

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>

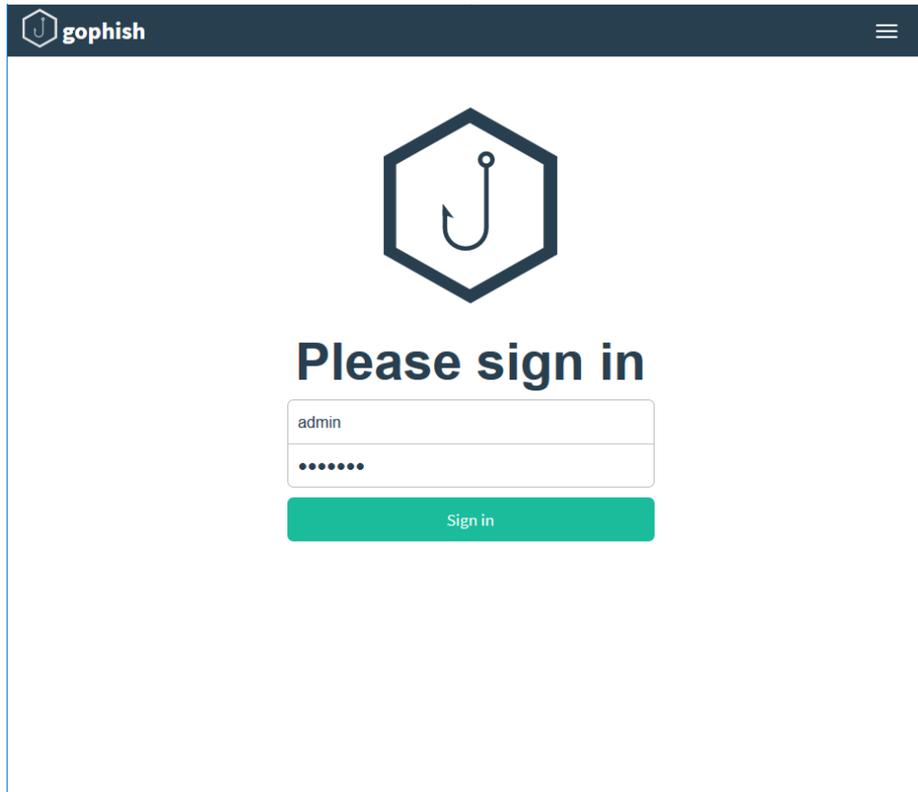


- SecurityIQ PhishSim – <https://securityiq.infosecinstitute.com/>



GOPHISH

Plataforma escolhida



The screenshot shows a web browser window with the URL 'gophish'. The page features a dark blue header with the 'gophish' logo and a hamburger menu icon. The main content area is white and contains a large hexagonal logo with a hook inside. Below the logo, the text 'Please sign in' is displayed. There are two input fields: the first contains the text 'admin' and the second contains six 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

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

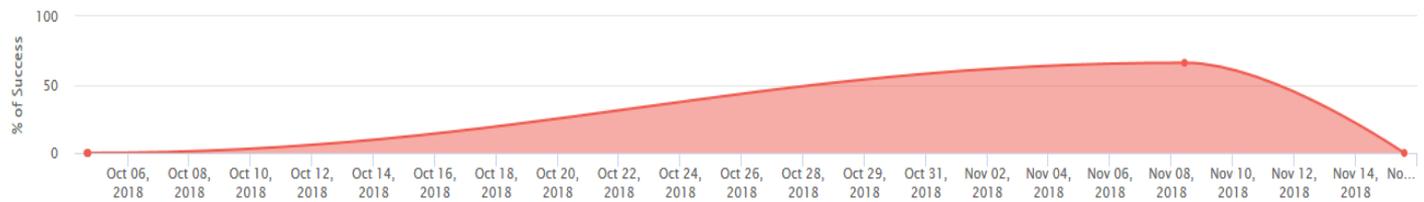
Settings

User Guide

API Documentation

Dashboard

Phishing Success Overview



Email Sent



Email Opened



Clicked Link



Submitted Data



Email Reported



Dashboards

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

- Dashboard
- Campaigns**
- Users & Groups
- Email Templates
- Landing Pages
- Sending Profiles
- Settings
- User Guide
- API Documentation

Timeline for Coordinator RCTS CERT

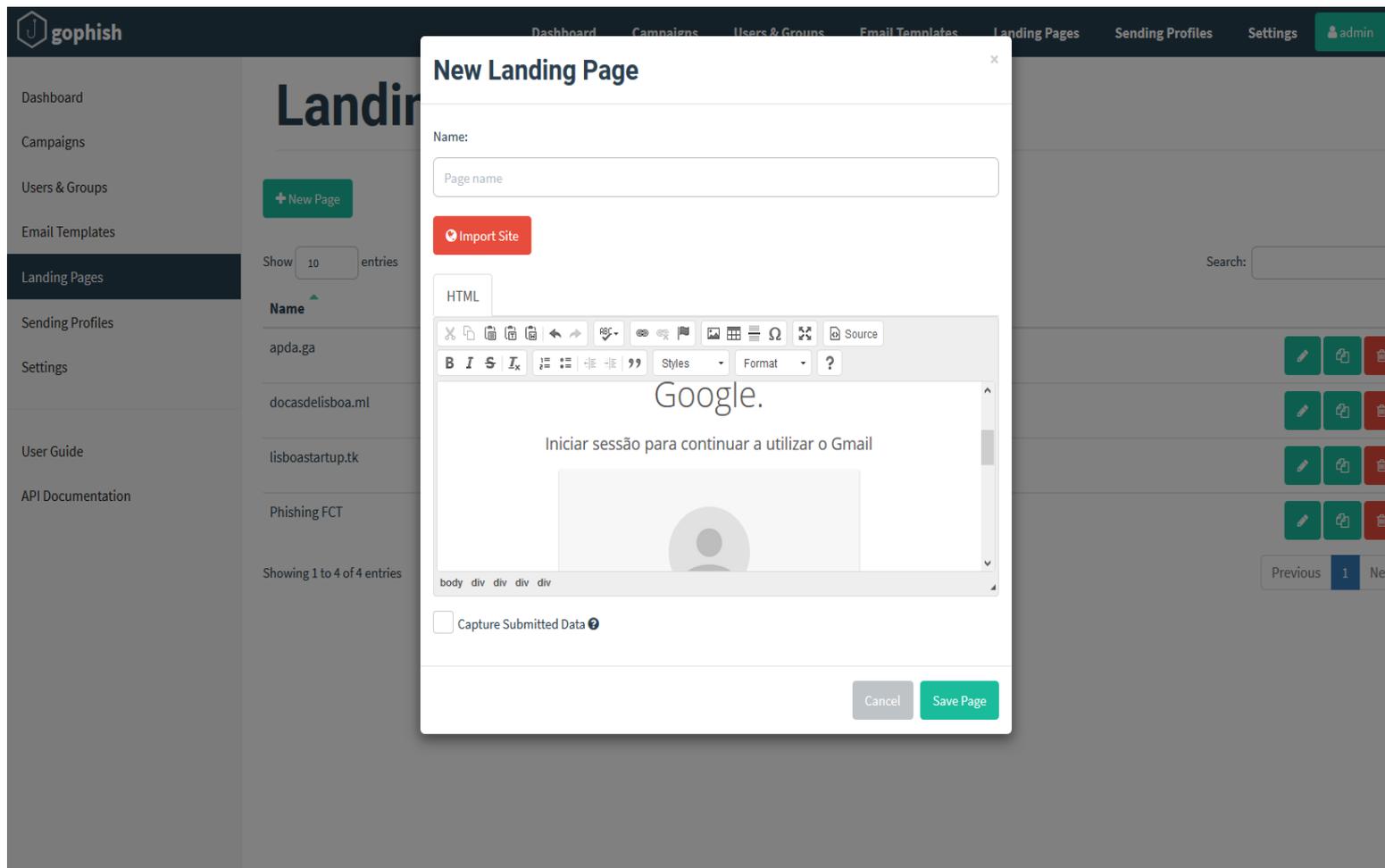
Email: coordinator@cert.rcts.pt

-  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

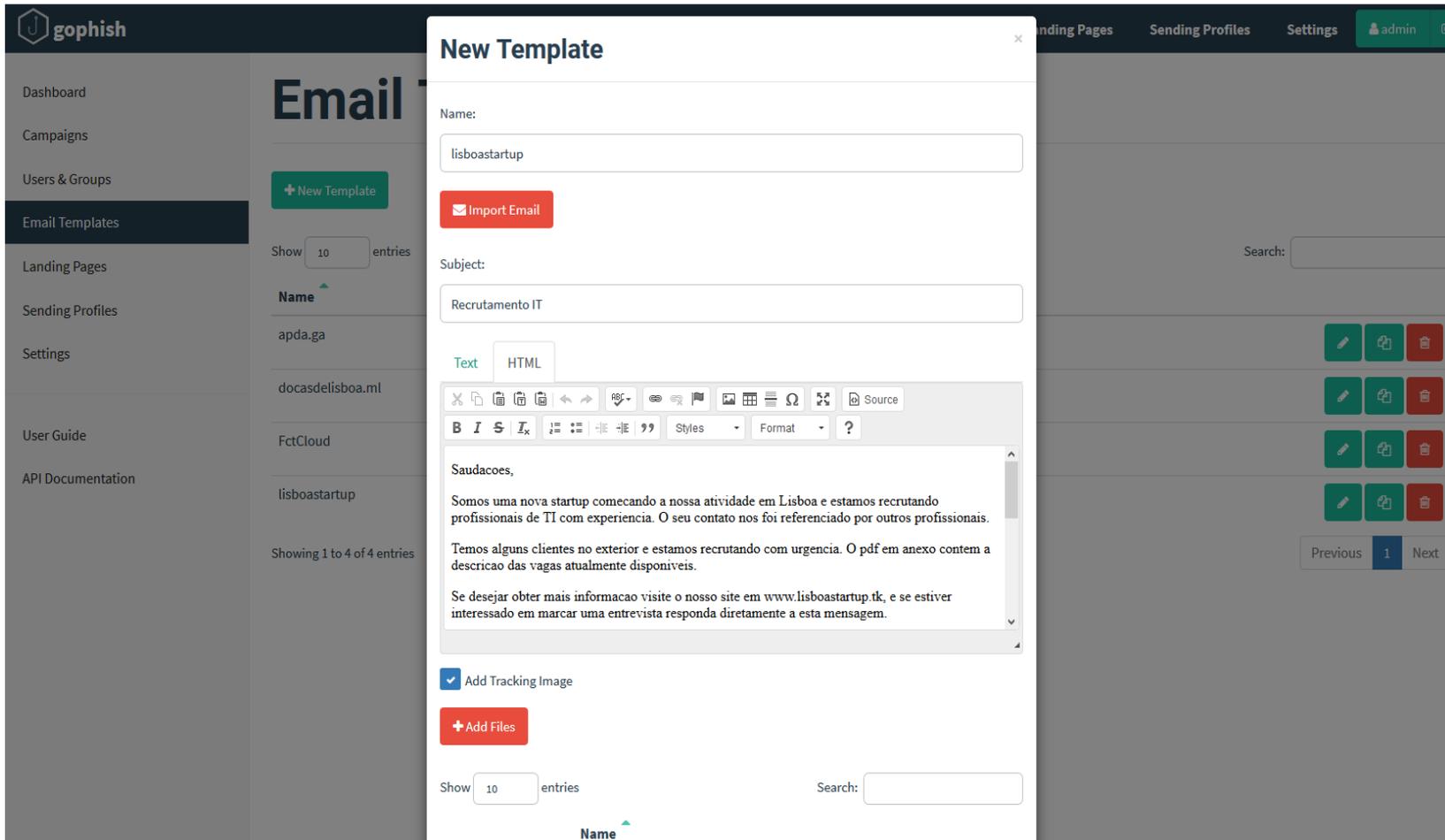


The screenshot displays the Gophish web interface with a 'New Landing Page' modal window open. The modal contains the following elements:

- Name:** A text input field labeled 'Page name'.
- Import Site:** A red button with a red arrow icon.
- HTML:** A rich text editor with a toolbar containing icons for undo, redo, bold, italic, strikethrough, link, unlink, list, and other formatting options. The editor shows a preview of a landing page with the text 'Google.' and 'Iniciar sessão para continuar a utilizar o Gmail'.
- Capture Submitted Data:** A checkbox with the label 'Capture Submitted Data'.
- Buttons:** 'Cancel' and 'Save Page' buttons at the bottom right of the modal.

