Considera segura sua atitude na internet?
Mário Mello

À medida que o uso da internet para operações cotidianas, como transações bancárias e compras on-line, torna-se mais comum, crescem também os riscos da exposição de dados sigilosos na rede, o que pode causar elevados prejuízos financeiros aos usuários. Segundo uma pesquisa realizada pela Febraban, somente em 2009 os golpes on-line movimentaram R$ 900 milhões, e no primeiro semestre de 2010 os danos atingiram R$ 450 milhões.

Há, no entanto, diversas maneiras de prevenir esse tipo de ataque, que dependem de cuidados tão simples, que, muitas vezes, sequer são levados em conta durante uma transação on-line. A maioria das pessoas sabe que existem e-mails de phishing circulando pela internet - talvez não com esse nome, mas como mensagens falsas, com certeza -, mas quando se trata de uma notificação do banco em que se tem conta ou da Receita Federal, por exemplo, é comum as pessoas ficarem apavoradas pela aparente gravidade do assunto, pela relevância da instituição envolvida e pelo possível vínculo dela com o usuário.

Quando esses fatores são combinados, os internautas podem se esquecer dos riscos que estão correndo e acabar fornecendo dados sigilosos. De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, as notificações de phishing já atingem quase metade (49,40%) dos ataques on-line existentes no País. O objetivo desse tipo de e mail é redirecionar o usuário para um site fraudulento, que pode ser muito similar à página oficial de uma empresa renomada.

O próximo passo do golpe é solicitar ao usuário informações pessoais, como número de cartão de crédito, CPF ou a senha da conta corrente. Se você não estiver atento, pode cair facilmente nesta armadilha e seus dados poderão ser utilizados em compras não desejadas. Os e-mails que começam com saudações genéricas, como "caro usuário", também devem merecer atenção redobrada.

As mensagens legítimas devem se referir a você pelo nome e sobrenome. Para tirar a dúvida, não hesite em entrar em contato com a empresa para checar do que se trata. Em caso de tentativa de golpe, avise imediatamente a instituição para que ela investigue o caso. Muitas mensagens falsas tentam enganar o usuário com a ameaça de que ele está correndo riscos se não atualizar os dados o quanto antes. A dica é: se o e-mail solicita que você forneça informações pessoais de forma urgente, provavelmente é fraudulento.

Vale a pena também sempre checar se as mensagens recebidas correspondem com as originais. Pode parecer óbvio, mas os golpistas costumam enviar mensagens falsas com um link que, aparentemente, é válido, mas que redireciona os internautas para um site fraudulento, que pode ter ou não uma URL (endereço eletrônico) diferente do link.

A sugestão é verificar sempre o local para onde o link o direcionará antes de clicar nele. Passe o mouse por cima da URL apresentada no e-mail e veja se é a mesma apresentada no navegador. Lembre-se sempre: não clique se parecer suspeito. Os anexos de e-mails também merecem atenção. Como ocorre no caso dos links falsos, os documentos anexados também podem ser perigosos.

A sugestão é nunca clicar neles para evitar downloads de spywares (programas automáticos de computador, que recolhem informações sobre o usuário) ou de vírus. Os meios seguros de pagamento on-line nunca enviarão e-mails com anexos ou solicitarão que você instale um software para atualizar seu computador. Outra dica importante é que o termo "https" deve sempre anteceder qualquer endereço de site (ou URL) no qual você insere informações pessoais. O "s" significa "seguro". Se você não vir o "https", significa que você não está em um ambiente com segurança e, portanto, não deve digitar suas informações.

Outro indício de fraude é quando o ícone do cadeado de segurança está fora do lugar: certifique-se de que este símbolo esteja na barra inferior da página do seu navegador, pois

muitos sites falsos trarão este elemento dentro da janela do navegador a fim de enganar os usuários. Orientações como essas, apesar de simples, podem evitar que você caia em golpes e forneça seus dados a fraudadores. O ideal é ter em mente que a falta de atenção no ambiente on-line pode resultar em grandes prejuízos. Além disso, ao realizar qualquer tipo de transação financeira, dê preferência aos meios seguros de pagamento on-line, que criptografam seus dados financeiros e os solicitam apenas uma vez, além de garantirem 100% de proteção contra pagamentos não autorizados, já que todas as operações exigem confirmação do titular da conta.

Fonte: DCI, São Paulo, 19 abr. 2011, São Paulo, p. C2.