UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS QUIXADÁ

BACHARELADO EM ENGENHARIA DE SOFTWARE

IURY PEREIRA DA SILVA

ENGENHARIA SOCIAL COMO AMEAÇA AO SETOR BANCÁRIO: USO DO PHISHING PARA COLETAR INFORMAÇÕES DOS CORRENTISTAS E A NECESSIDADE DE ESTRATÉGIAS DE SEGURANÇA.

QUIXADÁ

2019

IURY PEREIRA DA SILVA

ENGENHARIA SOCIAL COMO AMEAÇA AO SETOR BANCÁRIO: USO DO PHISHING PARA COLETAR INFORMAÇÕES DOS CORRENTISTAS E A NECESSIDADE DE ESTRATÉGIAS DE SEGURANÇA.

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Software do Campus Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau em Engenharia de Software.

Orientador: Prof. Me. Marcos Dantas Ortiz

QUIXADÁ

2019

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

S58e Silva, Iury Pereira da.
Engenharia social como ameaça ao setor bancário: Uso do phishing para coletar informações dos correntistas e a necessidade de estratégias de segurança / Iury Pereira da Silva. – 2019.
77 f.: il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Engenharia de Software, Quixadá, 2019.
Orientação: Prof. Me. Marcos Dantas Ortiz.

1. Engenharia Social. 2. Segurança computacional. 3. Bancos-Automação. 4. Instituições financeiras. 5. Fraude bancária. I. Título.

CDD 004.6

IURY PEREIRA DA SILVA

ENGENHARIA SOCIAL COMO AMEAÇA AO SETOR BANCÁRIO: USO DO PHISHING PARA COLETAR INFORMAÇÕES DOS CORRENTISTAS E A NECESSIDADE DE ESTRATÉGIAS DE SEGURANÇA.

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Software do Campus Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau em Engenharia de Software.

Aprovada em:_____/_____/_____.

BANCA EXAMINADORA

_____

Prof. Me. Marcos Dantas Ortiz (Orientador)
Universidade Federal do Ceará (UFC)

_____

Prof. Dr. David Senna de Oliveira
Universidade do Ceará (UFC)

_____

Prof. Me. Roberto Cabral Rabêlo Filho
Universidade do Ceará (UFC)

Dedico aos meus pais, Elizângela Vieira da Silva e Antônio Cicero Pereira da Silva, a meu amigo Ciro Soarez, minha irmã Yasmim Pereira da Silva, meu tio Cid Pereira, minhas avós Maria Pereira e Francisca Gomes pelo apoio incondicional.

AGRADECIMENTOS

Agradeço a Deus por me dar sabedoria e iluminar meus passos durante essa minha trajetória de vida;

A Universidade Federal de Quixadá (UFC), pelo ajuda, transparência no trabalho e incentivos;

Ao orientador, professor Marcos Dantas Ortiz, pela orientação durante o desenvolvimento da pesquisa;

A professora Dr.Tânia Saraiva de Melo Pinheiro pelas dicas durante o desenvolvimento da pesquisa;

Aos professores da banca que se dispuseram em avaliar e tecer suas contribuições de grande valia para o resultado final da pesquisa;

Aos professores reconheço um esforço gigante com muita paciência e sabedoria. Foram eles que me deram recursos e ferramentas para evoluir um pouco mais todos os dias;

Aos secretário, coordenadores, faxineiros, seguranças, bibliotecários, por desempenhar um belo trabalho que é feito na UFC de Quixadá;

As minhas avós, Maria Pereira e Francisca Gomes que já veio a falecer porém foram de fundamental importância no meu processo de educação;

Aos meus pais Elizângela Vieira da Silva e Antônio Cicero Pereira da Silva pelo total apoio desde o inicio do curso, por sempre me ajudar nas horas mais difíceis e nunca duvidarem de mim, obrigado pelo amor e exemplos de vida que vocês são.

Aos meus amigos, Ciro Soarez, Gerardo Feitosa, Edson de Queiroz, Jackson Maia, Romário Lima , Jordão Macedo, Pereira Neto, Cezar Filho, Iuri Breno, Willame Nogueira, pela troca de experiência de alguma maneira nesse processo de formação;

A todos aqueles que de alguma forma, direta ou indiretamente, emanaram energia positiva para conclusão dessa etapa de vida;

Muito obrigado!

“O conhecimento é o caminho para a liberdade..”

(Hacker Pyron)

RESUMO

Esta pesquisa analisa os riscos de segurança da informação de correntistas de bancos convencionais e digitais sob a ótica da engenharia social. Foram analisados os perfis dos usuários que tinham sido vítimas de ataques eletrônicos, baseados em *phishing/smishing*. A invasão de sistemas e a disseminação de programas espúrios são as atividades de maior relevância dos engenheiros sociais, portanto será exibido estratégias de defesa usadas pelos bancos nas plataformas digitais de acesso *internet banking*. O conhecimento pelos correntistas das armadilhas utilizadas pelos engenheiros sociais, nas suas práticas criminosas, é essencial para auxiliá-los na proteção contra as ameaças presentes na rede. Dessa forma, a segurança da informação é um processo dinâmico e complexo, cuja efetividade está constituída nas informações das pessoas e da maneira que é comunicada.

Palavras-chave: Engenharia Social. Segurança computacional. Bancos-Automação. Instituições financeiras. Fraude bancária.

ABSTRACT

This research analyzes the information security risks of conventional and digital bank account holders from the perspective of social engineering. We analyzed the profiles of users who had been victims of electronic attacks based on *phishing / smishing*. System intrusion and the spread of spurious programs are the most important activities of social engineers, so it will be displayed defense strategies used by banks in digital access platforms *internet banking*. Account holders' knowledge of the pitfalls used by social engineers in their criminal practices is essential to help them protect against network threats. Thus, information security is a dynamic and complex process whose effectiveness is constituted in people's information and the way it is communicated.

Keywords: Social engineering. Computational security. Bank-Automation. Financial Institution. Bank fraud.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

Febraban	Federação Brasileira de Bancos
IOS	iPhone OS
PIN	Personal Identification Number
QRCode	Quick Response
SMS	*Short Message Service*
TLS	Transport Layer Security
UCE	Mensagem Comercial Não-Solicitada

SUMÁRIO

1 INTRODUÇÃO

A *internet* existe há décadas e está crescendo dia após dia fazendo com que muitas pessoas a utilizem para facilitar suas vidas e otimizar suas tarefas diárias Razak (2016). Com essa infraestrutura, o setor bancário evoluiu bastante com maneiras atraentes de aumentar o âmbito dos seus serviços financeiros, oferecendo uma maior flexibilidade para seus clientes através do *e-banking*. Dessa forma, é permitido que clientes acessem suas contas bancárias através dos *sites* que os bancos disponibilizam, sem a necessidade de ir até o banco físico Safeena (2010). Entretanto, juntamente com esses avanços, há uma grande quantidade de ameaças que exploram as vulnerabilidades inerentes à *internet* e suas tecnologias associadas. Isso gera a necessidade de uma maior segurança no setor bancário devido sua importância no uso diário dos correntistas.

As instituições bancárias necessitam cada vez mais de proteção das informações de sua própria organização e de seus usuários, uma vez que os engenheiros sociais podem usar esses dados confidenciais em benefício próprio.

O engenheiro social é definido como um indivíduo com a capacidade de manipular as ações de outra pessoa a fim de obter acesso às suas informações privadas Mitnick (2003). Ele empreende ataques denominados phishing, que consistem em "pescar dados"privados dos usuários com dados de contas bancárias. O Brasil é o primeiro do *ranking* mundial relacionado á ataques de *phishing*, trinta por cento dos internautas já sofreram uma tentativa desse ataque Kaspersky (2017). O *smishing* é um exemplo de *phishing*, que funciona como serviços de mensagens curtas (*Short Message Service* (SMS)), com intuito de coletar informações bancárias. Há muitas maneiras de enganar as pessoas para adquirir essas informações do usuário através do ataque de engenharia social (MOUTON M. MALAN; VENTER, 2014).

