DOI: 10.5433/1981-8920.2013v18n1p17

COMUNICAÇÃO E A PREVENÇÃO DE DANOS NO USO DA INTERNET

LA COMUNICACIÓN Y LA PREVENCIÓN DE DAÑOS EN EL USO DE INTERNET

Antonio Carlos Machado - carlos.machado@unip.br
Mestre em Comunicação pela Universidade Municipal de São Caetano do Sul (USCS). Docente da Universidade Paulista (UNIP).

Gino Giacomini-Filho - gino.giacomini@uscs.edu.br
Doutor e Livre-docente em Comunicação pela Universidade de São Paulo (USP). Docente do Programa de Mestrado em Comunicação da Universidade Municipal de São Caetano do Sul (USCS). Docente Universidade de São Paulo (USP).

RESUMO

Introdução: A comunicação bancária tem registrado uso intenso de novas tecnologias e conteúdos, caso do *net banking*, o que gera novas possibilidades e relações com o cliente bancário. Trata-se de um consumidor que é incentivado a conhecer os serviços oferecidos por meio de novos canais, a visualizar esses atributos, mas se ele detectar restrições informativas ou falhas na comunicação, irá se manifestar de alguma forma. Muitos consumidores lidam com fraudes ou danos causados pelo sistema de acesso virtual disponibilizado pelos bancos. Tal contexto apresenta inovações no sistema de comunicação protagonizado pelos bancos e consumidores midiatizados pela internet.
Objetivo: Descrever a comunicação bancária voltada para a prevenção de danos quando do uso de seus *websites* pelos consumidores.
Metodologia: Foram pesquisados os *websites* dos bancos Bradesco, Itaú e Banco do Brasil, além de pesquisa de opinião com 130 usuários do *net banking* desses bancos.
Resultados: Os bancos reservam em seus *websites* espaços específicos e não padronizados para a prevenção de danos ao consumidor no uso do *net banking*, enquanto os clientes usam tais serviços de forma parcial.
Conclusões: Os resultados encontrados não podem ser generalizados, servindo o presente estudo como degrau para que outros trabalhos possam aprofundar o objeto de estudo apresentado a fim de dimensionar com maior amplitude e representatividade a gestão da prevenção de danos ao consumidor no contexto do *net banking*.

Palavras chave: comunicação; consumidor; prevenção de danos; internet; bancos

1 INTRODUÇÃO

Sabe-se que os bancos são instituições importantes para o consumidor, pois além de prestar serviços de pagamento, financiamento e empréstimos, realizam operações que lidam com a privacidade e os direitos dos consumidores, o que implica clara inserção nas práticas de responsabilidade social. A internet e os *sites* dos bancos (*net banking*) são recursos modernos imprescindíveis na comunicação dos bancos com o consumidor; no entanto pode apresentar problemas estruturais no sentido de trazer danos consumeristas, o que inspirou o presente estudo.

O propósito desta pesquisa é analisar a comunicação bancária voltada para a prevenção de danos quando do uso de seus *websites* pelos consumidores. O que se investiga é a comunicação dos bancos quanto aos procedimentos de segurança aos seus usuários e a forma como os usuários lidam com essa comunicação.

A prática de fraudes via internet tem sido uma realidade, levando milhares de pessoas a sofrerem danos sociais e econômicos. Tal ameaça tem ocorrido com certa frequência em *sites* de bancos, a ponto de causar desconfiança sobre o acesso aos serviços prestados por estas importantes instituições.

A comunicação é essencial para o consumidor decidir, informar-se e obter conhecimento relevante sobre a qualidade dos serviços bancários, algo que a internet incrementou ao oferecer conveniência, rapidez e profundidade na comunicação entre consumidores e bancos. O uso da internet e *websites* tornou-se rotineiro para consumidores e instituições bancárias.

Trata-se de um estudo exploratório que faz uso de referencial teórico sobre a comunicação bancária, internet e consumidor. A pesquisa de campo utilizada neste trabalho ocorreu na forma de pesquisa documental por meio da descrição de conteúdo dos *websites* dos bancos Itaú, Bradesco e Banco do Brasil, e pesquisa de opinião com usuários dos mesmos bancos.

2 SEGURANÇA NA INTERNET E O MERCADO BANCÁRIO

A internet permite a comunicação entre pessoas em qualquer lugar do planeta, até em tempo real; possibilita o envio de mensagens que são entregues em

segundos; a compra de produtos e serviços sem sair de casa; a interação social entre as comunidades locais, regionais ou mundiais; a informação e comunicação colaborativa; a construção coletiva de conhecimento.

A internet e o ciberespaço conceituado por Levy (1999) romperam com a ideia de tempo e local. O novo meio de comunicação digital acolhe um verdadeiro oceano de informações e conecta milhões de pessoas que utilizam e abastecem este universo. Computadores, internet e a web geraram uma gama de serviços até então inimagináveis e que permitem às pessoas estreitar relacionamentos e atuar no mundo sem sair de casa (LIMA, 2000). Para Tapscott e Williams (2007), a internet representa sólida plataforma que possibilita e apressa outras rupturas criativas. As informações e tendências sociais se espalham de maneira viral em redes de "muitos-para-muitos".

O mercado emergente da comunicação via internet tem sido associado a crescentes números em função de alguns fatores: riqueza acentuada de informações nas transações e relações; menor custo na procura por informações dos consumidores; troca de informação assimétrica entre vendedores e compradores; proximidade espacial eletrônica entre vendedores e consumidores; tempo de compra e posse do bem adquirido nas compras digitais (VARADARAJAN; YADAV, 2002).

Porém, a internet também revela pontos fracos e preocupantes, sendo um dos mais presentes em termos de relações de consumo seus aspectos de segurança aos usuários.

Chang (2008) afirma que a fraude pela internet representa uma epidemia crescente que acarreta gastos de milhões de dólares por ano; desde os anos 1990, segundo o autor, a internet tem sido um atrativo meio de comunicação para a prática de fraudes. Naím (2006) admite que as práticas fraudulentas pelo comércio via internet fazem parte da pirataria global em que marcas são copiadas, produtos são falsificados e a lavagem de dinheiro ocorre em escala planetária.

Fruto desse cenário, as empresas têm inserido mecanismos de segurança em seus *sites* e sistemas virtuais, caso do uso de diversas senhas, fases distintas de acesso a informações de caráter restrito, mensagens de advertência, acompanhamento do histórico de transações e outros procedimentos para inibir a prática de fraudes.

Chang (2008) referencia-se no Departamento de Justiça americano para conceituar a fraude pela internet como um tipo de esquema de fraude que usa um ou mais componentes da internet, caso de *chats*, *e-mail*, mensagens, *websites* para fazer solicitações fraudulentas na prospecção de vítimas, conduzir transações fraudulentas ou para transmitir procedimentos de fraude junto a instituições financeiras ou outros agentes conectados com o esquema.

Chen (2009) se referencia no sucesso das redes sociais para afirmar que a internet tornou-se importante recurso do dia-a-dia das pessoas e em muitos negócios, envolvendo fornecedores de serviços e consumidores, o que evidenciaria uma maior responsabilidade social das entidades usuárias do comércio eletrônico (*e-commerce*). Argumenta o autor que a responsabilidade social das organizações com o advento da internet não ocorre apenas no plano legal, mas também no plano ético já que envolve tanto a imagem e reputação de pessoas como sigilo e dados confidenciais. Como a internet envolve um grande número de usuários em amplas comunidades e públicos diversificados, as organizações devem considerar os aspectos sociais, ambientais e econômicos advindos de suas ações no mercado.

A internet, além de ser atualmente um poderoso instrumento de comunicação e de decisão de compra, apresenta-se como plataforma em que são oferecidos produtos, marcas e serviços, muitos deles essenciais; oferece também ambiente no qual o consumidor pode reclamar, protestar, elogiar empresas e organizações (REZABAKHSH et al., 2006).

Fletcher (2007) considera que, em termos simples, o *e-commerce* significa conduzir as transações comerciais no ciberespaço, sendo uma das formas mais importantes a B2C (*business to consumer*), ou seja, em que empresa e consumidor trocam informações, experiências e bens. Considera também o autor que as transações virtuais envolvem mais riscos do que as presenciais.

Kingston, Schafer e Vandenberghe (2004) apresentam um modelo de transação financeira em que o comprador oferece pagamento e ordens de serviço, enquanto o agente bancário certifica a operação e comunica os efeitos da transação. Porém com a inserção do ambiente virtual, as relações entre fornecedores de serviços bancários e consumidores tornaram-se mais complexa.

Em 2004, a quantia de dinheiro perdido em fraudes financeiras pela internet no Brasil foi semelhante às perdas ocorridas por roubos de bancos; em Londres, uma gangue roubou cerca de 400 milhões de libras em 2005 do banco japonês

Sumitomo por meio de internet e, no mesmo ano de 2005, um hacker retirou informações de 40 milhões de cartões de crédito usando também a internet (FLETCHER, 2007).

Além de acarretar problemas aos usuários, as crescentes atividades de fraude na internet têm causado uma crise de confiança nos sistema comercial amparado no comércio eletrônico (GAVISH; TUCCI, 2006) algo que atinge também o sistema bancário. A magnitude das fraudes bancárias tem feito com que o setor invista e desenvolva sistemas de segurança nos procedimentos eletrônicos presenciais e virtuais.

Levantamento efetuado pelo Banco Central do Brasil (2010) com os bancos com mais de um milhão de clientes (agosto/2010) apurou que problemas de segurança nos meios eletrônicos ocuparam as terceiras e sétimas posições entre os dez primeiros motivos procedentes de insatisfação dos clientes com os serviços bancários.

Parece ser vantajoso para os bancos que os clientes deixem de utilizar os serviços presenciais que oneram a folha de pagamentos e ajudam a formar filas, e passem a utilizar os canais eletrônicos de uso à distância como a internet. Para a realização de uma transação nesses novos meios é preciso que haja envolvimento dos usuários com esses canais de comunicação. Oliveira (2000) diz que os consumidores bancários, para se sentirem satisfeitos, precisam ter certeza de que não terão problemas com suas contas.

O internet *banking* é um ambiente onde ocorre a interação entre o cliente e o banco para disponibilizar informações mercadológicas, institucionais e soluções de banco eletrônico e/ou comércio eletrônico, direcionadas ao público externo, integrando a comunicação, informação, conhecimentos e processos para a gestão de recursos e de negócios do banco.

As instituições bancárias incorporaram rapidamente a internet nas suas estratégias de comunicação com o consumidor, porém desde o início tiveram que lidar com fraudes que atingiam seus clientes ou públicos de interesse. As manifestações de consumidores na mídia social exemplificam relações tensas que podem ocorrer entre consumidor e bancos quando sistemas virtuais apresentam problemas.

O movimento consumerista, face ao grande número de ocorrências, passou a exigir que os bancos melhorassem seus sistemas de segurança porque a clientela

tem se mostrado cética em relação ao uso dos serviços bancários pela internet, o que também deprecia a imagem institucional dos bancos em relação às suas responsabilidades sociais (GAVISH; TUCCI, 2006).

Rezabakhsh et al. (2006) afirmam que, embora o consumidor moderno desfrute de poder adicional nas relações de consumo com o uso da internet, mecanismos governamentais, legais e corporativos precisam ser ativos para coibir práticas danosas nas transações efetuadas.

3 PESQUISA COM *WEBSITES* E USUÁRIOS DE BANCOS

3.1 Pesquisa com *Websites* dos Bancos

Com o propósito de mostrar ações de bancos na internet quanto à prevenção de danos ao consumidor, desenvolve-se aqui pesquisa documental com os *sites* do Banco do Brasil (BB), Itaú e Bradesco considerados em 2010, nesta ordem, os três maiores bancos em termos de ativos totais pelo Banco Central[1]. A pesquisa de caráter descritivo segue o modelo de Hite, Bellizzi e Fraser (1988) em que se considera apenas o descritivo de categorias de análise, neste caso a *home page* (a página de abertura do *site* do banco) e *links* da *home page*, ou seja, conteúdos derivados de *links* presentes na *home page*. Tais conteúdos de fraude pela internet foram retirados do modelo teórico de Chang (2008).

A análise se restringe aos conteúdos "fixos", ou seja, não foram considerados ou descritos textos ou notícias eventuais, ou seja, foram descritos espaços regulares, seções contínuas, colunas fixas. A continuidade desses espaços foi aferida por acompanhamento dos *sites* durante 30 dias; porém, a identificação de tais conteúdos foi restrita a um determinado dia (24/4/2011) para que a descrição dos três bancos fosse mais uniforme e para que se tivesse uma "fotografia" da comunicação para prevenção de danos ao usuário.

Conforme seu próprio *site*[2], o BB possui 12.382 pontos de atendimento distribuídos pelo Brasil, sendo 3.155 agências e 9.227 postos de atendimento diversos. O banco Itaú (Itaú-Unibanco) informou no seu *site*[3] que totalizou em abril

[1] Data-base: Dezembro/2010. Banco Central do Brasil (2011).
[2] *Site* do Banco do Brasil. Disponível em:www.bb.com.br.
[3] *Site* do banco Itaú. Disponível em: http://www.itau.com.br.

de 2011 cerca de 2.300 agências e 22.000 caixas eletrônicos**.** O Bradesco, segundo seu *site*[4], possuía 3.628 agências, sendo 1.263 postos de atendimento e 32.015 máquinas de auto-atendimento (dados de dezembro de 2010); chegou em 2009 a uma quantia superior de 10 milhões de clientes que utilizaram o *internet Banking* [5].

Segundo o *ValueTheWebsite.com*[6], *site* que avalia domínios de internet na esfera mundial, o domínio "bb.com.br" (Banco do Brasil) estaria avaliado em abril/2011 em US$ 743,379, ocupando a classificação de número 2.991 no mundo e com 173.123 *pageviews* por dia; o domínio "itau.com.br" (Itaú) estaria avaliado em abril/2011 em US$ 1,162,421, ocupando a classificação de número 1.628 no mundo e com 318.065 *pageviews* por dia; o domínio "bradesco.com.br" (Bradesco) estaria avaliado em abril/2011 em US$ 664,918 ocupando a classificação de número 3.063 no mundo e com 169,053 *pageviews* por dia. São dados que indicam a relevância dos *sites* das instituições bancárias analisadas.

A *home page* do banco Itaú (www.itau.com.br), considerando o conteúdo de interesse da pesquisa, mostra a presença dos seguintes campos: Segurança Online e Dicas de Segurança.

- Segurança Online

O campo Segurança Online possui três *links*, dos quais dois são pertinentes ao tema da pesquisa: "Conheça o Programa Mais Segurança" e "Veja as fraudes mais comuns".

"Conheça o Programa Mais Segurança" é um espaço que leva ao quadro "Programa Mais Segurança Itaú", que disponibiliza formas de contatos para o internauta se informar, reclamar e esclarecer dúvidas sobre uso e acesso a dados bancários, caso de "fraudes mais comuns", "dicas de segurança" e o espaço para manifestação "Você acha que foi vítima de fraude?". Ainda dentro deste espaço, há uma espécie de jogo interativo ("Faça o teste") em que o usuário pode responder algumas questões a fim de saber se faz uso de atitudes seguras ou no sentido de prevenir danos a si mesmo.

"Veja as fraudes mais comuns" é um *link* que explica o que é uma fraude na internet. O mesmo texto apresenta em seguida 'dicas' para agir quando potenciais

[4] *Site* do banco Bradesco. Disponível em: http://www.bradesco.com.br/.
[5] *Site* do banco Bradesco. Disponível em: http://www.bancodoplaneta.com.br/site.
[6] ValueTheWebsite.com. Disponível em http://valuethewebsite.com.

fraudadores podem instalar programas espiões, *cookies*, vírus, utilizando artimanhas diversas. O texto alerta para a forma como a tela se apresenta ou para padrões suspeitos.

- Dicas de Segurança

O campo "Dicas de Segurança" traz o *link* "Saiba mais", que remete ao texto intitulado "Exemplos de fraudes", dando destaque ao vírus "Cavalo de Tróia". As dicas também fornecem informações sobre formas de "infecção", retirada do vírus, captura e dá exemplos de telas falsas já identificadas, terminando com recomendações para evitar tais problemas.

A *home page* do banco Bradesco (http://www.bradesco.com.br/), tendo em vista o conteúdo de interesse da pesquisa, registra a presença dos seguintes campos: Segurança da informação e Segurança.

- Segurança da informação

Ao se acessar o *link* "Segurança da Informação" surge uma janela fixa que acompanhará todos os acessos aos itens mostrados, em que o conteúdo simula uma sinalização de trânsito. Essa janela tem o título de Segurança e mostra os subitens: Cuidado!; Pare; Atenção; e Siga. No item "Cuidado!" menciona-se que "Pode ter gente de olho na sua tranquilidade", mostrando um cartão de senha criptografada sendo segurado pelos dedos de uma pessoa.

O conteúdo do *link* "Segurança da Informação" possui os espaços "O que é", "Processos", "Organização", "Política". Mostra também o espaço "Como usar com segurança", "pessoa física", além de diversos sub-campos em que cabe destaque ao "Usando o Bradesco internet *Banking*", pois mostra procedimento de prevenção no uso do *website* do Bradesco, reportando a recomendações da Federação Brasileira dos Bancos (FEBRABAN, 2011). No campo "e-mails Bradesco" há os sub-campos "Política Bradesco para Envio de E-mail" e "E-mails Falsos". No sub-campo "E-mails Falsos" há diversos *templates* de telas que mostram *e-mails* falsos e páginas "*fakes*".

- Segurança.

Nesse campo há um símbolo de cadeado acompanhando o título "Segurança", campo este que abriga dois sub-campos: "Conheça o *Site* Bradesco Segurança" e "*E-mails* falsos? Envie para evidencia@bradesco.com.br".

O mesmo campo oferece ainda o que denomina por “Outras dicas deste assunto”, ou seja: 1. Dicas gerais de utilização, 2. Cuidados com a senha, 3. Confira alguns cuidados e dicas ao abrir mensagens de *e-mail*, 4. Transações financeiras e Compras, 5. Instale e use um Firewall pessoal, 6. Vírus: Fique Alerta!, 7. “Cavalos de troia”, 8. Tela Falsa.

A *home page* do Banco do Brasil (www.bb.com.br), no que se refere ao conteúdo de interesse da pesquisa, exibe um único campo de segurança com o item “Dicas de Segurança”.

O *link* “Dicas de Segurança” remete a dois textos. Um texto intitulado “Módulo de Segurança” apresenta os recursos que o Banco do Brasil oferece aos usuários em termos de segurança de acesso. Destaca que o Módulo de Segurança é um sistema de proteção que atua no computador contra ataques de programas maliciosos durante a execução de transações na internet”. O outro texto tem o título “Cadastramento de Senhas” em que as informações são focadas nas etapas para se consolidar o cadastramento da senha com segurança.

3.2 Pesquisa de Opinião com Usuários dos Bancos

O objetivo da pesquisa foi colher indicadores opinativos de usuários dos bancos Itaú, Bradesco e Banco do Brasil acerca de questões ligadas à segurança na informação bancária, notadamente quanto a aspectos do *net banking*.

A enquete de caráter qualitativo e não amostral se refere a cidades situadas na região da Grande São Paulo no período de março a abril de 2011. Foram considerados dois públicos distintos: a) Clientes frequentadores das agências do banco Bradesco (Carapicuíba), Itaú (Barueri/Alphaville) e Banco do Brasil (Itapevi), ou seja, três agências bancárias, totalizando 30 clientes que responderam totalmente o questionário; b) Os 900 alunos de graduação e 150 alunos de pós-graduação que cursavam os cursos de administração da Universidade Paulista, campus Alphaville (Santana do Parnaíba-SP); em função de fatores restritivos (desistência/ausência na Universidade, transferência de curso, não usuários dos bancos selecionados) o total de respondentes resultou em 100 alunos de graduação e de pós-graduação.

Dessa forma, os dados da enquete para investigar aspectos ligados à prevenção de danos ao consumidor no uso de sistemas virtuais foram obtidos da aplicação de 130 questionários.

As questões e proposições foram formuladas a partir do texto “Segurança no uso da internet” elaborado pela Federação Brasileira dos Bancos (FEBRABAN, 2011), além do modelo teórico sobre o assunto na obra de Molina, Martin-Consuegra e Esteban (2007). As questões e proposições foram validadas por três professores doutores na área de informação e administração e avaliadas por pré-teste aplicados a seis correntistas e usuários de *internet banking*. O questionário conteve questões relativas ao perfil do respondente, além das proposições (frases afirmações) que compuseram os quesitos opinativos do respondente.

Do total de 130 respondentes, foram obtidos 44 usuários do Bradesco, 42 do Itaú e 44 do Banco do Brasil. Quanto ao gênero, 69 foram do gênero feminino e 61 do masculino. A idade média dos respondentes foi de 39,95 anos. Considerando o gênero, não se registrou diferenças significativas entre as faixas etárias. A renda mensal dos respondentes contemplou significativamente as faixas de renda de até R$ 5.000,00. A escolaridade declarada pelos respondentes correspondeu, em sua maior parte, ao nível Médio (34,6)%, seguido de Graduação (31,5%).

Na realização de transações financeiras pela internet e conhecimento dos riscos, a maioria mencionou as ações que deve fazer para ter segurança na internet, ou seja, consideram que cabe ao usuário lidar com essa questão. Ficaram atrás procedimentos como utilizar antivírus do banco e medidas de proteção que o banco oferece (caso de *softwares*).

Os resultados (quadro 1) também mostraram que sistemas com base na informação (confirmação de código via cartão) podem aumentar a sensação de segurança do usuário. Cabe destaque ao comportamento preventivo do usuário em não acessar o *net banking* em locais potencialmente perigosos, caso de *lan houses* e cibercafés, além de utilizar seu equipamento pessoal para acessar o *site* do banco. O consumidor declara utilizar costumeiramente o *site* do banco com facilidade, acesso esse inclusive para pagamento de contas, o que demanda atitudes de atenção quanto a fraudes potenciais, ações essas que os clientes tentam compatibilizar, em certa medida, com o uso de antivírus e troca de senha com frequência.

Quadro 1 - Quesitos com concordância superior a 70% dos respondentes

1.00	Ao término de uma operação, para confirmar, uso um código que está no meu Cartão de Segurança que mantenho sempre bem protegido
0.87	Eu não acesso o Banco em Cybercafés, Lan Houses ou similares
0.87	Consigo facilmente navegar no *site* do meu Banco
0.83	Costumeiramente acesso o *site* do meu Banco quando estou em casa
0.82	Mantenho meu antivírus sempre atualizado
0.82	Valorizo muito o fato de o *site* estar disponível quando acesso minha conta
0.80	Ao acessar o *site* do meu Banco estou ciente dos riscos que corro
0.80	Pago contas via Internet com frequência
0.75	Periodicamente observo se os débitos automáticos são legítimos
0.74	Eu só utilizo equipamento pessoal para acessar o *site* do meu Banco
0.73	Acesso a minha conta com poucos cliques
0.72	Acredito que o Banco me estimula a usar o Internet *Banking* quando há longas filas na Agência
0.71	Eu troco a minha senha do Internet *Banking* periodicamente

Fonte: Elaborado pelos autores

Os respondentes (quadro 2) apontaram desconhecer pessoas que já sofreram danos com o uso do *net banking*, mas alegam ter sofrido prejuízos com o uso do *internet banking*. O consumidor declara não ler usualmente o conteúdo do *site*, e não tem a iniciativa de contatar o atendimento em caso de dúvida. Aponta ser seu provedor confiável, mas se descuida na manutenção do antivírus sempre ativado.

Quadro 2- Quesitos com discordância superior a 80% dos respondentes

0.92	Conheço pessoalmente pessoas que já sofreram danos com uso do Internet *Banking*
0.90	Leio usualmente o conteúdo disponível no *site* do meu banco
0.86	Se algum procedimento me trouxer dúvida eu entro em contato com a central de atendimento do meu Banco
0.85	Mantenho meu antivírus sempre ativado
0.85	Meu provedor de Internet é confiável
0.83	Eu próprio já tive prejuízos com o uso do Internet *Banking*

Fonte: Elaborado pelos autores

4 CONSIDERAÇÕES FINAIS

O propósito desta pesquisa foi analisar a comunicação bancária voltada para a prevenção de danos quando do uso de seus *websites* pelos consumidores.

Com o evento das novas tecnologias da comunicação, em especial os serviços mediatizados pela internet, relacões comerciais assumiram novas configurações, caso do contexto mercadológico envolvendo os bancos e seus clientes.

Estes últimos, em boa parte, mostram-se integrados à nova mídia, fazendo uso frequente dela para diversos fins, inclusive para aquisição de serviços e informação perante os bancos. Por sua vez, as instituições bancárias vêem na internet uma realidade que incrementa seus negócios e com potencial para projetar positivamente sua imagem num mercado competitivo.

O referencial bibliográfico, os modelos teóricos (CHANG, 2008; KINGSTON; SCHAFER; VANDENBERGHE, 2004; GAVISH; TUCCI, 2006), a análise dos *websites* dos bancos pesquisados – Banco do Brasil, Itaú e Bradesco - e a pesquisa de opinião com usuários desses mesmos bancos mostraram que o processo de comunicação protagonizado pelos bancos e consumidores apresenta inovações importantes com a mediação da internet tendo em vista a prevenção de danos ao consumidor.

A investigação do objeto de estudo proposto evidenciou a preocupação dos bancos no sentido de transmitir segurança aos seus usuários no uso de sistemas virtuais, oferecento aos consumidores consistente informação a respeito dos riscos ao acessar os serviços via *net banking*.

Os três maiores bancos brasileiros tiveram seus *websites* descritos e todos revelaram campos dedicados à prevenção de danos aos consumidor. O conteúdo desses campos situados na *home page* e *links* a ela associados relacionam-se a informações quanto às peculiaridades do uso da internet, e-mails e uso de cartões bancários na rede. Encontram-se também dicas e até games para o internauta se familiarizar com o problema que tem causado prejuízos aos bancos e clientes.

No *website* do banco Itaú foi encontrado um espaço significativo para a prevenção de fraudes no *internet banking*, caso de campos que proporcionam formas de contatos para o internauta se informar, reclamar e esclarecer dúvidas sobre uso e acesso a dados bancários; há também uma espécie de jogo interativo

em que o usuário pode responder algumas questões a fim de saber se faz uso de atitudes seguras ou no sentido de prevenir danos a si mesmo.

O Bradesco oferece o *link* “Segurança da Informação” como uma janela fixa que acompanha todos os acessos aos itens do campo, janela essa cujo conteúdo simula uma sinalização de trânsito:

O Banco do Brasil apresenta o Módulo de Segurança, sistema de proteção que atua no computador do usuário contra ataques de programas maliciosos durante a execução de transações na internet.

A descrição dos *websites* mostrou conteúdos redundantes para segurança e prevenção de danos no uso da internet, algo que os respondentes da pesquisa de opinião também apresentaram como positivo.

A enquete com consumidores dos bancos ofereceu a visão destes quanto às questões ligadas a segurança e prevenção de danos relacionados ao *net banking*.

Dentre as iniciativas próprias para lidar com esse problema destacam-se as várias ações que o cliente deve fazer para ter segurança na internet, caso da utilização de antivírus e trocar de senha frequentemente, porém se descuida em manter o antivírus sempre ativado, algo que dá margem a fraudes.

A maioria tenta acessar os serviços bancários pela internet a partir de locais seguros, o que mostra uma adaptação do consumidor aos riscos oferecidos pela rede e corroborados pelo referencial teórico desse trabalho.

Os respondentes, em sua grande maioria, apontaram desconhecer pessoas que já sofreram danos com o uso do *net banking*, o que contraria o cenário apontado por reportagens e repercussão na mídia sobre a extensão desse problema; porém esse menor grau de conhecimento talvez se refira apenas a contatos pessoais, pois ele mesmo admite ter tido prejuízos com o uso o *net banking*.

Os resultados encontrados não podem ser generalizados devido ao limite de instituições bancárias, número de respondentes e amostra do material dos *websites* analisados, servindo o presente estudo como degrau para que outros trabalhos possam aprofundar o objeto de estudo apresentado a fim de dimensionar com maior amplitude e representatividade a gestão da prevenção de danos ao consumidor no contexto do *net banking*.

REFERÊNCIAS

BANCO CENTRAL DO BRASIL. **Ranking de instituições mais reclamadas**. Disponível em: <http://www.bcb.gov.br/?RED1-RANKING>. Acesso em: 4 out. 2010.

BANCO CENTRAL DO BRASIL. **50 maiores bancos e o consolidado do Sistema Financeiro Nacional.** Disponível em: <http://www4.bcb.gov.br/fis/TOP50/port/Top50P.asp>. Acesso em: 15 abr. 2011.

CHANG, Joshua J.S. An analysis of advance fee fraud on the internet. **Journal of Financial Crime**, Cambridge, v. 15, n. 1, p. 71-81, 2008.

CHEN, Stephen. Corporate responsibilities in internet- Enabled Social Networks. **Journal of Business Ethics,** Dordrecht, n. 90, p. 523-536, 2009.

FEDERAÇÃO BRASILEIRA DE BSNCOS - FEBRABAN. **Segurança no uso da internet**. Disponível em: <http://www.febraban.org.br/Arquivo/Servicos/Dicasclientes/dicas7.asp>. Acesso em: 2 mar. 2011.

FLETCHER, Nigel. Challenges for regulating financial fraud in cyberspace. **Journal of Financial Crime**, Cambridge, v. 14, n. 2, p. 190-207, 2007.

GAVISH, Bezalel; TUCCI, Christopher L. Fraudulent auctions on the internet. **Electronic Commerce Research***,* New York, n. 6, p. 127–140, 2006.

HITE, Robert E.; BELLIZZI, Joseph A.; FRASER, Cynthia. A content analysis of ethical policy statements regarding marketing activities. **Journal of Business Ethics,** Dordrecht, v.7, n. 10, p. 771-776, out. 1988.

KINGSTON, John; SCHAFER, Burkhard; VANDENBERGHE, Wim. Towards a financial fraud ontology: a legal modelling approach. **Artificial Intelligence and Law**, Edinburgh, n. 12, p. 419-446, 2004.

LÉVY, Pierre. **Cibercultura.** São Paulo: Ed. 34, 1999.

LIMA, Vinício A. **Mídia***:* teoria e política. São Paulo: Fundação Perseu Abramo, 2000.

MOLINA, Arturo; MARTIN-CONSUEGRA, David; ESTEBAN Águeda. Relational benefits and customer satisfaction in retail banking. **International Journal of Bank Marketing**, Bradford, v. 25, n. 4, p.253-271, 2007.

NAÍM, Moisés. **Ilícito**: o ataque da pirataria, da lavagem de dinheiro e do tráfico à economia global. Rio de Janeiro: Zahar, 2006.

OLIVEIRA, Roberto Almeida Campos de. **A internet banking e os hábitos de uso entre os clientes pessoa física***:* atributos e resistências. 2000. Dissertação (Mestrado em Administração) - Universidade Federal do Rio Grande do Sul – UFRGS, Porto Alegre.

REZABAKHSH, Behrang; BORNEMANN, Daniel; HANSEN, Ursula; SCHRADER, Ulf. Consumer Power: A comparison of the old economy and the internet economy. **Journal of Consumer Policy**, Neuwied, n. 29, p. 3-36, 2006.

TAPSCOTT, Don; WILLIAMS, Anthony D. ***Wikinomics***: como a colaboração em massa pode mudar o seu negócio. Rio de Janeiro: Nova Fronteira, 2007.

VARADARAJAN, P. Rajan; YADAV, Manjit S. Marketing Strategy and the internet: An Organizing Framework. **Journal of the Academy of Marketing Science***,* Greenvale, v. 30, n. 4, p. 296-312, 2002.

Title

Communication and preventing damage in the internet use

Abstract

Introduction: The bank communications have done intensive use of new technologies and contents, case of net banking, which creates new possibilities and relationships with the bank customer. He is a consumer who is encouraged to know the services offered by the new channels, to use these attributes, but if he detects restrictions of information or miscommunication, manifests itself in some way. Many consumers are dealing with fraud or damage caused by the virtual access system provided by banks. This context presents innovations in the communication system played by banks and consumers mediated by the internet.
Objective: To describe the bank communication oriented to prevent damage when their websites are used by consumers.
Methodology: It was searched websites of banks Bradesco, Itaú and Banco do Brasil, besides an opinion poll with 130 users of these net banking.
Results: The banks offer specific and non-standardized spaces on their websites to prevent damage to the consumer in using the net banking, as too customers use such services only partially.
Conclusions: The results cannot be generalized, thus this study serves as a step for that the further works might develop the study object presented in order to measure with greater scope and representativeness the management of prevention of damage to the consumer in the net banking context.

Keywords: Communication. Consumer. Preventing damage. Internet. Banks.

Título

La comunicación y la prevención de daños en el uso de internet

Resumen

Introducción: La comunicación bancaria ha venido practicando intenso uso de nuevas tecnologías y contenidos, caso del *net banking*, lo que crea nuevas posibilidades y relaciones con el cliente bancario. Hoy en día, en estos bancos se puede acceder desde casa a través de Internet, con lo que se tiene conveniencia para un número significativo de usuarios. Se trata de un consumidor que se anima a conocer los servicios ofrecidos por los

nuevos canales, para ver estos atributos, pero si detecta restricciones informativas o la falta de comunicación, se manifiesta de alguna manera. Muchos consumidores sufren con fraudes o daños causados por el sistema de acceso virtual de los bancos. Este contexto presenta innovaciones en el sistema de comunicación utilizado por los bancos y los consumidores, mediado por la internet.
Objetivo: Describir la comunicación bancaria orientada para prevenir daños cuando de lo uso de sus *websites* por los consumidores.
Metodología: Para responder a algunas de estas cuestiones, se realizaron búsquedas en los *websites* de los bancos Bradesco, Itaú y Banco do Brasil, y también fue realizada encuesta de opinión con 130 usuarios de estos *net banking*.
Resultados: Los resultados demostraron que los bancos ofrecen campos propios, y no estandarizados, en sus *websites* para la prevención de daño al consumidor, así como los clientes utilizan estos servicios de manera parcial.
Conclusiónes: Los resultados encontrados no se pueden generalizar, no obstante, el presente estudio sirve como escalón para que otros trabajos puedan profundizar el objeto de estudio presentado con el fin de dimensionar con más amplitud y representatividad la gestión de la prevención de daños al consumidor en el contexto del *net banking*.

Palabras claves: Comunicación. Consumo. Prevención de daños. Internet. Bancos.

Recebido em: 27.06.2011
Aceito em: 10.05.2013