

Exercícios de Phishing

Filipa Macieira



Agenda

- Para que servem?
- Requisitos
- GoPhish



PARA QUE SERVEM?

Para que servem os exercícios de phishing?

Utilizadores



Testar os utilizadores perante situações de Phishing

Educar e enriquecer o "*Awareness*" nos utilizadores

Para que servem os exercícios de phishing?

Organizações



Estimar o risco de ocorrência de incidentes perante ataques desta natureza

Avaliar se os utilizadores da organização carecem de algum tipo de formação perante este tipo de ataques

REQUISITOS

Requisitos



Ter um domínio específico para os exercícios



Criar um certificado específico para o website



Requisitos

Criar o registo SPF para o envio de emails

Instalar uma plataforma que faça a gestão do exercício



Serviço de Phishing



Retirado de <https://www.social-engineer.com/phishing-service/>

Plataformas gratuitas

- GoPhish – <https://getgophish.com>



- Phishing Frenzy –
<https://github.com/pentestgeek/phishing-frenzy>



- King Phisher –
<https://github.com/securestate/king-phisher>



- SecurityIQ PhishSim –
<https://securityiq.infosecinstitute.com/>



GOPHISH

Plataforma escolhida

A screenshot of the gophish web application login page. The interface has a dark blue header with the "gophish" logo and a hamburger menu icon. The main content area is white and features a large hexagonal icon with a fishing hook inside. Below the icon, the text "Please sign in" is displayed. There are two input fields: the first contains the text "admin" and the second contains seven dots representing a password. A green "Sign in" button is positioned below the password field.

gophish



Please sign in

admin

.....