Este trabalho tem como objetivo geral contribuir para segurança da informação com foco principalmente em vulnerabilidades associadas ao *internet banking* abordando tipos de ataques através da engenharia social, visando distinguir páginas *fakes* e originais enfatizando no *phishing*. Será mostrado como as instituições bancárias abordam a segurança em seus *sites* e como são usados mecanismos para dificultar que outros golpistas acessem as contas de correntistas fraudados. Pretende-se também analisar os perfis de usuários que são enganados nesse golpe, procurando esclarecer a enormidade das ameaças existentes para os dispositivos móveis, criando a conscientização sobre a gravidade do efeito do *phishing* e *smishing*.

2 OBJETIVOS

Neste Capítulo, serão apresentados o objetivo geral e os objetivos específicos deste trabalho.

2.1 Objetivo Geral

A presente pesquisa tem como objetivo analisar os riscos de segurança aos correntistas de bancos convencionais e digitais sob a ótica da engenharia social. Faremos o levantamento do perfil dos usuários (vítimas) de ataques baseados em *phishing/smishing*. Serão abordadas também as estratégias de ataque usadas pelos engenheiros sociais aos alvos que utilizam plataformas digitais de acesso *internet banking*. Por fim, demostraremos aos leitores algumas ações que podem ser tomadas para evitar que o ataque de um golpista seja bem-sucedido.

2.2 Objetivos Específicos

- Investigar técnicas da engenharia social às quais os usuários de instituições bancárias estão suscetíveis.
- Investigar o perfil dos correntistas fraudados a partir de dados coletados através da pesquisa de campo.
- Investigar medidas de segurança que vem sendo utilizadas pelas instituições bancárias para deixar seus usuários mais seguros.

3 FUNDAMENTAÇÃO TEÓRICA

Neste Capítulo, serão apresentados os principais conceitos presentes neste trabalho.

3.1 Segurança da informação

Com o avanço da tecnologia da informação e comunicação, o uso da *internet* causou grande impacto na sociedade, ocorrendo grandes mudanças nos sistemas informacionais, fazendo com que houvesse uma grande comunicação de dados, que envolve não somente as máquinas, mas também os usuários. Segundo Almeida (2007), o objetivo da Segurança da informação é manter a proteção de sistemas de informação contra, divulgação, alterações ou destruições de informações que são confidenciais por meio de acessos não autorizados. Está conectada a três aspectos: confidencialidade, integridade e disponibilidade. De forma simples, Benetti (2015) caracteriza estes aspectos como:

- Integridade significa garantir que a informação armazenada ou transferida está correta e é apresentada corretamente para quem a consulta, garantindo com que usuários autorizados possam ter acesso a essas informações e possivelmente fazer alterações.
- Confidencialidade é a propriedade da informação que não estará disponível ou divulgada a indivíduos, entidades ou processos sem autorização, a garantia que a informação seja acessível apenas aqueles autorizados a ter acesso.
- Disponibilidade garante que a informação possa ser obtida sempre que for necessária, isto é, que esteja sempre disponível para quem precisar dela no exercício de suas funções.

Assim, integridade, confidencialidade e disponibilidade são considerados princípios fundamentais para garantir a segurança da informação. O ritmo da evolução da humanidade está interligado ao aumento dos estoques informacionais. Tanto a disponibilidade, quanto a confidencialidade e integridade da informação podem ser comprometidas quando são manipulados por pessoas não autorizadas. As práticas criminosas exploram a tríade da segurança dainformação, comprometendo-a. As atividades em rede, que podem comprometer a segurança da informação envolvem: a invasão de *sites* de governos, de empresas e contas bancárias, com captura de códigos dos cartões e senhas, a exploração de informações particulares disponibilizadas em redes sociais usadas para a prática de extorsão contra os usuários, que serão analisadas posteriormente.

Quanto maior o controle e a quantidade de restrições para acessar uma informação, segundo Silva (2011), maior será o grau de desconforto do usuário, pois tal sentimento é diretamente proporcional ao grau de segurança, podendo alcançar o seu comprometimento dependendo das reações dos usuários e das medidas implementadas pelas organizações. Nesse sentido, Mitnick (2003) ressaltam que a segurança não é problematizada pela tecnologia, mas sim pelas pessoas, consideradas o elo mais fraco da segurança.

3.2 Engenharia social

Segundo a definição de Mitnick (2003) os engenheiros sociais são indivíduos com a capacidade de manipular a confiança de outra pessoa de modo a obter acesso às informações privadas. A disjunção dos termos "engenharia social" nos leva a um conceito literal, no qual, o termo "engenharia" aparece no sentido de construção e "social" por envolver pessoas, atividade realizada ao indivíduo situado em um determinado ambiente. Conforme Costa (2011) a construção está interligada ao desenvolvimento de táticas que permitam o acesso à informação não disponível naturalmente, mediante a exploração de vulnerabilidades das pessoas, relacionadas às suas características comportamentais.

O engenheiro social, portanto, emprega engano, influência e persuasão na coleta de informações comerciais ou pessoais, explorando as fragilidades das vítimas. O principal motivo aqui é adquirir informações relevantes que possam permitir-lhe obter acesso não autorizado a um sistema de valor e às informações que nele residem. Para o diretor técnico da *Symantec Security*, apenas cerca de 3 por cento dos *malwares* são lançados com o objetivo de explorar uma falha técnica, os outros 97 por cento estão tentando enganar um usuário através de algum tipo de esquema, que leva a uma exposição indevida de informações pessoais.

3.2.1 Phishing

Segundo Castro (2013) técnica mais utilizada de maneira desonesta por cibercriminosos para enganar internautas, fazendo com que lhe forneçam suas senhas, informações bancárias ou acesso a seu computador por meio de um *software* que ele mesmo o convenceu a instalar . O *phishing* pode ser traduzido como "pescaria", tem o intuito de aguçar algum sentimento que faça com que o usuário aceite e realize as operações solicitadas como quando uma página de *login* falsa de um *site* social popular, por exemplo, Facebook, Yahoo, *sites* de

leilões e processos de pagamento *on-line*. É enviada por um engenheiro social para um usuário comum em uma forma de *e-mail* ou páginas na *web*, dando início a um ataque. Essas mensagens ou *sites* são criados para se assemelhar ao site real, tornando quase impossível a identificação da tentativa de golpe. Seja o seguinte exemplo: uma mensagem de *e-mail* que solicita que o usuário realize algumas ações, como: "Você está prestes a exceder sua capacidade de armazenamento", "clique aqui para permanecer ativo". No momento que o usuário clica ou fornece as informações necessárias, imediatamente as informações dos usuários são capturados e enviados para a página do engenheiro social.

3.2.2 Smishing

O *smishing* é uma forma de *phishing* que usa serviços de mensagens curtas SMS ou mensagens de texto longas que são enviadas para os *smartphones*. O *smishing* obteve seu nome da tecnologia de mensagens de teste SMS. Existem dois processos principais para os golpes do *phishing*. O primeiro envolve receber uma mensagem de texto que supostamente originou-se de uma fonte conhecida e confiável, como seus banqueiros ou o administrador do sistema. O segundo envolve o recebimento de uma mensagem de texto sobre sua identidade ter sido roubada ou o número da conta ter sido congelado.

Em seguida, os golpistas encaminham você para um site ou número de telefone para a verificação das informações da conta. Os golpistas ao receber as informações vão fazer transações na conta ou abrir um novo cartão de crédito em nome da vítima. Outra tática usada pelos *smishers* é ameaçar a vítima e começar a cobrar uma tarifa diária pelo uso de um serviço, caso ela não clique em um link e insira as informações pessoais solicitadas.

3.2.3 Vishing

Quando um engenheiro social cria um sistema de voz automática para fazer chamadas de voz a usuários de telefone solicitando informações privadas é designado *vishing* ou *phishing* por voz. A intenção é a mesma que o *phishing* por *e-mail* ou por *smishing* por SMS. A chamada de voz cria uma sensação de urgência para que o usuário tome medidas e faculte informações adicionais.

