A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

- Engenharia Social
- Detectar / Parar os ataques de engenharia social
- Evitar futuros ataques

Engenharia Social

Visão Geral

Uma concepção equivocada que as pessoas têm sobre os atacantes cibernéticos é que eles só usam ferramentas e tecnologias avançadas de hacking para invadir os computadores, contas e dispositivos móveis das pessoas. Isso simplesmente não é verdade. Atacantes cibernéticos descobriram que uma das maneiras mais fáceis de roubar suas informações ou hackear seu computador é simplesmente falando com você de forma enganosa. Neste boletim vamos aprender como esses tipos de ataque a humanos, chamados de ataques de engenharia social, funcionam e o que você pode fazer para se proteger.

Editor Convidado

Alissa Torres é instrutora certificada SANS, especializada em computação forense avançada e resposta a incidentes. Sua experiência no setor inclui atuar na prática resolvendo incidentes e trabalhar em uma equipe de segurança interna como investigadora forense digital. Alissa pode ser encontrada no Twitter como **@sibertor**.

Engenharia Social

A engenharia social é um tipo de ataque psicológico onde um atacante lhe induz a fazer algo que eles querem que você faça. A engenharia social já existe há milhares de anos, a idéia de aplicar golpes ou enganar alguém não é nova. Entretanto, os atacantes cibernéticos descobriram que usar esta técnica na internet é extremamente eficaz e pode ser utilizada para atingir milhões de pessoas. A maneira mais simples de entender como funciona a engenharia social é parar e dar uma olhada em um exemplo comum do mundo real.

Você recebe um telefonema de alguém dizendo ser de uma empresa de suporte de informática, do seu provedor de acesso à Internet ou talvez do suporte técnico da Microsoft. O interlocutor diz ter notado que seu computador está se comportando estranhamente, fazendo varredura (scan) na Internet ou enviando spam (envio de e-mail não solicitado), e por isso eles acreditam que esteja infectado. Ele diz que recebeu a missão de investigar o problema e ajudá-lo a proteger o seu computador. Ele, então, utiliza vários termos técnicos para guiá-lo através de passos confusos e convencê-lo de que seu computador está infectado.

Por exemplo, eles podem pedir para verificar se você tem certos arquivos em seu computador e guiá-lo para encontrá-los. Quando você localizar esses arquivos, ele vai assegurar que são um sinal de que seu computador está infectado, quando na realidade esses arquivos não são nada mais do que arquivos de sistema comuns encontrados em cada computador. Uma vez que tenham lhe enganado e feito você acreditar que seu computador está infectado, eles vão pressioná-lo para ir a um site e comprar um software de segurança ou pedir-lhe para lhes dar o acesso remoto ao seu computador para que possam corrigir o problema. Entretanto, o software que eles estão vendendo é na verdade um programa malicioso. Se você comprar e instalar o software, ele não só terá lhe enganado para infectar o seu computador, como terá feito você

© The SANS Institute 2014

Engenharia Social

pagar para fazê-lo. Caso você dê o acesso remoto ao seu computador para corrigir o problema, eles na realidade vão assumir o controle do seu computador e infectá-lo.

Tenha em mente que os ataques de engenharia social não se limitam às chamadas telefônicas. Eles podem acontecer através de quase todo tipo de tecnologia, incluindo ataques de phishing (induzir você a clicar em links) via e-mail, mensagens de texto, Facebook, Twitter ou bate-papos on-line. O segredo é saber o que olhar.

Aprender a prevenir-se, detectar e parar os ataques de engenharia social é uma das medidas mais eficazes que você pode tomar para se proteger.

Detectar / Parar os ataques de engenharia social

A maneira mais simples para se defender contra ataques de engenharia social é usar o bom senso. Se algo parecer suspeito ou não parecer certo, pode ser um ataque. Alguns indicadores comuns de um ataque de engenharia social incluem:

- Alguém criando uma enorme sensação de urgência. Se você sente que está sob pressão para tomar uma decisão muito rápida, desconfie;
- Alguém pedindo informações as quais não deveriam ter acesso ou já deveria saber;
- Algo muito bom para ser verdade. Um exemplo comum é você ser notificado que ganhou na loteria, mesmo que você nunca tenha sequer jogado.

Se você suspeitar que alguém está tentando lhe fazer de vítima de um ataque de engenharia social, não se comunique mais com a pessoa. Se alguém ligar, desligue. Se for alguém conversando com você on-line, encerre a conexão. Se for um e-mail que você não confia, exclua. Se o ataque está relacionado com o trabalho, não se esqueça de informar o seu helpdesk ou equipe de segurança da informação de imediato.

Evitar futuros ataques de engenharia social

Felizmente, existem medidas de precaução que você pode tomar para evitar a exposição a futuros ataques de engenharia social:

- **Nunca compartilhe as suas senhas**. Nenhuma organização jamais entrará em contato com você pedindo sua senha. Se alguém está lhe pedindo sua senha, é um ataque;

- **Não compartilhe muito**. Quanto mais um atacante souber sobre você, mais fácil será encontrá-lo e enganá-lo para fazer o que ele quer. Mesmo compartilhando poucos detalhes sobre si mesmo, ao longo do tempo esses detalhes podem ser agrupados para criar uma imagem completa de quem é você. Quanto menos você compartilhar publicamente, inclusive em sites de mídia social, análises de produtos ou fóruns públicos e listas de e-mail, menor será a probabilidade de você ser atacado;

© The SANS Institute 2014

Engenharia Social

- **Verificar Contatos**. Às vezes você pode ser contactado pelo seu banco, empresa de cartão de crédito, operadora telefônica ou outras organizações por razões legítimas. Mas se você tem alguma dúvida sobre a legitimidade de um pedido de informação, solicite à pessoa que te ligou o seu nome e número de telefone para retornar. Em seguida, pegue o número de telefone da empresa em uma fonte confiável, como o número no verso do seu cartão de crédito, no seu extrato bancário, ou talvez no site da empresa (não clique em links, digite o endereço de Internet no navegador você mesmo). Dessa forma, quando você ligar para a organização, saberá que está falando realmente com eles. Embora isso pareça um aborrecimento, para proteger sua identidade e informações pessoais, esse passo adicional vale a pena.

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
Katia Lucia da Silva, Arquiteta de T/I, Tradutora - twitter.com/kl_silva

Recursos

Ataques de Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Redes Sociais com segurança:	http://www.securingthehuman.org/ouch/2013#march2013
Como evitar fraudes (em Inglês):	http://www.onguardonline.gov/topics/avoid-scams
Golpes na Internet:	http://cartilha.cert.br/golpes/
Cartilha de Segurança na Internet:	http://cartilha.cert.br/

OUCH! é publicado pelo “SANS Securing the Human” e distribuído sob o licenciamento Creative Commons BY-NC-ND 4.0 license. A distribuição ou utilização desta publicação em programas de treinamento é permitida desde que seu conteúdo não seja modificado. Para traduções ou mais informações entre em contato pelo ouch@securingthehuman.org

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

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus