



RNEP-GW

MÓDULO CAMPANHAS DE PHISHING



MALDADE



TREINO



Credits: Image generated with Freepik AI Suite

EXERCÍCIOS DE PHISHING

Para que servem?

Quais são as regras de ouro?

Acções de sensibilização



SE É NECESSÁRIO SABER O «QUEM»...

...então terão que construir a vossa própria campanha!

Nós nunca identificaremos quem «clickou» ou introduziu dados

Também nunca guardamos o que é introduzido numa «landing page»



REQUISITOS





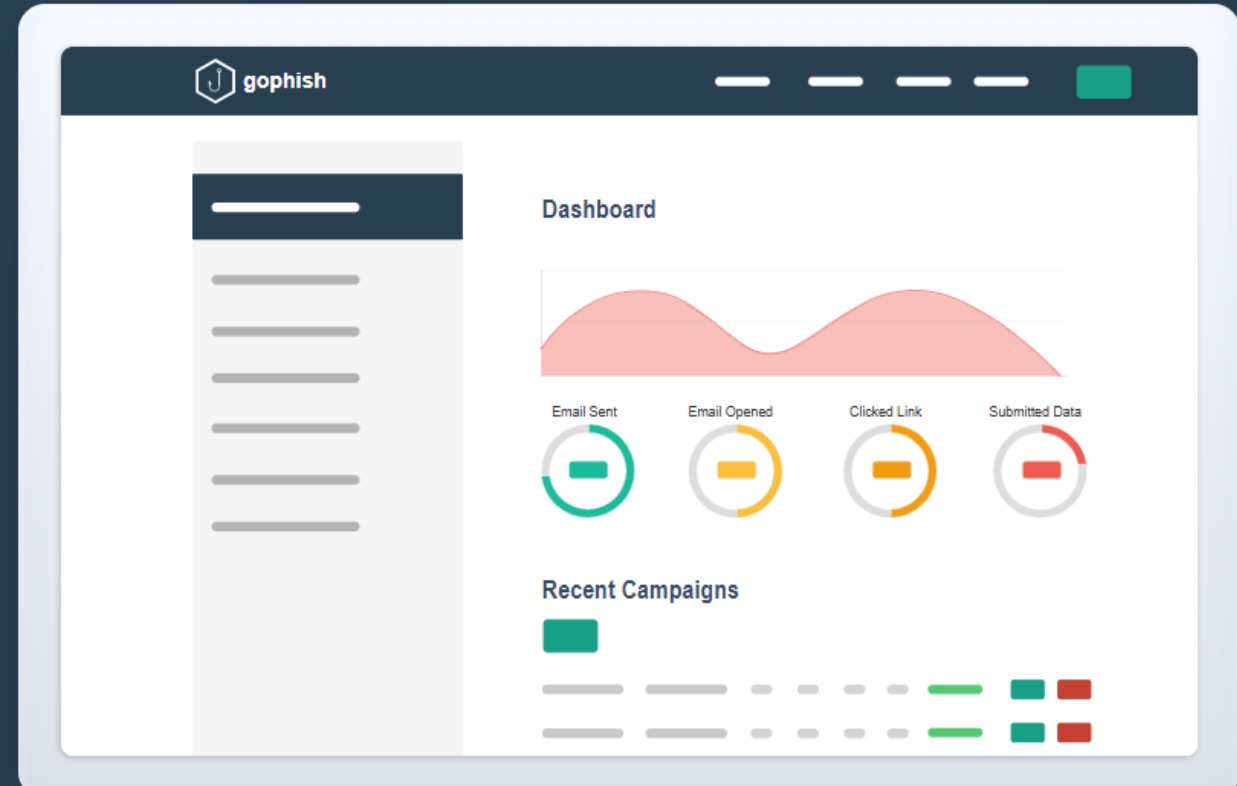
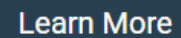
PLATAFORMAS GRATUITAS

GoPhish - <https://getgophish.com>

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

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

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



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

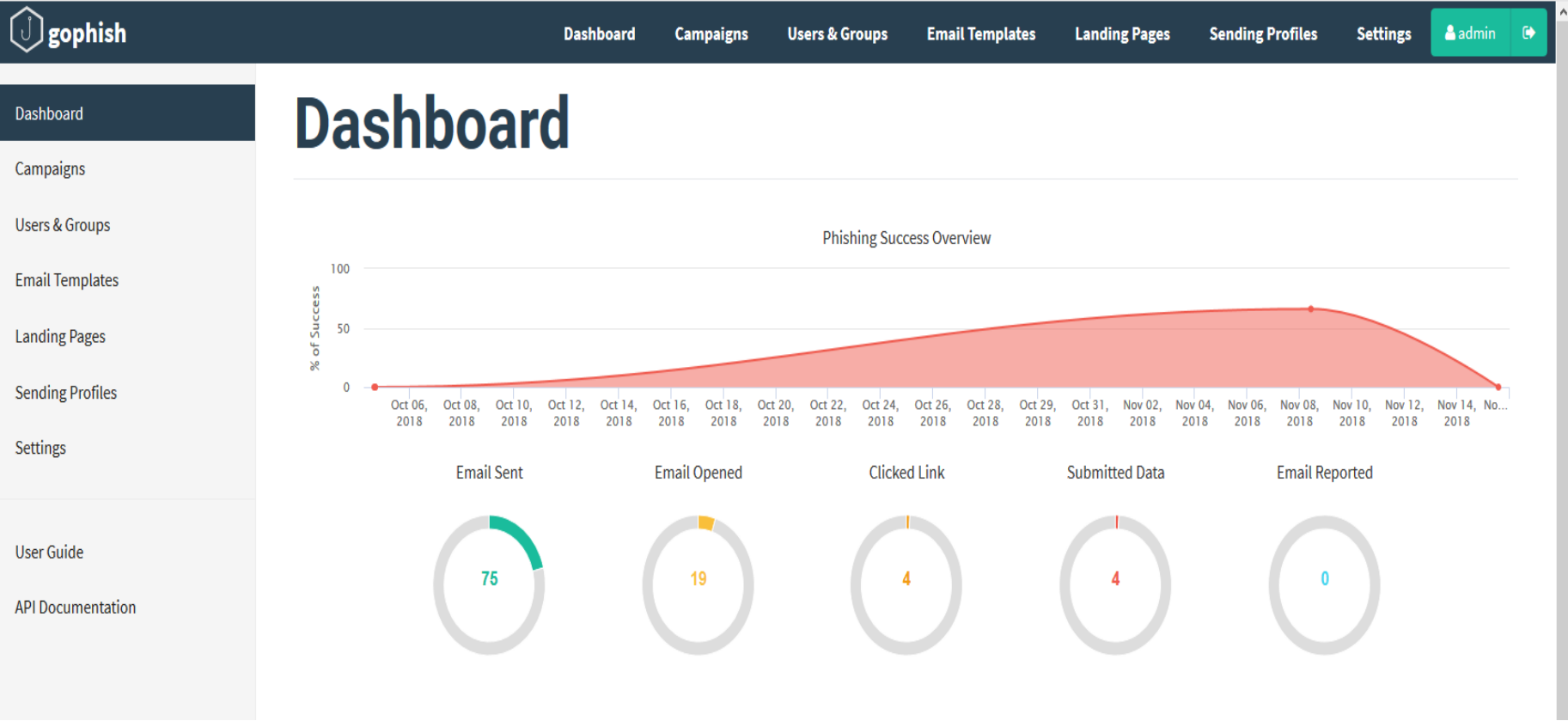


Fornece informação detalhada sobre as métricas associadas ao exercício de Phishing:

- quem abriu a mensagem;
- quem abriu o link acedendo ao website fraudulento;
- quem introduziu informações (i.e. credenciais).

Cada interacção com a plataforma tem um timestamp associado

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

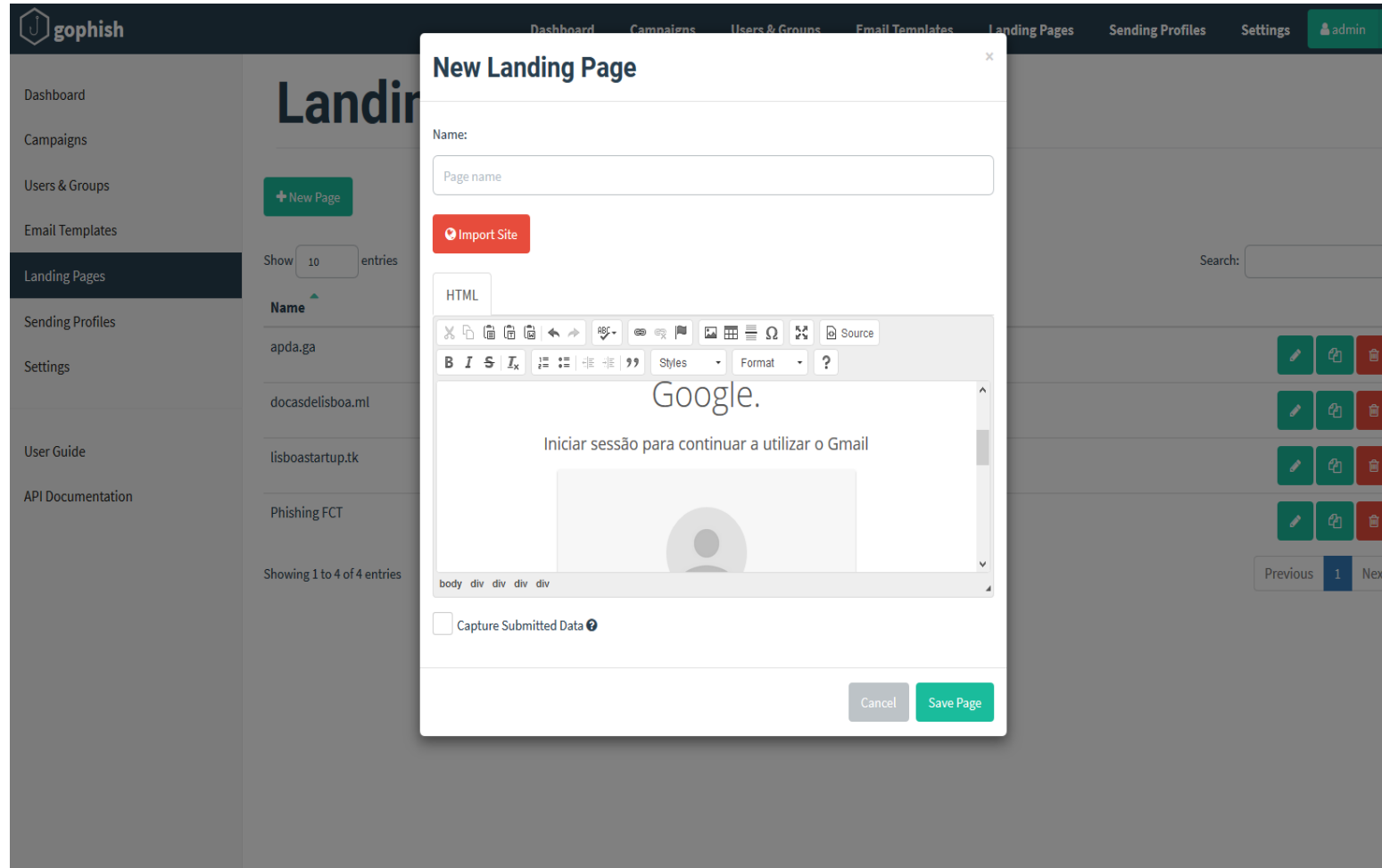


Clicked Link

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 with a 'New Landing Page' modal open. The modal contains the following elements:

- Name:** A text input field with the placeholder 'Page name'.
- Import Site:** A red button with a circular arrow icon.
- HTML Editor:** A rich text editor with a toolbar including icons for undo, redo, bold, italic, text color, background color, link, unlink, list, and source. The editor content shows the Google logo and the text 'Iniciar sessão para continuar a utilizar o Gmail' above a placeholder for a user profile picture.
- body div div div div div:** A text area at the bottom of the editor.
- Capture Submitted Data:** A checkbox with a question mark icon.
- Buttons:** 'Cancel' and 'Save Page' buttons at the bottom right.

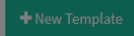
The background interface shows the Gophish dashboard with a sidebar menu (Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Settings) and a main content area with a 'New Page' button and a table of landing pages.

EMAIL TEMPLATES



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

Email Templates



Show entries

Name
apda.ga
docasdelisboa.ml
FctCloud
lisboastartup

Showing 1 to 4 of 4 entries

New Template

Name:

lisboastartup



Subject:

Recrutamento IT

Text

HTML



Saudacoes,

Somos uma nova startup começando 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.

☒ Add Tracking Image



Show entries

Search:

Name

Landing Pages

Sending Profiles

Settings

admin

Previous

1

Next

New Sending Profile

Name:

lisboastartup

Interface Type:

SMTP

From:

Yasmin Costa <yasmin.costa@lisboastartup.tlk>

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

EXEMPLOS DE CAMPANHAS

Promoções de Natal

Descontos em viagens

Descontos nos preços da energia

Testes Covid-19 grátis

Descontos em restaurantes

Serviços de entregas mais baratos



FEFEiA -
Fair Energy For Everyone in Academy





**BViagens, offering
unforgettable holidays for
over 10 years.**

Cruzeiros



Grécia, Itália e Croácia

7 noites | PC | Explorer of the Seas De Ravenna | ago. 2024

desde
€791
por pessoa



Grécia e Turquia

7 noites | PC | Costa Fortuna De Atenas | jun. e ago. 2024

desde
€806
por pessoa



Mediterrâneo

7 noites | PC | Costa Smeralda De Barcelona | jul. a set. 2024

desde
€963
por pessoa



Fiordes

7 noites | PC | Costa Diadema De Copenhaga | julho 2024

desde
€1.069
por pessoa



De Lisboa a Roma

10 noites | PC | Norwegian Viva De Lisboa | ago. e set. 2024

desde
€1.806
por pessoa



Europa do Norte

7 noites | PC | Costa Diadema | junho 2024

desde
€1.309
por pessoa

O RELATÓRIO

O tamanho das listas

Intervalos de tempo

Explicação da história

Descrição dos recursos usados

Análise da mensagem de texto

Tabela com os resultados

Sugestões gerais sobre ciberhigiene

MENSAGENS	STUDENTS	STAFF	TOTAL	%
Enviadas	3770	706	4476	
Abertas	1115	114	1229	27.45%
Clickadas	165	16	181	4.04%
Dados inseridos	64	2	66	1.47%

IDEIAS CHAVE



Não podem ser usadas marcas reais, nem identificamos utilizadores individualmente



Para organizar uma campanha minimamente credível é necessário ter um domínio, um servidor DNS, um servidor web com certificado SSL e um MTA



As mensagens enviadas terão que ser espaçadas no tempo senão é provável que o nosso MTA seja bloqueado



Questões?

Obrigado.



csirt.fct.pt/podcast



csirt.fct.pt/mooc



csirt.fct.pt/etc