Usando uma combinação de táticas de medo e manipulação emocional, eles tentam induzir as pessoas a abrirem suas informações. Esses *vishers* até criam perfis falsos de identificação de chamadas (chamados de 'falsificação de identificação de chamadas'), o que faz com que

os números de telefone pareçam legítimos.

3.2.4 Spam

Há algumas divergências quanto ao significa da palavra SPAM, mas a mais aceita é que ela é uma sigla para o termo (Sending and Posting Advertisement in Mass), que numa tradução livre significa “Enviar e postar publicidade em massa” (ALENCAR, 2016).

Assim, *spam* é o termo usado para se referir às mensagens eletrônicas que são enviadas para você sem o seu consentimento que, geralmente, são despachadas para um grande número de pessoas.

Esse tipo de “*e-mail* indesejável” contém, em sua grande maioria, propagandas. Neste caso, o *spam* também recebe o nome de Mensagem Comercial Não-Solicitada (UCE). No entanto, em outras ocorrências, essas mensagens contêm conteúdos mais agressivos (como vírus) e ainda conseguem obter suas informações pessoais — como dados bancários, porexemplo.

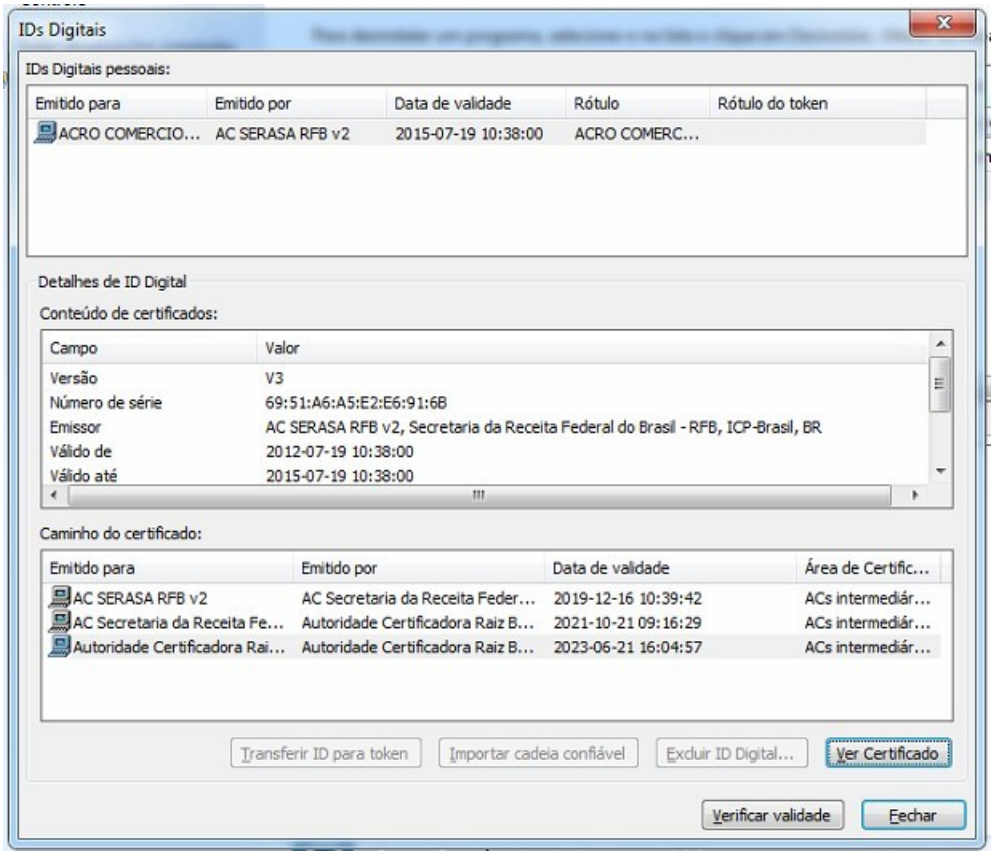
Segundo Schefler (2014), no Brasil ainda não é crime enviar *spam*, mas esta prática está sendo atualmente discutida no senado e pode virar lei. Mesmo sua proibição ainda não sendo oficial, sua prática acaba sendo regulamentada, pois o *spammer* é mal visto, seu produto ou empresa é desacreditado, seu provedor, domínio ou IP pode ser incluído nas listas de bloqueio dos administradores de rede. Por este motivo quase sempre o spam está ligado a práticas criminosas ou a ingenuidade do empreendedor.

3.3 Certificados Digitais e Infraestrutura de Chave pública

Um certificado digital como ilustrado na Figura 1, é um arquivo de computador que contém um conjunto de informações referentes a entidade para o qual o certificado foi emitido, seja uma empresa, pessoa física ou computador. Um certificado digital normalmente é usado para ligar uma entidade a uma chave pública. Para garantir a segurança, a certificação se baseia em dois possíveis modelos. No caso de uma Infraestrutura de Chaves Públicas (ICP), o certificado é assinado pela Autoridade Certificadora (AC) que o emitiu e no caso de um modelo de Teia de Confiança, como o PGP, o certificado é assinado pela própria entidade e assinado por outros que dizem confiar naquela entidade. Em ambos os casos, as assinaturas contidas em um certificado são atestamentos feitos por uma entidade que diz confiar nos dados contidos naquele certificado. No dia a dia, utiliza-se o certificado digital para efetivar transações e operações de maneira

remota, as quais não são possíveis de se autenticar de maneira presencial. Assim, com o uso do certificado, as partes têm a certeza de que enviam e recebem informações das pessoas certas, eliminando inúmeros riscos que a comunicação de dados via *internet* pode representar.

Figura 1 – Certificado Digital



Fonte: http://vciga.dyndns.org/manual/index.html?CertificadosDigitais.html

Um certificado normalmente inclui:

1. Informações refentes a entidade para o qual o certificado foi emitido (nome, email, CPF/CNPJ, PIS etc).
2. A chave pública referente a chave privada de posse da entidade especificada no certificado.
3. O período de validade.
4. A localização do "centro de revogação"(uma (URL) para download da CRL, ou local para uma consulta OCSP).
5. As assinaturas das AC/entidades que afirma que a chave pública contida naquele certificado confere com as informações contidas no mesmo.

3.3.1 Criptografia assimétrica e simétrica

A criptografia simétrica é a técnica mais antiga e mais conhecida. Uma chave secreta, que pode ser um número, uma palavra ou apenas uma sequência de letras aleatórias é aplicada ao texto de uma mensagem para alterar o conteúdo de uma determinada maneira. Conforme (SERAFIM, 2014), um sistema criptográfico deve ser seguro, mesmo que tudo sobre o sistema, exceto a chave, seja de conhecimento público .

O problema com chaves secretas está em trocá-las pela *internet* ou por uma grande rede e, ao mesmo tempo, impedir que caia em mãos erradas. Qualquer pessoa que conheça a chave secreta pode descriptografar a mensagem. Uma solução é a criptografia assimétrica, em que há duas chaves relacionadas a um par de chaves. Uma chave pública é disponibilizada gratuitamente a qualquer pessoa que queira enviar uma mensagem. Uma segunda chave privada é mantida em segredo, para que somente o dono saiba.

Qualquer mensagem (texto, arquivos binários ou documentos) que é criptografada usando a chave pública só pode ser decriptada pela respectiva chave privada. Qualquer mensagem que é criptografada usando a chave privada só pode ser descriptografada usando a chave pública correspondente.

Isso significa que você não precisa se preocupar em passar as chaves públicas pela *internet* (as chaves devem ser públicas). Um problema com a criptografia assimétrica, no entanto, é que ela é mais lenta do que a criptografia simétrica. Ela requer muito mais capacidade de processamento para criptografar e descriptografar o conteúdo da mensagem.

