



MÓDULO: TREINO

Filipa Macieira
RCTS CERT





AGENDA

Onboarding: Tópicos

Exercícios de Phishing

Ferramenta GoPhish



ONBOARDING: TÓPICOS



Informações

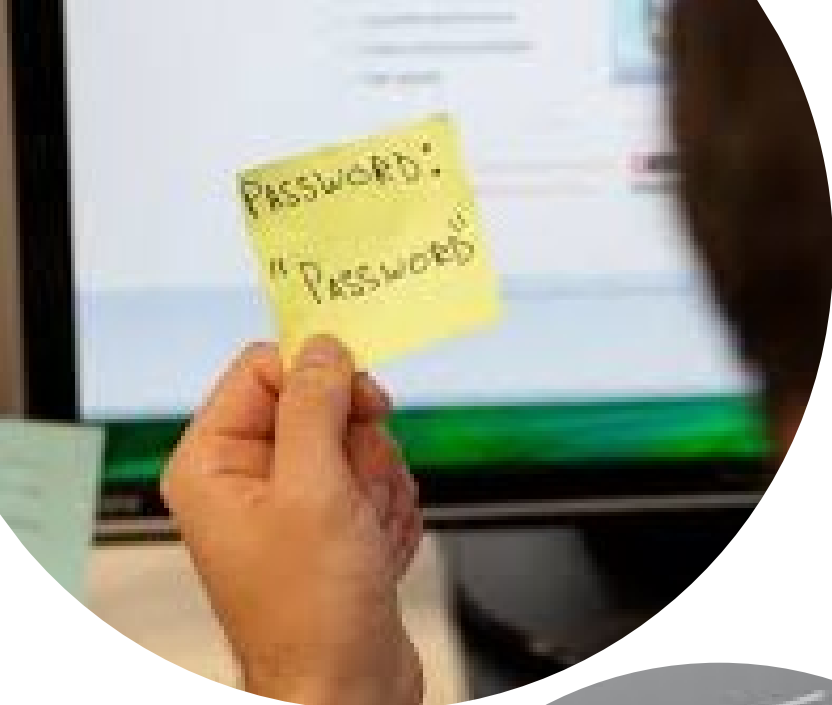
O que faz o CSIRT?, Políticas de Segurança, Trabalho guardado no Servidor, BYOD, Destruição de papel, Ransomware e Uso de tecnologias P2P



ONBOARDING: TÓPICOS

Pedidos

Verificar se o Anti-Vírus está a funcionar, Reportar tentativas de Phishing, Cuidados a ter com Passwords

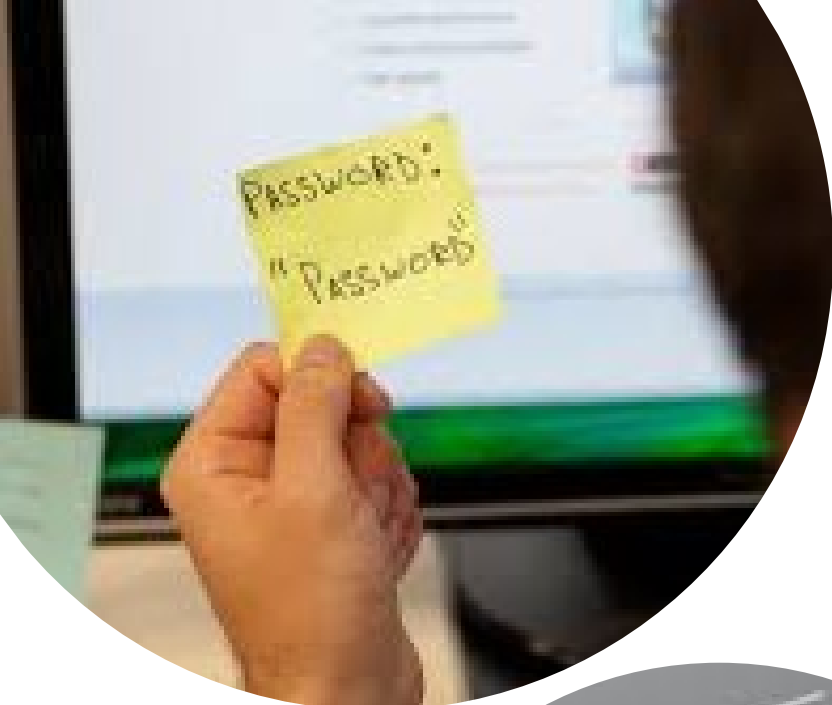


ONBOARDING: TÓPICOS



Conselhos

Fazer Backups com frequência,
Cuidados com Mensagens e Links,
Trancar Sistema Operativo quando se
abandona o teclado, Uso de 2FA
sempre que possível





Actividade 12

Onboardings

Discussão:

Que mensagem é mais importante transmitir?



EXERCÍCIOS DE PHISHING



Para que servem?

Quais são as regras de ouro?

Acções de sensibilização



EXERCÍCIOS DE PHISHING

Requisitos

Gophish





REQUISITOS



Ter um domínio específico para a campanha



Criar um certificado específico para o website





REQUISITOS



Criar o registo SPF para o envio de emails

Instalar uma plataforma que faça a gestão da campanha



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 - 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

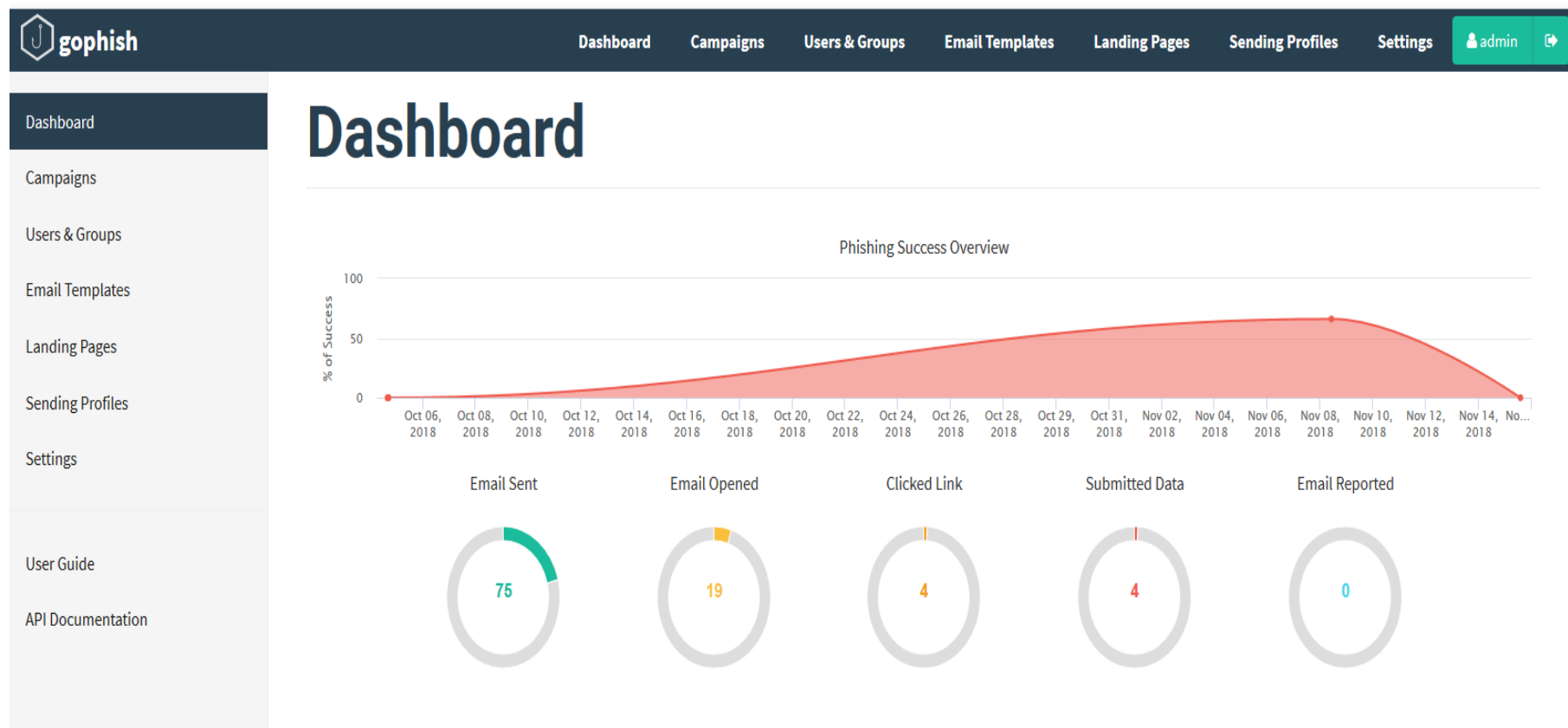


Fornecer informação detalhada sobre as métricas associadas ao exercício de Phishing:

- 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




 **gophish**

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)

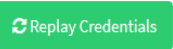


Submitted Data


November 9th 2018 10:14:07 am

 Windows (OS Version: 10)

 Chrome (Version: 70.0.3538.77)





