# ENGENHARIA SOCIAL: ATENÇÃO AO ATAQUE DE PHISHING.

Iago Piccoli Leite[1]
Fagner Coin Pereira[2]

## RESUMO

Este trabalho trata-se de uma breve explicação sobre o ataque de engenharia social chamado phishing, esta técnica é comumente utilizada por ter um baixo custo e uma alta taxa de propagação. A técnica utilizada na engenharia social é comummente encontrada em e-mails e redes sociais como Facebook, Tweeter, WhatsApp, e Instagram. Neste artigo serão citadas algumas dicas e cuidados para evitar este tipo de ataque, uma vez que a informação e conscientização do usuário para com o uso das redes sociais e cuidados com correio eletônico pode trazer uma redução no número de vitimas deste ataque.

Palavras chave: Phishing. Engenharia Social. Ataques.

## INTRODUÇÃO

Verificando as incidências do ataque conhecido como e phishing, foi elaborado um trabalho para que o usuário tenha um conhecimento base sobre este tipo de ataque, podendo ficar mais atento a tais ameaças. O termo phishing pode ser traduzido como pescaria, é o tipo mais comum de engenharia social utilizado hoje por criminosos no mundo todo, principalmente por ser barato e escalável para milhares, milhões de contas. Este artigo limita-se a uma breve explicação sobre phishing.

1Acadêmico do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. walkerdgp@gmail.com
2 Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. coin.pereira@gmail.com

## PHISHING

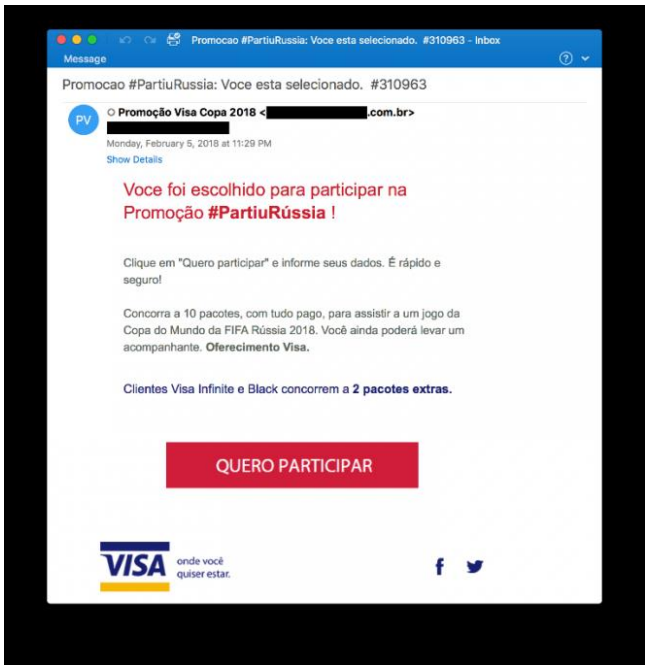
O método de phishing utiliza basicamente a estratégia do envio de e-mails falsos, fazendo-se passar por instituições financeiras, propagandas de lojas conhecidas com anúncios atraentes, ou até mesmo comunicados governamentais. Além de e-mails, o ataque pode-se apresentar de forma mais simples, como anúncios em redes sociais como a oferta de serviços solicitando dados das pessoas para execução do mesmo. Um exemplo disto é a oferta de cartões de credito personalizados como se pode ver na imagem abaixo:

Figura 1 – Dados de Cartão de Crédito no Twitter


Fonte: (CAMURÇA, 2019)

Outro exemplo de phishing bem elaborado foi lançado em 2018 com o tema da copa do mundo como se pode ver abaixo:

Figura 2 – Phishing de e-mail na Copa do Mundo 2018




Fonte: (CANALTECH, 2018)

Como visto nos exemplos acima o phishing tenta se passar por uma notícia, comunicado, e muitas vezes anúncios de fontes confiáveis, tendo como foco os usuários menos informados e demais desavisados do assunto. Segundo (Karspersky, 2019) o Brasil é o país com maior número de usuários atacados por phishing no primeiro trimestre de 2019, numa crescente de 3% em comparação com o mesmo período do ano anterior.

## CONSIDERAÇÕES FINAIS

Para fins de evitar este ataque, indica-se ao usuário que tome cuidados com a exposição excessiva de seus dados em redes sociais, evitar clicar em links sem antes passar o mouse em cima para verificar o apontamento real do destino, analisar possíveis erros de ortografia em anúncios e comunicados, caso haja suspeita de um remetente conhecido como um amigo, familiar ou colega, contate a pessoa imediatamente, pois este pode estar infectado e enviando mensagens para contatos sem saber.

## REFERENCIAS

RODRIGUES, Renato. Brasileiros são maiores vítimas de golpes phishing no mundo. **Kaspersky**, 2018. Disponível em: <https://www.kaspersky.com.br/blog/phishing-klsec-brasil-assolini/10642/>. Acesso em: 25/06/2019.

RODRIGUES, Renato. Brasil é o País com mais usuários atacados por phishing. **Kaspersky**, 2019. Disponível em: <https://www.kaspersky.com.br/blog/brasil-ataques-phishing/11826/> Acessado em: 24/10/2019

CANALTECH. , 2018. Disponível em: <https://canaltech.com.br/seguranca/phishing-golpe-usa-copa-do-mundo-para-roubar-cartao-de-credito-107888/> Acessado em: 22/10/2019

COMURÇA, Francisco. Usuários compartilham no Twitter dados de cartão de crédito em troca de customização. **Welivesecurity**, 2019. Disponível em: <https://www.welivesecurity.com/br/2019/05/30/usuarios-compartilham-no-twitter-dados-de-cartao-de-credito-em-troca-de-customizacao/> Acessado em: 21/10/2019