

4.2 SEGURANÇA DIGITAL

4.2.1 Estelionato digital e segurança em sites de comércio eletrônico

Riany Alves de Freitas

*Analista do Ministério Público de Minas Gerais
Pós-Graduada em Gestão Estratégica da Informação pela
Universidade Federal de Minas Gerais
Graduada em Tecnologia em Processamento de Dados pela
Fundação Mineira de Educação e Cultura
Acadêmica em Direito pela Pontifícia
Universidade Católica de Minas Gerais*

SUMÁRIO: 1. Introdução. 2. Estelionato digital. 3. Recomendações. 3.1. Recomendações aos clientes 3.2. Recomendações aos comerciantes. 4. Considerações finais. 5. Referências bibliográficas.

1. Introdução

Algumas pessoas têm procurado a Promotoria Estadual de Combate aos Crimes Cibernéticos, indagando sobre como

proceder para transmitir segurança aos seus clientes, em suas páginas de venda de produtos na internet, bem como quais padrões devem ser adotados para que nenhum crime digital seja cometido durante o processo.

Antes de tudo, é preciso frisar que a idoneidade vem da pessoa responsável pelas vendas e não do *site* propriamente dito. Não podemos afirmar que uma pessoa não vai ser vítima de um golpe na internet pelo fato de o *site* seguir todas as recomendações possíveis de segurança, ou vice-versa.

Apesar disso, existem algumas recomendações que ajudam o cliente a escolher em qual *site* comprar, bem como orientam o responsável pelas vendas na construção do *site*, recomendações estas que serão abordadas no tópico 3 deste artigo.

2. Estelionato digital

O mundo virtual oferece muitas facilidades para quem deseja fazer uma compra. Podem-se comprar produtos,



Informações Variadas

dos mais variados, sem sair de casa, com apenas poucos cliques, a preços mais baixos. Por isso, comprar através da internet pode trazer uma série de conveniências ao comprador, o que nem sempre ocorre.

O estelionato é um crime previsto no art. 171 do Código Penal brasileiro e consiste em “Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento”. Para esse crime, é prevista pena de reclusão, de um a cinco anos, e multa.

Não há dúvidas de que tal conduta pode ser praticada através da rede mundial de computadores. Aliás, tem sido bastante comum que pessoas sejam vítimas desse golpe através da internet.

(...) comete o crime de estelionato o agente que cria página na Internet ou faz anúncios por intermédio de *sites* como o Mercado Livre, por exemplo, simulando a venda de produtos com o objetivo de induzir a vítima em erro ao efetuar o pagamento antecipado da suposta mercadoria na ilusão de que está efetuando a sua compra e que irá recebê-la posteriormente, quando, na realidade, trata-se de um golpe utilizado pelo agente para obter vantagem econômica indevida, aproveitando-se da boa-fé das pessoas para enganá-las e acarretar prejuízo ao patrimônio destas. (RAMOS JÚNIOR, 2008, p. 41).

Existe hoje uma pacificação doutrinária e jurisprudencial acerca da aplicação do crime de estelionato cometido mediante rede mundial de computadores.

3. Recomendações

Procuramos demonstrar aqui algumas recomendações aos clientes que buscam *sites* seguros para efetuar suas compras, bem como aos comerciantes que disponibilizam páginas na internet para efetuarem suas vendas; porém, enfatizamos que as recomendações aqui expostas não esgotam a questão e não garantem a idoneidade e honestidade dos internautas em geral.

3.1. Recomendações aos clientes

Procure utilizar o navegador Firefox. Isso evitará que seu navegador execute programas maliciosos desenvolvidos especificamente para o Internet Explorer, que correspondem a mais de 90% deles.

Verifique se o *site* é seguro. O *site* seguro contém um símbolo de cadeado na parte inferior da janela. Isso indica que a loja virtual trabalha com certificado de segurança.

Consulte o *site* de vendas no endereço www.registro.br e verifique os dados completos de quem registrou o domínio, o CGC da empresa responsável bem como seu endereço.

