OUCH! | Julho de 2016

A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

CEO Impostor

O que é um CEO Impostor?

Os criminosos cibernéticos são sorrateiros, eles estão constantemente criando novas maneiras de obterem o que querem. Um de seus métodos mais eficazes é utilizar como alvo pessoas como você. Criminosos cibernéticos descobriram que, quando não capacitadas, as pessoas são o elo mais fraco em qualquer organização, mas eles se esqueceram de que pessoas esclarecidas, como os leitores do OUCH! podem ser a melhor defesa de uma organização.

Editor Convidado

Angela Pappas é diretora de treinamento e sensibilização em Segurança da Informação da Thomson Reuters. Em sua função, Angela é responsável pelo programa embaixador, eLearning e pela educação dos funcionários sobre phishing.

Criminosos cibernéticos desenvolveram um novo ataque chamado CEO impostor, também conhecido como E-mail Comercial Comprometido (sigla BEC em inglês). Nestes ataques, um criminoso cibernético finge ser um CEO ou outro executivo sênior de sua organização. Os criminosos enviam um e-mail para a equipe como você, tentando induzi-lo a fazer algo que você não deve fazer. Estes tipos de ataques são extremamente eficazes porque os criminosos fazem suas pesquisas. Eles procuram o site da sua organização para obter informações tais como onde ela está localizada, quem são seus executivos e outras organizações que trabalham com você. Os criminosos, em seguida, aprendem tudo o que puderem sobre seus colegas de trabalho em sites como LinkedIn, Facebook ou Twitter. Uma vez que eles sabem a estrutura de sua organização, eles começam a pesquisar e atacam funcionários específicos. Eles escolhem seus alvos com base em suas metas específicas. Se os criminosos cibernéticos estão à procura de dinheiro, eles podem buscar o pessoal no departamento de contas a pagar. Se eles estão procurando informações fiscais, eles podem buscar os recursos humanos. Se eles querem ter acesso a servidores de banco de dados, eles poderiam ter como alvo alguém da TI.

Uma vez que eles determinem o que querem e quem eles terão como alvo, eles começam a elaborar o seu ataque. Na maioria das vezes eles usam spear phishing. Phishing é quando um atacante envia um e-mail para milhões de pessoas com o objetivo de induzi-los a fazer algo, por exemplo, abrir um anexo infectado ou a visitar um site mal-intencionado. Spear phishing é semelhante ao phishing; no entanto, em vez de enviar um e-mail genérico para milhões de pessoas, eles enviam um e-mail personalizado objetivando um número muito pequeno e seleto de pessoas.Estes e-mails de Spear phishing aparentam ser extremamente realistas e são difíceis de detectar. Eles muitas vezes parecem vir de alguém que você conhece ou com quem trabalha, ou até mesmo o seu chefe. Os e-mails parecem ser realistas, pois podem

CEO Impostor

usar o mesmo jargão que seus colegas de trabalho usam; eles podem usar o logotipo da organização ou mesmo a assinatura oficial de um executivo. Esses e-mails muitas vezes criam um tremendo senso de urgência, exigindo-lhe a tomada de medidas imediatas e pedem para que não conte a ninguém. O objetivo do criminoso cibernético é apressá-lo a cometer um erro. Aqui estão três cenários comuns:

CEO Impostor é um ataque poderoso que pode transpor a maioria das nossas defesas de segurança. Em última análise, você é a nossa melhor defesa.

- **Transferência Bancária**: Um criminoso cibernético está atrás de dinheiro. Isso significa que eles pesquisam e descobrem quem trabalha no contas a pagar ou a equipe que lida com as finanças da sua organização. Os criminosos, em seguida, elaboram e enviam um e-mail fingindo ser seu chefe; o e-mail diz que há uma emergência e que o dinheiro tem que ser transferido de imediato para uma determinada conta;

- **Fraude Fiscal**: Criminosos cibernéticos querem roubar informações sobre seus colegas de trabalho para que eles possam se passar por funcionários em fraudes fiscais. Eles pesquisam sua organização e determinam quem lida com a informação do empregado, por exemplo, alguém dos recursos humanos. De lá, os criminosos enviam e-mails falsos fingindo ser um executivo sênior ou talvez alguém do departamento legal, exigindo que certos documentos sejam fornecidos imediatamente;

- **Representação de um Advogado**: Nem todos os ataques de CEO impostor envolvem apenas e-mail. Outros métodos, como o telefone podem ser utilizados. Neste cenário, os criminosos começam enviando um e-mail fingindo ser um líder sênior, avisando que um advogado vai ligar sobre um assunto urgente. O criminoso, então, liga para a vítima fingindo ser o advogado. O criminoso cria um tremendo senso de urgência ao falar sobre assuntos confidenciais e sensíveis ao tempo. Este sentido de urgência leva você a agir imediatamente.

Protegendo-se

Então, o que você pode fazer para proteger você e sua organização? O bom senso é a sua melhor defesa. Se você receber uma mensagem de seu chefe ou um colega, que não soa ou parece estar correta, pode ser um ataque. Pistas podem incluir um tremendo senso de urgência, uma assinatura que não parece original, um certo tom que você nunca esperaria, ou o nome usado no e-mail é diferente do que o nome que a pessoa normalmente usa para te chamar. Outra dica seria o criminoso estar usando um número telefônico ou endereço de e-mail que você nunca viu antes, ou ainda usarem um

CEO Impostor

endereço de e-mail muito semelhante, mas não exatamente o mesmo que o seu colega de trabalho ou chefe utiliza. Em caso de dúvida, ligue para a pessoa em um número de telefone de confiança ou fale com ela pessoalmente (não responda via e-mail) e confirme se ele enviou o e-mail. Nunca ignore políticas ou procedimentos de segurança. Sua organização pode ter políticas que definem os procedimentos adequados para autorizar a transferência de fundos ou a divulgação de informações confidenciais. Os pedidos que tentam contornar essas políticas, independentemente da sua origem aparente, devem ser considerados suspeitos e verificados antes de qualquer ação ser tomada. Se você receber esse pedido e não está certo do que fazer, contate o seu supervisor, o help desk ou equipe de segurança da informação imediatamente.

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 securingthehuman.sans.org/ouch/archives.

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://securingthehuman.sans.org/ouch/2014#november2014
Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
O que é um Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Verificação em Duas Etapas:	https://securingthehuman.sans.org/ouch/2015#september2015
Spear Phishing:	https://securingthehuman.sans.org/ouch/2013#july2013
Dica do dia (inglês):	https://www.sans.org/tip-of-the-day

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

