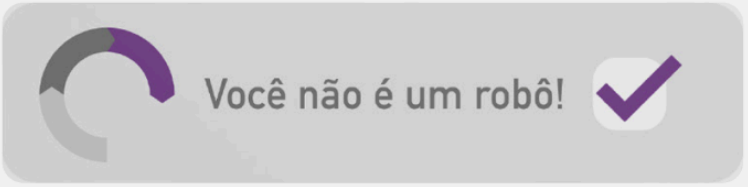
2025

Informe .seH



MANUAL DE USO DA FERRAMENTA GOPHISH

ANDIFES CGTIC .seH SEGURANÇA NO ELEMENTO HUMANO

Controle de versões			
Versão	**Data**	**Descrição**	**Responsáveis**
V.1.0	22/01/2025	Versão inicial do Manual de Uso da Ferramenta GoPhish	Rafael Padilha (UFPel); Erica Miranda (UFRN), Erasmo Evangelista (UFLA), Fernando Oliveira (UFLA), Plínio Torres (UFLA), Marcos Madruga (UFRN), Bruno Ferreira (UFRN)

Sumário

1 Introdução....4
2 Princípios éticos das campanhas de phishing....5
2.1 Propósito educacional e preventivo....5
2.2 Conformidade legal e organizacional....5
2.3 Consentimento e governança....5
2.4 Confidencialidade dos dados....5
2.5 Ética no projeto da campanha....6
2.6 Comunicação pós-campanha....6
3 Objetivos....7
4 Público alvo....7
5 Especificação dos requisitos de hardware....7
6 Pré-requisitos para uso da ferramenta GoPhish....8
7 Metodologia....8
7.1 Ciclo de vida das campanhas....8
7.2 Comunicação com a alta gestão e as áreas de negócio....9
7.3 Temáticas para as fases das campanhas....9
7.4 Ferramentas e materiais....10
7.4.1 Ferramentas....10
7.4.2 Materiais....10
7.5 Coleta e análise de dados....11
8 Plano de comunicação....12
9 Instalação e configuração....13
9.1 Requisitos prévios....13
9.2 Instalação no Linux....14
9.3 Instalação no Windows....14
10 Operação e exemplos de aplicação....15
10.1 Criação de um sending profile:....15
10.2 Criação do template de e-mail....16
10.3 Criando uma landing page (página de captura)....18
10.4 Criando grupos de disparos....20
10.5 Disparando a campanha....22
11 Análise de resultados....23
12 Conscientização e treinamento....24
Glossário....25

1 Introdução

GoPhish é uma ferramenta de código aberto, amplamente utilizada por empresas e profissionais de segurança da informação, para simular ataques de phishing em ambientes corporativos. Com ela, é possível avaliar a vulnerabilidade dos colaboradores a esse tipo de ameaça e implementar medidas para fortalecer a segurança da informação.

Para que serve o GoPhish?

- **Simular ataques de phishing:** cria e envia e-mails e páginas web altamente personalizados para imitar ataques reais.
- **Conscientizar sobre possíveis ataques:** orienta aos usuários a reconhecer sinais de phishing e outras ameaças cibernéticas, promovendo práticas seguras para proteger dados e sistemas.
- **Avaliar a conscientização dos colaboradores:** monitora as interações dos usuários com as mensagens e páginas, identificando quem clica em links maliciosos ou fornece informações confidenciais.
- **Mensurar a eficácia de treinamentos de segurança:** permite acompanhar a evolução da conscientização dos colaboradores ao longo do tempo.
- **Identificar vulnerabilidades:** Revela quais são os pontos mais fracos da sua organização em relação aos ataques de phishing.

Como o GoPhish funciona?

1. **Configuração de envio de e-mail:** o administrador precisa configurar o envio de e-mail pela ferramenta, através do item "**Sending Profiles**". Neste item, precisamos configurar o servidor de e-mail, que será utilizado para envio das campanhas.
2. **Paginas de capturas (landing pages):** o administrador deve criar páginas de capturas com layouts relevantes para induzir os usuários a preencherem os dados e serem capturados. Dentro do GoPhish existe a possibilidade de clonar uma página. O recurso realmente funciona, e pode reproduzir uma página existente substituindo a ação pela captura do GoPhish.
3. **Template de e-mails:** o administrador deve configurar os templates de e-mail, isto é, modelos de e-mails que serão utilizados nas campanhas. Um recurso extremamente útil é a opção de "clonar" um e-mail, para isso basta o administrador colar o código fonte do e-mail (recebido) para criar um clone da mensagem como template. O GoPhish também pode alterar todos os links do clone, para que sejam direcionados para páginas de captura da própria ferramenta.
4. **Importação dos usuários (users and groups):** neste item, o administrador criará os grupos de usuários, para que as campanhas sejam disparadas especificamente para estes grupos, ou seja, você pode criar um grupo "Professores" e enviar uma campanha específica para este grupo. Esta campanha abordará templates de e-mail e landing pages que dizem respeito a este grupo, potencializando o "ataque".
5. **Campanha:** último item de configuração da ferramenta, depois de todas as etapas configuradas, podemos criar uma (ou mais) campanhas e disparar

para os grupos de usuários. É importante segmentar o envio, pois isso faz com que a campanha tenha mais sucesso.

2 Princípios éticos das campanhas de phishing

O uso de ferramentas como o GoPhish para realizar campanhas de phishing controladas deve seguir princípios éticos e legais claros. Essas diretrizes asseguram que os testes sejam conduzidos de maneira responsável, sem prejudicar os colaboradores ou violar a confiança organizacional. Os principais princípios são:

2.1 Propósito educacional e preventivo

- A campanha de phishing deve ser realizada com o único intuito de avaliar a conscientização sobre segurança da informação e educar os colaboradores sobre as ameaças.
- Os resultados devem ser utilizados para identificar vulnerabilidades e implementar medidas corretivas e treinamentos específicos.
- O teste deve evitar causar constrangimento, punições ou penalidades aos usuários.

2.2 Conformidade legal e organizacional

- Antes de iniciar a campanha, é essencial obter aprovação formal da alta administração e envolver os setores de gestão de pessoas, encarregado de dados e de controle interno .
- Garantir a conformidade com leis de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados), respeitando a privacidade dos colaboradores e o uso adequado das informações coletadas.
- Embora a campanha utilize técnicas de phishing, a finalidade deve ser claramente informada às partes interessadas (sem prejudicar a eficácia do teste).

2.3 Consentimento e governança

- A campanha deve ser planejada com o conhecimento e a participação de áreas estratégicas, como TI, Gestão de Pessoas, Jurídico, Alta Administração e demais instâncias internas de governança.
- Consentimento implícito: ao ingressarem na instituição os servidores (como técnicos administrativos e docentes), prestadores de serviços, discentes e demais membros da comunidade acadêmica, mediante dispositivos constantes em políticas e normativos internos de segurança, devem estar cientes de que testes de segurança (inclusive phishing) podem ser realizados.
- A governança da campanha deve ser conduzida por uma equipe com autoridade e capacitação, responsável por todo o ciclo (planejamento, execução e análise).

2.4 Confidencialidade dos dados

- Dados sensíveis, como credenciais ou padrões biométricos individuais, devem ser tratados com sigilo e armazenados de forma segura.

- As informações obtidas durante a campanha devem ser utilizadas apenas para fins educacionais e de segurança.
- Sempre que possível, as análises e relatórios devem ser apresentados de forma generalizada, evitando a exposição de indivíduos.

2.5 Ética no projeto da campanha

- A campanha deve ser planejada de forma cuidadosa, evitando qualquer conteúdo que possa causar desconforto ou impacto negativo.
    - Não utilize mensagens com tom ofensivo, alarmista ou que induzam ao pânico.
    - Evite temas sensíveis, como problemas de saúde, crises pessoais ou ameaças à estabilidade do emprego, que possam gerar preocupações indevidas.
- Utilize templates de e-mails e páginas falsas que simulem situações reais de forma educativa, porém ética.
    - Evite associar a campanha a entidades externas legítimas (como bancos, fornecedores ou instituições públicas) para não comprometer a reputação dessas organizações.
    - Priorize cenários que reflitam ameaças comuns, mas que preservem a integridade da simulação e dos participantes.
- O foco da campanha deve ser avaliar comportamentos e interações, como cliques em links ou abertura de e-mails.
    - Evite capturar informações sensíveis ou desnecessárias, como senhas reais, dados pessoais ou credenciais confidenciais.
    - Certifique-se de que os dados coletados sejam utilizados exclusivamente para análise de segurança e treinamento, respeitando as políticas de privacidade e proteção de dados.

2.6 Comunicação pós-campanha

- Após a conclusão da campanha, os colaboradores devem receber orientações diretas e didáticas sobre os riscos associados ao phishing. O feedback deve explicar como identificar e evitar tentativas maliciosas no futuro, reforçando boas práticas de segurança.
- Os dados obtidos devem ser utilizados para direcionar treinamentos e ações de conscientização, focando nas principais vulnerabilidades identificadas durante a campanha. O objetivo é promover um ambiente de aprendizado contínuo, sem expor ou constranger colaboradores individualmente.
- Os resultados da campanha devem ser apresentados à administração de maneira transparente e profissional, com análises detalhadas das vulnerabilidades encontradas e sugestões de melhorias.
    - Priorize relatório que anonimize dados individuais, mantendo o foco nos comportamentos gerais e nas lições aprendidas.
    - Destaque as ações corretivas propostas e os ganhos esperados em termos de segurança organizacional.

- Utilize os resultados da campanha como uma oportunidade para reforçar a importância da segurança da informação e fomentar uma cultura organizacional mais consciente e preparada para lidar com ameaças cibernéticas.

3 Objetivos

Dando ênfase ao que já foi mencionado, e com a intenção de melhorar a segurança da informação no âmbito das instituições e sua comunidade, alguns objetivos precisam ser estabelecidos para uso da ferramenta GoPhish. Assim são objetivos específicos deste manual:

- Indicar os parâmetros éticos e legais para a utilização da ferramenta GoPhish a partir dos princípios éticos definidos, da legislação e dos regulamentos aplicáveis;
- Construir documento que permita instalação, configuração e uso da ferramenta para uso seguro e em ambiente controlado;
- Definir alvos e grupos de pessoas a serem atingidas pela ação;
- Indicar formas de monitoração do progresso da campanha de phishing;
- Recomendar estratégias de avaliação institucional da segurança da informação com o uso da ferramenta; e
- Designar a forma de compartilhamento das informações sumarizadas obtidas em pré e pós-exposição a um dos temas específicos do projeto SEH (Phishing e Outros Golpes), que trata técnicas de ataque a partir de e-mails, mensagens de texto, telefonemas, redes sociais ou sites fraudulentos, por exemplo.

4 Público alvo

Considerando o interesse de investigar junto à comunidade das instituições participantes do projeto SEH e cientes dos possíveis desdobramentos, neste momento, optou-se por definir como público alvo desta fase da campanha os servidores, prestadores de serviço e discentes destas instituições, desde que seja possível identificar cada um desses grupos e, para os casos que não sejam possíveis, apenas servidores.

A estratégia de abordagem de cada grupo de pessoas deve ponderar seus tipos de vínculo e interesses, para de fato investigar a possível falta de conhecimento ou desatenção aos preceitos e cuidados necessários no uso de serviços online na Internet.

5 Especificação dos requisitos de hardware

Para instalação do software os requisitos de hardware mínimo são:

- Servidor físico ou virtual com 4GB RAM;
- 4 Cores (núcleos de processamento); e
- 50GB de espaço em disco.

6 Pré-requisitos para uso da ferramenta GoPhish

6.1 Requisitos técnicos

a) Instância de processamento (Servidor)
b) Servidor SMTP (para envio de e-mails)

6.2 Requisitos de negócio

a) Lista de usuários a serem abordados (público alvo)
b) Template para envio de mensagens

6.3 Observações

A respeito da instância de processamento, a ferramenta pode ser instalada utilizando servidor físico, ou virtual (diretamente no linux) ou ainda utilizando docker. É recomendado que este servidor tenha um IP válido para facilitar o acesso às páginas de captura (landing pages). Já o **servidor SMTP** pode ser instalado no mesmo servidor onde o GoPhish será executado. Lembre-se de autorizar o envio de e-mails a partir do servidor em seu firewall e DNS, para reduzir a chance dos e-mails de phishing simulados serem marcados como spam. Tanto para *templates* de e-mails quanto para *landing pages* a ferramenta pode fazer clone de mensagens e páginas já existentes, isso vai possibilitar criar iscas mais convincentes utilizando layouts e textos padronizados da instituição.

7 Metodologia

Considerando o exposto, a metodologia para aplicação da ferramenta GoPhish deve observar o público alvo e contexto definidos. Ademais, é necessário ter alguns cuidados para orientar e dar rigor ao trabalho a ser realizado com o propósito de facilitar reprodutividade em âmbito nacional, principalmente, nas instituições vinculadas à ANDIFES, bem como garantir a objetividade e imparcialidade na interpretação dos resultados.

Quatro campanhas de phishing serão realizadas durante a divulgação dos temas do Projeto SEH, sendo uma campanha pré-exposição aos temas do Projeto SEH, outra após a veiculação do tema “Phishing e Outros Golpes”, outra após o tema “Segurança Aplicada a Redes Sociais” e, no final após a vinculação dos doze temas uma campanha de pós-exposição.

7.1 Ciclo de vida das campanhas

O primeiro passo é definir os ciclos de vida de cada campanha a ser realizada. O ciclo de vida de cada campanha será composto por cinco etapas principais:

1. **Envio do e-mail:** realização do disparo inicial das mensagens simulando o ataque de phishing.

2. **Coleta de dados:** registro e armazenamento das interações dos usuários com as iscas enviadas.
3. **Análise dos resultados:** avaliação detalhada das métricas obtidas, incluindo taxas de cliques, capturas e padrões de comportamento.
4. **Divulgação dos resultados macros:** apresentação dos resultados consolidados, com foco em estatísticas gerais e sem exposição individual, às instituições participantes da ANDIFES.
5. **Descarte de material:** realizado ao final do Projeto SEH, garantindo que todo material digital qualitativo seja eliminado de forma segura e irreversível.

7.2 Comunicação com a alta gestão e as áreas de negócio

O segundo passo a ser dado é comunicar às autoridades da alta gestão e das áreas de negócio das instituições estritamente necessárias, para que entendam o propósito da ação e não haja nenhum mal entendido. Dessa forma, recomenda-se que seja feita uma reunião com os representantes da alta gestão e das áreas de negócio com a exibição de slides contendo a definição dos termos e estratégias a serem adotadas. Salienta-se que não devem ser informados o período e o veículo a ser utilizado para o ataque.

7.3 Temáticas para as fases das campanhas

O público alvo será abordado de diferentes formas por e-mail institucional dada a diversidade do interesse de cada grupo. Dessa maneira, sem a comunicação da área de negócio, com a finalidade de obter o estado atual sem ainda nenhuma intervenção, foram estipulados como assunto a ser tratado na primeira fase da campanha de phishing:

- Técnicos administrativos: e-mail com uma portaria falsa para atualizar e-mail até o fechamento da folha;
- Docentes: e-mail informando sobre o cálculo errado da progressão, Relatório de Atividade Acadêmica Docente (RAAD), e é necessário informar e-mail;
- Prestadores de serviços: e-mail com o endereço do formulário de pesquisa no Google Form sobre o término do contrato e solicitando e-mail para contato; e
- Discentes: e-mail informando as mudanças no sistema acadêmico, sendo necessário informar e-mail para atualizar cadastro.

