-228.ngrok.io
[-] URL 2 : https://is.gd/5sKp0o
[-] URL 3 : https://blue-verified-badge-for-facebook-free@is.gd/5sKp0o
[-] Waiting for Login Info, Ctrl + C to exit ...
```

Acessando o zphisher

Phishing com Facebook

O endereço aponta para uma URL diferente do site oficial



```
root@kali: /opt/zphisher
File Actions Edit View Help

ZPHISHER 2.3.5

[-] URL 1 : https://cec1-187-38-62-228.ngrok.io
[-] URL 2 : https://is.gd/5sKp0o
[-] URL 3 : https://blue-verified-badge-for-facebook-free@is.gd/5sKp0o
[-] Waiting for Login Info, Ctrl + C to exit ...
[-] Victim IP Found !
[-] Victim's IP : 187.38.62.228
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : teste
[-] Password : teste
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. █
```

Acessando o zphisher

Phishing com Netflix

```
root@kali: /opt/zphisher
File Actions Edit View Help

ZPHISHER 2.3.5

[01] Localhost
[02] Ngrok.io [Account Needed]
[03] Cloudflared [Auto Detects]
[04] LocalXpose [NEW! Max 15Min]

[-] Select a port forwarding service : 02
```

```
root@kali: /opt/zphisher
File Actions Edit View Help

ZPHISHER 2.3.5

[01] Localhost
[02] Ngrok.io [Account Needed]
[03] Cloudflared [Auto Detects]
[04] LocalXpose [NEW! Max 15Min]

[-] Select a port forwarding service : 02
```

```
root@kali: /opt/zphisher
File Actions Edit View Help

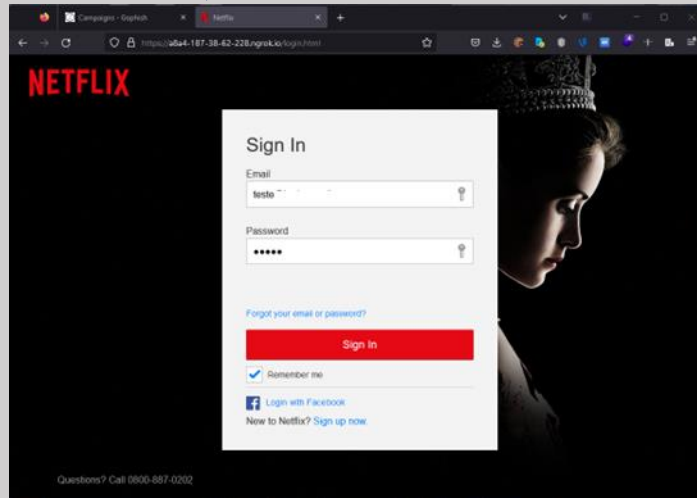
ZPHISHER 2.3.5

[-] URL 1 : https://a8a4-187-38-62-228.ngrok.io
[-] URL 2 : https://is.gd/zk0b3i
[-] URL 3 : https://upgrade-your-netflix-plan-free@is.gd/zk0b3i
[-] Waiting for Login Info, Ctrl + C to exit ...
```

Acessando o zphisher

Phishing com Netflix

O endereço aponta para uma URL diferente do site oficial





Phishing