Usuário da internet é quem deve se precaver contra vírus e crackers

Em tempos recentes, quando a internet está cada vez mais difundida em nossa sociedade graças aos esforços governamentais de inclusão digital, à facilidade de acesso à rede, aos celulares com tecnologia 3G que possibilitam o acesso de qualquer parte e a qualquer tempo, os furtos de senhas bancárias e outras vêm ocorrendo com alguma frequência. É a atuação dos chamados *crackers*, que seriam os "*hackers* do mal", pessoas que utilizam seu conhecimento de informática e meios telemáticos para prejudicar terceiros e locupletar-se de alguma forma com isso.

As empresas, por sua vez, investem em sistemas de segurança, garantindo o acesso apenas ao usuário que apresente uma infinidade de dados corretos, supostamente sabidos apenas pelo titular do serviço. Mas, e quando o usuário fornece todos estes dados, inconscientemente, ao c*racker*, permitindo assim o acesso a sites de empresa como se ele fosse?

Antes de mais nada é necessário fazer um raciocínio de ordem pragmática: se, por razões do negócio, o empresário possibilita ao seu cliente utilizar a internet, é porque isso lhe diminui os custos, mas, por outra via, se o meio se desmoraliza, deixa de ser utilizado. Logo, é do interesse do empresário ofertar o máximo de segurança à utilização de seus serviços informáticos e é justamente o que se tem averiguado na prática. As empresas têm realizado notórios investimentos em segurança, buscando certificar-se de estar falando apenas com seu cliente, este considerado aquele que detém senhas, perguntas secretas e *tolkens* e outros artifícios de segurança, mas tudo isso é jogado na lata do lixo se seu usuário é de alguma forma enganado no mundo virtual e passa ao terceiro de má fé a chave do cofre, seja por não manter um antivírus atualizado em seu computador, seja por confiar em falsas páginas de Internet ou falsos e-mails.

A utilização da nova ferramenta atrai benefícios não apenas para bancos e sites de internet, mas para os clientes também, por óbvio. O que se espera de quem se lança a utilizar essa ferramenta é informar-se minimamente como ela funciona e que cautelas específicas exige. O fato foi enaltecido pelo juiz Alex Gonzales Custódio (processo 001/1.07.0145354-4 – Vara Cível do Foro Regional Tristeza – Porto Alegre – RS), em recente decisão em que analisava a responsabilidade pelos prejuízos causados por *crackers* que causaram prejuízos ao autor em um site na internet.

O juiz ponderou em sua decisão que cada usuário da rede deve zelar por seus dados, se precaver contra vírus e *crackers* e que essa é a responsabilidade de todo aquele que se propõe a utilizar a internet:

"O que o bom senso exige é que cada usuário de sistemas de venda em mercados pela internet se proteja utilizando seguranças em seu sistema de computadores pessoal ou profissional, como contra-medidas para eventuais vírus e evitar prováveis hackers.

Assim, se culpa houve não foi da empresa, mas sim dos próprios autores, especialmente em sendo especialistas na área de informática, porque afirmam serem vendedores de notebooks pela internet e, mais ainda, deveriam utilizar proteção e segurança adicionais, a fim de evitar serem vítimas de furto por meio da internet."

O entendimento não é inovador, ao contrário, o Superior Tribunal de Justiça já havia se posicionado,

entendimento que mereceu o seguinte comentário na imprensa: “Para o juiz Demócrito Filho, finalmente os bancos ‘fizeram o dever-de-casa’. ‘Recentemente o Superior Tribunal de Justiça trouxe uma nova jurisprudência em favor das empresas, no sentido de que a tecnologia atual não permite a ação dos phishers. E se o usuário passou a senha para o criminoso, o banco não está obrigado a indenizá-lo, finaliza. (R.M.)´”[1]

Cada vez mais os magistrados vêm ressaltando a falta de cautela dos usuários como instrumento que afasta a responsabilidade do fornecedor ou empresário. Outro exemplo é o pronunciado por Edson Luiz De Queiroz, juiz da 3ª Vara Cível de Santo Amaro – São Paulo – SP (processo 583.02.2008.125175-1) em que decidiu pela isenção de responsabilidade de uma empresa fundamentando:

“A autora não observou essas cautelas, acessando “link” que não pertencia à ré e não possuía sistema de segurança, permitindo que seus dados fossem alterados. Com isso, houve causa de prejuízos para as partes e para terceiros. A responsabilidade pelo ato é exclusivo da autora, não se podendo falar em responsabilidade concorrente ou exclusiva por parte da ré. e um site de compra e vendas”

Como se vê, os entendimentos recentes analisam a falta de cautela dos usuários que deixam de atentar para as recomendações mais básicas àqueles que navegam pela internet, recomendações que em tempos remotos poderiam ser comparadas aos conselhos de nossos pais para não falar com estranhos na rua, não fornecer dados pessoais, telefone e endereço da residência, ou seja, os cuidados são os mesmos de sempre, mas agora no meio eletrônico: não “clique” em links estranhos, delete e-mails de quem não conhece antes mesmo de abri-los, verifique sempre por onde está navegando, principalmente se for fornecer algum dado pessoal.

Incumbe às empresas informar seu usuário quanto a essas cautelas simples. mas eficazes, a fim de poderem beneficiar-se da limitação de responsabilidade que vem sendo reconhecida nas hipóteses aqui comentadas.

[1] Publicado em 14.11.2007 – Veículo: **Jornal do Commércio**

Date Created
25/03/2009