UNIVERSIDADE FEDERAL DO PARANÁ

MICHELE GEREMIAS FERREIRA DA SILVA

PRINCIPAIS FRAUDES DE ENGENHARIA SOCIAL ENVOLVENDO PESSOAS FÍSICAS NO SETOR BANCÁRIO BRASILEIRO

CURITIBA
2018

MICHELE GEREMIAS FERREIRA DA SILVA

PRINCIPAIS FRAUDES DE ENGENHARIA SOCIAL ENVOLVENDO PESSOAS FÍSICAS NO SETOR BANCÁRIO BRASILEIRO

Monografia apresentada ao Departamento de Ciências Contábeis, do Setor de Ciências Sociais Aplicadas, da Universidade Federal do Paraná, como pré-requisito para obtenção do título de Especialista em MBA – Auditoria Integral.

Orientador: Prof. Ms. Antonio César Pitela

CURITIBA

2018

TERMO DE APROVAÇÃO

MICHELE GEREMIAS FERREIRA DA SILVA

PRINCIPAIS FRAUDES DE ENGENHARIA SOCIAL ENVOLVENDO PESSOAS FÍSICAS NO SETOR BANCÁRIO BRASILEIRO

Monografia aprovada como requisito parcial à obtenção do título de Especialista, Curso de Especialização em Auditoria integral, Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná. Universidade Federal do Paraná, pela seguinte banca examinadora:

_____

Prof. Antonio César Pitela

Orientador – Departamento de Ciências Contábeis – UFPR

_____

Prof.

Departamento de

_____

Prof.

Departamento de

_____

Prof.

Departamento de

Curitiba, 30 de junho 2018.

A meu esposo Vilson Rodrigues de Campos, que não mediu esforços para me ajudar nessa etapa tão importante da minha vida.

AGRADECIMENTOS

Ao meu pai, Antonio Teixeira Vissossi, por ser a pessoa que sempre me incentivou a procurar aprimorar todo e qualquer conhecimento.

À Nicole Cristina minha filha, pela compreensão na ausência nos dias de sábados durante meses.

À minha mãe, Claudia Geremias, por ser uma pessoa especial e inspiração em minha busca de conhecimento.

Ao professor Blênio Cezar Severo Peixe, coordenador do curso de pós-graduação MBA em Auditoria Integral da UFPR, pelo apoio e incentivo quanto à conclusão dessa monografia.

Ao professor Antonio César Pitela, professor da UFPR e orientador dessa monografia, pelo total apoio.

“Se o dinheiro for a sua esperança de independência, você jamais a terá. A única segurança verdadeira consiste numa reserva de sabedoria, de experiência e de competência.”

Henry Ford

RESUMO

Apresenta-se neste trabalho qual o motivo da continuidade das fraudes sofridas por clientes pessoas físicas de bancos comerciais, com foco no setor bancário brasileiro, mesmo com toda a tecnologia desenvolvida para esse setor em seus variados canais de atendimento. Verifica-se a diferença entre fraude e erro, suas correlações e implicâncias financeiras, além de detalhar como cada qual é estabelecido dentro do setor estudado. Como o foco é a fraude trabalhando com a tecnologia em desenvolvimento, verifica-se dentre as fraudes o internet banking e mobile banking, estendendo-se a outras práticas como o scam, phishing e pharming, além de ressaltar as punições específicas para esse tipo de operação fraudulenta. Mostra-se como ocorrem os diversos tipos de fraudes, além de detalhar cada operação. Outro destaque é o perfil dos fraudadores e suas vítimas, tentando demonstrar se existe relação entre ambos. E para finalizar são destacados quais os métodos utilizados pelas instituições financeiras brasileiras para minimizar as fraudes contra seus clientes pessoas físicas.

Palavras-chave**:** Instituições Financeiras. Fraudes. Internet Banking. Mobile Banking.

ABSTRACT

It is presented in this paper the reason for the continuation of the frauds suffered by individual clients of commercial banks, focusing on the Brazilian banking sector, even with all the technology developed for this sector in its various service channels. The difference between fraud and error, its correlations and financial implications is verified, besides detailing how each one is established within the sector studied. As the focus is fraud working with the technology in development, internet banking and mobile banking are among the scams, extending to other practices such as scam, phishing and pharming, as well as highlighting specific punishments for this type of fraud. fraudulent operation. It shows how the various types of fraud occur, in addition to detailing each operation. Another highlight is the profile of the fraudsters and their victims, trying to demonstrate if there is a relationship between the two. And finally, the methods used by financial institutions in Brazil to minimize fraud against their individual customers are highlighted.

Key words: Financial Institutions. Frauds. Internet banking. Mobile Banking.

LISTA DE SIGLAS

BACEN	-	Banco Central do Brasil
CEF	-	Caixa Econômica Federal
CMN	-	Conselho Monetário Nacional
DECIC	-	Departamento de Combate a Ilícitos Financeiros
DNS	-	Domain Name System
FEBRABAN	-	Federação Brasileira de Bancos
FTP	-	File Transfer Protocol
HTML	-	HyperText Markup Language
SMTP	-	Simple Mail Transfer Protocol
UFPR	-	Universidade Federal do Paraná

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTO E PROBLEMA

Na antiguidade, anteriormente mesmo ao dinheiro na forma como o conhecemos (cédulas, moedas e outros documentos que acertem a saciedade ao crédito), as operações comerciais aconteciam por meio de escambo, que consiste na troca direta de bens e serviços por outros bens e serviços, em vez de ocorrer à troca por dinheiro.

