OUCH! | Dezembro de 2015

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

Phishing

Visão Geral

O e-mail é uma das formas primárias com que nos comunicamos. Nós não só o utilizamos todos os dias no trabalho, como também para ficar em contato com nossos amigos e familiares. Além disso, é através do e-mail que a maioria das empresas fornece serviços on-line, tais como confirmação de sua compra on-line ou a disponibilidade de seus extratos bancários. Uma vez que tantas pessoas ao redor do mundo dependem do e-mail, este tornou-se um dos métodos de ataque principais usados por criminosos cibernéticos. Neste boletim vamos explicar o phishing, um método comum de ataque através do email, e os passos que você pode tomar para usar o e-mail com segurança.

Editor Convidado

Dr. Lance Hayden é Diretor Administrativo do Grupo de Pesquisa de Berkeley. Um especialista em cultura e comportamento de segurança, ele é o autor de People-Centric Security: Transforming Your Enterprise Security Culture (ainda sem tradução para o português) da McGraw-Hill. Você pode encontrá-lo através do link **www.linkedin.com/in/drhayden**.

Phishing

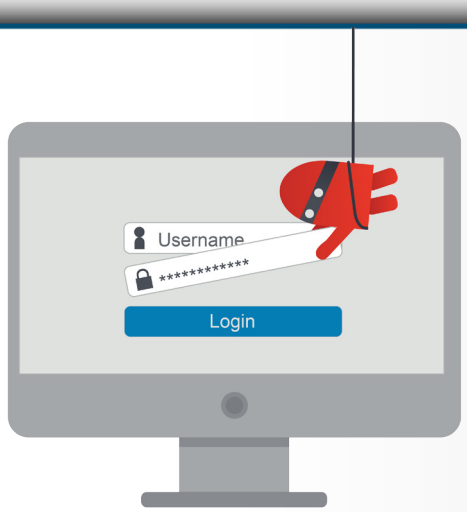
Phishing refere-se a um ataque que usa o e-mail ou um serviço de mensagens, como os de sites de mídia social, e que usa artimanhas ou engana você para que tome uma ação, como clicar em um link ou abrir um anexo. A vítima de um ataque deste tipo corre o risco de ter suas informações altamente confidenciais roubadas e/ou o computador infectado. Os criadores desse ataque trabalham duro para tornar seus e-mails de phishing convincentes. Por exemplo, eles vão fazer o e-mail parecer que tenha vindo de alguém ou de algo que você conhece, como um amigo ou uma empresa confiável que utiliza frequentemente. Eles vão mesmo adicionar logotipos de seu banco ou forjar o endereço de email para a mensagem parecer mais legítima. Em seguida, estas pessoas mal intencionadas irão enviar esses e-mails de phishing para milhões de pessoas. Eles não sabem de fato quem vai se tornar vítima, tudo o que eles sabem é que quanto mais e-mails enviarem, maior a chance de sucesso. Phishing é semelhante ao uso de uma rede de pesca, você não sabe o que você vai pegar, mas quanto maior for a rede, mais peixe você pode encontrar. Essas pessoas usam o phishing de várias maneiras para conseguir o que querem.

- **Coleta de Informações**: O objetivo do atacante é colher suas informações pessoais tais como suas senhas, números de cartões de crédito ou dados bancários. Para isso, enviam um link que leva você para um site que parece legítimo. Este site, em seguida, pede-lhe para fornecer informações de sua conta ou dados pessoais. No entanto, o site é falso, qualquer informação que você entrar vai diretamente para o atacante;
- **Links Maliciosos**: O objetivo do atacante é tomar o controle do seu dispositivo. Para fazer isso, eles enviam um email

Phishing

com um link. Se você clicar no link, ele leva você para um site que inicia um ataque no seu dispositivo que, se bem sucedido, infecta seu sistema;

- **Anexos Maliciosos**: O objetivo do atacante é o mesmo, infectar e assumir o controle do seu dispositivo. Mas, em vez de um link o atacante envia e-mails com um arquivo infectado, como um documento do Word. Abrir o anexo desencadeia o ataque, potencialmente dando ao atacante o controle do seu sistema;
- **Varreduras**: Alguns e-mails de phishing não são nada mais do que os trapaceiros que se tornaram digitais. Eles tentam enganá-lo dizendo que você ganhou na loteria, fingindo ser uma instituição de caridade que necessitam de doações ou pedir sua ajuda para movimentar milhões de dólares. Se você responder a qualquer destas perguntas, eles vão dizer que eles precisam primeiro do pagamento por seus serviços ou acesso a sua conta bancária, esses golpes focam em tirar todo o seu dinheiro.



Sua melhor defesa é o bom senso. Se um e-mail ou mensagem é estranha, suspeita, ou boa demais para ser verdade, ela pode ser um ataque de phishing.

Protegendo-se

Em quase todos os casos, abrir e ler um e-mail ou mensagem não tem problema. Para um ataque de phishing funcionar os bandidos precisam induzí-lo a fazer algo. Felizmente, existem indícios de que uma mensagem é um ataque. E aqui estão os mais comuns:

- O e-mail cria um senso de urgência, exigindo “medidas imediatas” antes que algo ruim aconteça, como fechar a sua conta. O atacante quer apressá-lo a cometer um erro sem pensar;
- Você receberá um e-mail com um anexo que você não estava esperando ou um e-mail convidando-o a abrir o anexo. Os exemplos incluem um e-mail dizendo que tem um anexo com detalhes de demissões não anunciadas, informação do salário do empregado ou uma carta da Receita Federal dizendo que está sendo processado;
- Em vez de usar o seu nome, o e-mail usa uma saudação genérica como “Prezado Cliente”. Lembre-se que a maioria das empresas ou amigos que entra em contato com você escreve o seu nome;
- Solicitações de e-mail de informação altamente sensível, como o número do seu cartão de crédito ou senha;
- O e-mail diz que se trata de uma organização oficial, mas tem uma gramática ou ortografia ruim, ou utiliza um endereço de e-mail pessoal, como @gmail.com, @yahoo.com ou @hotmail.com;
- O link parece estranho ou não oficial. Uma dica é passar o mouse sobre o link até que um pop-up mostre onde esse link realmente leva você. Se o link no e-mail não corresponde ao destino pop-up, não clique nele. Em dispositivos móveis se

Phishing

pressionar o dedo em um link recebe o mesmo pop-up. Um passo ainda mais seguro é copiar e colar a URL do e-mail em seu navegador ou digitar o link correto;

- Você recebe uma mensagem de alguém que você conhece, mas o tom ou a forma da mensagem não soa como dele ou dela. Se você tem alguma suspeita, entre em contato com o remetente para verificar se ele ou ela a enviou. É fácil para um atacante cibernético criar um e-mail que parece ser de um amigo ou colega de trabalho.

Se você acredita que um e-mail ou mensagem é um ataque de phishing, simplesmente exclua-o. Em última análise, o bom senso é a melhor defesa.

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em http://www.securingthehuman.org.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

Recursos

Engenharia Social:	https://www.securingthehuman.org/ouch/2014#november2014
Cinco Passos para Ficar Seguro:	https://www.securingthehuman.org/ouch/2014#october2014
Fui Hackeado, e agora?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online (em ingles):	https://www.onguardonline.gov/phishing
SANS - Dica de segurança do dia (em inglês):	https://www.sans.org/tip_of_the_day.php

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser