USO DO INTERNET BANKING: MÉTODOS DE ACESSO SEGURO

ALESSANDRO WIKANSKI[26]
PATRÍCIA KLINKERFUS DE CAMPOS[27]
VIVIANE RAMALHO DE AZEVEDO[28]
JOSÉ EDUARDO DO COUTO BARBOSA[29]

RESUMO

O Internet Banking é um termo utilizado para descrever operações financeiras realizadas através da internet, de forma mais simples e eficaz, porém considerada menos segura. Nos últimos anos tivemos mudanças consideráveis na maneira como as pessoas e instituições trocam informações. A maioria destas mudanças tem sido proporcionada pelas Tecnologias da Informação, com destaque para o setor financeiro, tendo como importante mecanismo os bancos eletrônicos. Por se tratar de informações sigilosas na web, preocupações com segurança devem estar entre as prioridades do usuário.

PALAVRAS CHAVE: Internet banking, Tecnologia da Informação, Segurança, Métodos.

[26]Graduando do 6° semestre do curso de Tecnologia em Gestão da Tecnologia da Informação da Faculdade de Tecnologia de Bragança Paulista (FATEC Bragança Paulista) – “Jornalista Omair Fagundes de Oliveira”. E-mail: alessandrowik@hotmail.com

[27] Graduação em Análise de Sistemas pela Universidade São Francisco - Itatiba (1992); Pós graduação - Latu Sensu - em Administração de Empresas, com ênfase em Marketing - Universidade São Francisco - Bragança Paulista (2002); Graduação em Licenciatura Plena em Matemática pelo Instituto Educacional Oswaldo Quirino - Faculdades Oswaldo Cruz - São Paulo (2003); Mestrado em Educação pela Universidade São Francisco - Itatiba (2007) e Pós graduação - Latu Sensu - em Designer Instrucional - Universidade Federal de Itajubá (2010). Docente na FATEC de Bragança Paulista e na Faculdade de Ciências Aplicadas de Extrema (FAEX).

[28] Mestre pela Faculdade de Engenharia Elétrica e de Computação da UNICAMP na área de Automação (2015), Especialista em Design Instrucional pela UNIFEI (2011), Graduada em Análise de Sistemas pela Pontifícia Universidade Católica de Campinas (2000). Docente da da Faculdade de Tecnologia de Bragança Paulista (FATEC Bragança Paulista) – “Jornalista Omair Fagundes de Oliveira”.

[29] Mestre pela Universidade Federal de Juiz de Fora. Coordenador do NUPAC e Docente na Faculdade de Ciências Sociais Aplicadas de Extrema (FAEX). E-mail: joseduardoo@yahoo.com.br

USE OF THE INTERNET BANKING: METHODS OF SAFE ACCESS

ABSTRACT

Internet Banking is a term used to describe paragraph financial operations carried out through the internet, so more simple and effective, however considered Less safe. In the last year we had significant changes in the way as people and institutions exchange information. Most of these changes has been provided through information technology, especially pair the financial sector, tendon how important so banks electronics engine. Because it is sensitive information on the web, with security concerns should being among the priorities as user.

KEYWORDS: Internet banking, Information Technology, Security, Methods.

INTRODUÇÃO

O acelerado crescimento dos canais de comunicação e a necessidade de atender diversos tipos de clientes têm impulsionado as instituições financeiras a estimular o uso do *Internet Banking*. Os próprios clientes estão identificando cada vez mais, o potencial da Internet para suas atividades financeiras, sempre buscando comodidade e economia de tempo.

De acordo com dados do IBOPE (2010), desde o surgimento da internet comercial, entre os conteúdos que mais cresceram, estão inclusos, o comércio eletrônico ou *e-commerce* e o internet banking ou *e-banking*, que já contam com 7,4 milhões e 5,3 milhões de usuários residenciais, respectivamente, em março de 2006. Porém, os mesmos dados indicavam que houve uma diminuição no número de usuários de sites de bancos desde o fim de 2003, em comparação aos usuários de e-commerce.

“As mudanças organizacionais e o suporte das novas tecnologias estão provocando mudanças significativas no uso comercial da comunicação eletrônica em geral, em atividades de comércio eletrônico, e-business e demais transações financeiras e de comunicação. As aplicações abertas e com conectividade irrestrita, utilizando a grande rede como plataformas tecnológicas são os principais direcionadores das atuais tecnologias e soluções de comunicação. Navegadores, editores eletrônicos, servidores de Internet e Intranets, sistemas de gestão de redes e demais produtos que trafegam sob o protocolo TCP/IP, assim como os dispositivos de segurança que devem estabelecer critérios de segurança para esta infinidade de acessos, são apenas alguns exemplos desta realidade” (O’BRIEN, 2004, p.150).

Em uma reportagem feita pelo jornal O Globo (2005), um estudo realizado entre 14 países, colocou o Brasil como o país que menos atualiza seus programas de defesa contra hackers e o que mais sofre chamados ataques de negação de serviço (DDoS, na sigla em inglês) - aqueles em que invasores sobrecarregam um sistema para tirá-

lo do ar. Ainda de acordo com a pesquisa, mais da metade dos entrevistados disse que sofrem constantes ataques de negação de serviço e roubo de dados.

"Os serviços financeiros têm um componente de intangibilidade que faz com que a apreciação do serviço dependa muito da relação que se estabelece com o cliente". (GALLEGO, 1998). Pode-se dizer que a grande vantagem que os bancos devem explorar em relação aos seus concorrentes é a confiança, através de recursos de segurança e relacionamento.

Segundo Diniz (1999, p.79), "as características básicas da *Web* podem contribuir para incrementar o relacionamento dos bancos com seus clientes, com destaque a interatividade, resposta imediata, conectividade, interoperabilidade, multimídia e facilidade de uso." No entanto, todas devem estar associadas a processos seguros para promover maiores níveis de atratividade.

O **objetivo** deste artigo é apresentar métodos de segurança relativos às transações realizadas nos canais de atendimento bancários por meio do *Internet Banking*. Descrevendo conceitos, técnicas, objetivos, vantagens e desvantagens dos principais mecanismos de segurança em *Internet Banking, que podem ser* usados pelos usuários e aqueles que as principais instituições bancárias utilizam para proteger o sistema.

A **relevância** deste artigo é demonstrar que existem formas de se utilizar o Internet Banking, sem que seus dados sofram algum tipo de ameaça, principalmente para o usuário comum, que possivelmente possua dificuldades em saber se está utilizando o sistema de forma segura.

Em termos **metodológicos**, a pesquisa é descritiva exploratória, considerada como aquela que expõe as características de uma situação, um grupo ou um indivíduo específico, ou seja, aquela que estabelece critérios, métodos e técnicas para a elaboração de uma pesquisa. Quanto à forma de abordagem do problema, esta é uma pesquisa qualitativa, no qual serão utilizados artigos, teses, dissertações, sites conceituados, entre outros, como base de pesquisa.

2. REFERENCIAL TEÓRICO

À medida que ocorreu o surgimento da moeda no período das grandes civilizações, o ato de emprestar, tomar emprestado e guardar dinheiro de outros foi algo quase inevitável. Acredita-se que as primeiras operações bancárias da história tenham sido desenvolvidas na civilização fenícia. Entretanto, o nome banco foi concebido pelos romanos.

De acordo com o Professor Bruno Ferreira (2014), para facilitar a troca entre as diferentes moedas, surgiram os banqueiros, pessoas que ficavam em bancos trocando moedas e cobrando juros para tais serviços, oferecendo também o controle de tais transações, através de documentos, que mostravam o quanto tinham emprestado e a data em que teriam que devolver o dinheiro.

Ainda de acordo com o professor Ferreira (2014), com a chegada do mercantilismo e das grandes navegações os banqueiros e a burguesia ganharam força, e a partir desse momento se espalharam pelo o mundo, tornando-se a classe que mais enriquece, ganhando enormes lucros e promovendo o capitalismo. Com o fim da modernidade, os bancos e burgueses que dominavam a economia, passaram a influenciar o mundo moderno, financiando projetos. Com o surgimento da América e da industrialização dos Estados Unidos surgiu à bolsa de valores de Nova York e através dela que o mundo tem a sua primeira crise mundial.

A bolsa de valores é um mercado onde se negociam ações, contratos futuros e derivativos de companhias de capital aberto, públicas e privadas. Entre as principais funções da bolsa de valores estão inclusos, o levantamento do capital para negócios, mobilizar e criar oportunidades em investimentos para o pequeno investidor e facilitar o crescimento das companhias, criando um ambiente confiável e adequado à realização de negócios de valores imobiliários.

