IDG NOW! tecnologia em primeiro lugar http://www.idgnow.com.br

**SEGURANÇA > ATAQUES E AMEAÇAS**

# Engenharia social: pessoas ainda são elo mais fraco, diz especialista

(http://idgnow.uol.com.br/seguranca/2010/05/25/engenharia-social-pessoas-ainda-sao-elo-mais-fraco-diz-especialista)

**Por Joan Goodchild, da CSO/EUA**

Publicada em 25 de maio de 2010 às 08h20

## Depois de 25 anos na área, consultor americano constata que nenhuma iniciativa de conscientização em segurança supera a natureza humana.

Winn Schwartau tem escrito, ensinado e prestado consultoria sobre segurança por mais de 25 anos. Para o fundador da Security Awareness Company, a tecnologia pode ter mudado, mas o fator mais influente em segurança– o funcionário ou o usuário final - não.

“Nós não tocamos em redes, nós tocamos nas pessoas”, diz Schwartau. “Porque, no fim, o elo mais fraco em todas essas coisas é a pessoa que está à frente da tela.”

Para Schwartau, os gerentes de segurança estão atentos contra a combinação de ignorância, apatia e arrogância que aflora quando o assunto é a conscientização do indivíduo em relação aos riscos.

“Uma coisa que tivemos de reconhecer nos últimos anos é que o usuário não liga para a empresa na qual trabalha. Ele liga para o pagamento, sua avaliação, seus aumentos de salário”, explicou. “Muitas empresas dizem ter algum tipo de política sobre o comportamento do usuário, mas dada a retidão política do mundo, mesmo que você tenha uma política que diz ‘não faça isso ou pagará o preço’, geralmente o preço não é pago.”

Schwartau relembrou alguns momentos marcantes que vivenciou em décadas de consultoria em treinamento de segurança. A engenharia social, diz ele, tem novos atores e formatos, mas as técnicas que servem de base são as mesmas.

**1::A insegurança chega pelos Correios**

Diz Winn Schwartau: Nós fomos contratados por uma grande firma de serviços financeiros em Nova York, para um treinamento de conscientização em segurança. Queríamos elaborar uma métrica de como as pessoas estavam em relação a essa conscientização, usando como base todos os treinamentos e as políticas com as quais tinham lidado antes de nosso envolvimento com eles. Assim, criamos um teste de engenharia social.

Mas não era o tradicional ‘ligue para alguém e tente aplicar engenharia social nele’. O que fizemos foi escrever uma carta. Nós a enviamos por correio comum a cerca de 30% dos empregados. Aproximadamente 1.200 pessoas. A carta dizia essencialmente ‘ei, nós somos da segurança de informação corporativa. A razão pela qual você está recebendo esta carta é porque você sabe que ocorre engenharia social no trabalho e que nós estamos atualizando nossos sistemas’. Então, citamos algum bla-bla-blá técnico sobre a migração da base de dados e outras coisas que uma pessoa média simplesmente não entenderia.

A carta completava: “Nós sabemos que você está preocupado com segurança e esta é a razão desta carta. Não queremos que você comunique quaisquer dessas informações sobre qualquer forma a não ser pelo correio, que é o único meio seguro de fazer isso. Nós precisamos de seus detalhes pessoais sobre os temas a seguir para que possamos transferi-las para o sistema e verificar sua precisão porque temos tido problemas com os bancos de dados nessa transição.”

Nós dissemos aos destinatários: “Por favor, não mande essas informações nem por e-mail, nem por fax. Use somente o envelope selado e endereçado anexo”, e o endereço não era o da companhia. Nós contamos que fizemos assim para que ninguém no trabalho pudesse interceptar a carta no escritório. Nós também dissemos que tínhamos providenciado uma caixa postal especial e segura, à qual somente o departamento de segurança tinha acesso.

Depois que enviamos, recebemos uma resposta de 28%. Um teste muito simples de engenharia social e mais de um quarto das pessoas-alvo caíram nele.

Nós repetimos este teste em outros lugares, com e-mails impostores (phishing). Em uma empresa, enviamos uma oferta gratuita incrivelmente tentadora, via email. E fizemos isso depois de treinar e certificar extensivamente toda a organização, que teve mais de 95% de seu pessoal aprovado nas avaliações de conscientização. Mas a resposta ao e-mail phishing, mesmo depois do treinamento, foi de 40%.

Não importa quantos testes, avaliações e outras métricas você use. Não é possível trabalhar contra a natureza humana. Nós podemos ajudá-los com treinamento, e medir um aumento incremental no nível de conscientização, mas você nunca irá alcançar

um sucesso de 100%.

A lição: Parte dos treinamentos de conscientização precisa incluir instruções de não dar informações pessoais para qualquer pessoa ou departamento.

“Avise de forma clara: nosso departamento de segurança nunca perguntará sobre esse tipo de informação”, disse Schartau. “O procedimento correto no lançamento de um novo sistema é emitir novas credenciais. Você nunca pedirá as credenciais atuais.”

**2::Queimando-se depois de ler**
Conta Schwartau: Eu recebi recentemente um e-mail que pareceu ser do Bank of America. Sou cliente deste banco e faço 98% de minhas atividades bancárias online.

O e-mail veio do SiteKey,seu sistema de verificação de sites, que é realmente um sistema muito bom. A mensagem dizia “Ei, isso veio do SiteKey e é realmente urgente porque você transferiu algum dinheiro e nós precisamos verificar isso.”

A partir desse ponto eu sabia que era um scam, pois sou um paranóico profissional. Mas olho o e-mail, os endereços, e eles estão corretos! Os logos, a informação do SiteKey; tudo ok. Tudo que eu poderia pensar era “como eles foram emitir isso?”

Então eu examinei os links; passei o mouse sobre eles para ver o que estava havendo. Estava tudo certo. Cliquei em alguns links, para ver até onde eu poderia ir com isso, e capturei algumas telas para uso em treinamento. Ainda não tinha conseguido descobrir nada.

Finalmente, depois de algum tempo, eu percebi. A razão pela qual eu não poderia descobrir é que eu estava em meu laptop com uma tela de 13 polegadas e baixa resolução. Debaixo dos links, os endereços diziam ‘bank of americil.com’ – i minúsculo, l minúsculo. Eu sabia desde o começo que era uma fraude. Mas quantas pessoas deverão cair numa peça como essa?

A lição: Tal como o departamento de segurança, uma instituição financeira legítima nunca lhe pedirá credenciais por e-mail. Eles farão com que você ligue para o número no verso do cartão, ou visite a página web que você sempre usa. Nunca confie em alguém que aparece pedindo suas credenciais, disse Schwartau. Não é assim que é feito.