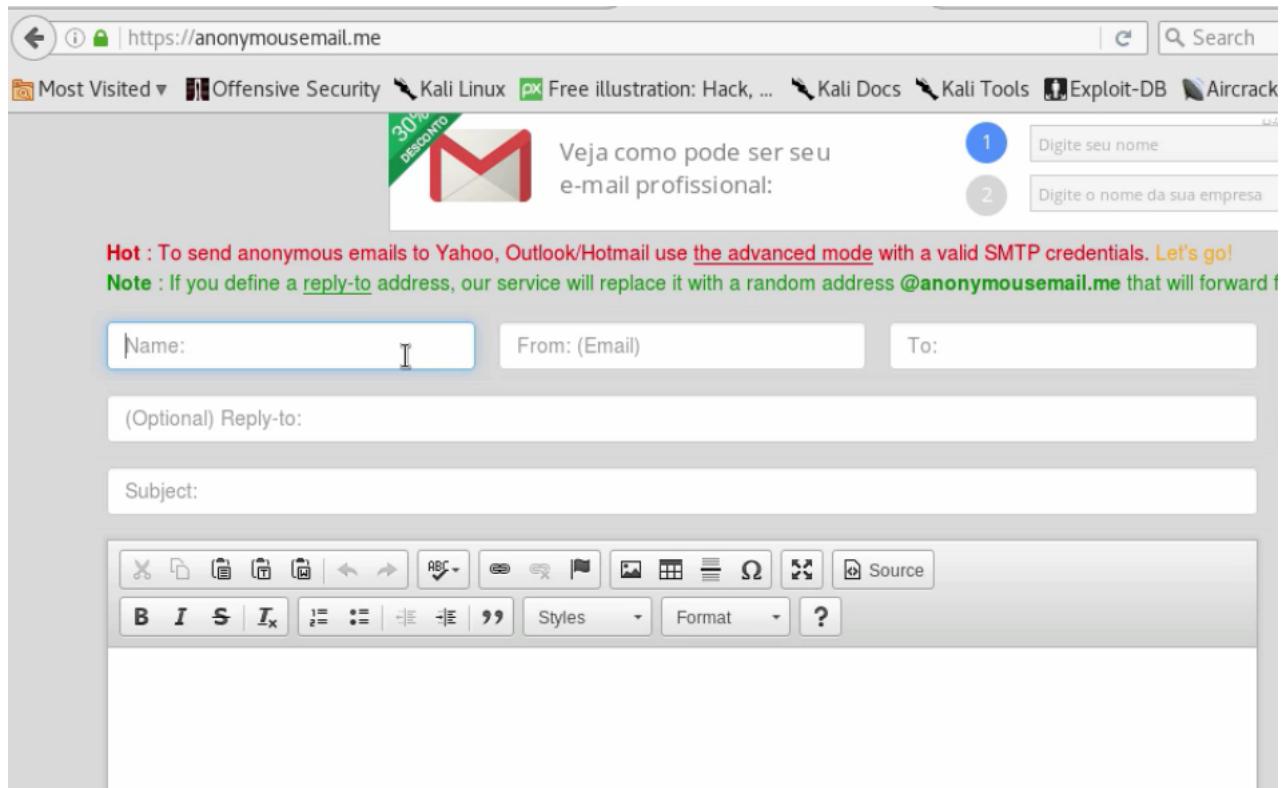


06

## Melhorando engenharia social com e-mail

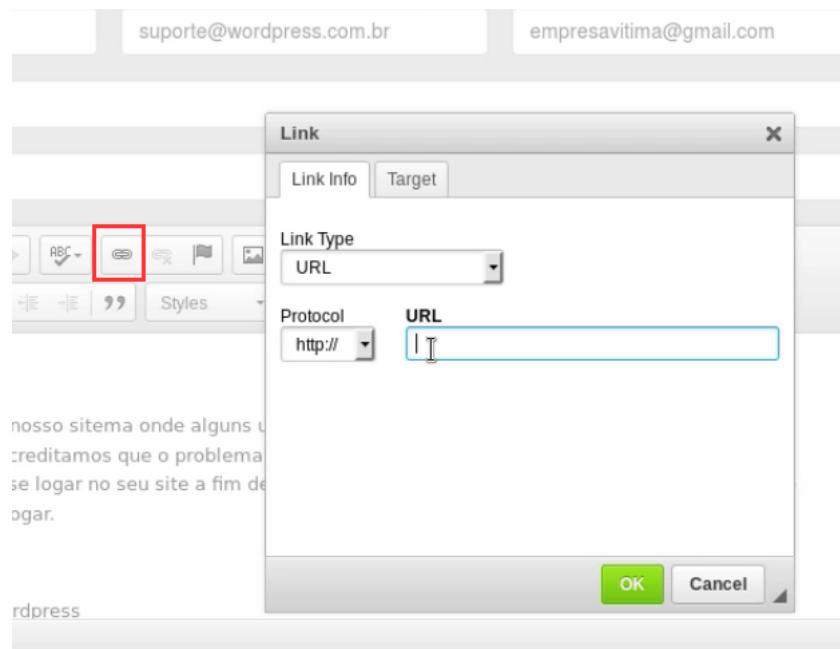
### Transcrição

Outra forma de enviar um e-mail é utilizando alguns sites. Um dos servidores disponíveis é o Anonymous email:



Assim que acessamos o site, basta preencher o formulário acima com as informações pedidas: o endereço de quem receberá a mensagem, o e-mail fictício de quem envia, o assunto e o conteúdo.

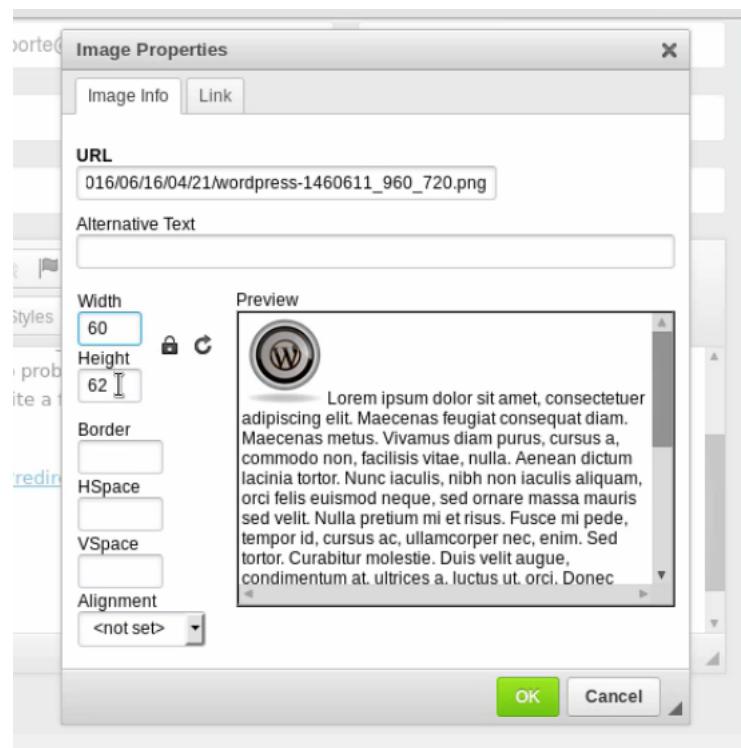
Para referenciar um link podemos clicar no botão mostrado na imagem abaixo e preenchemos a seguinte janela:



Nesse formulário inserimos a URL parcialmente verdadeira o que gera um link que acrescentamos no corpo do e-mail. Adicionamos também um logotipo para que a mensagem ganhe credibilidade, utilizamos o seguinte ícone:



Ao clicar no botão abre-se o seguinte formulário no qual acrescentamos a URL da imagem e ajeitamos as dimensões dela:



Finalmente, para enviar o e-mail basta dar um *check* na caixa que encontra-se bem embaixo na página dizendo que não somos um robô e clicamos em *Send Email*.

Vamos acessar o gmail do usuário e verificar que a mensagem é efetivamente recebida. Temos o seguinte:

**Problemas de autenticação** Inbox Print

**Supporte Wordpress** suporte@wordpress.com.br via orbit.eternalimpact.info 12:16 PM (0 minutes ago) Star Forward Reply

to me Translate message Turn off for: Portuguese

Caro cliente,

Tivemos um problema em nosso sistema onde alguns usuários apresentaram problemas de login em suas respectivas plataformas. Acreditamos que o problema tenha sido solucionado. Pedimos à gentileza de clicar no link abaixo para que tente se logar no seu site a fim de confirmar que tudo está. Talvez seja necessário mais do que uma tentativa para se logar.