Na segunda fase da campanha de phishing, os assuntos seriam:

- Técnicos administrativos: e-mail com a assunto “solicitação de troca de senha do sistema acadêmico aconteceu com sucesso” e como texto a mensagem de resposta: “sua senha do Instagram foi alterada com sucesso! Clique aqui caso não tenha solicitado <link>.”;
- Docentes: e-mail com a assunto “solicitação de troca de senha do sistema acadêmico aconteceu com sucesso” e como texto a mensagem de resposta: “sua senha do Instagram foi alterada com sucesso! Clique aqui caso não tenha solicitado <link>.”;

- Prestadores de serviços: e-mail com a assunto “solicitação de troca de senha do sistema administrativo aconteceu com sucesso” e como texto a mensagem de resposta: “sua senha do Instagram foi alterada com sucesso! Clique aqui caso não tenha solicitado <link>.”; e
- Discentes: e-mail com a assunto “solicitação de troca de senha do sistema acadêmico aconteceu com sucesso” e como texto a mensagem de resposta: “sua senha do Instagram foi alterada com sucesso! Clique aqui caso não tenha solicitado <link>.”.

Na terceira fase da campanha de phishing, os assuntos seriam:

- Técnicos administrativos: e-mail com o endereço do formulário de pesquisa no Google Form sobre adesão compulsória ao novo regime de trabalho;
- Docentes: e-mail com o endereço do formulário de pesquisa no Google Form sobre nova carga horária para docentes de acordo com o regime de trabalho;
- Prestadores de serviços: e-mail informando a mudança de unidade a qual está vinculado; e
- Discentes: e-mail informando a mudança de curso compulsória e a necessidade de clicar em link caso não deseje.

Na quarta e última fase opcional da campanha de phishing, os assuntos seriam:

- Técnicos administrativos: e-mail com uma portaria informando a mudança na base de cálculo da aposentadoria;
- Docentes: e-mail com uma portaria informando a mudança na base de cálculo da aposentadoria;
- Prestadores de serviços: e-mail pedindo a confirmação de vínculo para o pagamento do décimo terceiro salário; e
- Discentes: e-mail da coordenação informando que o prazo máximo de conclusão de curso foi atingido.

7.4 Ferramentas e materiais

7.4.1 Ferramentas

- Plataforma de simulação de phishing: a proposta é utilizar o GoPhish para a criação e gerenciamento das campanhas de simulação de phishing.
- Softwares Auxiliares: Ferramentas adicionais para coleta, análise e visualização de dados, incluindo planilhas eletrônicas, soluções de BI (Business Intelligence) e softwares de análise estatística.
- Formulários de pesquisa, por exemplo, no Google Forms: Para coletar feedback ou informações adicionais dos participantes, garantindo maior detalhamento na análise.

7.4.2 Materiais

Templates de e-mails e cenários simulados:

- E-mails: Mensagens personalizadas para simular tentativas de phishing realistas, respeitando diretrizes éticas. Os templates devem abordar temas relevantes ao contexto organizacional, sem exploração de tópicos sensíveis ou potencialmente ofensivos.

Relatórios pós-campanha:

- Documentos detalhados contendo análises quantitativas e qualitativas.
- Gráficos e tabelas que ilustram métricas como taxa de cliques, capturas e padrões de comportamento.
- Recomendações práticas para reforço da segurança da informação e capacitação dos colaboradores.

Esses materiais e ferramentas são indispensáveis para a condução eficaz e ética das campanhas de phishing, garantindo resultados significativos e alinhados aos objetivos do projeto.

7.5 Coleta e análise de dados

Os resultados da campanha serão coletados de formas estruturadas (.csv e .json), utilizando os relatórios gerados pela ferramenta GoPhish. Essa coleta tem como objetivo centralizar as informações e facilitar a análise dos dados relacionados ao comportamento dos usuários e à eficácia das iscas digitais utilizadas.

A análise dos dados se concentrará em:

- Identificação de padrões de comportamento, considerando os parâmetros especificados na Seção 11 deste documento;
- Detecção das principais vulnerabilidades;
- Mapeamento das áreas que requerem maior atenção ou reforço em treinamentos de segurança.

Para preservar a privacidade dos colaboradores, serão aplicadas técnicas de anonimização sempre que possível, evitando a exposição de informações individualizadas.

Sobre o resultado, para que se possa realizar comparativos entre as instituições participantes do Projeto SEH, bem como obter um panorama nacional sobre a segurança da informação, a coleta de resultados quantitativos deve seguir o seguinte padrão com identificações globais: isca, captura, total de usuários, público. Sendo,

- **Isca**: título da campanha e assunto abordado como estão ditos no texto do plano de conscientização do projeto SEH;
- **Captura**: quantidade de capturas (usuários fisgados);
- **Total de usuários**: Total de usuários na lista de distribuição (total do público alvo dessa campanha);
- **Público:** como padrão, a ferramenta deve abordar apenas o público alvo da instituição (servidores - técnicos administrativos e docentes, prestadores de serviço e discentes).

Ressalta-se que dados qualitativos não devem ser compartilhados para garantir privacidade e segurança dos membros das instituições participantes, e que cada um dos grupos deve ser identificado no relatório, para que os dados possam ser comparados adequadamente.

Agora com relação ao descarte dos dados digitais qualitativos desse trabalho em cada instituição, este deve ser feito de forma segura e completa, evitando que a informação seja recuperada. Para isso, é possível:

- Verificar se há um repositório posterior à exclusão dos dados;
- Utilizar softwares específicos terceirizados ou a tecnologia da informação;
- Certificar-se de que a exclusão foi completa de qualquer banco de dados digital.

Destaca-se ainda que os dados quantitativos não serão descartados, por esses servirem como retrato situacional e panorâmico da segurança da informação nos usuários finais dos serviços e sistemas nas instituições participantes e em âmbito nacional, além de servirem como base (ponto de partida) para futuros projetos de conscientização de segurança da informação.

8 Plano de comunicação

O plano de comunicação é uma etapa crucial para o sucesso da implementação do projeto de phishing. No entanto, o conteúdo a ser desenvolvido precisa estar alinhado com as melhores práticas de comunicação interna e externa da organização. Abaixo, estão os elementos principais a serem considerados nas etapas do processo:

Antes da simulação:

- Informar a alta gestão sobre o projeto, destacando seus benefícios e objetivos, como a identificação de vulnerabilidades e o fortalecimento da cultura de segurança da informação;
- Garantir transparência com a alta gestão, abordando possíveis preocupações ou resistências em relação aos "incidentes simulados" e solicitando suporte ativo;
- Notificar o(a) representante máximo das áreas de negócio relacionadas à temática abordada na simulação, garantindo ciência sobre o uso da temática, mas mantendo confidencialidade sobre datas e detalhes específicos para não comprometer a simulação;
- Estabelecer e divulgar um cronograma das simulações (equipe responsável pela simulação), alinhado com os responsáveis pela execução;
- Assegurar que os usuários tenham acesso a um repositório institucional, base de conhecimento ou central de serviços com orientações claras sobre como identificar e responder a tentativas de phishing reais.

Durante a simulação:

- Preparar orientações específicas para o gabinete institucional e áreas de negócio sobre como proceder em caso de registro de Boletim de Ocorrência relacionado ao phishing simulado considerando as estratégias de avaliação institucional da segurança da informação, e os dispositivos constantes em políticas e normativos internos de segurança;
- Instruir a equipe de TI a adotar uma abordagem cautelosa ao responder a solicitações de usuários sobre possíveis phishings durante a simulação, para evitar comprometimento dos resultados;
- Evitar notificar individualmente os usuários participantes antes do término da simulação, pois isso pode gerar alertas internos que comprometam a eficácia do exercício;
- Estar preparado para intervir de forma empática caso algum participante reaja emocionalmente à simulação, fornecendo suporte e orientações sobre como agir em situações reais de phishing.