3.3.2 Assinatura e autenticação

Conforme Stallings (2006), uma assinatura digital é um mecanismo de autenticação que permite ao criador de uma mensagem anexar um código que atue como uma assinatura. A assinatura é formada tomando o *hash* da mensagem e criptografando-o a chave privada do criador. A assinatura garante a origem e a integridade da mensagem. Outro conceito importante da assinatura digital é a autenticação. A autenticação é o processo de verificar se a informação vem de uma fonte confiável. A criptografia e a autenticação, trabalham juntas nas assinaturas digitais. Dessa forma assinatura digital é um conjunto de operações criptográficas aplicadas a um determinado arquivo digital.

Além de garantir que o arquivo foi gerado por uma pessoa autorizada e devidamente

identificada, também confirma a origem e a integridade de determinado documento. Dessa forma, é possível visualizar se houve alguma alteração no documento eletrônico, por menor que ela tenha sido, o que o resguarda de eventuais interceptações que possam comprometer o seu conteúdo.

Por fim, a autenticação eletrônica é ainda uma ferramenta útil para autorizar os leitores finais de um documento, já que só terão acesso ao arquivo após passarem por um processo de confirmação de identidade. Essa característica é muito útil já que permite não apenas assegurar a veracidade do emissor do documento, mas também controlar quem serão os destinatários do arquivo enviado, mantendo o sigilo das informações a outraspessoas.

A assinatura digital é uma ferramenta de segurança da informação, e ela garante dois princípios básicos: a autenticidade e a integridade dos documentos. Isso é realizado em função de um processo altamente capaz de autenticar a autoria de determinado documento em meio eletrônico.

Conforme as ações foram se aperfeiçoando em ambiente virtual, muitos processos passaram a exigir a autenticidade e a integridade que a assinatura digital pode conferir. Segundo Gandini *et al.* (2002), para ser considerada uma assinatura digital, ela deve estar presente necessariamente em um documento eletrônico e é por esse motivo que ela pode ser chamada também de assinatura eletrônica. Nesse processo, a autenticação dos documentos é feita a partir do uso da técnica da criptografia assimétrica invertida.

3.3.3 Infraestrutura de chaves públicas

Segundo Vivian (2019), uma ICP é composta por um conjunto de entidades (máquinas, pessoas, servidores, etc.), políticas (conjunto de normas e práticas que regem uma ICP), mecanismos criptográficos e técnicas de gestão. O objetivo da ICP é fazer com que a utilização de criptografia de chave pública facilite, tendo como principais componentes as autoridades certificadoras, autoridades de registro e o repositório.

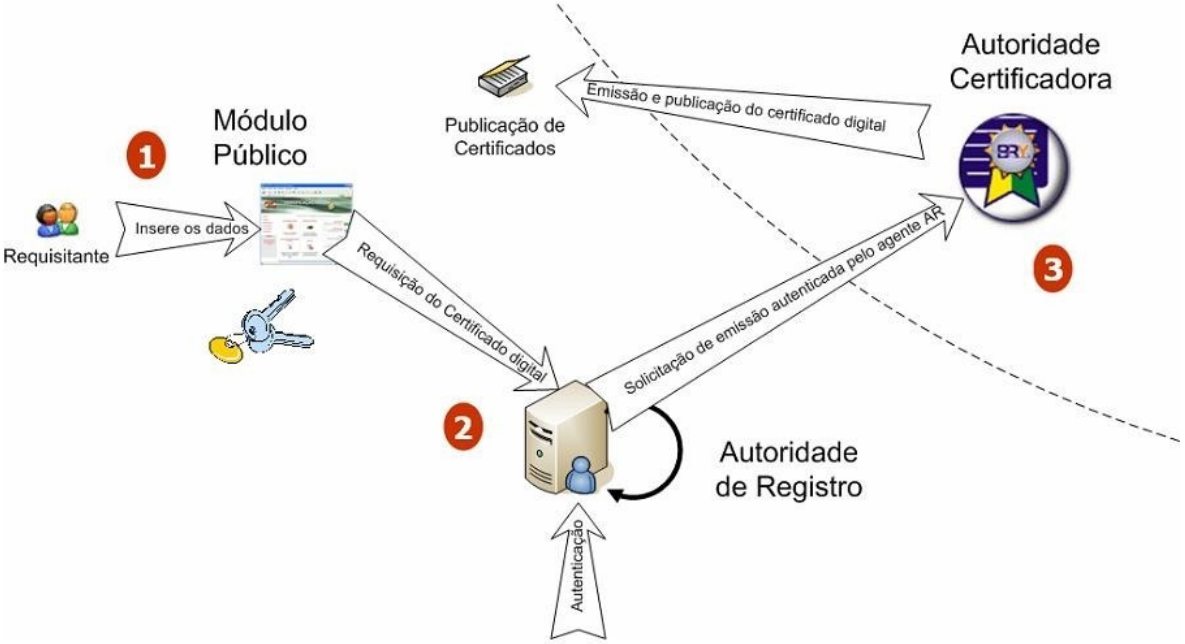
As Autoridades Certificadoras (ACs) são responsáveis por gerenciar o ciclo de vida dos certificados digitais, controlando os processos de solicitação, emissão e revogação dos mesmos.

Uma ICP pode ser composta de uma única AC, mas, em algumas situações, é preciso que algumas tarefas sejam delegadas a outras entidades para minimizar a carga de atividades da AC.

Nestes casos, a AC Raiz delega às ACs intermediárias a responsabilidade de emissão de certificados, reduzindo sua carga de trabalho, facilitando o crescimento da estrutura e aumentando a abrangência e o escopo das emissões de certificados digitais. Se autorizado pela AC Raiz, uma AC Intermediária pode delegar a tarefa de emissão para outras ACs que estiverem abaixo dela.

A Autoridade de Registro (AR) e o Repositório de Certificados Digitais também recebem tarefas delegadas da AC Raiz. À AR cabe a tarefa de verificar o conteúdo de requisições de certificados, enquanto que o Repositório de Certificados Digitais tem como objetivo publicar os certificados digitais e as listas de certificados revogados emitidos por uma ou mais ACs. Todo esse fluxo é ilustrado na Figura 2.

Figura 2 – Infra-estrutura de chaves públicas



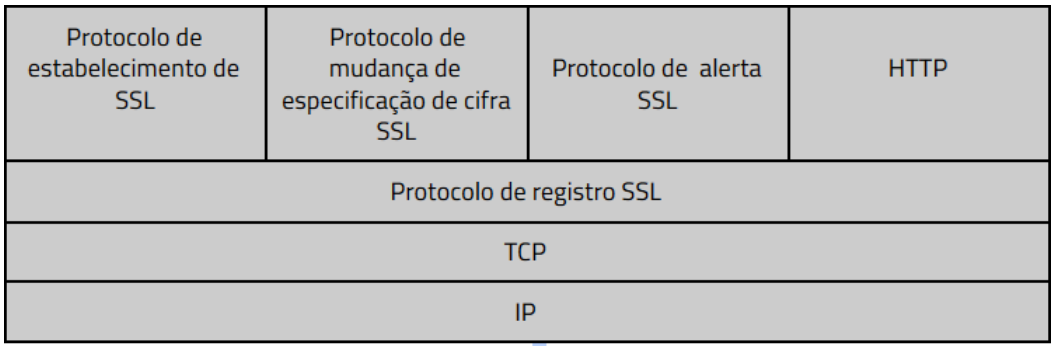
Fonte: https://www.gta.ufrj.br/grad/07_2/delio/Infra-estruturadeChavesPblicas.html

3.3.4 SSL/TLS e HTTPS

Segundo Stallings (2006), o SSL(Secure Sockets Layer) é projetado para utilizar TCP para ofecer um serviço seguro e confiável de ponta a ponta. O SSL não é um protocolo isolado, contendo mas duas camadas de protocolo, conforme ilustra a figura 3.

É oferecido serviços básicos de segurança para vários protocolos de camada superior. Em particular, o Hypertext Transfer Protocol(HTTP), que oferece o serviço de transferência para interação cliente/servidor *Web*, pode operar em cima do SSL. Três protocolos de camada

Figura 3 – Pilha de protocolos SSL



Fonte: Elaborada pelo autor

superior são definidos como parte do SSL: o protocolo de estabelecimento de sessão(Handshake Protocol), o protocolo de mudança de especificação de cifra (Change Cipher Spec Protocol) e o protocolo de alerta (Alert Protocol). Esses protocolos específicos do SSL são usados para gerenciamento de trocas SSL.