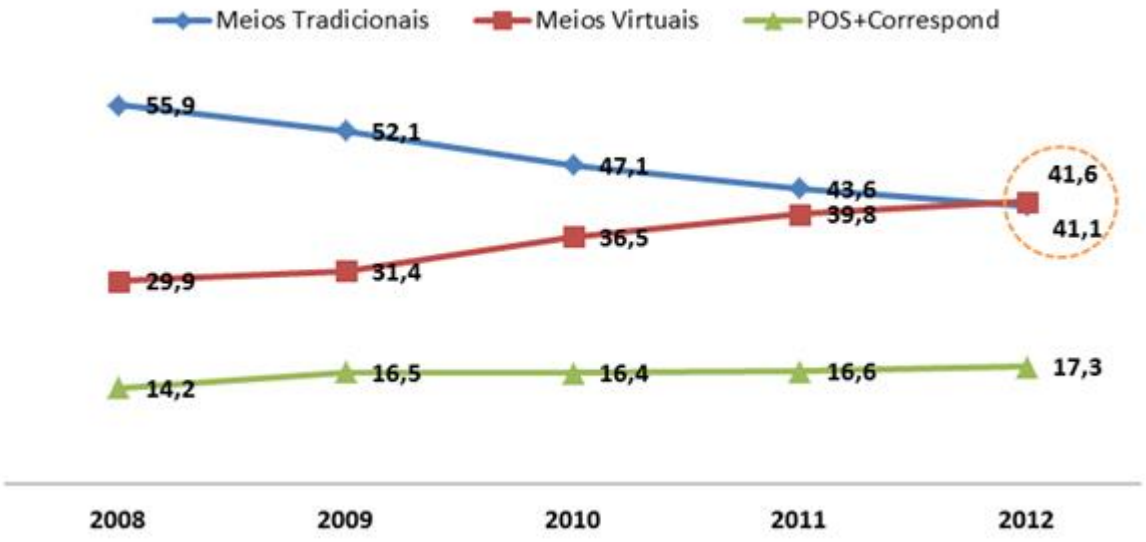
Com o fim do socialismo da URSS em 1991 e a queda do muro de Berlim, o mundo passou a ser predominantemente capitalista, o mercado financeiro foi

integrado e passou a estar sob o comando de apenas uma única potência, os Estados Unidos.

O Internet banking, isto é, a utilização da Internet para oferta de serviços bancários, é a principal inovação tecnológica incorporada aos serviços bancários na última década. Associado à demanda dos clientes por maior conveniência e ao interesse dos bancos por economia, precisão e automação, o Internet banking, que no início era considerado apenas mais um canal para a distribuição de serviços bancários, "passou a estar no centro das discussões sobre a evolução e o futuro dos bancos" (DINIZ, 2004, p. 8).

Segundo dados da Febraban (2005), no período de 1998 a 2004 as transações bancárias feitas através da internet tiveram um grande crescimento de aproximadamente 100% ao ano. Esse crescimento é ainda mais significante se relacionado a outros canais: no mesmo período, as transações em caixas eletrônicos cresceram 24% em média ao ano.

Gráfico 1. Canais de Relacionamento com os Bancos, preferidos pelos clientes (%)



Fonte: FENABRAN de Tecnologia Bancária 2012

Mais do que um canal com os clientes, a Internet já aderiu a processos internos, no desenvolvimento de portais corporativos (DINIZ, 2004), por permitir uma coleta de

dados muito mais abundante de clientes e estruturação de metodologias de CRM (Customer Relationship Management) e BI (Business Intelligence) nos bancos.

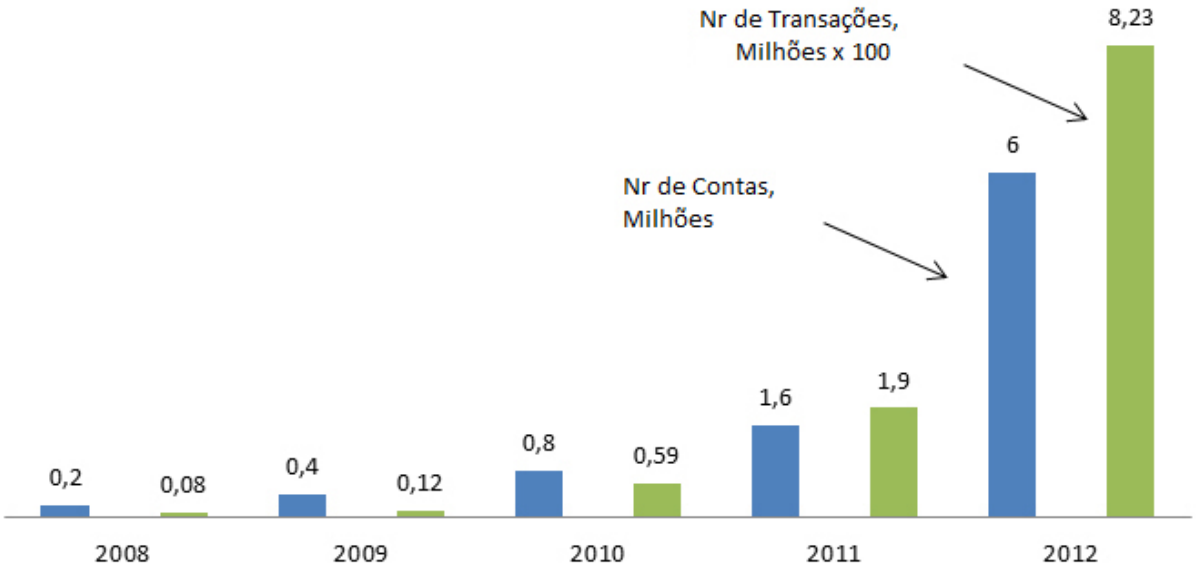
Apesar de toda esta importância, a incorporação desta tecnologia no ambiente bancário ainda merece atenção especial, devido a constante mudança de mercado e o surgimento de novas tecnologias. De acordo com Bijker e Law (1992), as tecnologias não evoluem somente sob o ímpeto de uma lógica interna, tecnológica ou científica. Se evoluem, ou mudam, é porque são pressionadas na direção deste novo formato.

Os Bancos viram na Internet um meio rápido e também seguro de aumentar seus negócios, criando o Internet Banking. Cartolo (2013) explica que o surgimento do Internet Banking trouxe diversos pontos positivos para os bancos, havendo uma economia de recursos na construção de agências físicas, salário e treinamento de funcionários, até a superação física das agências e dos ATMs (caixas eletrônicos), onde hoje uma pessoa pode acessar sua conta bancária, e fazer transações em qualquer lugar.

A FEBRABAN (2012) apontou que as transações feitas pela Internet Banking representam cerca 24% das operações do setor em 2011. Em 2002 eram 9 milhões de contas correntes com acesso a Internet Banking, hoje já são mais 42 milhões, se igualando a países desenvolvidos, como os EUA, Alemanha e Reino Unido.

A evolução bancária é alavancada pelo crescimento de contas correntes e poupanças. Uma nova pesquisa da FEBRABAN (2013), informa que a crescente concentração de recursos financeiros tem sido alavancada por questões econômicas, além do acesso aos meios digitais como Internet Banking e Mobile Banking, que estão mais acessíveis à toda população.

Gráfico 2. Evolução do Mobile Banking no Brasil



Fonte: FENABRAN de Tecnologia Bancária 2012

A popularização dos smartphones, a conveniência para o cliente e os investimentos dos bancos em segurança eletrônica mostra que o mobile só tende a ganhar importância, diz Gustavo Fosse, diretor setorial de tecnologia e automação bancária da FEBRABAN.

Ainda de acordo com Cartolo (2013), o banco tem investido alto no setor de segurança, pois há muitos casos de dados, programas e contas bancárias violadas com a finalidade de infringir correntistas e bancos.

Em 2011, de acordo com o site G1 , os Bancos nacionais tiveram um prejuízo de R$1,5 bilhões com fraudes eletrônicas, quase 60% maior que no ano anterior. Quando se trata de qualquer forma de interação digital, seja por Internet Banking ou compras virtuais, no mundo o prejuízo chega a US$ 338 bilhões revela a revista Exame assinada por Flavio Takemoto.

Segundo o relatório da Symantec , em 2011, pelo menos 431 milhões de usuários de computadores foram de alguma forma prejudicados. A FEBRABAN registrou que as 16 principais Instituições Financeiras do Brasil, ou seja, 90% dos ativos nacionais, investiram cerca US$ 9 bilhões em tecnologia em 2011,

crescimento de 27% em relação ao ano de 2009 e muito superior aos US$ 2,7 bilhões investidos em 1992, quando ainda estavam no processo de incorporação dessa tecnologia.

No entanto, Affonso Júnior esclarece que não basta os bancos oferecerem recursos de proteção, há de se ensinar o usuário o básico para se precaver contra fraudes, pois “a segurança sem um treinamento não basta” (AFFONSO JÚNIOR, Carlos Morais, op. cit., p. 4)

Assim como qualquer outra transação financeira, o uso do internet banking requer cuidados por parte dos usuários. Mas se as pessoas tomarem as medidas necessárias, dificilmente, elas serão vítimas de cibercriminosos, destaca Camilo Di Jorge, gerente nacional da ESET Brasil .

A aplicação de recursos dos bancos em segurança deve ser levada em consideração, porém, a aptidão de seus clientes em utilizar de forma segura o internet banking também deve ser considerada, diz Affonso Júnior.

3. ANÁLISE DE RESULTADOS

Após o surgimento do canal de atendimento bancário, proporcionando serviços via internet a seus clientes, os bancos tiveram que aderir a medidas de combate ao roubo de informações e garantir que as transações ocorressem de forma segura.

Caso um intruso consiga fraudar o sistema e ter acesso às informações bancárias de um cliente, ele terá a possibilidade de movimentar quantias de dinheiro, passando, também, a ter acesso a informações financeiras e pessoais, o que pode colocar em risco a segurança destes clientes.

Devido à enorme quantidade de problemas, que o roubo de informações pode gerar, é de grande importância implementar técnicas de segurança de dados nos sistemas de informação para Internet Banking.

Para evitar prejuízos, os bancos veem se empenhando em educar seus clientes e estão cada vez mais implementando técnicas e dispositivos de segurança que são disponibilizados aos mesmos.

Muitas são as tecnologias que foram desenvolvidas e disponibilizadas aos clientes. Uma grande vantagem para os bancos é que as tecnologias disponibilizadas normalmente são muito bem aceitas, os clientes sentem-se mais seguros e por consequência utilizam com maior frequência ao Internet Banking.

Os bancos disponibilizam diversas técnicas para segurança do Internet Banking e estão constantemente investindo em tecnologia, entretanto isso não significa que devemos abandonar alguns procedimentos simples para garantir na sua maior segurança ao acessar o Internet Banking. Nos próximos tópicos serão descritas as principais técnicas, apontando seu objetivo, benefícios e malefícios ao utilizá-las.

O teclado virtual é um software que permite entrada de texto em programas de computador de maneira alternativa ao teclado convencional, trata-se de uma técnica para adição de senhas em operações financeiras, onde o usuário clica com o mouse sobre um teclado disponibilizado no site, onde a imagem clicada é convertida para um caractere de texto, que é escrito na tela do editor.

Tem como finalidade evitar que programas espiões, ou keyloggers (programas que capturam o que os usuários digitam), apoderem-se de dados confidenciais, como senhas, e transferi-los para Crackers, (termo usado para designar quem pratica a quebra de um sistema de segurança) ou (cracking), de forma ilegal ou sem ética. O teclado virtual dificulta a captura dos dados digitados antes de serem criptografadas pelo navegador de Internet.

Por outro lado, os Crackers podem utilizar programas que capturam a imagem da tela do computador, para terem acesso às informações utilizadas no teclado virtual. Outra desvantagem a utilização do teclado virtual, permite que outras pessoas observem aquilo que o usuário está clicando.

O encerramento de sessão trata-se de uma técnica, em que a interrupção do acesso ao Internet Banking de forma automática caso haja ociosidade por um tempo determinado.

Sua principal função é evitar que após a ausência do usuário, outra pessoa realize operações quando este não faz o encerramento do acesso. Pode-se apresentar como desvantagem, autenticações repetitivas, caso o tempo de encerramento de sessão seja pequeno.

O bloqueio de senha por tentativas de autenticação, tem como meta principal impossibilitar que um possível invasor acesse informações de terceiros, após fazer várias tentativas de autenticações para testar combinações, ou seja, o bloqueio ocorre, quando alguém erra um determinado número de vezes uma senha. Sua desvantagem ocorre caso o usuário tenha esquecido ou confundido sua senha e tente inserir combinações erradas, tendo como consequência o bloqueio de sua senha.

O plugin trata-se de um programa vinculado ao navegador, tem como função aumentar sua função de segurança na utilização do Internet Banking, servindo como complemento e evitando que softwares instalados no computador roubem dados. O plugin também deve ser compatível com versão atual do navegador, como alguns navegadores têm atualizações de versão constantemente, o plugin pode ficar incompatível com o navegador até que surja uma adequação para ele.

A identificação do computador é um método de segurança que identifica os computadores, validando o acesso ao Internet Banking apenas a computadores cadastrados pelo usuário. De acordo com Sálvio Santiago Brandão e Iremar Nunes De Lima (2012), para fazer o cadastro do computador, o usuário faz uma solicitação, geralmente através de algum meio de comunicação que não seja a internet (telefone ou presencialmente), para receber um código de autorização, normalmente composto por caracteres alfanuméricos e com prazo de validade. Após acessar o Internet Banking o usuário informa o código que recebeu para que seja feita a identificação e cadastro da máquina, que passa a ser autorizada a realizar transações. Geralmente

os bancos oferecem dois tipos de cadastros, o temporário e o definitivo, o que ajuda a reforçar a segurança.

No cadastro temporário o computador fica autorizado por um tempo determinado, que pode ser de dias ou horas. Tem como objetivo ser usado para cadastro de um computador que não será habitualmente utilizado pelo usuário, como por exemplo, computadores de hotéis durante o período de viagem. O outro tipo de cadastro é o definitivo e nele a máquina fica autorizada ao acesso por um tempo indeterminado. Tem como objetivo ser usado para cadastro de um computador que será frequentemente utilizado pelo usuário.

De acordo com o site do banco Santander, o cartão de senhas foi criado para aumentar a segurança na realização de transações financeiras pelo Internet Banking, contendo em seu verso 50 códigos numéricos de 4 algarismos, onde cada usuário deverá ter um cartão único.

Sálvio Santiago Brandão e Iremar Nunes De Lima (2012), descrevem o funcionamento da seguinte forma, quando um usuário for efetivar uma transação, será solicitado que ele informe a senha de uma determinada posição do cartão. O sistema então verifica se a senha informada está correta e libera a transação.

Token é um dispositivo físico, de segurança, que são utilizados para provar sua identidade eletrônica. O token é utilizado como complemento ou em substituição de uma senha. De acordo com Sálvio Santiago Brandão e Iremar Nunes De Lima (2012), nas versões sem conexão física com o computador ele é semelhante a um chaveiro com um visor para exibir os números gerados aleatoriamente. Nas versões com conexão via porta USB é semelhante a um pen drive possuindo certificados digitais. Ambos são utilizados como complementos de segurança nas transações de Internet Banking. Já nas versões sem conexão física com computadores, os tokens geram senhas aleatoriamente, toda vez que é ativado de acordo com uma fração de tempo determinada previamente, geralmente de alguns segundos, através de um clique do botão. A cada transação é solicitado ao usuário que ele informe uma

senha gerada pelo dispositivo e essa senha somente é válida por alguns segundos. O sistema então verifica se aquela senha poderia ser gerada pelo token do usuário.

Uma tecnologia semelhante ao token é a chave temporal enviada via celular, esta tecnologia tem como objetivo gerar senhas aleatórias, com o objetivo de confirmar transações bancárias.

> Nas transações financeiras é solicitado que o usuário informe uma senha. Para gerar essa senha o usuário deve acessar o aplicativo instalado no celular, informar a senha de acesso do aplicativo e obter a chave necessária para completar a transação. A instalação do aplicativo é feita após download no site onde está disponibilizado e a configuração é feita automaticamente, sendo a conexão com a internet somente necessária neste momento (Sálvio Santiago Brandão e Iremar Nunes De Lima, 2012).

O SMS (serviço de mensagens curtas) é um serviço muito usado para troca de mensagens de textos breves que podem ser enviadas ou recebidas através de um aparelho celular.

Os bancos têm utilizado este serviço como um complemento de segurança para envio de senhas necessárias para efetivação de transações em Internet Banking, para utilizar o serviço o usuário deve cadastrar e autorizar os celulares em que deseja receber o SMS. Feito isso, ao realizar uma operação no Internet Banking, o sistema envia uma mensagem contendo um código de segurança ao aparelho celular que o cliente informou, podendo substituir o serviço de token.

Sálvio Santiago Brandão e Iremar Nunes De Lima (2012), citam como vantagem, a possibilidade de qualquer aparelho celular poder receber mensagens via SMS. O problema das mensagens via SMS é que seu envio depende das operadoras, e cada mensagem tem um custo. Não existe garantia do tempo de entrega, podendo a senha demorar vários segundos ou até minutos para ser recebida. Outra

desvantagem é que mensagens SMS não são criptografadas, facilitando ataques maliciosos.

Antivírus é um software de computador criado para prevenir, detectar e possivelmente eliminar vírus de computador. São programas usados para proteger e prevenir computadores e outros aparelhos de códigos, a fim de dar mais segurança ao usuário.

A contaminação por vírus pode acontecer de diversas formas, através da troca de mensagens instantâneas, com desconhecidos ou com um computador infectado, troca de e-mails com links ou arquivos maliciosos ou originários de computadores infectados ou que possuam código malicioso, visita a sites de conteúdo duvidoso, ou que sejam foco de disseminação de vírus, download de arquivos infectados ou contaminados, provenientes de sites ou através de programas de compartilhamento, instalação de cartões de memória ou pen drives contaminados no computador, ocorrendo geralmente quando o cartão de memória ou pen drive é utilizado em computadores com grande número de usuários como em lan houses.

Segundo a Microsoft, é preciso atualizar seu software antivírus regularmente, para que o antivírus instalado seja eficaz, o usuário deve copiar essas vacinas do site do fabricante, de modo a tornar seu sistema imune às novas ameaças. Os downloads de atualização de vacinas costumam ser gratuitos e podem ser feitos automaticamente pelos próprios programas de antivírus.

Firewalls são sistemas que estabelecem regras e filtros de tráfego entre computadores e serviços, como Internet Bankings, por exemplo. São utilizados como defesa contra ameaças externas e são considerados como separadores e analisadores, utilizados para delimitar perímetros e ambientes lógicos, seja numa Intranet, rede local ou até mesmo na Internet (O'REILLY, 1998). Um firewall cria uma barreira entre o computador e a Internet, protegendo-o contra invasões.

Segundo Jonathan D. Machado (2012), aplicações com a função de firewall já são parte integrante de qualquer sistema operacional moderno, garantindo a segurança do seu PC desde o momento em que ele é ligado pela primeira vez. Os

firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino final, outra medida muito usada são os filtros por portas e aplicativos. Com eles, o firewall pode determinar, exatamente, quais programas do seu computador podem ter acesso ao link de internet ou não.

Diversas ameaças são criadas com o intuito de explorar as vulnerabilidades dos sistemas operacionais. Uma forma eficiente de se proteger é atualizando o sistema operacional na mais recente versão disponibilizada pelo fabricante.

O protocolo SSL (Secure Socket Layer) é um servidor com encriptação de dados, para utilização em transações via internet, fornecendo privacidade e integridade entre os dois aplicativos de comunicação. Foi desenvolvido pela Netscape Communicatons, com o objetivo de transferir dados e informações de modo seguro na internet, sendo necessário que o servidor e o cliente apoiem o protocolo.

De acordo com o Prof. Marco Câmara, o SSL providencia autenticação, confidencialidade e integridade dos dados, sendo planejado para autenticar o servidor e opcionalmente o cliente. Como este padrão é aberto, vários desenvolvedores podem aprimorá-lo, inclusive implementar com novas características e funções.

O SSL permite que o usuário se conecte ao site Web e, de forma transparente, estabeleça uma sessão segura que exige intervenção mínima do usuário final. Uma vez que esta conexão é feita, informações, como o número de cartões de crédito, senhas de contas corrente, poderão ser fornecidas sem que outra pessoa possa interceptar os dados, ou seja, de uma maneira segura. De modo pratico o navegador alerta o usuário através de um Certificado SSL, exibindo o ícone de um cadeado ativado no navegador.

Esta segurança é garantida pela encriptação, os usuários que interceptarem a mensagem no caminho, ficam impedidos de acessar o conteúdo da mensagem, já que não conseguem entender o que está sendo transmitido.

O protocolo SET é um conjunto de especificações que facilitam transações através do comércio eletrônico, sendo utilizado para pagamento com cartões de

crédito via internet. Este protocolo permite confidencialidade, autenticação e integridade de dados, entre as partes envolvidas.

O SET assegura que as informações do pagamento serão mantidas seguras e que só poderão ser acessadas pelo destinatário. A especificação precisa garantir que o conteúdo das mensagens não seja alterado durante a comunicação entre o emissor e receptor, descreve Helô Petry.

O SET realiza a autenticação verificando a origem dos dados, aplicando algoritmos de verificação de assinatura digitais. A autenticação tem como objetivo, garantir que todos os dados enviados entre as partes permaneçam sigilosos. Desta forma, o receptor pode validar o emissor pela verificando os dados recebidos.

CONSIDERAÇÕES FINAIS

A maior parte dos métodos de segurança apresentadas neste artigo, são empregadas pelas instituições bancárias que oferecem o internet banking, ou são de fácil obtenção para o usuário. Diversas são aplicadas em simultâneo, destacando-se as que utilizam criptografia operando com certificação digital, por possuírem técnicas mais competentes no combate a fraudes. Há métodos que trabalham em substituição de outras, mesmo assim é incomum que sejam utilizadas individualmente.

Os outros métodos também são satisfatoriamente competentes, porém deve-se ter uma maior atenção ao utilizá-los, eles requerem uma maior atenção do usuário, uma vez que a utilização dependa da instalação pelo usuário ou que descuidos no momento de preenchimento de senhas e dados pessoais acabem permitindo que pessoas com má intenção burlem o sistema.

A partir deste artigo foi possível identificar que o emprego dos serviços de internet banking concedidos pelos bancos estão em constante evolução, atendendo a grande demanda de clientes.

Gostaria de destacar que os investimentos em recursos de segurança no internet banking, trazem uma maior percepção de segurança aos usuários,

possibilitando que novas oportunidades de negócios tanto para os clientes quanto para a instituição financeira, aumentando quantidade de transações e a credibilidade das instituições.

REFERÊNCIAS BIBLIOGRÁFICAS

BREI, Vinícius Andrade; ROSSI, Carlos Alberto Vargas. **Confiança, valor percebido e lealdade em trocas relacionais de serviço:** um estudo com usuários de Internet Banking no Brasil. Curitiba. Disponível em:<http://www.scielo.br/scielo .php?pid=S1415-65552005000200008&script=sci_arttext>. Acesso em 08 Ago. 2014.

CAMARGO, Adriano. **Saiba como evitar riscos no uso do internet banking.** 2012. Disponível em: <http://ultradownloads.com.br/dica/Saiba-como-como-evitar-riscos-no-uso-do-internet-banking/>. Acesso em 08 Ago. 2014.

CARTOLO, Leandro. **Breve comentário histórico sobre a segurança da Internet Banking no Brasil.** 2014. Disponível em: <http://leandrocarloto.jusbrasil.com.br/artigos/111941203/breve-comentario-historico-sobre-a-seguranca-da-internet-banking-no-brasil>. Acesso em: 10 Jan. 2015.

COSTA, Luciano R; OBELHEIRO, Rafael R;FRAGA, Joni S. **Autenticação em Web Banking por Credenciais Biométricas Suportadas pelos Padrões de Serviços Web**. 2007. Florianópolis. Disponível em: <http://gcseg.das.ufsc.br/wssec/pubs/costa07-sbrc-biom-web-banking.pdf>. Acesso em: 15 Ago. 2014.

DAMIANO, André Luís.**As fraudes no Internet Banking e sua evolução para o Social Banking.** São Carlos. Disponível em:<http://www.teses.usp.br/teses/disponiveis/18/18157/tde-12092013-094137/en.php>. Acesso em 07 Ago. 2014.

DINIZ, Eduardo. **Evolução do uso da Web pelos bancos.** 2000. Curitiba. Disponível em: <http://www.scielo.br/scielo.php?pid=S1415-65552000000200003&script=sci_arttext>. Acesso em: 10 Ago. 2014.

DINIZ, Eduardo H; SANTOS, Heloísa Mônaco dos. **Internet Banking**. 2006. Disponível em: <http://rae.fgv.br/sites/rae.fgv.br/files/artigos/gvexec_41-45.pdf>. Acesso em 20 Ago. 2014.

E-CENTRO. **Benefícios e Riscos da Internet Banking:** Desafios da Internet Banking. 2013. Disponível em: <http://centrodeartigos.com/conhecimento/artigo-3852.html> . Acesso em 08 Ago. 2014.

EQUIPE INFO MONEY. **Internet banking:** dicas de segurança para se proteger das fraudes. 2014. São Paulo.Disponível em: <http://www.infomoney.com.br/educacao/guias/noticia/529923/internet-banking-dicas-seguranca-para-proteger-das-fraudes>. Acesso em 10 Ago. 2014.

FERRARI, LuisRafael.**A contribuição do bancário na segurança da informação do cliente usuário do Internet Banking.** 2011. Rio Grande do Sul. Disponível em:**<**http://www.lume.ufrgs.br/handle/10183/77519**>**.Acesso em 09 Ago. 2014.
GALLAO, Rafael Vaz. **Segurança do internet banking no brasil**. 2014. Americana. Disponível em: <http://www.fatec.edu.br/revista/wp-content/uploads/2013/06/Seguran%C3%A7a-do-Internet-Banking-no-Brasil.pdf>. Acesso em: 21 Ago. 2014.

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social.** 5. Ed. São Paulo: Atlas, 1999.

MAGALHÃES, Alexandre Sanches. **E-commerce e e-banking no brasil uma perspectiva do usuário.** 2007. São Paulo. Disponível em: <http://www.teses.usp.br/teses/disponiveis/12/12139/tde-21012008-145601/pt-br.php>. Acesso em: 20 Ago. 2014.

O'BRIEN, James. **Sistemas de informação e as decisões gerenciais na era da Internet.** São Paulo: Saraiva, 2004. Acesso em: 07 Ago. 2014

O GLOBO. **Brasil é um dos países mais vulneráveis a ataques cibernéticos.** 2011. Disponível em: <http://oglobo.globo.com/politica/brasil-um-dos-paises-mais-vulneraveis-ataques-ciberneticos-diz-pesquisa-3060528#ixzz3E2ohWImz> acesso em 20 Set. 2014

REDAÇÃO OLHAR DIGITAL. Dicas de como evitar riscos no uso do internet banking. 2012. Disponível em:<http://olhardigital.uol.com.br/noticia/dicas-de-como-evitar-riscos-no-uso-do-internet-banking/24184 >. Acesso em 07 Ago. 2014.

RIBAS, Sthefanie Taborda. Dicas para utilizar o internet banking com segurança. 2014. Disponível em: <http://blog.comparaonline.com.br/financeiro/cartao-de-credito/2014/05/dicas-para-utilizar-o-internet-banking-com-seguranca/>. Acesso em 10 Ago. 2014.

SOARES, Karla. **Internet banking: dicas de segurança para se proteger das fraudes.** 2014. Disponível em**: <**http://www.techtudo.com.br/noticias/noticia/2014/04/internet-banking-dicas-de-seguranca-para-se-proteger-das-fraudes.html>. Acesso em 09 Ago. 2014