Para que o sistema de escambo ocorra, existe a necessidade de ambos os lados coincidirem seus desejos. Ou seja, para efetuar a troca, um dos lados precisa querer o objeto oferecido, e o outro lado precisa aceitar o que será oferecido em troca de seu produto, bem, serviço, entre outros. Geralmente, esse tipo de troca ocorre em economias relativamente rudimentares, com uma variedade pequena de bens trocados.

Esse método foi suficiente para as culturas da época, porém com o surgimento de sociedades mais complexas, foi determinante alterar ou modernizar esse modelo, para estabelecer sistemas mais estáveis aos diversos tipos de negociações. Surgiu assim o conceito de moeda, ou seja, algo produzido com materiais diferenciados e que traziam seu valor comercial baseado no material utilizado em sua produção. As moedas entraram em circulação e revolucionaram o mundo, originando os conceitos de empréstimos, dívidas, contratos e práticas comerciais.

Porém, o conceito de banco já era utilizado por antigos palácios reais e templos que ofertavam locais seguros para guardar algumas mercadorias. Todas essas operações era mantidas sob controle por meio de recibos e documentos. E com a revolução da moeda, surgem as casas privadas, que se envolvem nesse tipo de operação e trazem leis e regulamentações para continuar a realizar esse tipo de atividade. As moedas foram padronizadas, desenvolvendo diversas formas de trabalho com as unidades financeiras monetárias estrangeiras, e o órgão regulador destas operações é o Banco Central do Brasil - BACEN.

O BACEN foi criado sob a forma de autarquia federal, integrando o Sistema Financeiro Nacional, executa as deliberações do Conselho Monetário Nacional (CMN) sobre a política financeira e cambial do País. Para efetiva regularização e controle das operações financeiras, o BACEN conta com o Departamento de Combate a Ilícitos Financeiros (DECIC). Todos os órgãos foram planejados para controlar as diversas transações financeiras que ocorrem em todo o país. As transações financeiras diretas ou indiretas, nacionais e internacionais, são feitas por operações bancárias dos mais variados tipos, e o volume de dinheiro correndo abundantemente deslumbra algumas pessoas. Com essa rotatividade financeira, surgem os chamados fraudadores. Percebe-se que indivíduos que praticam fraudes, estelionatos ou qualquer tipo de crime de influência, persuasão, extorsão, entre outros, possuem facilidade no diálogo e um ardiloso raciocínio. Dessa forma, o golpista está sempre um passo à frente de sua vítima (pessoa física ou pessoa jurídica).

No Brasil, estima-se que foram feitas pouco mais de 140.000 mil (cento e quarenta mil) tentativas de fraudes. Segundo pesquisa publicada pelo SERASA EXPERIAN.

> (...) 141.008 tentativas de fraude de identidade foram aplicadas no país. São cerca de 4,7 mil tentativas por dia, nas quais dados pessoais são usados por criminosos para firmar negócios sob falsidade ideológica ou mesmo obter crédito com a intenção de não honrar os pagamentos. (SERASA EXPERIAN, Indicador de Tentativas de Fraudes, em abril de 2016).

Diante desse universo de informações, tecnologias, ideias novas, surgem os fraudadores e suas respectivas fraudes. E os clientes tornam-se os mais frágeis no contexto, tentando provir segurança de sua instituição.

1.2 OBJETIVOS

• Objetivo Geral

Determinar qual o motivo da continuidade das fraudes por engenharia social sofridas por clientes pessoas física de bancos comerciais, com foco no setor bancário brasileiro, mesmo com toda a tecnologia desenvolvida para esse setor. Além de detalhar as principais fraudes envolvendo esse perfil de usuários. E demonstrar se essas fraudes carregam um perfil específico entre vítima e fraudador.

• Objetivos Específicos

- Identificar os tipos de fraudes por engenharia social que envolvem as transações relacionadas às pessoas físicas no setor bancário brasileiro;
- Mapear o perfil dos fraudadores de pessoas físicas em nível Brasil;
- Consolidar por meio da identificação as fraudes mais comuns relacionadas ao perfil dos fraudadores do setor bancário brasileiro.

Para Beltran (2015) e Guimarães (2018), estamos vivendo em uma época cercada de fraudes de diversas origens e formas.

1.3 JUSTIFICATIVA

Mesmo com os mais diversificados métodos que existem contra fraudes, as pessoas físicas vêm alavancando os percentuais brasileiros, nos índices de fraudes envolvendo as instituições financeiras.

De acordo com Lau (2006, p.5) a definição de fraude está relacionada à distorção intencional da verdade ou de um fato, que busca em geral a obtenção de lucro ilícito.

O Banco Central diversas vezes evidencia alguns alertas, informando a seus consumidores quais fraudes podem vir a ser praticadas contra eles, porém os resultados não estão se tornando satisfatórios.

Segundo Luiz Rabi, economista da empresa Serasa Experian, é possível que os golpistas estejam mais incentivados a aplicar fraudes, já que momentos de maior fluxo de pessoas podem ser considerados como ambiente propício pelos fraudadores.

E nesse emaranhado de suspeitas, fraudes, roubos, entre outros, está o consumidor, que mesmo protegido pela sumula 479 do Superior Tribunal de Justiça, onde informa que “as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias”, é o mais prejudicado.

De acordo com Adriano Volpini, diretor setorial de prevenção a fraudes da Federação Brasileira de Bancos (FEBRABAN) e diretor de segurança corporativa do Itaú Unibanco, os bancos têm agido em três frentes principais para aumentar a segurança: desenvolvimento de novas tecnologias, parcerias com órgãos públicos e comportamento do consumidor.

> A Engenharia Social consiste em um “conjunto de métodos e técnicas que têm como objetivo obter informações sigilosas e importantes através da exploração da confiança das pessoas, de técnicas investigativas, de técnicas psicológicas, de enganação etc.”. Existem dois tipos de ataques de engenharia social: 1) Diretos, no qual o atacante entra diretamente em contato com a vítima por email, telefone, ou pessoalmente, ouse já, têm alvo fixo; e 2) Indiretos, que não têm alvo fixo ou vítima específica ou definida. (PARODI, 2005, p.5).

O autor ainda afirma que hoje, sessenta por cento das fraudes ainda estão vinculadas à engenharia social: alguém que vai até o cliente e, para efetivar a fraude,

busca dados, seja por e-mail, ligação telefônica ou por meio do golpe do falso motoboy na entrega de cartões. A tecnologia, o chip e a senha são suficientes para proteger o cliente, mas esses exemplos mostram que ainda é preciso investir para mudar o comportamento do consumidor. Além de tornar mais rigorosa a legislação para quem comete esses crimes.

2 REVISÃO DE LITERATURA

2.1 FRAUDE

Fraude é o ato praticado que tenha a intenção de causar danos a terceiros e consequentemente trazer benefícios para si. Esse ato deve ser devidamente analisado, para não ser confundido com o erro. Existem fraudes com vários graus, sendo eles mais ou menos danosos.

O mágico ou o ilusionista que vem a praticar sua arte, não pode ser considerado um fraudador, pois o participante passivo sabe de toda sua intenção, e até mesmo paga por isso. Já aquela pessoa que solicita ao médico um atestado, somente para justificar sua ausência em determinado compromisso, pode vir a ser classificado como fraudador.

De acordo com Pereira (1987, p.220) “a palavra fraude tem origem do latim fraus, fraudis (engano, má-fé, logro), a fraude é normalmente compreendida como o engano malicioso, intentado de má-fé, destinado a encobrir a verdade ou a contornar um dever”.

Segundo Gil (1998, p.91): A fraude tem o caráter de ação intencional e prejudicial, é o ato praticado com intenção de lesar terceiros, fazendo uso de informação privilegiada em benefício próprio. É a obtenção para si ou para outrem, de vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro.

2.2 TIPOS DE FRAUDE

A fraude se estende a diversas classificações, dentre elas:

- Furto: de acordo com o decreto-lei n. 2.848, de 07 de dezembro de 1940, artigo 155, furto é subtrair, para si ou para outrem, coisa alheia móvel. (BRASIL, Código Penal, 1940).

- Roubo: de acordo com o decreto-lei n. 2.848, de 07 de dezembro de 1940, artigo 157, subtrair coisa móvel alheia, para si ou para outrem, mediante grave ameaça ou violência a pessoa, ou depois de havê-la, por qualquer meio, reduzido à impossibilidade de resistência. (BRASIL, Casa Civil, 1940).

- Extorsão: de acordo com o decreto-lei n. 2.848, de 07 de dezembro de 1940, artigo 158, constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa. (BRASIL, Casa Civil, 1940).

- Apropriação indébita: de acordo com o decreto-lei n. 2.848, de 07 de dezembro de 1940, artigo 168, apropriar-se de coisa alheia móvel, de que tem a posse ou a detenção. (BRASIL, Casa Civil, 1940).

- Estelionato: de acordo com o decreto-lei n. 2.848, de 07 de dezembro de 1940, artigo 171, 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. (BRASIL, Casa Civil, 1940).

Em contra ponto com a fraude, existe o erro. Esse também causa danos a terceiros, porém não existe a intenção de se causar esse dano, ele é tido como involuntário.

O erro é um crime culposo (quando não existe a intenção de se cometer aquele fato). E tem as seguintes classificações:

- Negligência;
- Imprudência;
- Imperícia;

Embora ambos os atos camuflem a verdade, um é tido como doloso e outro culposo. Sendo necessário sempre averiguar a situação, e benefícios trazidos por

aquele ato, de má fé ou não. Dessa forma, pode-se dizer que a fraude nada mais é que um erro voluntário.

2.3 FRAUDE INTERNA NA INSTITUIÇÃO FINANCEIRA

Existem princípios de controle interno que permitem alguns objetivos específicos que são bem colocados por Peter e Machado (2003, p. 25) são:

Relação custo/benefício: consiste na minimização da probabilidade de falhas/desvios quanto ao atendimento dos objetivos e metas. Este conceito;

Reconhece que o custo de um controle não deve exceder aos benefícios que possa proporcionar;

Qualificação adequada, treinamento e rodízio de funcionários: a eficácia dos controles internos está diretamente relacionada com a competência e integridade do pessoal. Assim, é imprescindível que haja uma política de pessoal que contemple;

Delegação de poderes e determinação de responsabilidades: visam assegurar maior rapidez e objetividade às decisões, fazendo-se necessário um regimento/estatuto e organograma adequado, onde a definição de autoridade e consequentes responsabilidades sejam claras e satisfaçam plenamente às necessidades da organização; e manuais de rotinas/procedimentos claramente determinados, que considerem as funções de todos os setores do órgão/entidade;

