

Exercícios de Phishing

Hélder Fernandes

ASA / SEG

20-Nov-2018



Para que servem os exercícios de phishing?

Utilizadores

- Testar os utilizadores perante situações de Phishing
- Educar e enriquecer o “*Awareness*” nos utilizadores



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 para exercícios de phishing

- Ter um domínio específico para os exercícios
- Criar um certificado específico para o website
- 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/>

Exemplos de plataformas gratuitas

- GoPhish – <https://getgophish.com>



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



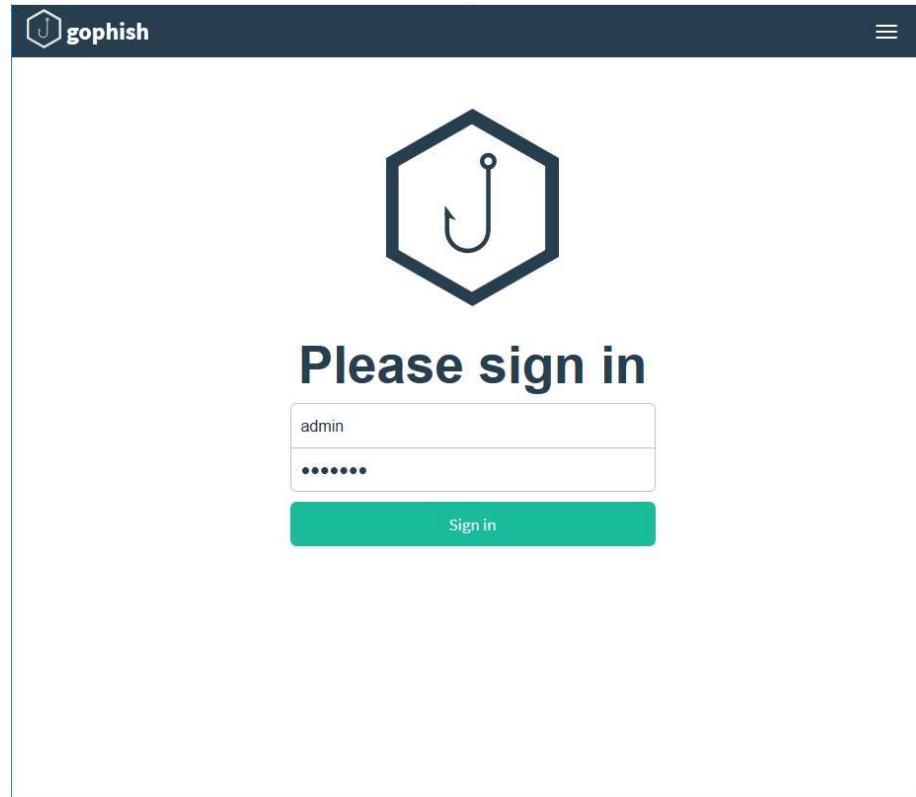
- King Phisher - <https://github.com/securestate/king-phisher>



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



Plataforma escolhida pelo RCTS CERT

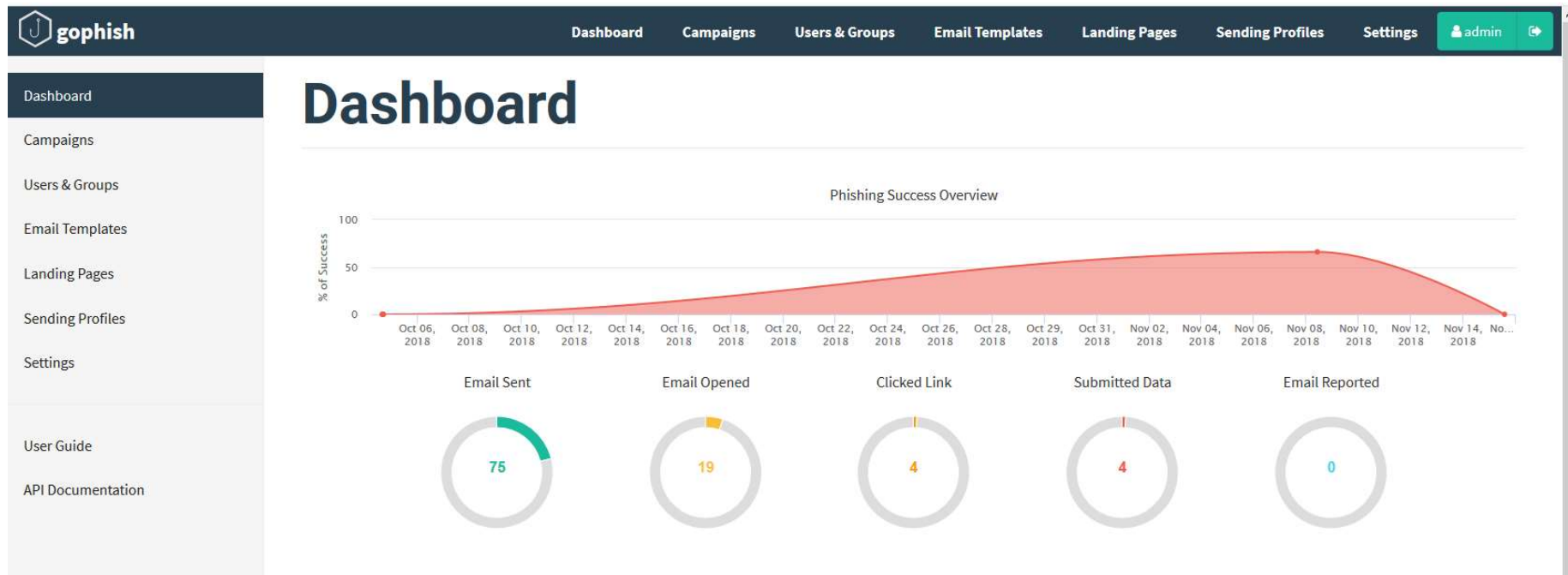


The image shows a screenshot of the gophish web application's login page. At the top left, there is a dark blue header with the 'gophish' logo and name. A hamburger menu icon is visible in the top right corner. The main content area is white and features a large hexagonal logo with a fishhook inside. Below the logo, the text 'Please sign in' is displayed in a bold, dark font. Underneath, there are two input fields: the first contains the text 'admin', and the second is a password field with six dots. A green 'Sign in' button is positioned below the password field.

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
- 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*”
- Criação de Headers específicos para o emails

Dashboards



Dashboards

The screenshot displays the Gophish dashboard interface. At the top, there is a navigation bar with the Gophish logo and several menu items: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Settings, and a user profile for 'admin'. A left sidebar contains a list of navigation options: Dashboard, Campaigns (highlighted), Users & Groups, Email Templates, Landing Pages, Sending Profiles, Settings, User Guide, and API Documentation.

The main content area shows a 'Timeline for Coordinator RCTS CERT' for the email address 'coordinator@cert.rcts.pt'. The timeline consists of the following events:

- Campaign Created** (November 9th 2018 10:00:49 am): Represented by a green rocket icon.
- Email Sent** (November 9th 2018 10:00:51 am): Represented by a green envelope icon.
- Clicked Link** (November 9th 2018 10:13:20 am): Represented by an orange cursor icon. Below this event, the user agent is listed as 'Windows (OS Version: 10)' and 'Chrome (Version: 70.0.3538.77)'. A green button labeled 'Replay Credentials' is visible below the user agent information.
- Submitted Data** (November 9th 2018 10:14:07 am): Represented by a red exclamation mark icon. Below this event, the user agent is listed as 'Windows (OS Version: 10)' and 'Chrome (Version: 70.0.3538.77)'. A link labeled 'View Details' is visible below the user agent information.
- Clicked Link** (November 9th 2018 10:14:43 am): Represented by an orange cursor icon. Below this event, the user agent is listed as 'Windows (OS Version: 10)' and '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 is titled 'New Landing Page' and contains the following elements:

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

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

Email templates

The screenshot displays the Gophish web interface. On the left, a sidebar contains navigation links: Dashboard, Campaigns, Users & Groups, Email Templates (highlighted), Landing Pages, Sending Profiles, Settings, User Guide, and API Documentation. The main content area is titled 'Email' and features a '+ New Template' button. Below this, a list of templates is shown with columns for 'Name' and 'entries'. The templates listed are 'apda.ga', 'docasdelisboa.ml', and 'FctCloud'. A search bar and pagination controls are visible at the bottom of the list.

The 'New Template' modal form is open, showing the following fields and options:

- Name:** Input field containing 'lisboastartup'.
- Subject:** Input field containing 'Recrutamento IT'.
- Text/HTML:** A rich text editor with a toolbar including icons for bold, italic, underline, link, unlink, list, indent, outdent, and source. The text area contains:

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.
- Tracking:** A checked checkbox labeled 'Add Tracking Image'.
- Files:** A '+ Add Files' button.

At the bottom of the modal, there is a 'Show 10 entries' dropdown and a search bar.

Sending Profiles

The screenshot displays the Gophish web interface with a modal window titled "New Sending Profile" open. The background shows the "Sending Profiles" management page with a list of profiles and a "New Profile" button. The modal form contains the following fields and options:

- Name:** Input field containing "lisboastartup".
- Interface Type:** Dropdown menu set to "SMTP".
- From:** Input field containing "Yasmin Costa <yasmin.costa@lisboastartup.tk>".
- Host:** Input field containing "127.0.0.1:25".
- Username:** Input field containing "Username".
- Password:** Input field containing "Password".
- Ignore Certificate Errors**
- Email Headers:** A table with two columns: "X-Sender" (input field) and "XPTO" (input field). A red "+ Add Custom Header" button is to the right.
- Footer:** "Cancel" and "Save Profile" buttons.

The background interface includes a sidebar with navigation links (Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Settings, User Guide, API Documentation) and a main content area with a "New Profile" button, a "Show 10 entries" dropdown, and a table of existing profiles. The table has columns for "Name" and "Created Date".

Perguntas



Obrigado pela atenção!

info@cert.rcts.pt