Ofereça o mínimo possível de informações para completar a transação. Evite acrescentar informações

que não têm relação alguma com a concretização do negócio.

Procure certificar-se de que todas as informações fornecidas pelo *site* estão corretas, como razão social, CNPJ, endereço e telefone de contato. Cuidado quando o *site* fornecer como forma de contato apenas um telefone celular.

Procure efetuar compras somente em *sites* conhecidos e indicados por parentes ou amigos.

Não forneça senhas a ninguém. Procure utilizar senhas com o maior número de caracteres possível. Tente escolher uma senha entre 6 e 12 caracteres, alternando letras minúsculas, letras maiúsculas e números de forma aleatória.

Verifique a política de privacidade da loja virtual. Saiba qual o compromisso do vendedor em relação à manipulação dos dados que você informa.

Evite também colocar sua senha ou seus dados pessoais em *links* fornecidos por *e-mails*, ainda que eles aparentemente tenham sido enviados pelo *site* no qual você se cadastrou.

Verifique na página do fabricante do produto o qual tem interesse em comprar se suas características condizem com as fornecidas pelo *site* do vendedor.

Verifique as características do produto, condições de entrega, tarifas de envio, formas de pagamento, condições de troca e tarifas de envio.

Registre toda a negociação e transação, como *e-mails*, anúncios, as telas do *site* de compra e toda a comunicação feita com a loja. Caso seja vítima de um estelionato, registre sua denúncia, com todos os comprovantes, no *site* da Promotoria Estadual de Combate aos Crimes Cibernéticos.

3.2. Recomendações aos comerciantes

Disponibilize *site(s)* compatível (is) com o navegador Mozilla Firefox.

Ofereça páginas seguras, através de protocolos e mecanismos que provejam autenticação das partes envolvidas e criptografia nos dados transmitidos.

O protocolo HTTPS é utilizado, em regra, quando se deseja evitar que a informação transmitida entre o cliente e o servidor seja visualizada por terceiros, como por exemplo no caso de compras *online*. A existência na barra de tarefas (normalmente do lado direito) de um cadeado demonstra a certificação de página segura (SSL). (WIKIPEDIA).

Ofereça informações detalhadas aos clientes, como características do produto, condições de entrega, tarifas de envio, formas de pagamento e condições de troca.

Forneça um telefone fixo para contato, razão social, CNPJ, endereço e outras formas de contato além do *e-mail*, bem como Registro na Junta Comercial da empresa.

4. Considerações finais

Enfatizamos novamente que as orientações aqui fornecidas não excluem o risco de efetuar uma transação através da internet. Assim como os cuidados a serem tomados ao efetuar uma compra em loja física, também existem aqueles que devem ser tomados ao adquirir produtos de lojas virtuais.

Acreditamos que o sucesso nas vendas é adquirido ao longo do tempo, quando a credibilidade do vendedor se torna elevada, à medida que ele se esforça em manter o cliente satisfeito.

5. Referências bibliográficas

CÂMARA BRASILEIRA DE COMÉRCIO ELETRÔNICO. **Comércio Eletrônico**: Cartilha do Consumidor. Disponível em: <<http://www.camara-e.net/e-consumidor/>>. Acesso em:

25 mar. 2009.

RAMOS JÚNIOR, Hélio Santiago. Estudo sobre a aplicabilidade das leis penais aos crimes informáticos no Brasil. In: **Proceedings of the Third International Conference of Forensic Computer Science**. Rio de Janeiro: ABEAT, 2008. p. 36-47.

REZENDE, Pedro Antonio Dourado. **Segurança no comércio eletrônico**. 2006. Disponível em: <<http://www.cic.unb.br/docentes/pedro/trabs/entrevistaPB.html>> Acesso em: 25 mar. 2009.

WIKIPÉDIA, a enciclopédia livre. **HTTPS**. Disponível em: <<http://pt.wikipedia.org/wiki/HTTPS>>. Acesso em: 25 mar. 2009.