Segregação de funções: a estrutura de um controle interno deve prever a separação entre as funções de autorização ou aprovação de operações e a execução, controle e contabilização das mesmas, de tal forma que nenhuma pessoa detenha competências e atribuições em desacordo com este princípio;

Instruções devidamente formalizadas: para atingir um grau de segurança adequado é indispensável que as ações, procedimentos e instruções sejam disciplinados e formalizados utilizando instrumentos eficazes, ou seja, claros e objetivos e emitidos por autoridade competente;

Controles sobre as transações: é imprescindível estabelecer o acompanhamento dos fatos contábeis, financeiros e operacionais, objetivando que

sejam efetuados mediante atos legítimos, relacionados com a finalidade do órgão/entidade e autorizados por quem de direito;

Aderência às diretrizes e normas legais: é necessária a existência, no órgão/entidade, de sistemas estabelecidos para determinar e assegurar a observância das diretrizes, planos, normas, leis, regulamentos e procedimentos administrativos internos.

2.4 FRAUDE E TECNOLOGIA

Esse tipo de fraude que envolve a informática pode vir a ser considerada civil ou penalmente, dependendo da situação envolvida. Algumas empresas ao descobrir essa fraude, prefere não anunciar ao público, pois considera uma vulnerabilidade em seu controle interno e tem o medo de trazer essa informação a seu cliente e ser taxada.

> Segundo (CUNHA, 2003), citando Romney, Steinbart e Cosching (*) “fraude em computador é definida pelo Departamento de Justiça Americano como ‘qualquer ato ilegal para cuja perpetração, investigação ou condenação, o conhecimento da tecnologia de computadores é essencial’”. (*) ROMNEY, Marschall B., STEINBART, Paul J., CUSHING, Barry E. Accounting information systems. 7. ed. USA: Addison-Wesley Publishing Co. 1997. p. 503 Tradução livre.

As instituições entendem que anunciar que seus clientes foram vítimas de fraude, contribui para uma má reputação da empresa. E consequentemente decrescente índice de novos clientes.

E com o intuito de diminuir os índices, as instituições tem se valido de cartilhas de informação impressas e on-line para informar a seus clientes alguns métodos de prevenção, em sua maioria, recomendam:

- Atualizar o antivírus sempre que possível;

- Identificar se realmente está no sítio da instituição que deseja, não se tratando de um sítio falso, verificando a área de segurança do site;

- Sempre que acessar o site, digitar a senha incorreta pela primeira vez, pois somente os sites verdadeiros conseguem apresentar informação de erro, já os sites falsos, tem único propósito em capturar a senha correta;

- Fazer acompanhamento da conta corrente, para conseguir identificar com rapidez qualquer valor que sofra discrepância de suas contas;

- Redobrar a atenção ao receber e-mails com arquivo anexado e que não seja de conhecimento;

- Não realizar operações em locais públicos, e que não tenha instalado programa antivírus;

- Ao escolher um provedor, prefira um com política de segurança e confiabilidade;

- Utilizar versões de browsers (programas de navegação) atualizadas;

- Fazer download (transferência de arquivo) somente de sites conhecidos e confiáveis;

- Periodicamente trocar a senha de acesso ao internet banking e/ou mobile banking.

> A informação é um facho de luz, uma vara, um galho, um freio, dependendo de quem a controla e da maneira como o faz. A informação possui tamanho poder que a suposição de tê-la, ainda que inverídica, já cria a impressão de competência. (Levitt, 2005 p. 65).

O economista Levitt (2005) explica que uma das chaves para entender como o mundo funciona nos dias de hoje é observando o poder da informação. Para o autor, dependendo de quem a controla, a informação se torna uma fonte de poder.

2.4.1 INTERNET BANKING

O Internet Banking é uma modalidade que permite acesso por meio de navegadores aos seus usuários. Com esse intermédio é possível consultar saldos, fazer investimentos e aplicações, pagar contas, efetuar transferências, entre outros.

Por se tratar de uma modalidade ágil e econômica, seu crescimento tem se destacado dentro dos serviços oferecidos pela instituição. Sua economia retornada ao setor chega a um percentual de até 107% (cento e sete por cento).

Mas, a agilidade também se sobressai aos fraudadores, que com a modalidade do Internet Banking utilizam outras técnicas: scam, phishing e parming. Os ataques surgem de maneiras diferentes, porém utilizam o mesmo embasamento.

2.4.2 MOBILE BANKING

Mobile Banking segue os mesmos princípios do internet banking e sua maior diferença é o meio pelo qual é utilizado. As operações, nesse caso, são efetuadas com o uso de aplicativos instalados em aparelhos de celular e tablet.

Segundo pesquisas realizadas no ano de 2016 pela FEBRABAN, esse canal passou a ser o mais utilizado pelos brasileiros, superando pela primeira vez o internet banking. Isso devido à facilidade, embasamento de segurança e praticidade no uso do aparelho celular, que está sempre disponível, não existe a necessidade de enfrentar filas de espera: “movimentar-se durante o uso ou entre instantes de uso” (BALLARD, 2007). Isso se deve porque o usuário “normalmente está envolvido em várias atividades que ocorrem simultaneamente (...) com a atenção dividida entre o uso do equipamento, as outras atividades que ele está realizando e o ambiente que o cerca” (CYBIS, 2007).