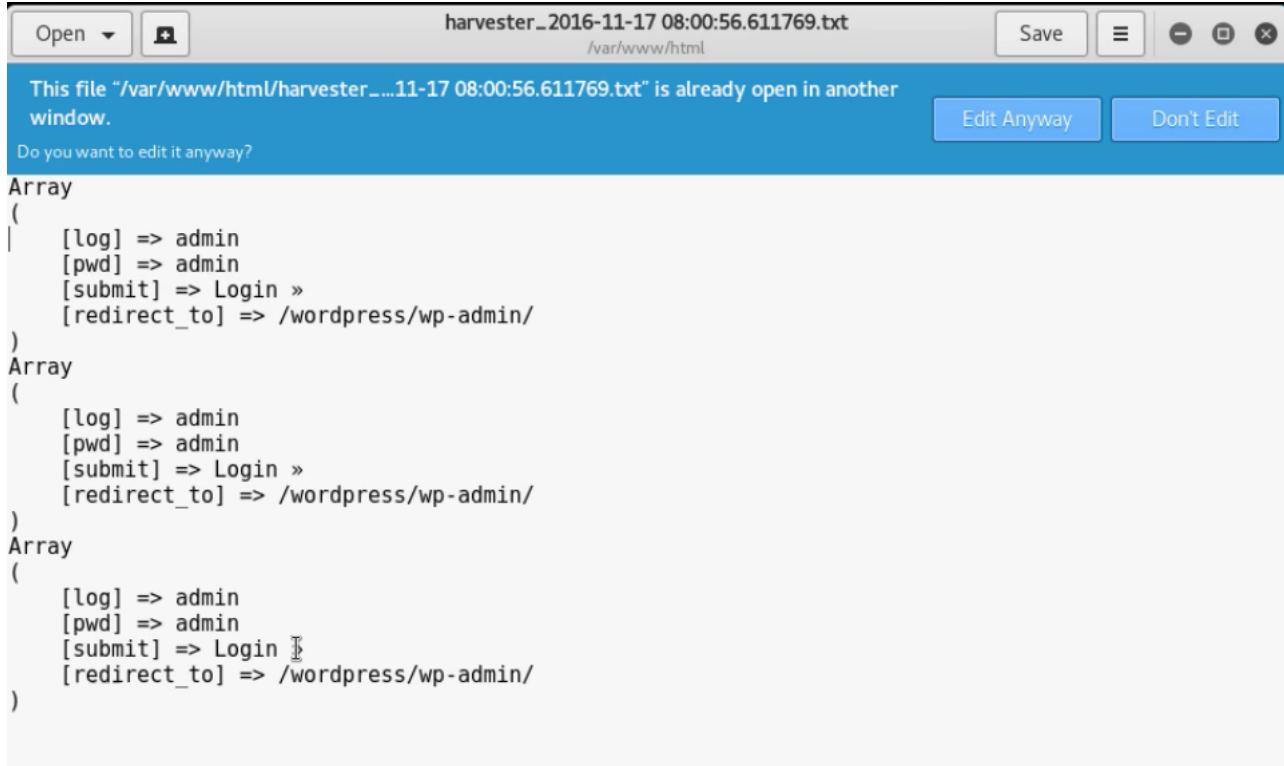
[http://192.168.1.37/wordpress/wp-login.php?redirect\\_to=http://192.168.1.39/](http://192.168.1.37/wordpress/wp-login.php?redirect_to=http://192.168.1.39/)

Atenciosamente

Equipe Wordpress

O e-mail parece estar correto, ademais, transmite maior confiança do que o primeiro que enviamos. Se clicarmos no link da mensagem seremos redirecionados para a página que leva a URL falsa.

Supondo que o usuário preencha seus dados na página falsa, podemos verificá-los através do "Computer > var > www > html", no arquivo "harvest-2016-11-17". Teremos o seguinte:



```
harvester_2016-11-17 08:00:56.611769.txt
/var/www/html

This file "/var/www/html/harvester_2016-11-17 08:00:56.611769.txt" is already open in another window.
Do you want to edit it anyway? [Edit Anyway] [Don't Edit]

Array
(
|   [log] => admin
|   [pwd] => admin
|   [submit] => Login »
|   [redirect_to] => /wordpress/wp-admin/
)
Array
(
|   [log] => admin
|   [pwd] => admin
|   [submit] => Login »
|   [redirect_to] => /wordpress/wp-admin/
)
Array
(
|   [log] => admin
|   [pwd] => admin
|   [submit] => Login »
|   [redirect_to] => /wordpress/wp-admin/
)
```

O *username* e a *password* do usuário!

Ou seja, nós utilizamos um link verdadeiro para redirecionar a página e dessa forma, conseguimos acesso aos dados da vítima! Então, perceba o quanto perigoso é esse tipo de ataque!