Uma Visão Geral sobre Fraudes Bancárias Online

Marcelo Santos Guimarães

Desde o princípio das atividades econômica existem pessoas que se dedicam a praticar os mais diversos tipos de fraudes. Um dos mais antigos conjuntos de leis que se tem notícia, o código de Hammurabi (aprox. 1700 a.C.), define vários casos de fraudes e suas punições. Por exemplo, a palavra vigarista surgiu devido ao "Conto do Vigário", fraude praticada por vigários que pagavam pouco pelo ouro roubado por escravos.
A evolução dos hábitos da humanidade e o advento de novas ferramentas e tecnologias cria também oportunidades para os fraudadores. É o caso da Internet. Além de facilitar operações como transações bancárias e compras ela fez surgir uma nova modalidade de fraudes: as fraudes online.

O principal meio de fraude na Internet é o phishing, que se baseia no envio de um e-mail fraudulento com o objetivo de obter códigos de acesso e dados financeiros. A obtenção destes dados pode ser feita de diversas maneiras. As mais comuns são os bankers, que monitoram a troca de informações entre a vítima e os sistemas dos bancos, e as páginas falsas, que tentam se passar por páginas verdadeiras de bancos.

Mas a grande maioria das fraudes online requer o "consentimento" da vítima, ou seja, na grande maioria dos casos a fraude ocorre por alguma falha da vítima. O simples recebimento de um e-mail fraudulento não instala, por exemplo, um banker no computador da vítima.

O processo normal de uma fraude é o seguinte:
1. A vítima recebe um e-mail fraudulento.
2. Por algum motivo a vítima acessa o link disponível na fraude recebida.
3. Este link leva a uma página falsa ou a um banker que requer a confirmação de instalação pela vítima.
4. A vítima acessa a página falsa e fornece dados sensíveis ou, após a instalação do banker, acessa a página verdadeira do banco.
5. Os dados são capturados pela página falsa ou pelo banker instalado no computador.

Os e-mails fraudulentos utilizam-se de temas que supostamente dizem respeito à vítima ou que mexem com sua curiosidade. Para aumentar a credibilidade da fraude são usados logos das empresas originais, linguajar adequado, estrutura fiel à da mensagem original, remetente falso se passando pela empresa em questão, etc. Entre os temas mais recorrentes temos:
-bancos pedindo que a vítima atualize o dispositivo de acesso ao Internet Banking, sob pena de bloqueio;
-notícias falsas de forte apelo, como morte de alguma celebridade ou algum tema atual;
-fotos e vídeos sensuais, fotos provando traições;
-recebimento de alguma mensagem de texto acessível em alguma página, como torpedos, telegramas online;
-notificações financeiras e cadastrais diversas (pendências de CPF, título eleitoral e de crédito, avisos de débitos e cobranças, transações de comércio eletrônico, orçamentos).

Além de seguirem os modelos das mensagens oficiais, como é o caso de notificações de bancos, as fraudes possuem algumas características comuns que auxiliam na identificação:
-erros de português grotescos;
-remetente suspeito;
-impessoalidade, como Olá gbsantos1970;
-a imagem do logo possui defeitos;
-as imagens estão todas em miniatura;
-informação improvável, como promoções exageradas;
-links "esquisitos" que não têm a ver com os links da página oficial;
-links para arquivos com extensões .scr, .exe, .bat.

Alguns cuidados são necessários para que o usuário não seja vítima de uma fraude. Entre eles, os seguintes pontos devem ser observados:
- Nunca envie informação pessoal que lhe seja solicitada por e-mail tal como: nº de cartão de crédito, username, senha, etc.
- Não confie cegamente no conteúdo de um e-mail supostamente enviado por uma instituição. Verifique no próprio site da empresa ou use outros meios de contato para confirmação das informações.
- Assim como o conteúdo do e-mail, não confie no nome do emissor da mensagem, que pode ser facilmente forjado.
- Digite o endereço do site em seu navegador, não clique em links prontos que chegam em mensagens de correio eletrônico. Existem técnicas para mascarar o real destino de um link, podendo direcioná-lo para um site clonado.
- Desconfie de e-mails impessoais que se dizem de uma entidade com a qual mantém relações, seja um site de e-commerce ou uma instituição financeira. Normalmente os e-mails destas entidades dirigem-se ao cliente pelo nome.
- Em caso de dúvida, contate a entidade para confirmar a veracidade do e-mail, mas nunca use os contatos indicados no e-mail.

Os bancos, de forma geral, investem pesado em segurança da informação e disponibilizam cada vez mais recursos para seus clientes, tais como senhas adicionais, teclados virtuais e certificados digitais. Porém, a grande brecha no sistema continua sendo o usuário. O número de pessoas que utilizam a Internet para realizar operações bancárias e movimentações financeiras em geral é crescente. Portanto é muito importante que as práticas de segurança no ambiente virtual sejam disseminadas. As referências abaixo possuem algumas páginas dedicadas ao assunto.

Fontes:

http://br.mozdev.org/firefox/fraude

http://www.mhavila.com.br/topicos/seguranca/scam.html

http://www.guiadoimigrante.com/materia-2303.Fraudes-online-antigos-golpes-ainda-causam-grandes-prejuzos.html

http://www.bb.com.br/portalbb/page22,105,5212,0,0,1,1.bb?codigoNoticia=2976&codigoMenu=579