2.4.3 SCAM

O Scam é um aprimoramento ao Spam, onde existe o envio de mensagens em massa, porém com um diferencial, esse tipo de mensagem carrega link de condução a download de arquivo. Ao efetuar o download, o usuário proporciona a instalação de arquivos de vírus em seu computador. Nesse caso, existe primeiramente um furto, ocasionado danos ao correntista e ao banco, resultado da perda financeira.

As mensagens que carregam o scam instigam as vítimas, tornando-as curiosas, pois têm aparência da instituição financeira, onde informam notícias de destaque, downloads de programas, promoções, entre outros.

O arquivo baixado por meio de download colhe os dados armazenados em texto e os envia ao fraudador através do File Transfer Protocol (FTP) e Simple Mail Transfer Protocol (SMTP). A vítima não percebe o que está acontecendo, não é informada da retirada de seus dados e informações pessoais, pois foi ela quem correu ao encontro do link, acreditando ser algo vantajoso e inofensivo. No Brasil, o scam é

uma das modalidades do Internet Banking mais usual, devido a sua simplicidade, praticidade e mitigação, como ocorre com o spam.

2.4.4 PHISHING

O método phishing que também é conhecido como phising scam é comumente confundido com o scam. Porém são técnicas praticadas de forma diferenciada.

O termo surgiu por volta de janeiro de 1996, quando crackers (hacker que utiliza seu conhecimento para próprio benefício, proporcionando malefício a terceiros), conseguiram algumas senhas de acesso do provedor America Online.

Thomas (2007, p. xx), alega que “os hackers sempre têm uma nova meta em mente quando selecionam um alvo”.

O ataque é semelhante ao scam, porém a vítima é levada a uma página montada para o crime, chamadas de páginas falsas. Assim ao informar qualquer dado pessoal, a vítima está enviando via HyperText Markup Language (HTML) todas as informações ao fraudador.

O phishing é um método mais caro e trabalhoso que o scam. Dessa forma seus números sempre foram menores em comparação as outras técnicas e cada vez mais tem perdido campo de lastreio.

2.4.5 PHARMING

Já o método pharming surgiu no decorrer de farming, um termo utilizado na indústria agrícola, que estuda a modificação genética de hospedeiros para o desenvolvimento incremental de drogas medicinais.

O nome é devido à semelhança com a técnica, uma vez que também é modificado o hospedeiro chamado de Domain Name System (DNS), que detém informação no funcionamento da rede. O “ph” no inicio é utilizado, para mencionar os preakers (fraudadores de sistema telefônico).

Em meados de 2002 e 2003, as instituições financeiras sofreram grandes prejuízos financeiros, e decidiram investir junto a seus servidores, reduzindo assim esse tipo de ataque. E desde 2004 quase que foi extinta a prática no cenário brasileiro.

Pharming consistia em levar o usuário a um sítio falso, por mais que fosse digitado o sítio correto e sem fraudes. As vítimas eram facilmente enganadas, pois não notavam as informações de segurança expostas em seu sistema e navegadores.

2.5 HISTÓRIA DAS FRAUDES EM INTERNET BANKING NO BRASIL

Segundo dados publicados pelo Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores, no ano de 2001 surgiram os primeiros ataques ao Internet Banking. Os ataques surgiram em forma de apelos para que os usuários realizassem atualizações em seu sistema, com a promessa de que esse procedimento se fazia necessário para posterior acesso a página da instituição financeira. Com pouco conhecimento, os usuários aderiam a essas atualizações, carregando para seu sistema os arquivos conhecidos como vírus, ou eram levados as páginas falsas.

O teclado utilizado pelo usuário foi a primeira fonte de informação invadida pelos fraudadores. A prática, porém, demandava muito tempo, o que não satisfazia a capacidade e meta do fraudador. Nesse tempo, o scam progrediu e somente quando a vítima utilizava o navegador, seus dados eram obtidos. Para coibir a ação, foram desenvolvidos teclados virtuais, mas como o fraudador sempre está um passo a frente, não perdeu tempo e logo lançou novas práticas e métodos para contrapor a coibição.

Como as informações obtidas das vítimas eram enviadas por arquivos FTP e SMTP, os órgãos de investigação conseguiram fazer o rastreamento e codificar quais as informações capturadas pelos fraudadores.

As instituições financeiras investiram em servidores com proteção de suas bases de dados, o envio de scam e phishing foi intensificado. Com isso, em 2004, houve a quase extinção do método pharming.

Como todo método, os scams foram aprimorados, passando a ter tamanho reduzido, trazendo maior confiabilidade e tornando seus arquivos de guarda de dados, um sucesso.

A evolução acompanhou também o conteúdo desenvolvido pelo fraudador. Anteriormente, os dados que eram lapidados envolviam somente as instituições financeiras. Logo, foram abordadas as instituições públicas e grandes empresas e por último, foram inclusos e-mails sensacionalistas, utilizando conteúdo mais pessoal. Scam e phishing passam a ser quase imperceptíveis, se não houver o cuidado de seus usuários.

O ataque mais usual no Brasil é o scam, devido a sua facilidade na instalação e disseminação, além de resultar em maior coleta de dados com relação ao phishing e o quase extinto pharming.

2.6 PERFIL DOS FRAUDADORES

Entre discussões que ocorrem em todo o cenário brasileiro, cresce o número de fraudadores, que observam a facilidade no ato, a falta de punição e cometem atos contra o patrimônio de terceiros. E os mesmos, não são pessoas que apresentem passado criminoso ou família desestruturada. Em sua maioria, são homens, estudantes, que fazem parte da classe média e com conhecimento da área de informática.

Pesquisadores, porém, afirmam não existir um perfil específico do fraudador. Pois com o avanço da tecnologia, surgimento de novos métodos e possibilidades, o fraudador vai sendo moldado por essa crescente, surgindo a cada dia um novo perfil de fraudador e fraude. E como afirma Emílio C. Viano, em A Criminalidade Informática, "[...] O anonimato e a distância física fazem com que as pessoas on-line se sintam protegidas por sua imunidade não só de serem facilmente detectadas, bem como das consequências imediatas de suas ações".

As recentes prisões no Brasil, com relação às fraudes envolvendo o setor bancário, confirmam a afirmativa. As quadrilhas possuem teor intelectual, não carregam antecedentes e residem em imóvel próprio. Já os fraudadores com menor

teor intelectual, são considerados apenas aliciadores e são utilizados para acobertar diversas operações.

2.7 CONSOLIDAÇÃO DE VÍTIMAS E FRAUDADORES

Investigação é o ponto crucial para a descoberta da criminalidade nas redes. O número de casos, vítimas e usuários cresce compassadamente à tecnologia. Os usuários tendem a buscar junto às instituições uma resposta, um ato de segurança múltipla, porém os esforços não estão atendendo esse clamor de usuários.

Surge assim a perspectiva de cadastro de usuários de redes, que instiga dois lados. Alguns acreditam que se aplicada à tecnologia e método certo, existirá um acompanhamento e consequente redução de fraudes, até se chegar à extinção. Outros, afirmam que o método poderá trazer benefícios, porém serão passageiros, uma vez que o fraudador também busca alcançar a evolução em sua busca de benefício próprio.

Para defender a tese de que o método não funcionará, o lado não tão convicto da ideia, traz exemplos de cadastros já utilizados, como a biometria. Onde mesmo afirmando que cada ser humano possui uma crista e sulco diferente em seus dedos, ainda assim existem fraudes na biometria. Afirmam também que o sistema judiciário brasileiro é falho e não conseguiria acompanhar a tecnologia de cadastro de usuário de redes.

O fraudador se beneficia da falta de conhecimento da maioria dos usuários dos serviços das instituições financeiras, pois segundo pesquisa realizada pelo IPSOS, demonstrando que existe um percentual de 70,07 de usuários sem curso de informática que já utilizam o internet banking, o que facilita a captura de dados pessoais.

Pesquisadores em Harvard também chegaram a essa conclusão, quando checaram os dados de uma pesquisa envolvendo phishing. Acreditam que o despreparo é o principal fator do aumento de vítimas, como diz pesquisa:

> Este estudo ilustra que, mesmo no melhor cenário, quando os usuários esperam que as falsificações estejam presentes e estejam motivados para descobri-las, muitos usuários não conseguem distinguir um site legítimo de um site falsificado. Em nosso estudo, o melhor site de phishing foi capaz de enganar mais de 90% dos participantes. Indicadores projetados para sinalizar confiabilidade não foram compreendidos (ou percebidos) por muitos participantes. 5 de 22 (23%) participantes usaram apenas o conteúdo do site para avaliar sua autenticidade, sem olhar para outras partes do navegador. Um número de participantes disse incorretamente que um ícone de cadeado é mais importante quando exibido dentro da página do que se fosse apresentado pelo navegador. Outros participantes foram mais persuadidos por gráficos animados, imagens e toques de design, como favicons (ícones na barra de URL) do que os indicadores SSL. (DHAMIJA, Rachna; TYGAR, J.D.; HEARST, Marti. Opus citatum, tradução livre).

A vítima brasileira se torna ligeiramente mais vulnerável em razão da tardia inclusão digital proporcionada por nosso país. Como o número de usuários aos serviços de internet, ofertados pelas instituições financeiras cresceu desproporcionalmente à tecnologia desenvolvida para combater os diversos tipos de ataques às redes, a situação proporcionou um nicho de mercado ao fraudador.

Pesquisa realizada pelo Núcleo da Informação e Coordenação do Ponto BR – NIC.br, aponta que o perfil da vítima brasileira é: reside na região metropolitana das cidades de São Paulo e Curitiba; a maioria constitui uma renda familiar superior a R$ 1.801,00; possuem grau de escolaridade em nível superior completo; são do sexo masculino; fazem parte da classe A e B e estão na faixa de idade que compreende 16 a 34 anos.

2.8 INSTITUIÇÕES FINANCEIRAS E SUAS QUESTÕES PENAIS

A polícia federal por ter um quadro de funcionários maior com relação a policia estadual, não que se seja suficiente, conseguiu obter sucesso em diversos casos de fraudes envolvendo o setor bancário brasileiro.

Já a policia estadual, possui poucas delegacias especializadas, o que converge em uma situação bem mais difícil. Além de a mídia promover menor divulgação, prejudicando o estudo com relação ao avanço da fraude.

A Constituição Federal, inciso IV do artigo 109, dá competência a juízes para julgar “os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral”. (BRASIL, Constituição Federal, 1988). Analisando a competência, toda a justiça estadual tem o dever de combater com mais folego o crescente caso de fraude envolvendo pessoa física no setor bancário de seu estado.

Feito um levantamento de fraudes no setor bancário, foi verificado que a instituição que sofreu menos impacto com relação às fraudes, foi a Caixa Econômica Federal – CEF. Outros bancos que depositaram menor grau de importância em segurança do cliente resultaram em números elevados de fraudes.

Porém ainda temendo correr o risco, a empresa incentivou outras práticas, como estabelecer limites para transações on-line, com o intuito de proteger seus usuários e a própria instituição. Pois na maioria das vezes, os bancos ressarcem os clientes, sem ocasionar qualquer propaganda para não trazer aquela imagem de despreparo na aquisição de novos clientes.

Nos casos de crimes que abrangem união e estado, o Superior Tribunal de Justiça entende que: "Compete a Justiça Federal o processo e julgamento unificado dos crimes conexos de competência federal e estadual, não se aplicando a regra do artigo 78, II, "a", do Código de Processo Penal". (BRASIL, Código de Processo Penal, 1994).

2.9 CONTINUIDADE DO USO DA ENGENHARIA SOCIAL EM FRAUDES

Mesmo com toda a tecnologia e questões penais aplicadas, os índices de aplicação da engenharia social, estão em nível crescente. Segundo alguns especialistas, isso se deve a falta de preparo no uso da tecnologia pela equipe da instituição, ou seja, grande parte dos incidentes envolvendo questões de segurança da informação está ligada ao fator humano.

> A maioria das organizações visa quase completamente à segurança técnica. Os agressores sabem disso e com frequência usam a rota fácil as suas informações confidenciais – sua equipe. Com uma indústria em expansão concentrada em vender "soluções" em hardware e software, isso traz a você um desafio real para solução dos seus riscos com proteção de engenharia social adequada, o que requer uma compreensão do processo de segurança. (MANN, 2011, p.25).

A tecnologia está em constante crescimento e visa ajudar no desenvolvimento de todos os setores, porém ela deve ser manuseada de forma hábil, com completo conhecimento e controle, e o sistema bancário está um passo atrás desse conhecimento. No entanto, o fraudador, vem acompanhando a tecnologia de bloqueio dessas instituições, ultrapassando e quebrando os limites bancários, ocasionando o constante crescimento em diversas fraudes.

> A segurança normalmente é apenas uma ilusão que é facilitada e tornada mais acreditável pela ignorância ou ingenuidade de qualquer um da organização. Não coloque toda confiança em produtos de segurança; se o fizer, estará destinado à ilusão da segurança. Todo processo de segurança deve ser implementado, ou seja, tanto a "tecnologia" como as regras. (THOMAS, 2007, p.33).

MANN (2011) e THOMAS (2007) entendem que as instituições não investem no treinamento e conscientização da equipe humana (seus funcionários), deixando seu elo mais fraco de segurança sem qualquer respaldo.

> "Os próprios hackers veem a engenharia social de um ponto de vista psicológico, enfatizando como criar o ambiente psicológico perfeito para um ataque. Os métodos básicos de persuasão são: personificação, insinuação, conformidade, difusão de responsabilidade e a velha amizade. E ainda afirma que um ou mais dos empregados de uma empresa pode se tornar um inimigo sem estar conivente com o crime que está sendo praticado". (DAWEL, 2005, p.45).

PARODI (2005) afirma que por mais controverso que possa parecer, o método mais simples, usual e infelizmente, com amplo grau de eficiência para descobrir informações confidenciais é perguntando.

Dessa forma, o fator humano é o maior complicador para a tecnologia de segurança desenvolvida. Pois, se alguém detém determinada informação, está suscetível a perder esse dado a terceiros. E isso pode ocorrer com um simples clique em informações falsas ou o aceite de e-mails fraudulentos.

3 METODOLOGIA DA PESQUISA

3.1 TIPOLOGIA DA PESQUISA QUANTO AOS OBJETIVOS

A presente pesquisa enquadra-se quanto aos fins a que se destina como do tipo descritiva, pois expõe as características de determinada população usuária de um tipo de serviço ofertado.

3.2 TIPOLOGIA DA PESQUISA QUANTO AO PROBLEMA DE PESQUISA

O problema da pesquisa tem a tipologia qualitativa, pois o objeto de estudo é entender o porquê da continuidade de vítimas a fraudes mesmo com toda a tecnologia em desenvolvimento, definindo o comportamento dos fraudadores e suas vítimas.

3.3 TIPOLOGIA DA PESQUISA QUANTO AOS PROCEDIMENTOS

A pesquisa tem abordagem bibliográfica e documental, pois reúne informações e dados que servem de embasamento as informações e dados, construindo assim a proposta a partir do tema determinado.

Lopes (2016), diz que a diferença crucial é que na pesquisa documental, ainda não houve um filtro analítico, e os materiais podem sofrer reelaboração de acordo com os objetivos da pesquisa.

3.4 COLETA DOS DADOS E INFORMAÇÕES

Os objetivos específicos são abordados pela técnica da pesquisa documental e bibliográfica, segundo índices econômicos:

Perfil vitima pessoa física de fraudes;

Principais motivos que as levaram a serem vítimas;

Privacidade e segurança;

Identificar principais situações de risco;

Análise de serviços pela internet e pessoais;

Perfil do fraudador.