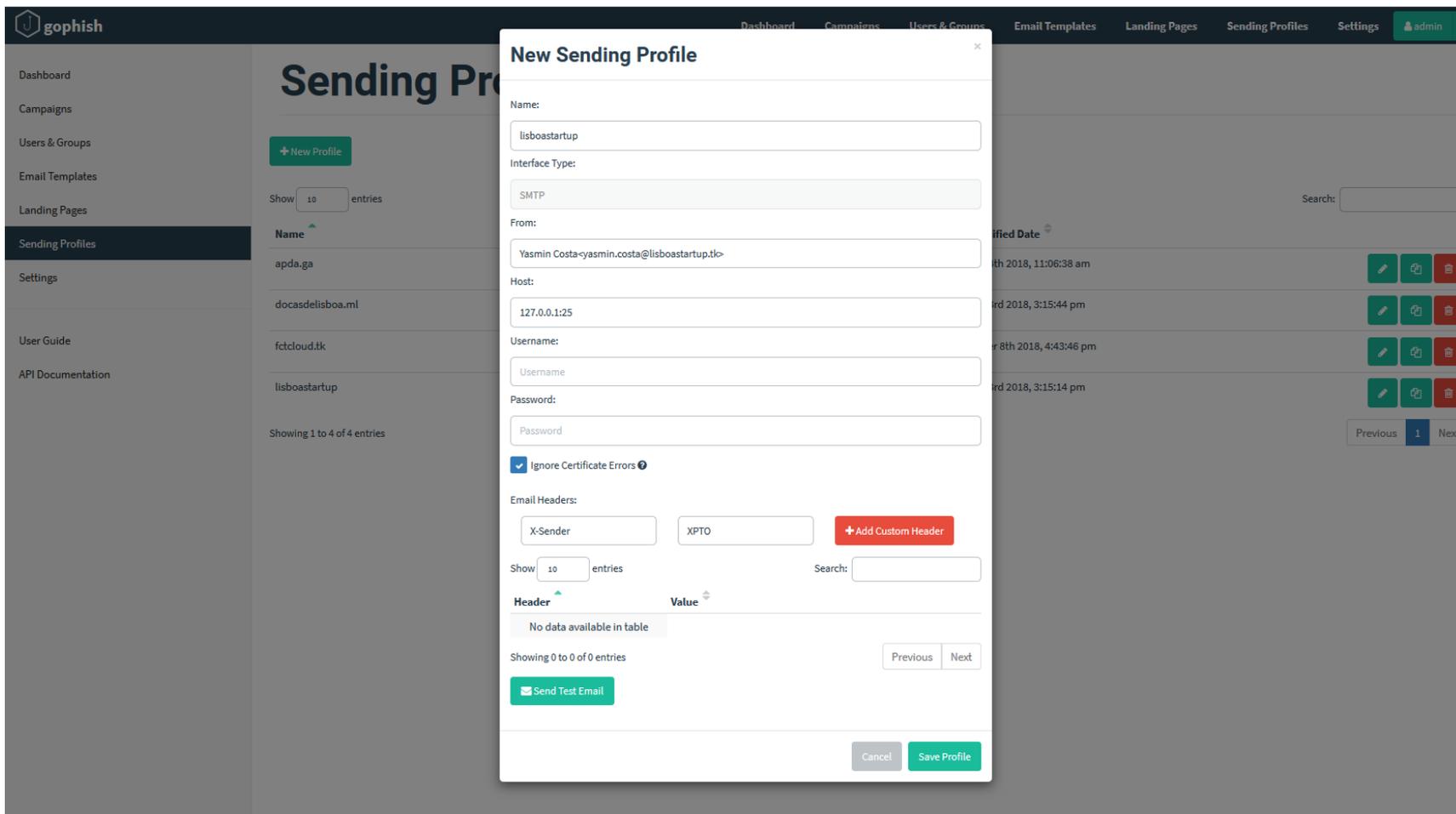
The background interface shows a sidebar with navigation options like 'Dashboard', 'Campaigns', 'Users & Groups', 'Email Templates', 'Landing Pages', 'Sending Profiles', 'Settings', 'User Guide', and 'API Documentation'. The main content area displays a list of landing pages with columns for 'Name' and 'entries'.

Email Templates



The screenshot displays the Gophish web interface for managing email templates. On the left, a sidebar menu includes Dashboard, Campaigns, Users & Groups, Email Templates (highlighted), Landing Pages, Sending Profiles, Settings, User Guide, and API Documentation. The main content area shows a list of templates with columns for Name and entries. A modal window titled "New Template" is open, allowing the user to create a new template. The modal includes a "Name" field with the value "lisboastartup", an "Import Email" button, a "Subject" field with the value "Recrutamento IT", and a rich text editor with "Text" and "HTML" tabs. The rich text editor contains the following text: "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 contem 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." Below the editor, there is a checked "Add Tracking Image" option and an "Add Files" button. The modal also features a "Show 10 entries" dropdown and a search field.

Perfis de Envio



The screenshot displays the 'gophish' web interface. A modal window titled 'New Sending Profile' is open, allowing the user to configure a new sending profile. The background shows the 'Sending Profiles' management page with a list of existing profiles and a '+ New Profile' button.

New Sending Profile Form:

- 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
- Header Table:**

Header	Value
No data available in table	

Buttons: 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