Pós-simulação:

- Divulgar aos participantes a ocorrência da campanha de conscientização em segurança da informação e, na sequência, uma avaliação. O foco esteve no aprendizado do conteúdo e na identificação de vulnerabilidades específicas com a intenção de promover estratégias para evitar o compartilhamento inadvertido de informações sensíveis.
- Compartilhar relatórios detalhados com gestores, apresentando os resultados da simulação, incluindo taxas de engajamento e análise de vulnerabilidades detectadas;
- Comunicar aos gestores das áreas de negócio simuladas sobre as lições aprendidas, acompanhadas de recomendações práticas para fortalecer a postura de segurança da organização;
- Organizar workshops e treinamentos direcionados, focados nas fragilidades identificadas, para promover conscientização e habilidades práticas;
- Estar preparado para esclarecer possíveis mal-entendidos ou responder a resistências por parte dos usuários, ajustando as estratégias de comunicação e reforçando a importância do projeto.

9 Instalação e configuração

Estas instruções abordam o processo de instalação para os sistemas operacionais Linux e Windows através dos binários executáveis disponíveis.

9.1 Requisitos prévios

1. Acesse o repositório oficial: https://github.com/gophish/gophish/releases

2. Baixe a versão do GoPhish compatível com seu sistema operacional.

3. Certifique-se de que as portas 3333 e 80 estejam abertas no firewall para acesso interno e externo à máquina (servidor) a ser utilizada.

4. Tenha permissões administrativas no sistema.

9.2 Instalação no Linux

1. Baixe o instalador através do navegador ou via terminal, use o comando **wget**, substituindo **`vx.x.x`** pela versão mais recente disponível:

```
wget
https://github.com/gophish/gophish/releases/download/vx.x.x/gophish-vx.x.x-linux-64bit.zip
```

2. Extraia os arquivos utilizando o comando **unzip** e em seguida acesse a pasta utilizando o comando **cd**:

```
unzip gophish-vx.x.x-linux-64bit.zip
cd gophish
```

3. Execute o GoPhish utilizando as credenciais de administrador:

```
sudo ./gophish
```

4. Acesse a Interface Web através do endereço:

```
https://localhost:3333
```

O usuário padrão é admin e a senha será exibida no terminal na primeira inicialização.

9.3 Instalação no Windows

1. Baixe o instalador .zip correspondente ao Windows, substituindo **`vx.x.x`** pela versão mais recente disponível:

```
https://github.com/gophish/gophish/releases/download/vx.x.x/gophish-vx.x.x-windows-64bit.zip
```

2. Use o Explorador de Arquivos ou uma ferramenta como WinRAR/7-Zip para extrair o conteúdo.

3. Navegue até a pasta extraída e execute o gophish.exe.
4. Acesse a Interface Web através do endereço:

https://localhost:3333

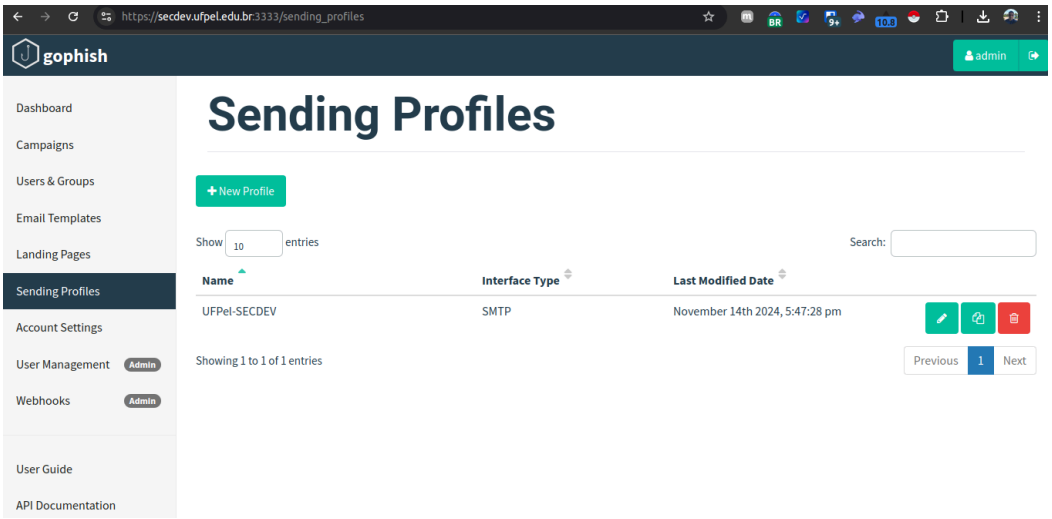
O usuário padrão é admin e a senha será exibida na janela do terminal ao executar o programa.

10 Operação e exemplos de aplicação

10.1 Criação de um sending profile:

Primeiro passo para utilizar a ferramenta é criar um “Sending Profile”, este será responsável por enviar os e-mails.

Para criação de um novo “Sending Profile” acesse a opção “Sending Profiles” localizado no menu à esquerda logo após clique em “New Profile”.



Ferramenta GoPhish - Sending Profiles

Para inserir um novo Sending Profile, você precisará das seguintes informações:

- Profile Name: Identificação deste profile no sistema
- Servidor SMTP a ser utilizado
- Usuário de conexão com servidor SMTP
- Senha para conexão com servidor SMTP

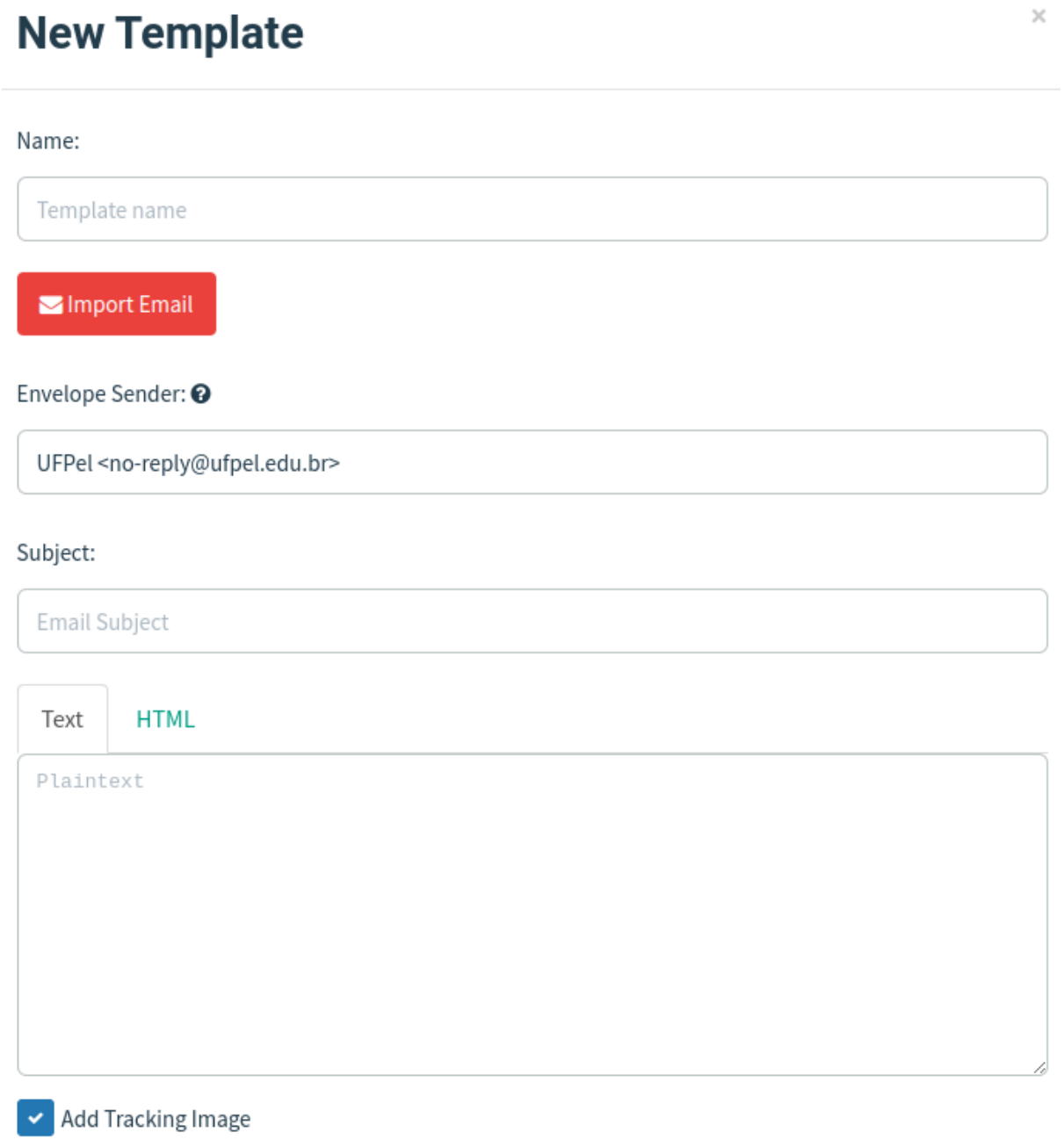
- SMTP From (Nome que aparecerá quando o e-mail for enviado)

Você pode ter mais de um sending profile cadastrado e definir qual utilizar em cada campanha.

10.2 Criação do template de e-mail

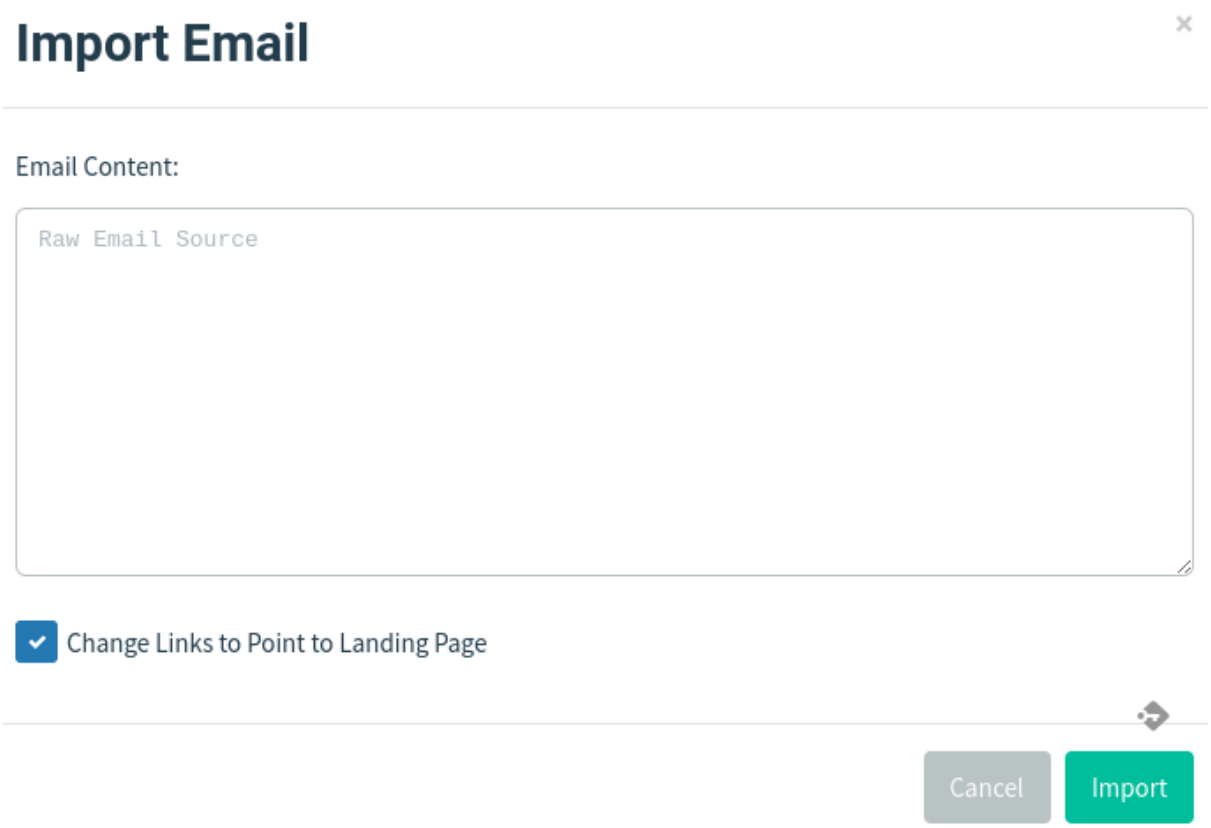
O próximo passo é criar um template de e-mail.

Para criação do template de e-mail acesse a opção “email Template” localizado no menu à esquerda, e clique em “New Template”.

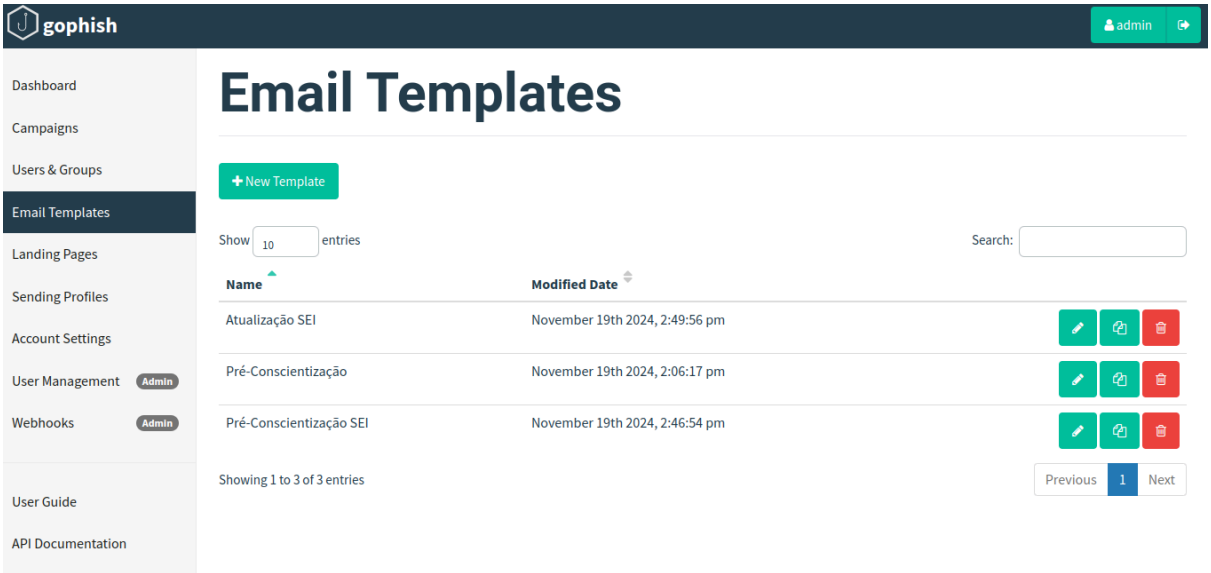


GoPhish - adicionar um novo template de e-mail

Nesta tela, podemos criar um template de e-mail manualmente ou importar o código fonte de um e-mail recebido previamente, para que a ferramenta GoPhish crie um clone do layout deste e-mail.