O sucessor do SSL é o Transport Layer Security (TLS) (Transport Layer Security), embora o protocolo SSL tenha sido descontinuado com o lançamento do TLS 1.0 em 1999, ainda é comum se referir a essas tecnologias relacionadas como "SSL"ou "SSL/TLS". A versão mais atual é o TLS 1.3, definido na RFC8846 (2018).

3.3.4.1 SSL/TLS e navegação segura na Web

No protocolo HTTP é utilizado para enviar e receber informações na *web*. Segundo Russell (2019), um *site* HTTPS público configurado corretamente inclui um certificado SSL / TLS assinado por uma autoridade de certificação pública. Os usuários que visitam um *site* HTTPS podem ter certeza de:

- Autenticidade. O servidor que apresenta o certificado está na posse da chave privada que corresponde à chave pública no certificado.
- Integridade. Os documentos assinados pelo certificado (por exemplo, páginas da *web*) não foram alterados em trânsito por um homem no meio .
- Criptografia. As comunicações entre o cliente e o servidor são criptografadas.

Devido a essas propriedades, SSL / TLS e HTTPS permitem que os usuários transmitam com segurança, informações confidenciais, como números de cartão de crédito, números de previdência social e credenciais de login pela *internet*, e verifique se o *site* para o qual eles estão enviando é autêntico. Com um *site* HTTP inseguro, esses dados são enviados como texto sem formatação, prontamente disponíveis para qualquer "bisbilhoteiro"com acesso ao fluxo de

dados. Além disso, os usuários desses *sites* desprotegidos não têm garantia de terceiros confiável de que o site que estão visitando é o que afirma ser.

Figura 4 – Certificado SSL/TLS

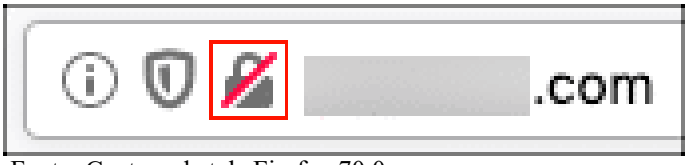
Fonte: Captura de tela Firefox 70.0

Dado a ilustração da Figura 4:

- Um ícone de cadeado à esquerda da (URL). Dependendo do seu navegador e do tipo de certificado que o site instalou, o cadeado pode ser verde e / ou acompanhado por informações de identificação sobre a empresa que o administra.
- Se mostrado, o protocolo no início da (URL) deve ser https : // , não http : // . Observe que nem todos os navegadores exibem o protocolo.

Os navegadores de desktop modernos também alertam os visitantes para *sites* inseguros que não possuem um certificado SSL / TLS. A captura da Figura 5 é de um site inseguro visualizado no Firefox e mostra um cadeado riscado à esquerda do (URL):

Figura 5 – Certificado SSL/TLS



Fonte: Captura de tela Firefox 70.0

3.4 Internet Banking

Segundo Oliveira (2000), a *internet banking* é a nova maneira para acesso ao seu banco que se torna disponível através de meios eletrônicos, para distribuir quase todos os seus produtos e serviços, os quais eram anteriormente oferecidos de modo exclusivo através de atendimento pessoal em agências bancárias.

Diante do ritmo de vida acelerado, a necessidade de otimizar tarefas para a praticidade de serviços bancários se tornou essencial, porém, também as instituições bancárias tiveram que buscar por segurança, mobilidade e conveniência os clientes bancários se mostram mais confiantes nos canais digitais e o *mobile banking* passa a ser a opção preferida para transações

e outros serviços. Em contrapartida, os bancos têm investido cada vez mais em tecnologia e buscam oferecer soluções e diferenciais que os deixem confortável (FEBRABAN, 2018).

Mais de 140 milhões de pessoas mantinham algum relacionamento bancário, como contas de depósitos à vista, contas-correntes, contas de depósitos de poupança e contas-correntes de depósitos para investimento. Esse número corresponde a 86,5 por cento das pessoas com mais de 15 anos (CENTRAL, 2018).

Segundo o diretor da Federação Brasileira de Bancos (Febraban) Gustavo Fosse, os números mostram que o mobile *banking* se consolida como o canal preferido dos brasileiros. "Por conta da facilidade, percepção de segurança e barateamento da tecnologia, cada vez mais clientes estão usando *smartphones*. Pagar um boleto no celular hoje é muito mais prático que na própria *internet*", afirma.

O número de postos, agências e caixas de autoatendimento bancários vem reduzindo no Brasil, enquanto o acesso a serviços financeiros digitais, através de celular, por exemplo, cresce significativamente, é o que aponta um relatório Febraban (2018). As transações por aplicativos, *internet banking* e *call centers* registraram expansão significativa 21 por cento, de 2016 a 2017 representam 66 por cento do total das transações realizadas.

Os bancos têm investido na segurança utilizando avisos de movimentações via SMS para o proprietário, chave de segurança nas transações. *Personal Identification Number (PIN)*, *Quick Response (QRCode)* para confirmações e liberação de transferências bancárias. Conforme Santiago (2013), o uso da criptografia com certificação digital é de fundamental importância para segurança da *internet* banking e são as tecnologias que mais destacam diante as outras tecnologias abordadas, pois utilizam os mecanismos mais eficazes no combate a fraudes do sistema.

Os *sites* das instituições bancárias na *aba* de segurança tratam pontos como: dicas de segurança, denuncie aqui, aprenda a evitar fraudes na *internet*, aprenda a evitar o golpe da página, previna-se do roubo de dados, como citado está sendo usado diversas técnicas para dificultar que criminosos furtem dados privados de correntistas.

3.5 Bancos Digitais

Desde 2016, os bancos digitais vêm buscando seu espaço no mercado brasileiro, diferentemente dos bancos tradicionais onde você pode fazer uma gestão parcial da sua conta pelo aplicativo ou site, são instituições que não possuem atendimento presencial. Da abertura

da conta bancária ao esclarecimento de dúvidas, todas as necessidades dos clientes podem ser resolvidas pela *internet*. Sem fila, sem burocracia e sem precisar sair de casa.

São novas propostas, algumas ainda em consolidação que estão em busca de resolver problemas como tarifas elevadas, falta de transparência, conflito de interesses, entre outros. O objetivo é ter mais agilidade no atendimento e, assim, atingir um número maior de consumidores. Os principais serviços que eles oferecem são:

- conta-corrente digital sem tarifa.
- cartão de crédito, em muitos casos sem anuidade.
- investimentos.
- seguros.
- consórcios.
- empréstimos.

Existem diversos bancos digitais atualmente (Nubank, Inter, Banco Original, Neon, Next, Agibank), porém, segundo (PROMOBIT, 2019) os dois mais populares são:

Nubank: Começou com um serviço de cartão de crédito sem anuidade, mas atualmente oferecem também a opção "NuConta", uma conta digital sem tarifas e que é totalmente gerenciada pelo aplicativo. É possível realizar a abertura online, pelo (app) Nubank, disponível para *Iphone(IOS)* e *Android*. A conta oferece a função de débito, além de saques na rede Banco24horas, porém é cobrado uma taxa de seis reais e cinquenta centavos a cada saque. A "NuConta"não possui taxa de manutenção e o valor deixado na conta-corrente possui um rendimento automático, além de não ser cobrado taxas de transferências para outrosbancos.

Banco Inter: É uma instituição financeira que oferece a abertura de contas digitais sem cobrança de tarifas. A abertura pode ser feita online pelo (app) do banco, disponível para *Iphone(iPhone OS (IOS))* e *Android*. O Inter não tem tarifas de manutenção ou transferências, não cobra pelos saques na rede Banco24horas. A instituição oferece pagamentos por meio de *QRCode* e é possível gerar boletos e fazer depósitos de cheques por meio de imagem.

4 TRABALHOS RELACIONADOS

Este Capítulo apresenta trabalhos que analisam fraudes relacionadas ao *phishing* que ocorreram através do *internet banking* na área da segurança da informação, apresentando suas semelhanças e diferenças no que pretende ser desenvolvido.

4.1 Um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de Instituições Bancárias

O trabalho de Klettenberg (2016) trata sobre a segurança da informação e a engenharia social. O trabalho analisa a segurança da informação de usuários de instituições bancárias a partir da perspectiva da engenharia social mostrando 132 correntistas de uma instituição bancária vitimas de fraudes eletrônicas. Utilizando as características do usuário e o seu grau de entendimento sobre o assunto. Nesse trabalho são obtidos dados de correntistas que foram fraudados e será apresentado uma análise de usuários, para entender bem todas as suas características e o que os levaram a terem sido vítimas de fraudes bancárias. Também é mostrado como são desenvolvidos as táticas de ataques para enganar correntistas criadas pelos *phishers*, havendo assim um maior entendimento de como funciona o ataque e como a vítima interpreta quando recebe alguma tentativa de *phishing*.

4.2 Smishing ameaça contra dispositivos móveis

O trabalho de Yeboah-Boateng (2014) avalia os três principais ataques da engenharia social *Phishing*, *Smishing* e *Vishing* aplicados a dispositivos móveis, são examinadas as implicações do comportamento do usuário final para mitigar os riscos representados pelo uso de dispositivos móveis para serviços e instalações on-line mostrando como ocorrem. Yeboah observou e entrevistou estrategicamente 20 usuários finais sobre seus conhecimentos, percepções e comportamento quando confrontados com situações de ataques na web.

A forma com que são tratadas as questões da engenharia social e principalmente o *Smishing* é de grande importância para esse trabalho, visto que o *smishing* é muito praticado no Brasil. Essa pesquisa irá mostrar maneiras que *phishers* usam desse ataque para benefício próprio.

4.3 Segurança de *e-banking* Internet Hacking Phishing Attacks

Segundo Alsayed (2017) desde a introdução do *internet banking* no setor bancário, muitos usuários descobriram formas de usar o *e-banking*, com isso, também abriram novas possibilidades de riscos dos seus dados financeiros. O autor trata a segurança como uma preocupação frequente para bancos e usuários, também são apresentados os principais ataques de *phishing* e como correntistas devem se defender via web. A relação com esse trabalho é a forma de como os *phishers* tentam roubar os dados dos usuários e realizar fraudes financeiras, explicando como os usuários do banco podem proteger suas transações on-line com soluções de segurança.

4.4 Comparação dos trabalhos relacionados

O Quadro 1 faz uma comparação entre os três trabalhos relacionados com este trabalho sobre os seguintes pontos: técnicas de engenharia social utilizadas, se foi feita pesquisa de campo e o objetivo da pesquisa. Pode ser notado que todos os trabalhos avaliam o uso de *phishing*, porém, Yeboah abordou também *vishing* e *smishing*. Neste trabalho será abordado o *phishing* como todos os trabalhos, mas serão abordadas algumas práticas de *smishing*. O trabalho de Yeboah relata também técnicas de ataques e como elas vêm sendo usadas pelos engenheiros sociais. Os dois primeiros trabalhos executam pesquisa de campo abordando os perfis dos correntistas que foram fraudados igualmente como foi executado neste trabalho, inclusive os questionários executados por eles serviram de referência para elaboração do formulário aplicado neste trabalho. O objetivo principal dos três trabalhos colaboram bastante com que foi feito neste trabalho que é a análise do perfil de correntistas fraudados e a segurança que é oferecida pelos sistemas bancários.

Quadro 1 – É ilustrado as especificações de cada trabalho relacionado

Trabalhos	Tecnicas Engenharia Social	Pesquisa de campo	Principal Objetivo
Klettenberg	Phishing	Sim	Análise do perfil de correntistas fraudados e Segurança
Yeboah	Phishing,Vishing,Smishing	Sim	Tecnicas de Engenharia Social
Alsayed	Phishing	Não	Segurança
Este trabalho	Phishing, Smishing	Sim	Análise do perfil de correntistas fraudados e Segurança

Fonte: Elaborada pelo autor

5 METODOLOGIA

Esta seção destina-se a demonstrar os métodos aplicados na coleta e tratamento dos dados obtidos com intuito de alcançar resultados e as suas respectivasrepercussões.

5.1 Abordagem e metodologia da pesquisa

Objetivo da pesquisa foi desenvolvido a partir de uma metodologia quali-quantitativa com substrato em dados obtidos no ambiente da pesquisa, que serão descritos e quantificados.

Considerando as diretrizes retratadas pelos autores Gil (2002) e Moreira (2005), a metodologia utilizada para o desenvolvimento do estudo é classificada como exploratória e descritiva. Na análise exploratória, para Gil (2007), o objetivo é ampliar o conhecimento sobre um determinado assunto tratado com intuito de promover modelos, enquanto que na pesquisa descritiva se procura descrever as características determinantes de uma população ou fenômeno, ou ainda, correlacionar variáveis.

Tais conceitos foram utilizados como alicerces para o desenvolvimento de uma pesquisa bibliográfica com intuito de identificar nas produções científicas os conceitos e cenários norteadores, principalmente, da segurança da informação, engenharia social e suas técnicas, os riscos e ameaças informacionais, relacionando-os com a área da Ciência da Informação.

Como mostra o Quadro 2, optou-se por desenvolver a pesquisa em quatro fases distintas.

A primeira fase irá identificar técnicas abordadas pelos bancos para dificultar as ações de engenheiros sociais, visto que nos últimos anos cresceram as práticas de golpes no uso da *internet banking* impactando no maior investimento na área da segurança. Será mostrado passo a passo como ocorre a liberação do aplicativo para cada instituição e os requisitos de segurança que elas impõem até que possa ser feito uma transação com sucesso.

A segunda fase engloba a análise dos *sites* das três maiores instituições bancárias do Brasil, segundo Globo (2018): Itaú, Banco do Brasil e Bradesco. Esta fase tem o intuito de demonstrar quais informações sobre segurança estão disponíveis aos usuários e correntistas.

A terceira fase tem objetivo de mostrar como ocorrem práticas de ataques a usuários que possuem contas bancárias, visando mostrar técnicas usada por engenheiros sociais usando (SMS, Redes Sociais, Email, Anúncios de promoções, Telas Fakes) para obter lucro diante de pessoas que não têm o conhecimento dessas práticas. Essa fase tem o intuito de alertar os

Quadro 2 – É exibido atividades e objetivos de cada fase

Pesquisa	**1º Fase**	**2º Fase**	**3º Fase**	**4º Fase**
Atividade	Será exibido métodos que foram melhorados pelos bancos para maior segurança das transações bancárias	Analisar os sites das três maiores instituições bancárias no quesito segurança	Formas de ataques Phishing Smishing	Análise dos usuários dado a pesquisa
Objetivo	Mostrar métodos de segurança dos bancos na atualidade	Demonstrar quais informações sobre segurança da informação estão disponíveis nos sites	Informar usuários bancários mostrando as formas de ataque	Analisar as principais características dos correntistas vítimas dos engenheiros sociais

Fonte: Elaborada pelo autor

correntistas, caso algum dia for abordados por alguma dessas tentativas facilite a identificação, evitando uma possível perda de dados confidenciais.

A quarta envolveu a aplicação de um questionário com usuários que realmente foram vítimas de engenheiros sociais. Foram realizadas entrevistas através de um formulário *online* com perguntas de múltiplas escolha e subjetiva com intuito de conhecer melhor o perfil dos usuários suscetíveis às técnicas do *phishing*. Foi coletada uma amostra de quinze correntistas, cujas informações sigilosas foram comprometidas pelo ataque.

A pesquisa foi realizada no período de 04/11/2019 a 11/11/2019. No contato inicial foi descrito o propósito da pesquisa científica, os seus conceitos-chave, e em seguida foi aplicado o formulário, após a concordância da vítima em participar.

As entrevistas foram descritas integralmente, porém, para o que se pretendia com este trabalho foram consideradas algumas passagens relevantes para se atingir os objetivos da pesquisa. Optou-se por não anexar a transcrição integral das entrevistas pela quantidade de páginas resultantes. Para compor a tabulação dos dados obtidos com as entrevistas, foi utilizado como ferramenta o Google (Apresentações Google, Formulários Google), permitindo a constituição dos gráficos e tabelas.

5.2 Procedimento da coleta de dados

Os dados da amostra foram obtidos basicamente em 3 ambientes diferentes. O primeiro foi através "Facebook"verificando páginas de *phishing* onde foram encontrados vários relatos de usuários que foram vítimas dos golpes e outros que quase foram enganados, mas foram

alertando por outros usuários. O segundo foi realizado através de pesquisas no "YouTube"de "alertas"a tipos de golpe em que foi observado diversos comentários de correntistas fraudados. Por fim, o terceiro foi através da divulgação da pesquisa em outras faculdades, entre amigos e nas redes sociais "Instagram"e "Facebook".

Em relação à fraude: estado que os correntistas residia na época do golpe (Santa Catarina, Distrito Federal, Ceará e Rio Grande do Sul); tipos de golpes eletrônicas (internet e cartões de débito e crédito); modalidades de fraude considerando os tipos (auxílio de terceiro, token, central de atendimento e internet - internet banking), o canal explorado pelo fraudador para realizar a fraude (internet, smartphones ou caixas eletrônicos); tipo de transação fraudulenta (pagamento de boletos, transferências eletrônicas, saques ou compras) e a forma como ocorreu a fraude (ação indireta do engenheiro social com envio de *phishing*, ou ação direta do engenheiro social, como a troca de cartão ou a retenção do cartão); Quanto ao correntista fraudado: gênero, idade, grau de escolaridade, classe social, estado que habitava na época do golpe.

Sobre a fraude: 1-frequência com que o usuário utiliza o aplicativo (nenhuma, 3 ou 7, ou acima de 7 vezes por semana), 2- o que levou a fornecer as informações bancárias (estava compartilhando informações com banco, perca do cartão, premiação do site, não sabe como obtiveram os dados), 3- quando foi notado que as informações tinham sido roubadas (SMS e APP, ligação do setor bancários, acesso à conta e não ter valor disponível), 4- quais dados bancários foram fornecidos (dados bancários, cartão de crédito, os dois), 5- antes do golpe era pesquisado por medidas de segurança propostas pela instituição, as perdas foram ressarcidas pelo banco, 6- possibilidade de haver outro sucesso do engenheiro social em alguma tentativa de *phishing* com o correntista.

6 ANÁLISE DOS DADOS, RESULTADOS E REPERCUSSÕES

A seguir serão apresentadas as análises e repercussões de cada fase da pesquisa com intuito de alcançar os objetivos traçados.

6.1 Análise das medidas de segurança das três maiores instituições bancárias do Brasil

Neste Capítulo serão apresentados os resultados encontrados a partir do estudo das três maiores Instituições Bancárias do Brasil, Banco do Brasil, Itaú e Caixa Econômica Federal, demonstrando quais informações sobre medidas de segurança cada instituição utiliza para evitar fraudes bancárias.

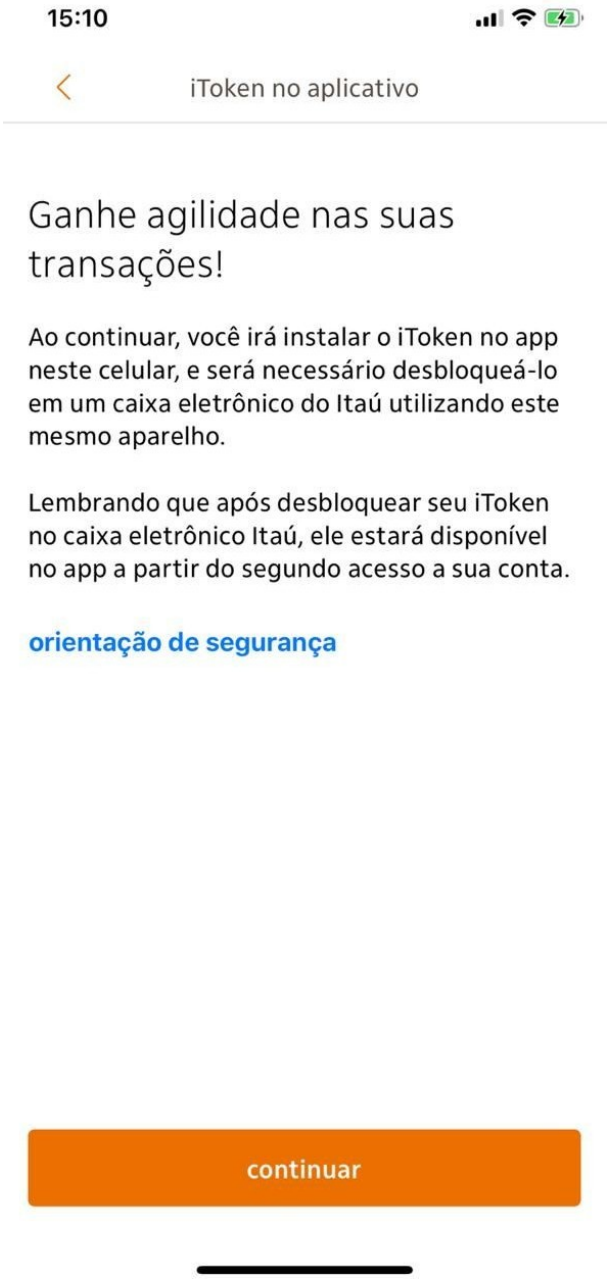
6.1.1 Liberação do app no banco Itaú em dispositivos móveis

Primeiramente o usuário terá que fazer a solicitação da liberação do *itoken* pelo aplicativo, nesse passo é pedido somente que o usuário coloque a senha de 6 dígitos do seu cartão como mostra na Figura 2. Correntista terá que ir a um caixa eletrônico do Itaú com o mesmo aparelho celular que foi realizada a solicitação do *itoken* e deve seguir os seguintespassos:

1. Acesse sua conta com seu cartão da conta-corrente (não é possível habilitar usando somente a biometria).
2. Clique em "ver agora" na mensagem de desbloqueio do *itoken* . Caso a mensagem não seja exibida, acesse: produtos e serviços- outros> segurança> *itoken* no (app) celular-desbloqueio.
3. Confirme o desbloqueio apenas se foi você quem realizou a instalação do *itoken* , clicando em "sim".
4. Siga os passos indicados e posicione seu celular para ler o código *QRCode* que aparecerá na tela do caixa eletrônico.
5. Para finalizar, digite o número do *itoken* gerado no seu celular no campo habilitado no caixa eletrônico e clique em "ok".

Para que seu *itoken* esteja disponível, após habilitar no caixa eletrônico, você deve acessar o (app) Itaú com sua agência, conta e senha eletrônica. Em seguida, basta sair da conta para que o código *itoken* comece a ser gerado normalmente.

Figura 6 – App Itaú - Liberação iToken



Fonte: (ITAU, 2019).

6.1.2 Liberação do (app) no banco Bradesco nos dispositivos móveis

Como utilizar o *Token* no Celular:

1. Acesse o Aplicativo Bradesco instalado em seu aparelho.
2. Selecione a opção Chave de Segurança.
3. Digite o *PIN* (senha de 4 dígitos cadastrados).
4. Digite no Canal de Atendimento, a chave (senha numérica) apresentada novisor do seu celular.