Sign in

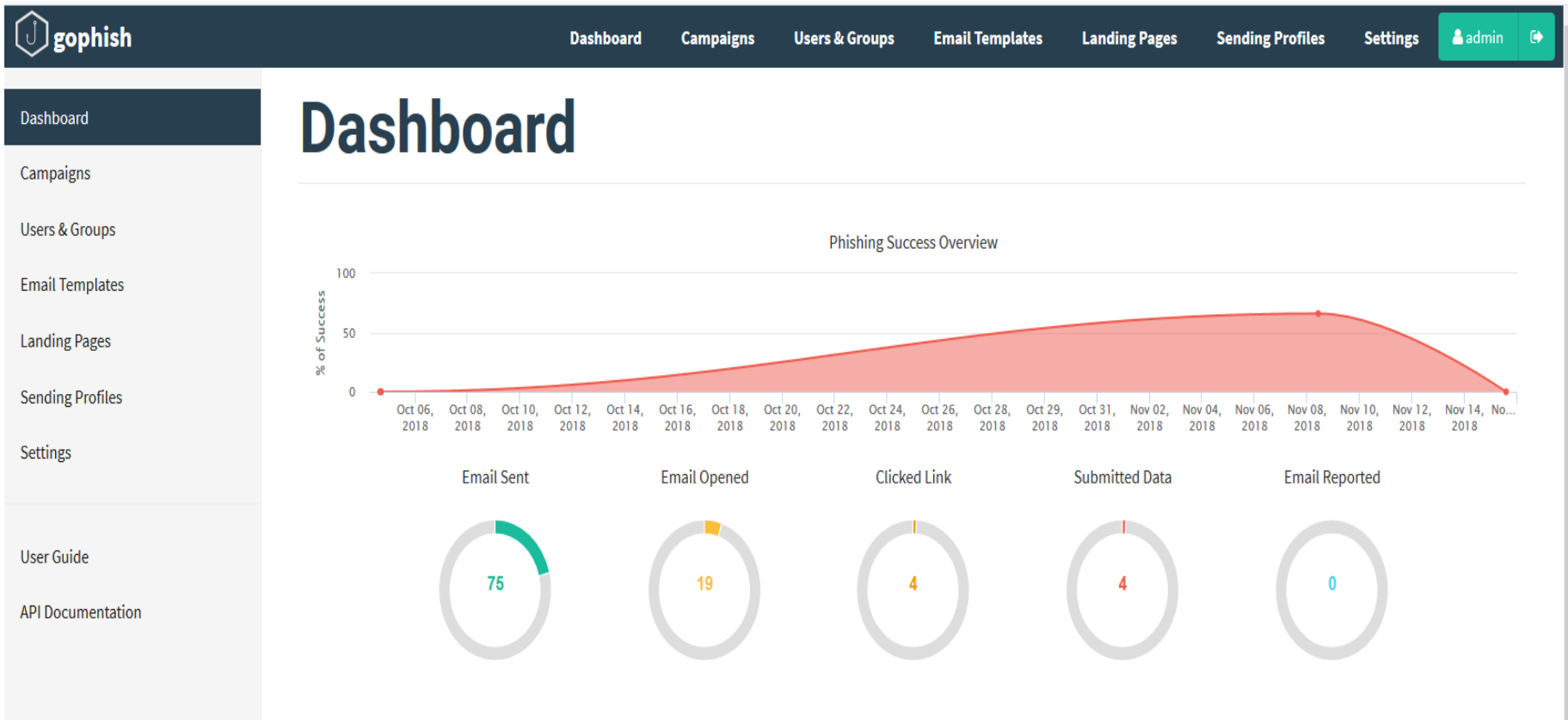
GoPhish - Funcionalidades

- Executa múltiplas campanhas em simultâneo
- Efetua cópias de websites para replicar numa campanha de phishing
- Permite a elaboração de vários *templates* de websites e emails através de HTML e CSS


GoPhish - Funcionalidades

- Criação de Headers específicos para os e-mails
- Fornece informação detalhada sobre as métricas associadas ao exercício de phishing, como por exemplo **quem abriu o email, quem abriu o website e quem introduziu informações sobre credenciais**, tudo com o seu respetivo *“timestamp”*

Dashboards



Dashboards




DashboardCampaignsUsers & GroupsEmail TemplatesLanding PagesSending ProfilesSettingsadmin

DashboardCampaignsUsers & GroupsEmail TemplatesLanding PagesSending ProfilesSettingsUser GuideAPI Documentation


Timeline for Coordinator RCTS CERT

Email: coordinator@cert.rcts.pt




Campaign Created

November 9th 2018 10:00:49 am



Email Sent

November 9th 2018 10:00:51 am




Clicked Link

November 9th 2018 10:13:20 am

Windows (OS Version: 10)

Chrome (Version: 70.0.3538.77)



Submitted Data


November 9th 2018 10:14:07 am

Windows (OS Version: 10)

Chrome (Version: 70.0.3538.77)