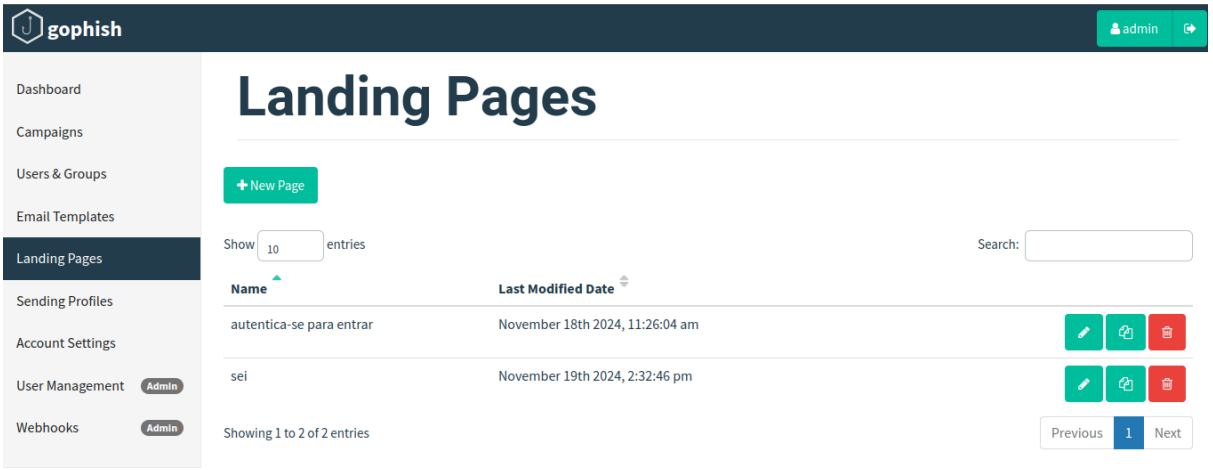
GoPhish - Importação de e-mail para criação de um novo template



GoPhish - Lista de Templates de e-mail

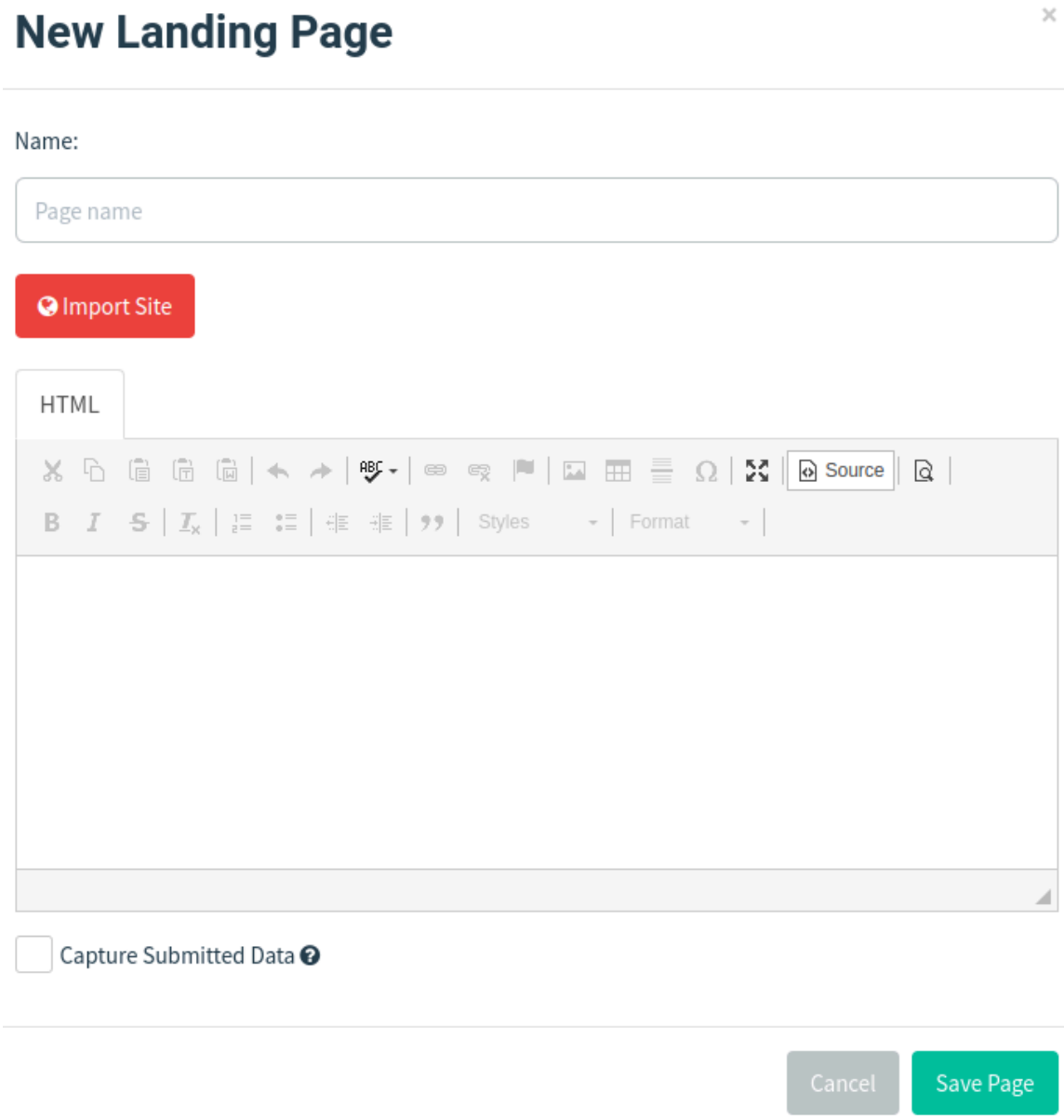
10.3 Criando uma landing page (página de captura)

Agora vamos criar uma página de aterrissagem (também conhecida como página de captura), é para esta página que os usuários serão direcionados quando clicarem no e-mail de phishing. Acesse o menu “Landing Pages” localizado no menu à esquerda.

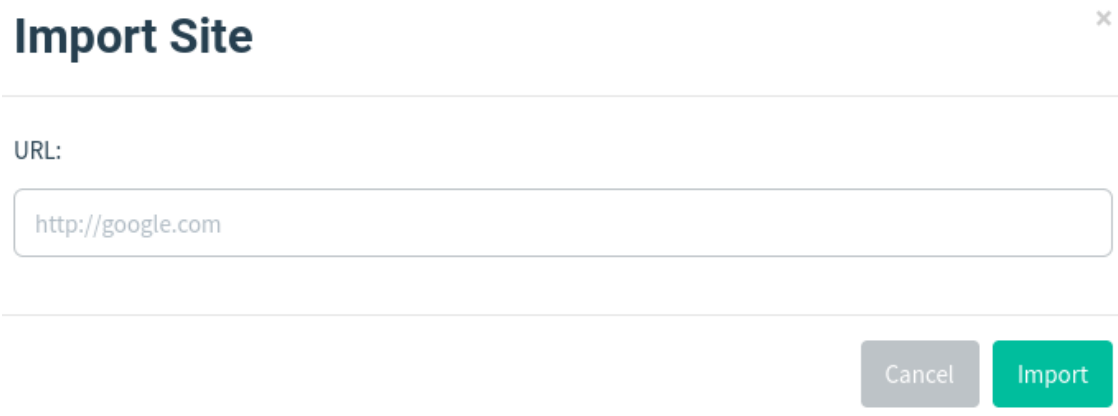


GoPhish - Lista de páginas de capturas (landing pages)

Clique em “New Page” para adicionar uma nova página, e preencha o nome da página e insira os códigos html. Você pode utilizar a opção “Importe site” para fazer o clone de uma página existente, deixando a experiência do usuário ainda mais fiel com a realidade.



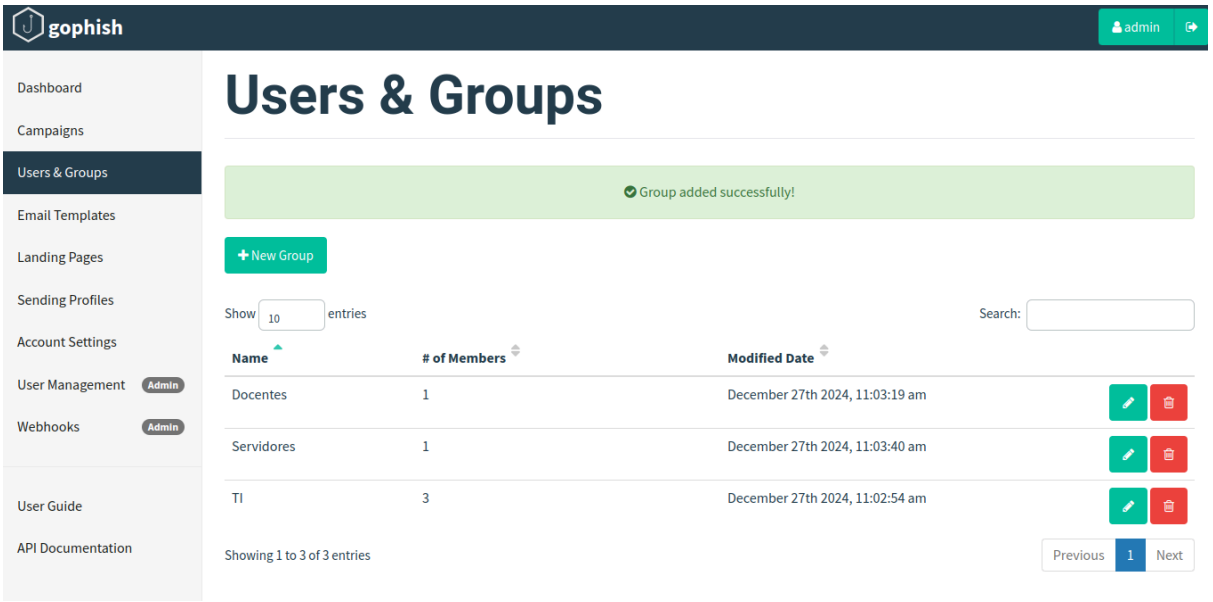
GoPhish - adicionar uma nova página de captura



GoPhish - Importar uma página pronta para criar uma nova página de captura

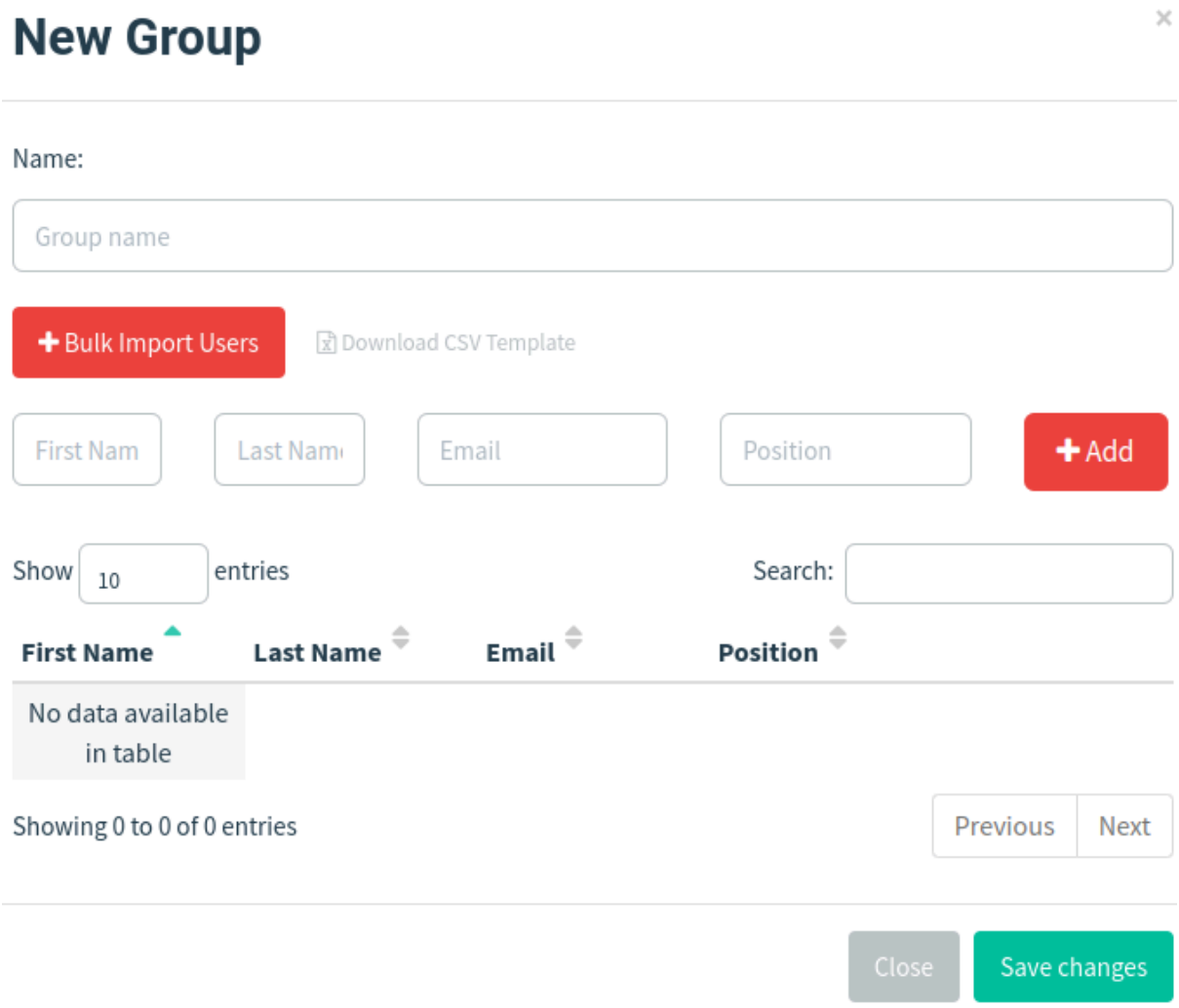
10.4 Criando grupos de disparos

Antes de dispararmos nossa campanha de phishing, precisamos parametrizar os grupos de disparos, para isso, acesse o menu “User & Groups”.



GoPhish - Lista de grupos alvos

Adicione um novo grupo alvo acessando o botão “New Group”.

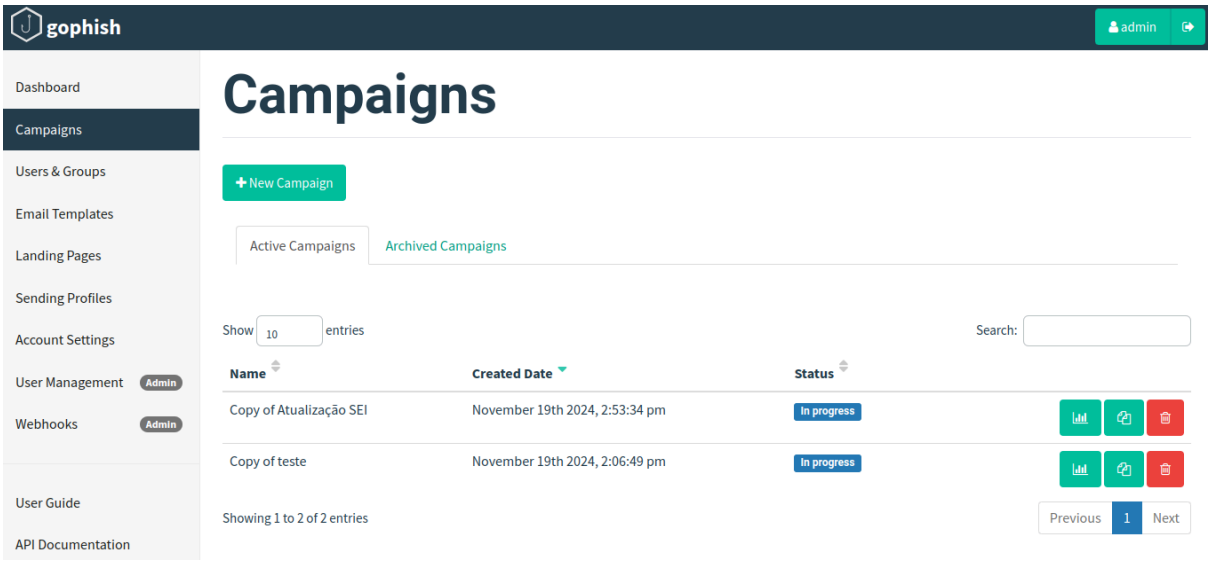


GoPhish - Adicionar um novo grupo alvo

Para adicionar um novo grupo você pode inserir manualmente os endereços ou fazer a importação de um arquivo .csv. Utilize o modelo de .csv disponível para download em “Download CSV Template”.

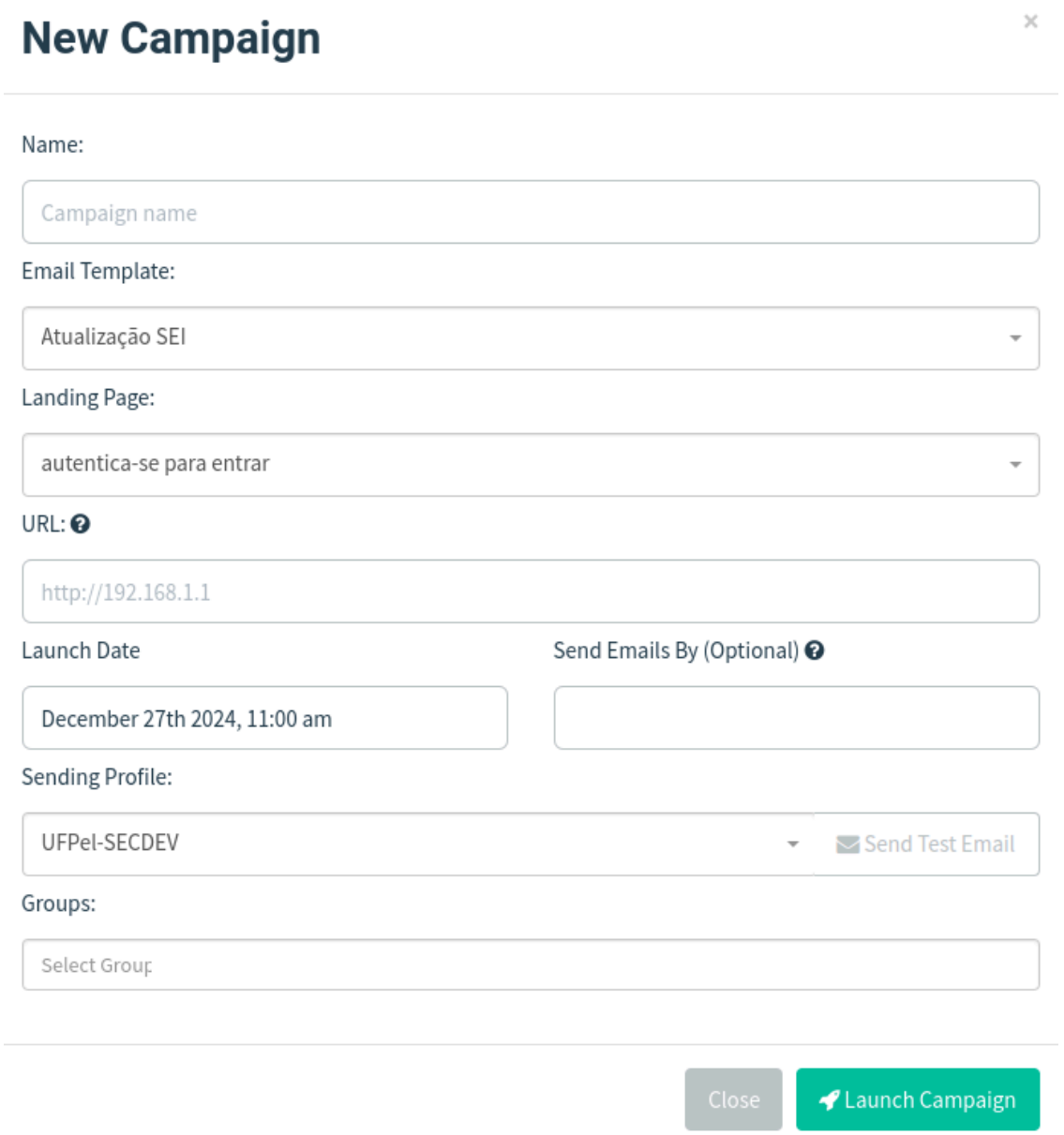
10.5 Disparando a campanha

Finalmente, depois de tudo configurado, vamos disparar a campanha de phishing Para isto, acesse o menu “Campaigns” localizado à esquerda.



GoPhish - Lista de campanhas

Clique em “New Campaign” e preencha os dados solicitados para criar uma nova campanha.



GoPhish - Criação de uma nova campanha

11 Análise de resultados

A análise dos resultados obtidos poderá indicar os maiores problemas observados e as oportunidades de melhoria da segurança da informação nas instituições participantes. Assim, com aplicação de diferentes instâncias desta campanha ou, simplesmente, com a pré e pós-exposição ao material a ser vinculado pelo projeto SEH poderá trazer indicativos valiosos.

Isso permitirá traçar o panorama de situações comuns aos ataques de phishing, que afetaram a maioria dos usuários, e possibilitar novos treinamentos direcionados. Com esse

propósito, são indicados parâmetros que servirão de base para essa análise mencionada, na Subseção 7.5:

1. Taxa de abertura de e-mails: porcentagem de e-mails que foram abertos pelos alvos em relação ao total de e-mails enviados;

2. Taxa de clique: porcentagem de alvos que clicaram em um link dentro do e-mail de phishing em comparação com o número de e-mails entregues;

3. Taxa de submissão de informações: porcentagem de alvos que preencheram informações sensíveis (como nome de usuário, senha, dados bancários, dentre outras informações) em uma página de captura simulada;

4. Taxa de detecção de phishing (reconhecimento de phishing): quantidade de alvos que marcaram o e-mail como spam ou phishing, ou relataram a tentativa de phishing de alguma outra forma;

5. Comportamento de retorno: usuários que clicaram no link de phishing ou forneceram informações sensíveis mais de uma vez durante a campanha;

6. Análise de resultados por grupo de alvos: segmentação dos resultados com base em grupos de alvos;

7. Acompanhamento do feedback dos usuários: feedback dos usuário sobre a campanha de phishing e seus resultados;

8. Análise de tendências ao longo do tempo: análise da campanha frente outras ações, inclusive outras campanhas, para identificar tendências e padrões ao longo do tempo.

12 Conscientização e treinamento

Consideramos que a conscientização é a campanha de phishing, enquanto que o treinamento já está abarcado nos treinamentos sobre segurança da informação previstos no contexto do plano de conscientização de segurança do projeto SEH.

Glossário

Colaborador: é qualquer indivíduo que, direta ou indiretamente, contribui para o funcionamento, o desenvolvimento e o alcance dos objetivos institucionais da universidade nas áreas de ensino, pesquisa, extensão e gestão. Isso inclui docentes, discentes, técnicos administrativos, prestadores de serviços, parceiros externos, ex-alunos e pesquisadores associados.

DNS: sigla para Domain Name System, que significa Sistema de Nomes de Domínio. É um serviço que funciona como uma agenda telefônica da internet, permitindo que os usuários acessem a web por meio de nomes de domínio, como nytimes.com ou espn.com, em vez de endereços IP. Neste serviço também são configurados quais servidores têm autorização para enviar e-mails do domínio específico através da entrada *SPF.*

Firewall: dispositivo de segurança que controla o tráfego de rede, permitindo ou bloqueando o acesso de dados de acordo com um conjunto de regras. O objetivo é evitar que dados não autorizados sejam transmitidos entre redes e que atividades mal-intencionadas sejam realizadas.

Landing page: conhecida como página de conversão, de aterrissagem, de captura ou de destino, é uma página da web criada para converter visitantes em leads ou vendas. Em nosso escopo a *landing page* será utilizada para aterrissar os usuários e coletar as informações.

Prestadores de serviço ou terceirizados: profissionais contratados para funções operacionais, como limpeza, segurança e manutenção, que atuam dentro do ambiente universitário.

Servidor SMTP: computador ou software que envia e retransmite e-mails, utilizando o protocolo Simple Mail Transfer Protocol (SMTP). Ele é também conhecido como servidor de e-mail de saída.

ANDIFES

CGTIC

SEH
SEGURANÇA NO
ELEMENTO
HUMANO