



BARRETTO JR. E ASSOCIADOS

Logística . Segurança . Qualidade

CNPJ: 008.946.632/0001-54



ENGENHARIA SOCIAL E A INTERNET

Denomina-se engenharia social a obtenção de informações sigilosas e importantes realizada por pessoas mal intencionadas que, para isso, exploram falhas de segurança utilizando, se possível, de meios sofisticados. Apesar das empresas carregarem altos investimentos em tecnologias de segurança de informações e na proteção física de seus sistemas, essas não possuem ainda métodos eficazes que protejam seus recursos humanos de “golpes”, que venham a expor de forma grave seu patrimônio. A questão se torna mais séria quando usuários domésticos e que não trabalham com informática são envolvidos. Engenharia social é, portanto, a utilização de métodos físicos ou eletrônicos que têm a finalidade de enganar ou explorar a confiança das pessoas, para a obtenção de informações sigilosas e importantes que possam trazer qualquer tipo de vantagem a meliantes e, por consequência, prejuízos às entidades ou cidadãos fraudados. Para isso, o enganador pode maquiar sua identidade, se fazendo passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, desenvolver ou se utilizar de ferramentas eletrônicas ou de outra natureza. A exploração da internet, pela facilidade que apresenta na ligação entre empresas e pessoas, se constitui num campo altamente fértil para a prática desse ilícito.

Um dos ataques eletrônicos mais comuns é a utilização de vírus que se espalham por “e-mail” que são enviados de forma dolosa. Na maioria dos casos é necessário que o usuário, ao receber o “e-mail”, execute o arquivo posto em anexo para que seu computador seja imediatamente contaminado. O criador do vírus então se utiliza de atrativos para que o usuário acesse esse anexo que pode, por exemplo, ser um texto que trate de sexo, de amor, de notícias atuais, admiradores secretos, cartões virtuais de amizade, etc. Em todos os casos, o autor explora assuntos capazes de “mexer com o emocional” de qualquer pessoa. Ao receber a mensagem, muitos acessam no anexo contaminando o computador expondo-se, dessa forma, à pesquisa idealizada pelo fraudador. Alguns vírus eletrônicos possuem a característica de se espalhar muito facilmente e por isso recebem o nome de “worms” (vermes) sendo, por conseguinte, bastante utilizados pelo “agente” da engenharia social. Um “worm” se espalha por “e-mail” sendo veiculado agregado a um tema que chame a atenção como, por exemplo, cartões virtuais de amizade. O internauta ao acreditar na mensagem contamina seu computador e o “worm”, ao se propagar, envia cópias da mesma mensagem para a lista de contatos existente no PC da vítima e coloca o endereço de “e-mail” dela como remetente. Quando alguém da lista acessa a mensagem, vai supor que estará mesmo recebendo um cartão virtual de seu amigo. A tática de engenharia social para este caso utiliza a amizade como isca.

BARRETTO JR. e ASSOCIADOS

Endereço: Rua Genésio José de Moura S/ N Casa 01 – Lote 07/ Quadra 24 – Chácara de Pinhão – Tanguá/ RJ – CEP: 24890-000 | Filial 01: Av. Nossa Senhora de Copacabana, 36/ 1101 – Leme – Rio de Janeiro/ RJ – CEP: 22010-122 – Tel.: (21) 3507-5949 | Filial 02: Av. Angélica, 868/51 – Higienópolis – São Paulo/ SP – CEP: 01228-000 Tel.: (11) 3666-2580 | Email: contato@barrettojreassociados.com.br



BARRETTO JR. E ASSOCIADOS

Logística . Segurança . Qualidade

CNPJ: 008.946.632/0001-54



Outro ataque muito utilizado é o emprego de “e-mails” falsos utilizados para obter informações financeiras da pessoa, como número de sua conta-corrente e senhas. Nesse caso, o aspecto explorado é a confiança. Tendo em vista serem os sistemas dos bancos bem protegidos se torna praticamente inviável sua burla, ficando mais fácil para o criminoso tentar enganar as pessoas, para que elas forneçam as informações de seu interesse. O fraudador adquire uma lista de “e-mails” e depois copia o “layout” da página do “site” de um banco muito conhecido e o salva em um “site” provisório, que tem a URL semelhante ao “site” do banco. Podemos citar como exemplo os seguintes endereços: www.bancodobrasil.com.br (original) e www.bbrasil.com.br (falso). Neste último “site”, ele disponibiliza campos específicos para o usuário digitar seus dados confidenciais. No passo seguinte seria enviada uns “e-mail” às pessoas da lista adquirida. O “e-mail” é sempre acompanhado por um “link” que conduz ao “site” falso. Para fazer com que o internauta clique nesse “link”, o texto da mensagem trata de um assunto de interesse do usuário como, por exemplo, sugerir uma premiação do tipo: “Você acaba de ser premiado com 50 mil reais. Clique no link para atualizar seu cadastro e verificar as regras para resgatar o prêmio”. Como a instituição bancária escolhida geralmente é muito conhecida e a maioria das pessoas sente satisfação em receber correspondências, a probabilidade de que o internauta recebedor do “e-mail” possa ser cliente do banco são consideráveis. Dessa forma, ele pode ser iludido de que, de fato, foi o seu banco que enviou aquela mensagem afinal o “e-mail” e o “site” do “link” tem o “layout” da instituição. O golpista, nesse caso, usa a confiabilidade da imagem que o banco possui, para lograr as pessoas. Existem outros tipos de ataque empregados pela engenharia social que não somente os eletrônicos, como os acima citados. Esse tipo de crime merece atualmente uma maior reflexão por parte das empresas, no intuito de eliminá-lo ou reduzi-lo. A questão é séria e mesmo uma pessoa muito atenta pode se tornar uma vítima, pela facilidade de se atuar nos aspectos emocionais de qualquer ser humano.

A melhor arma contra a engenharia social é a informação. A utilização de sistemas ultra protegidos por parte das empresas são importantes, mas podem se tornar ineficientes, caso seus funcionários não tenham ciência dos golpes que possam vir a sofrer. No caso dos usuários domésticos, os responsáveis devem informar a seus familiares sobre os perigos existentes no fornecimento de dados particulares, mormente, quando estiverem “navegando” pela Internet. Muitos provedores de acesso à Internet, na atualidade, têm contribuído com seus sistemas de segurança para minimizar essa problemática. Ao mesmo tempo, setores da mídia alertam sobre os golpes existentes na nessa imensa rede mundial de informações, ajudando na divulgação de formas de prevenção. Mas ainda há muito a ser feito por setores do governo e entidades especializadas em segurança de organizações. A utilização da internet tem mostrado alguns perigos que podem se traduzir em riscos danosos aos negócios das empresas e aos lares dos cidadãos.

BARRETTO JR. e ASSOCIADOS

Endereço: Rua Genésio José de Moura S/ N Casa 01 – Lote 07/ Quadra 24 – Chácara de Pinhão – Tanguá/ RJ – CEP: 24890-000 | Filial 01: Av. Nossa Senhora de Copacabana, 36/ 1101 – Leme – Rio de Janeiro/ RJ – CEP: 22010-122 – Tel.: (21) 3507-5949 | Filial 02: Av. Angélica, 868/51 – Higienópolis – São Paulo/ SP – CEP: 01228-000 Tel.: (11) 3666-2580 | Email: contato@barrettojreassociados.com.br