4 CONSIDERAÇÕES FINAIS

Nos últimos anos surgiram novas modalidades de fraudes praticadas, principalmente no meio virtual, no ambiente internet banking. Com isso a subtração de valores dos clientes de instituições financeiras em nível de Brasil cresceu. Não existe a possibilidade de afirmar o verdadeiro número de vítimas, pois as instituições com medo de perder a boa imagem de confiança da empresa, preferem acobertar esse tipo de informação.

Evidenciou-se a falta de meios para conter essa crescente de fraudadores, fraudes e vítimas. O poder judiciário, considerado falho, não dispõe de recursos para promover as devidas investigações. São poucos os especialistas no assunto e o fraudador está sempre à frente, com maior “munição” que a própria polícia estadual e suas vítimas.

Existe a necessidade de investimento por parte das instituições, em sistemas para combater os números de fraudes. O Brasil, porém, não acompanha e incentiva tal progresso de tecnologia.

As vítimas continuam a apresentar como culpada, a instituição financeira a qual sofreu fraude. Não aceitando que ele deveria manter zelo e cuidado ao utilizar os serviços comerciais oferecidos pelo banco.

E o fraudador não é alguém cujo teor social o levou a praticar o crime, pois geralmente são homens com ensino superior, classe média e sem antecedentes. Mas que enxergam no falho sistema, uma oportunidade de alcançar benefícios, proporcionado malefícios a terceiros.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. **A criminalidade informática**. São Paulo: Juarez de Oliveira, 2006. p. 23.

ALMEIDA, Paula Carneiro de. **Segurança da Informação Bancária: Aplicação de *Internet Banking***. Universidade do Vale do Sapucaí. Porto Alegre, 2008.

BANCO CENTRAL DO BRASIL. **BC alerta para tentativas de fraude**. Acesso em: 10 de outubro de 2017.

BRASIL. Casa Cívil. **Código penal**. Brasília, 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 01 de junho de 2018.

BRASIL. Superior Tribunal de Justiça. Recurso ordinário em Habeas Corpus nº 19846. Recorrente: Casimiro Júnior Marinho Aguiar. Recorrido: Tribunal Regional Federal da 1ª Região. Relator: Ministro Gilson Dipp. Brasília, 12 de setembro de 2006. **Diário da Justiça.** 09.10.2006. p. 316.

BITENCOURT, Cezar Roberto; CONDE, Francisco Muñoz. **Teoria geral do delito.** 2. ed. São Paulo: Saraiva, 2004. p. 121-122.

CARVALHO, Fernando J. Cardim de; SOUZA, Francisco Eduardo Pires de; SICSÚ, João, PAULA, Luiz Fernando Rodrigues de; SUDART, Rogério. **Economia Monetária e Financeira.** Rio de Janeiro, 2002. Editora Campus.

CARVALHO, Fernando J. Cardim de; SOUZA, Francisco Eduardo Pires de; SICSÚ, João, PAULA, Luiz Fernando Rodrigues de; SUDART, Rogério. **Economia Monetária e Financeira.** Rio de Janeiro, 2002. Editora Campus.

DAWEL, George. **A segurança da informação nas empresas: ampliando horizontes além da tecnologia**. Rio de Janeiro: Editora Moderna Ltda, 2005.

FORTUNA, Eduardo. **Mercado Financeiro.** Produtos e Serviços. 15. ed. Rio de Janeiro: Qualitymark, 2002. p. 148.

GRAEBER, David. **O mito do escambo**. Editora Subta, 2011.

GRECCO FILHO, Vicente. **Interceptação telefônica.** São Paulo: Saraiva, 1996.

JESUS, Damásio E. de. **Direito penal.** Parte Especial. 24. ed. rev. e atual. São Paulo: Saraiva, 2001. v.2. p. 328.

LAU, Marcelo. **Análise das fraudes aplicadas sobre o ambiente *Internet Banking*.** Dissertação apresentada à Escola Politécnica de São Paulo, 2006.

LEVITT, Steven D., DUBNER, Stephen J. ***Freaknomics*: o lado oculto e inesperado de tudo que nos afeta**. Editora Campus. 7ª Edição. 2005.

LOPES, João do Carmo & Rossetti, José Paschoal. **Moeda e bancos**. São Paulo, Atlas, 1980.

MANN, Ian. **Engenharia Social: Série prevenção de fraudes**. São Paulo: Blucher, 2007.

MONITOR DAS FRAUDES. **Pequenos golpes populares**. Acesso em 01 de outubro de 2017.

PARODI, L. **Manual das fraudes 2.a edição**. Editora Brasport, 2005

PARODI, L. **Manual das fraudes 2.a edição**. Editora Brasport, 2008

ROMNEY, Marschall B., STEINBART, Paul J., CUSHING, Barry E. ***Accounting information systems***. 7. ed. USA: Addison-Wesley Publishing Co. 1997. p. 503 Tradução livre.

SANTANDER. **Do escambo à criação do dinheiro**. Acesso em: 10 de junho de 2018.

SERASA EXPERIAN. **Riscos de fraudes**, 2016. Acesso em: 06 de outubro de 2017.

SODRÉ, L.M; Lettermer, Brígida. **A fraude contra o seguro e suas conseqüências econômicas na sociedade**. Revista de divulgação técnico – científica do ICPG. VOL.2, n.6 – jul./set./2004.

THOMAS, Tom. **Segurança de redes: primeiros passos**. Rio de Janeiro: Ciência Moderna Ltda, 2007.