Replay Credentials

View Details



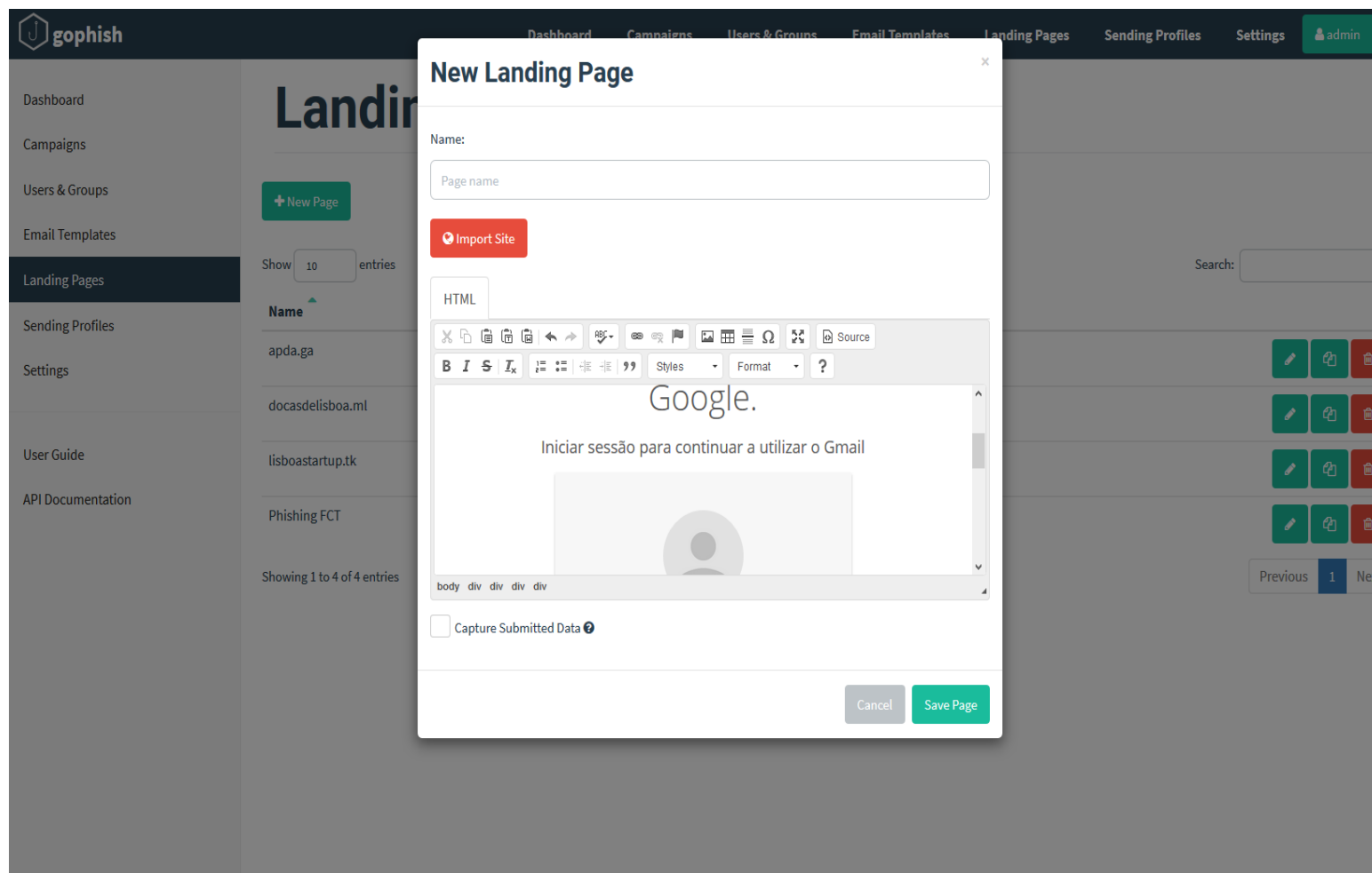
Clicked Link

November 9th 2018 10:14:43 am

Windows (OS Version: 10)

Chrome (Version: 70.0.3538.77)

Landing Pages

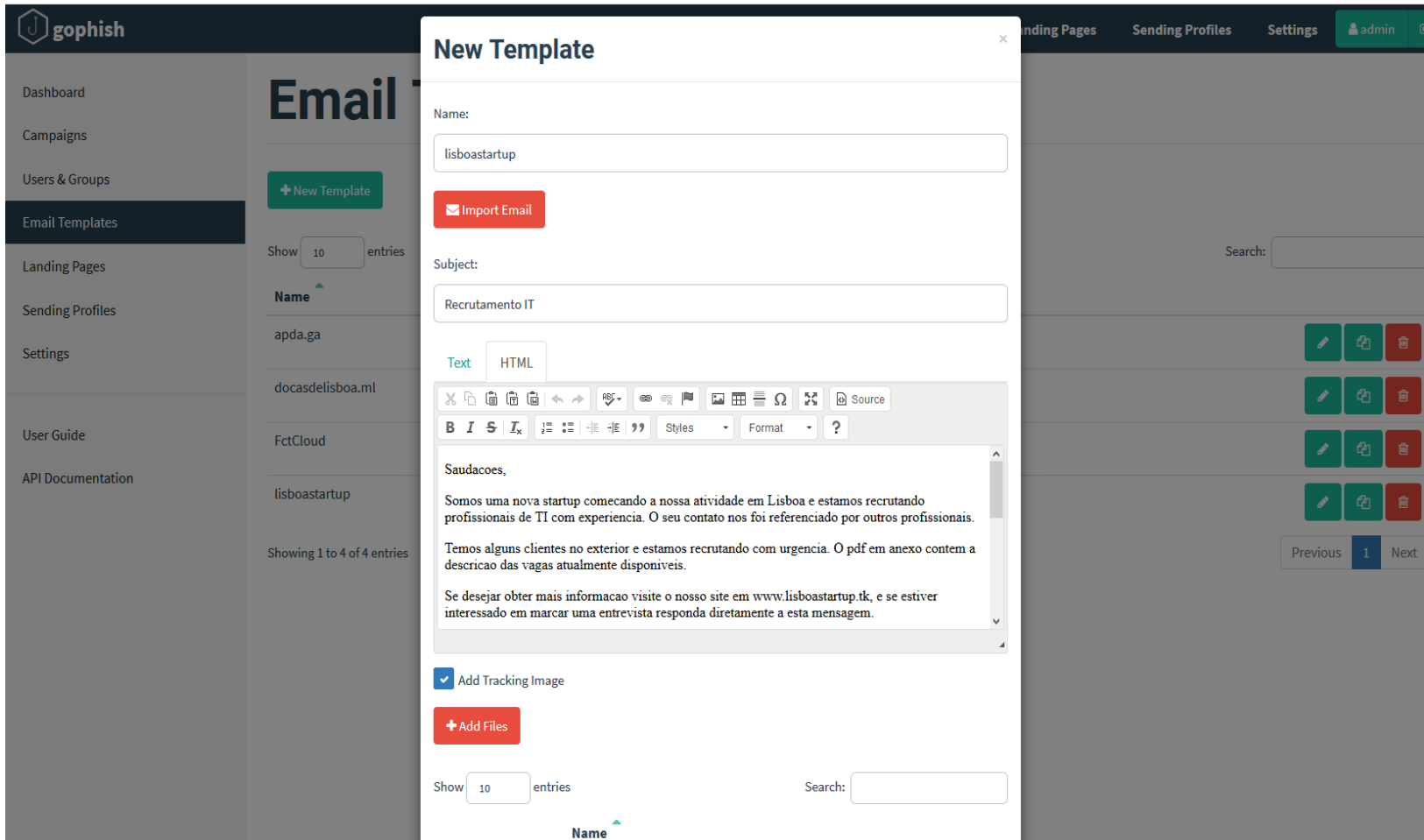


The screenshot displays the Gophish web interface. A modal window titled "New Landing Page" is open in the center. The modal contains the following elements:

- Name:** A text input field with the placeholder "Page name".
- Import Site:** A red button with a heart icon and the text "Import Site".
- HTML:** A tab labeled "HTML" is selected, showing a rich text editor. The editor contains the text "Google." and "Iniciar sessão para continuar a utilizar o Gmail" above a placeholder image of a person's profile.
- Capture Submitted Data:** A checkbox labeled "Capture Submitted Data" with a help icon.
- Buttons:** "Cancel" and "Save Page" buttons at the bottom right of the modal.

The background interface shows the Gophish dashboard with a sidebar on the left containing links to Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages (highlighted), Sending Profiles, Settings, User Guide, and API Documentation. The main area displays a list of landing pages with columns for Name, Show, and entries. The list includes entries like "apda.ga", "docasdelisboa.ml", "lisboastartup.tk", and "Phishing FCT".

Email Templates



The screenshot displays the Gophish web interface. On the left is a sidebar with navigation links: Dashboard, Campaigns, Users & Groups, Email Templates (selected), Landing Pages, Sending Profiles, Settings, User Guide, and API Documentation. The main content area is titled 'Email Templates' and features a '+ New Template' button. Below this is a list of existing templates with columns for 'Name' and 'entries'. The 'New Template' modal is open, showing the following fields and options:

- Name:** A text input field containing 'lisboastartup'.
- Import Email:** A red button with an envelope icon.
- Subject:** A text input field containing 'Recrutamento IT'.
- Text/HTML:** Two tabs, with 'Text' currently selected.
- Rich Text Editor:** A toolbar with icons for bold, italic, underline, strikethrough, bulleted list, numbered list, link, unlink, image, table, horizontal line, undo, redo, and a 'Source' button. Below the toolbar is the text content:

Saudacoes,

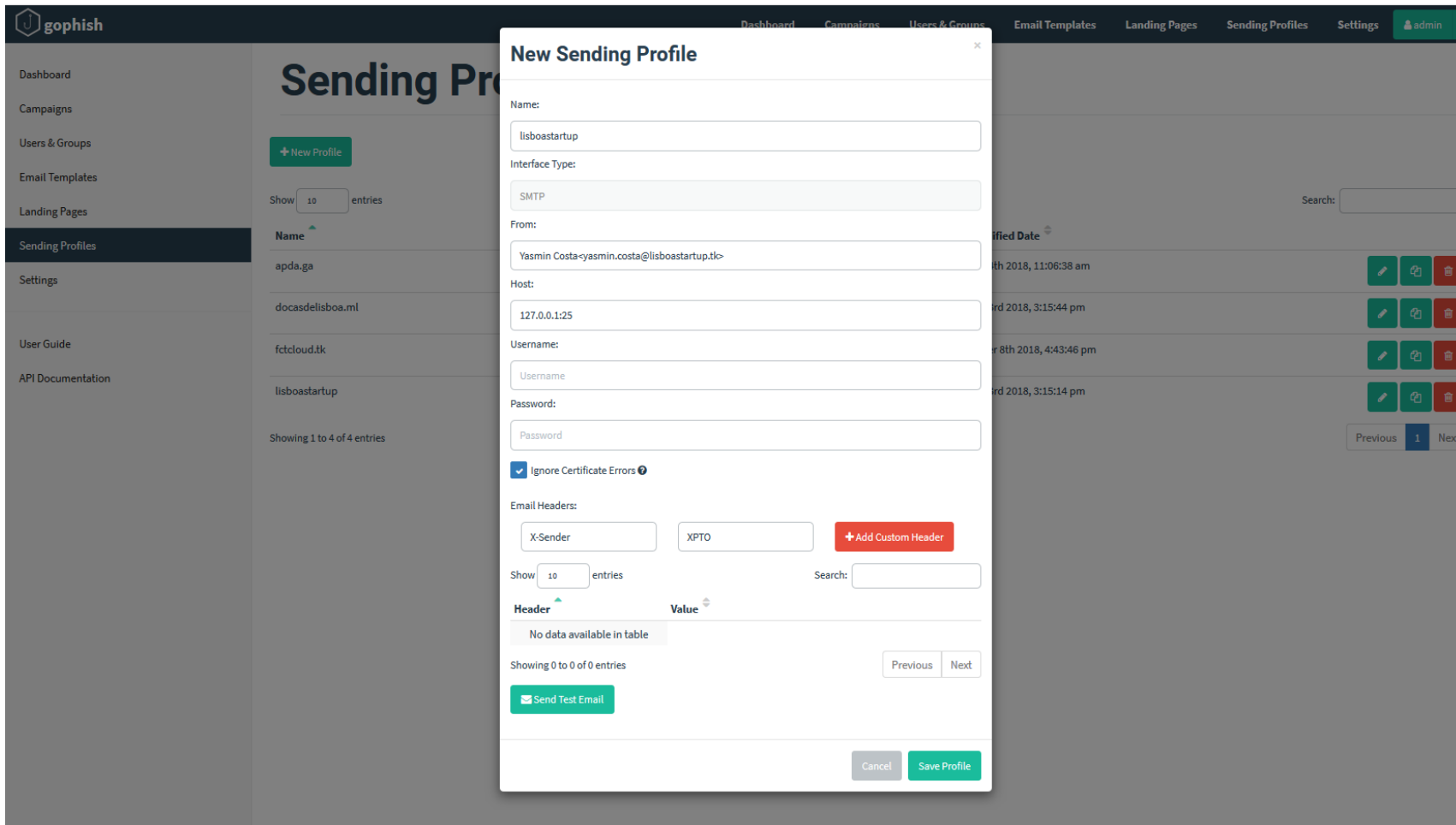
Somos uma nova startup comecando a nossa atividade em Lisboa e estamos recrutando profissionais de TI com experiencia. O seu contato nos foi referenciado por outros profissionais.

Temos alguns clientes no exterior e estamos recrutando com urgencia. O pdf em anexo contam a descricao das vagas atualmente disponiveis.

Se desejar obter mais informacao visite o nosso site em www.lisboastartup.tk, e se estiver interessado em marcar uma entrevista responda diretamente a esta mensagem.
- Add Tracking Image:** A checked checkbox.
- Add Files:** A red button with a plus icon.
- Footer:** 'Show 10 entries' and a 'Search:' input field.

The background shows a list of templates with names like 'apda.ga', 'docasdelisboa.ml', 'FctCloud', and 'lisboastartup'.

Perfis de Envio



The screenshot displays the 'gophish' web application interface. A modal window titled 'New Sending Profile' is open, allowing the user to configure a new email sending profile. The background shows the main dashboard with a sidebar menu and a 'Sending Profiles' table.

gophish

Dashboard Campaigns Users & Groups Email Templates Landing Pages Sending Profiles Settings admin

Sending Profiles

+ New Profile

Show 10 entries

Name
apda.ga
docasdelisboa.ml
fctcloud.tk
lisboastartup

Showing 1 to 4 of 4 entries

New Sending Profile

Name: lisboastartup

Interface Type: SMTP

From: Yasmin Costa <yasmin.costa@lisboastartup.tk>

Host: 127.0.0.1:25

Username: Username

Password: Password

☒ Ignore Certificate Errors

Email Headers:

X-Sender	XPTO	+ Add Custom Header
----------	------	---------------------

Show 10 entries Search:

Header	Value
No data available in table	

Showing 0 to 0 of 0 entries Previous Next

Send Test Email

Cancel Save Profile

Em Resumo



Testar os utilizadores perante situações de Phishing



Estimar o risco de ocorrência de incidentes perante ataques desta natureza



Requisitos para realizar um exercício de Phishing: investimento zero



Obrigado