A responsabilidade dos Bancos pelos prejuízos resultantes do 'phishing'

Demócrito Reinaldo Filho*

Sumário:1- Introdução. 2- Definições; 2.1 – Definição de phishing; 2.2- Definição de pharming; 2.3- Definição de DNS poisoning; 3- Inviabilidade de se responsabilizar o provedor de acesso à Internet ou de hospedagem; 4- Inviabilidade de se responsabilizar os provedores de serviços de e-mail; 5- Insuficiência das leis que criminalizam a conduta do ofensor direto (phisher); 6. Teoria da responsabilidade dos bancos prestadores de serviços de Internetbanking; a) argumento de ordem econômica; b) incentivo ao desenvolvimento de ferramentas tecnológicas; c) argumento da possibilidade técnica de evitar a fraude; 6.1. Adequação do novo padrão de responsabilidade à legislação existente; 6.1.1 Responsabilidade contratual regida pelo CDC. 7. Soluções tecnológicas empregadas pelos bancos para evitar fraudes eletrônicas . a) Firewall. b) Criptografia de dados (SSL); c) Teclado Virtual; d) Certificado Digital. 8. Proporção entre adoção de práticas seguras pelos bancos e a diminuição do grau de responsabilização. 9. Conclusões

1- Introdução

O desenvolvimento do comércio eletrônico está intimamente relacionado com as medidas que os legisladores e juízes adotam em respeito a certos temas que assomam no ciberespaço. O incremento dos negócios e a evolução da própria rede dependem de como os legisladores e as cortes judiciárias se posicionam em relação a conflitos que surgem a cada dia. Um exemplo de decisão judicial que certamente tem impacto no mundo dos negócios na rede mundial é aquela relacionada com a responsabilidade civil dos bancos por

ataques de phishing1. Dependendo de como os tribunais e juízes passem a decidir essa questão, responsabilizando (ou não) os bancos pela reparação dos seus clientes, vítimas desse tipo de fraude tecnológica, pode haver alteração no modelo de negócios hoje estabelecido e disseminado na rede. Não é difícil, por exemplo, prever uma diminuição da utilização dos serviços bancários on line, se os clientes de banco perderem a certeza quanto a uma reparação completa dos danos financeiros decorrentes do phishing. Por outro lado, os bancos certamente procederão a modificações no modelo de relacionamento bancário na Internet, se a Justiça se inclinar a responsabilizá-los de forma objetiva por toda e qualquer fraude financeira.

Como se vê, o tema da responsabilidade dos bancos no ressarcimento dos prejuízos causados pelos ataques de phishing é realmente delicado, e de interesse de todo o conjunto da sociedade, em razão da disseminação dos serviços de Internetbanking2, já tão incorporados ao nosso dia-a-dia e sem os quais não mais seria possível o atendimento bancário de forma eficiente. Sem o uso das tecnologias da informação, sobretudo a utilização da rede mundial de comunicação (Internet), na prestação dos serviços bancários, é certo dizer que seria impraticável o fornecimento desses serviços de forma massificada, conveniente e eficiente, tal qual são prestados atualmente. O maior desafio nessa área, no entanto, é superar os problemas de segurança e definir responsabilidades pelas conseqüências de ataques e invasões de sistemas informáticos. Definir, com precisão, as responsabilidades dos prestadores dos serviços bancários on line ajuda a impulsionar o desenvolvimento desse mercado, já que elimina as incertezas quanto a quem deve e em quais circunstâncias arcar com os prejuízos do phishing e outras práticas tecnológicas fraudulentas.

Acontece que estabelecer esquemas de atribuição de responsabilidade civil nesse contexto não é tão fácil, dada a intricada cadeia de papéis e funções que cada um dos atores da comunicação informática assume. Para propiciar a comunicação na prestação do serviço de Internetbanking, exige-se algum tipo de envolvimento ou participação do provedor de Internet, do fabricante do programa gerenciador de e-mail, do fabricante dos softwares e soluções de segurança, do fabricante do software de navegação, da instituição bancária, da

pessoa que desenvolve e dá manutenção ao sistema (de Internetbanking) e do próprio internauta (cliente do banco). É justamente a participação e o envolvimento desses diversos atores da comunicação informática que faz com que se torne difícil definir qual deles e em quais circunstâncias pode ser responsabilizado a reparar os prejuízos financeiros resultantes de fraudes tecnológicas como o phishing. Isso faz com que esse tema se torne pouco explorado e dos mais complexos.

A complexidade e a importância do tema nos instigou a incursionar na matéria, para colaborar na tarefa de definir esquemas de imputação de responsabilidade aos prestadores de serviços bancários on line. O aumento gradativo dos ataques de phishing nos últimos anos3, e a apreensão que isso tem causado ao comércio eletrônico, também nos estimulou a escolher esse tema como foco de nossa investigação científica. A falta de trabalhos doutrinários sobre a matéria da mesma forma funcionou como fator decisivo na escolha da definição do campo de pesquisa. Pelo menos até onde sabemos, não há registro na doutrina brasileira de qualquer trabalho sobre a questão da responsabilidade civil dos bancos pelas conseqüências dos ataques de phishing. Mesmo na doutrina alienígena (de acordo com pesquisa que fizemos na Internet)4, não encontramos referência a qualquer artigo ou ensaio científico sobre esse assunto. Alguns autores estrangeiros escreveram sobre a possibilidade da responsabilização dos intermediários da comunicação eletrônica (como os provedores de acesso à Internet)5, mas não especificamente sobre a responsabilidade civil dos bancos diante desse tipo de fraude financeira.

No nosso trabalho, procuraremos identificar o esquema de imputação de responsabilidade - se baseado na culpa, fundado no dever objetivo de reparar o dano (responsabilidade objetiva) ou apoiado na noção de vício (do serviço) - que melhor se enquadra aos bancos, em face dessas situações (ataques fraudulentos). Em outro trecho, mostraremos a inviabilidade de se responsabilizar o provedor de acesso à Internet pelos prejuízos decorrentes do phishing.

É importante esclarecer que só iremos tratar da responsabilização do banco pelos tipos primitivos (e mais conhecido) de phishing, aqueles que pressupõem sempre o logro ao

destinatário de uma mensagem eletrônica (e-mail), que o faz repassar suas informações pessoais (bancárias) ao criminoso (fraudador), seja clicando num link (que descarrega o vírus), abrindo arquivo anexo (que contém o vírus) ou inserindo manualmente informações em um site falso. Em ambas essas situações, o indivíduo recebe previamente a mensagem de e-mail enganosa, induzindo-o a abrir o arquivo anexo contendo vírus ou a clicar em um link que descarrega o vírus ou o leva para um site falso.

Esses são os casos mais comuns de “identity theft” (furto de identidade, traduzido para o português) cometidos com uso de comunicações eletrônicas, em que o primeiro estágio da fraude consiste no logro do usuário do serviço de Internetbanking, levando-o a pensar que está fornecendo suas informações pessoais à instituição confiável, com quem mantém relação contratual, quando na verdade está repassando seus dados bancários ao phisher (agente do crime de phishing). O destinatário da mensagem também é enganado quando é induzido a clicar sobre um link (no corpo da própria mensagem) ou abrir arquivo anexado a ela, ação que descarrega um programa malicioso (malware) que se apodera de seu computador e repassa as informações nele contidas ao phisher, ou intercepta as comunicações feitas pelo terminal infectado com os sites de bancos6, capturando informações como número de contas e senhas.

Esses tipos de fraudes, portanto, compreendem sempre esse elemento, da burla, do ato ou efeito de enganar a pessoa para que forneça seus dados pessoais. Isso ocorre tanto quando um indivíduo preenche um formulário em um spoofing site (site falso estruturado com a aparência do site legítimo) ou quando abre um arquivo que contém vírus, o qual é ativado e, apropriando-se de sua máquina (da vítima), funciona repassando os dados contidos no computador para o fraudador (hacker ou criminoso cibernético). Em ambas essas situações, o indivíduo recebe previamente a mensagem de e-mail enganosa, induzindo-o a abrir o arquivo anexo contendo vírus ou clicar em um link que descarrega o vírus ou o leva para um site falso.

Faremos uma exceção para incluir em nosso trabalho um único tipo de fraude que não pressupõe necessariamente, no seu iter criminoso, a remessa prévia de uma mensagem de e-

mail para o sujeito vítima da trama. Trata-se da fraude conhecida como pharming, procedimento que redireciona os programas de navegação (browsers) dos internautas para sites falsos. Podemos explicar a razão dessa inclusão. Mesmo essa espécie pressupõe um ataque dirigido à pessoa do usuário (cliente) dos serviços bancários, para captura de informações. Mesmo aí ainda há o elemento do logro ao usuário, o qual, apesar de não ter recebido uma mensagem prévia de e-mail7, teve seu browser direcionado para um site falso. O engano corresponde a encarar o site falso como legítimo, e por conta desse engano, entrega suas informações pessoais ao criminoso, pensando estar diante do operador do site legítimo. O alvo primário do criminoso, mesmo nesse caso de pharming, é sempre o cliente bancário (ou seu computador pessoal).

Uma modalidade de pharming não será enquadrada dentre os tipos de fraude objeto do nosso estudo, já que nessa hipótese o provedor de acesso à Internet é o juridicamente responsável (na órbita civil) pela reparação de seus efeitos. É o chamado DNS poisoning (algo próximo a "evenenamento do DNS"). Nessa modalidade também ocorre, como nos demais casos, uma ação destinada a coletar informações pessoais da vítima (para depois serem utilizadas na fase seguinte do crime). Com o servidor DNS do provedor "envenenado", e alteradas as configurações de um determinado endereço web, o internauta é direcionado para um site falso mesmo teclando o endereço correto. Nessa situação, no entanto, o ataque inicial não foi direcionado ao computador da vítima (cliente do banco), mas sim ao sistema informático do seu provedor de Internet, que pode, por essa razão, ser tido como responsável pelas conseqüências do ataque, por falha de segurança do sistema8.

Em suma, o nosso trabalho abrange a investigação sobre responsabilização dos bancos em todos aqueles casos em que a fraude tem como alvo primário o cliente bancário. É o seu computador que é infectado por um vírus ou é a própria vítima que, induzida por uma mensagem fraudulenta, repassa as informações para o fraudador. Não se trata de invasão ou ataque direto ao próprio sistema informático do banco, nem tampouco ao do provedor de Internet ou exploração de alguma falha no software de navegação (ou qualquer outro). Todas as modalidades de phishing a serem estudadas como pressuposto para a responsabilização do banco (fornecedor do serviço de Internetbanking), têm no elemento do

logro ao usuário ou infecção do seu computador a origem do procedimento criminoso. São casos em que o alvo primário da fraude é o cliente do banco, de quem (ou de seu computador) são capturadas as informações pessoais para a consecução das etapas seguintes do esquema criminoso. O sistema informático do banco não sofre propriamente um ataque em que são exploradas suas vulnerabilidades ou falhas de segurança, pois o criminoso nele ingressa como se fosse o legítimo usuário (já que se apropria previamente das informações pessoais e sigilosas deste). O acesso se dá pelos meios permitidos pelo próprio sistema, através da digitação da senha e informações do usuário.

É em face desse tipo de fraude ou ação criminosa que examinaremos a responsabilidade do banco, pelos prejuízos econômicos ao patrimônio das vítimas (clientes). Nesse esforço, investigamos se o fundamento da responsabilidade deve ser o do risco de sua atividade (responsabilidade objetiva), se deve responder com base no aspecto subjetivo de sua conduta (culpa) ou se lhe deve ser reconhecida uma responsabilidade especial (fundada na noção de vício do serviço). Uma vez definida a noção de vício como fundamento da responsabilização, procuramos apontar quais situações específicas podem denotar a imprestabilidade do serviço on line (vício de inadequação) capaz de justificar o dever do banco de reparar o dano sofrido por seus clientes.

Estamos certos de que, com esse escorço que ora apresentamos, contribuímos de forma decisiva para a evolução da teoria da responsabilidade civil em nosso país, já que, conforme antes referimos, ainda não existe na doutrina brasileira qualquer trabalho sobre a matéria objeto de nossa investigação.

Revista Jus Vigilantibus, Quarta-feira, 30 de julho de 2008

* Juiz de Direito (32ª. Vara Cível do Recife).

Disponível em:
http://jusvi.com/artigos/35040
Acesso em: 19 agosto 2008.