View Details



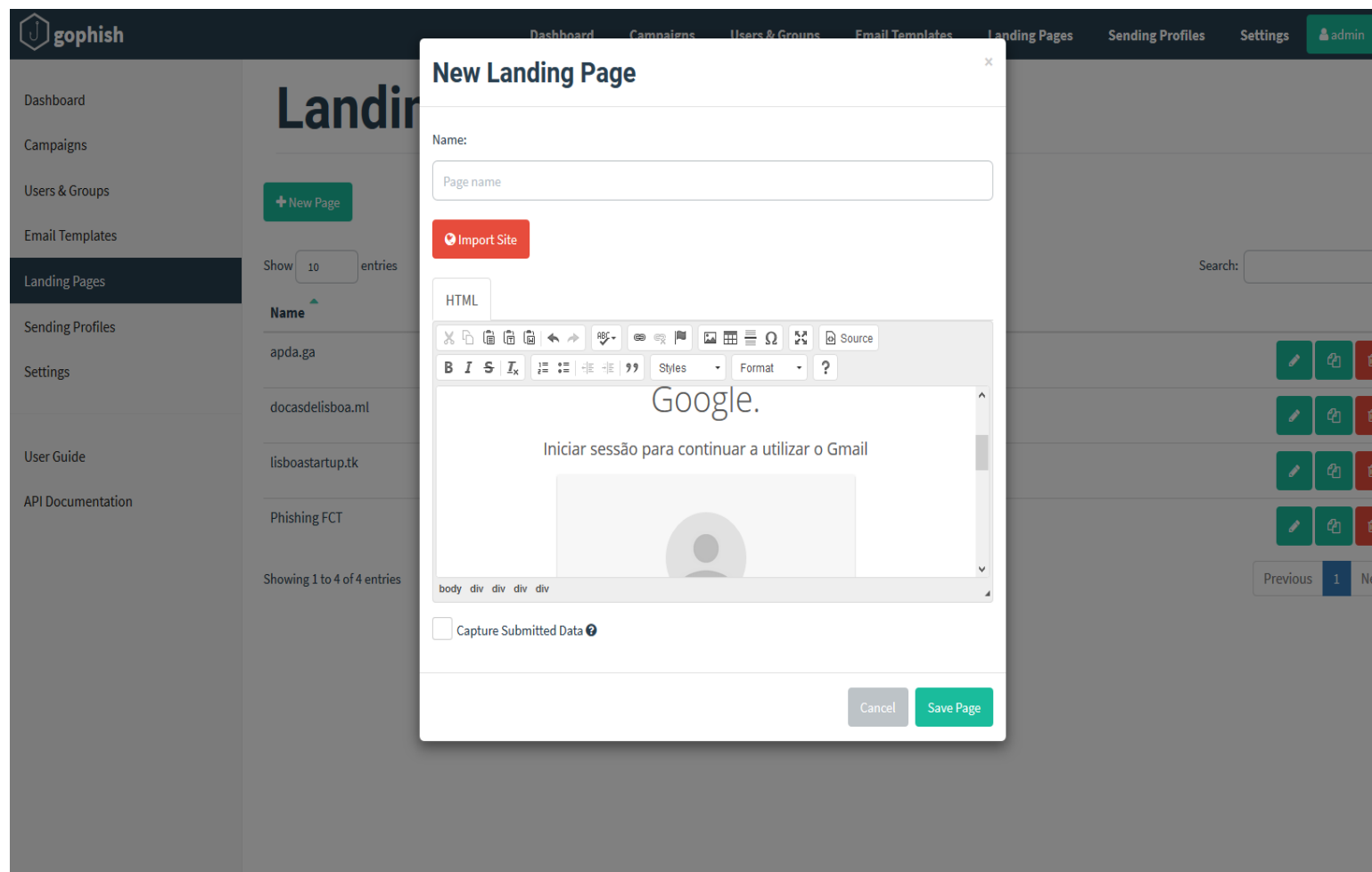
Clicked Link

November 9th 2018 10:14:43 am

 Windows (OS Version: 10)

 Chrome (Version: 70.0.3538.77)

LANDING PAGES



EMAIL TEMPLATES



The screenshot shows 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 shows a list of templates with columns for Name, Subject, and Content. A 'New Template' modal is open in the center. The modal has fields for Name (filled with 'lisboastartup'), Subject (filled with 'Recrutamento IT'), and a rich text editor for the body content. The body content includes a greeting, a paragraph about a startup in Lisbon, and a paragraph about recruitment. There are also checkboxes for 'Add Tracking Image' and 'Add Files'. The modal is titled 'New Template' and has a close button in the top right corner.

PERFIS DE ENVIO



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



Actividade 13

Exercício de Phishing

Tarefa 1: Definir a história da campanha

Tarefa 2: Definir domínio DNS a registar

Tarefa 3: Escrever mensagem a enviar

Tarefa 4: Escrever texto do que surge quando alguém é «phished»



EM RESUMO



Onboarding: Informações, pedidos, conselhos



Testar os utilizadores perante situações de Phishing



Obrigada!