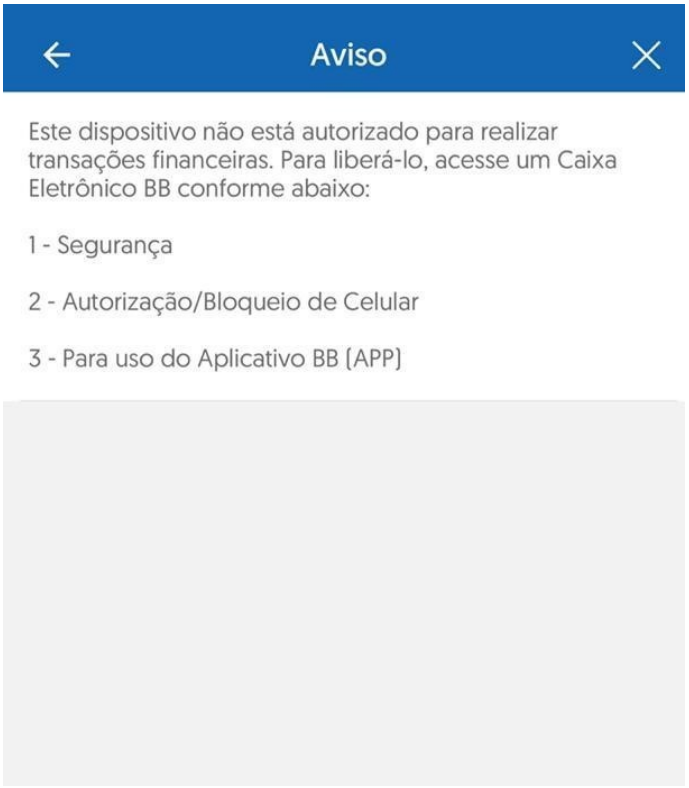
Figura 7 – Site Bradesco - Liberação Token

Fonte: (BRADESCO, 2019).

6.1.3 Liberação do app no banco do Brasil para dispositivos móveis

Para autorizar o *smartphone*, será necessário acessar sua conta no (app) com a senha de 8 dígitos e solicitar o link de liberação, que será enviado para o número de celular autorizado. Para isso, o chip com o número de celular cadastrado deve estar inserido no *smartphone* a ser liberado. No caso de *smartphone* com sistema operacional *Android*, não há necessidade de clicar no link recebido para concluir a autorização. Para *smartphones* com sistema operacional *IOS* há necessidade de clicar no link recebido.

Figura 8 – App Banco do Brasil - Transação Bancária



Fonte: (BRASIL, 2019).

O Quadro 3 compara as técnicas de liberação do (app) das principais instituições bancárias. Pode ser visto que as três instituições bancárias utilizam técnicas diferentes. O banco Itaú usa *itoken* para solicitação da liberação do dispositivo, o banco Bradesco utiliza o *PIN* e o banco do Brasil utiliza o número de celular, ás três instituições utilizam de técnicas diferentes para fazer para a solicitação do dispositivo para transferência.

A confirmação em caixa da habilitação do aparelho celular para realizar transações bancárias é feita de forma diferente pelos bancos analisados. O banco Itaú utiliza o *QrCode* para confirmar que o mesmo dispositivo que solicitou a liberação é o que está sendo utilizado quando o correntista vai liberar no caixa, ou seja, há uma confirmação no caixa para confirmar a solicitação de liberação. O Bradesco utiliza a confirmação do *PIN*, no qual é confirmado o

Quadro 3 – Aspecto comparativo da liberação do App nas instituições bancárias

Banco	**Itoken**	**PIN**	**Número celular (SMS)**	**Validação QrCode (Caixa)**	**Validação PIN (Caixa)**	**Validação número (Caixa)**	**Biometria Digital**
Itaú	**X**			**X**			**X**
Bradesco		**X**			**X**		**X**
Brasil			**X**			**X**	**X**

Fonte: Elaborada pelo autor

código gerado no aplicativo do dispositivo, fazendo a confirmação desse código em caixa. O Banco do Brasil utiliza confirmação por SMS no qual o usuário ver a solicitação em caixa e faz a autorização do dispositivo. Todas ás três instituições possuem biometria digital como uma forma a mais de segurança em caixa.

É de grande importância os mecanismos de segurança para os bancos relacionados as autenticações de usuários. Os mecanismos de autenticação de usuários dividem-se em três categorias: baseados no conhecimento (o que se sabe), baseados em propriedade (o que se possui) e baseados em características (o que se é). O que você sabe: para se autenticar é necessário saber alguma informação para ser verificada, a senha pode ser um exemplo, é necessário que seja informada corretamente, do contrario não será autenticado, e terá o acesso barrado. O que você tem: para autenticação baseada em propriedade é caracterizado por um objeto físico que o usuário possui, comumente é um cartão ou *token*. É normal ver a combinação de autenticação baseada em propriedade *token* com autenticação baseada em conhecimento (senhas), fornecendo dois fatores de autenticação. O que você é: essa autenticação é mais rigorosa pois é necessário o reconhecimento de uma pessoa com base em alguma característica física, utilizando a biometria, um bom exemplo deste tipo é a leitura da impressão digital.

Diversas instituições financeiras já utilizam a autenticação baseada em três fatores. O aumento dos fatores no processo de autenticação, geralmente, aumenta o trabalho e a dificuldade de um atacante em executar uma fraude.

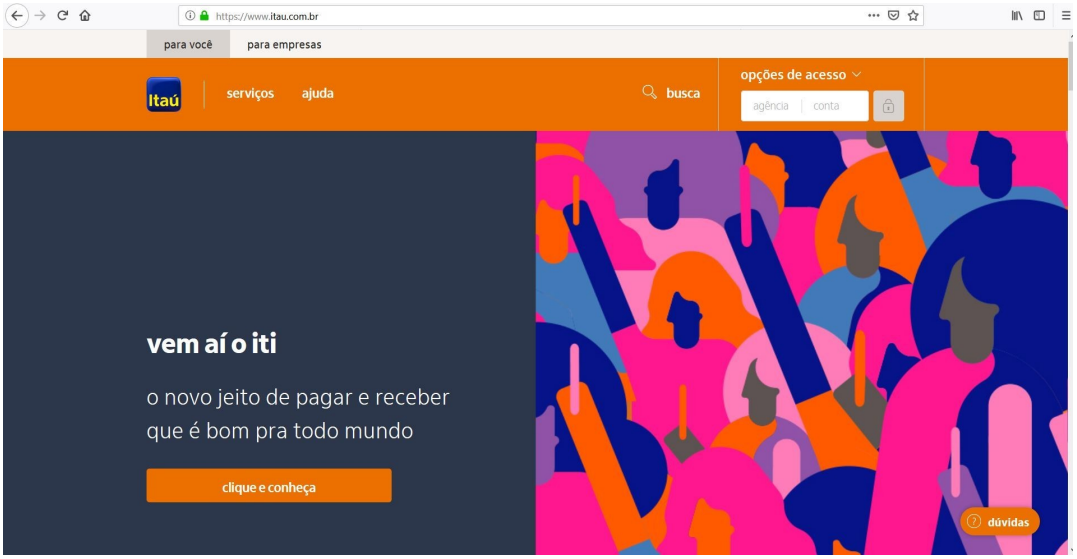
6.2 Análise dos sites das três maiores instituições bancárias do Brasil no quesito segurança

Os aplicativos nos celulares estão sendo bem mais usados para transações bancárias do que computadores e caixas físicos dado sua praticidade como já citado nesse trabalho. O banco Itaú é o único que retorna conteúdos relacionados a segurança no aplicativo móvel, enquantoo banco Bradesco e Brasil não abordam nada sobre o conteúdo em seus (app). Grande parte do conteúdo é abordado somente nos *sites*, por isso será analisado orientações sobre segurança na página *web* e a maneira que cada instituição trata esse ponto de suma importância, procurando exibir semelhanças e diferenças entre às três maiores instituições bancárias brasileiras.

6.2.1 Site do Banco Itaú

O *site* do banco Itaú, no ano de 2019 pode ser acessado por usuários que já possuem conta do banco ou não. Na página inicial é dada a opção de acesso para pessoa física ou jurídica. Também é disponibilizado um menu com opções "serviços", "ajuda", "busca", opções de acesso que são "agência"e "conta", mais abaixo novidade sobre um novo (app) chamado "Iti"e um "botão de dúvidas".

Figura 9 – Página inicial

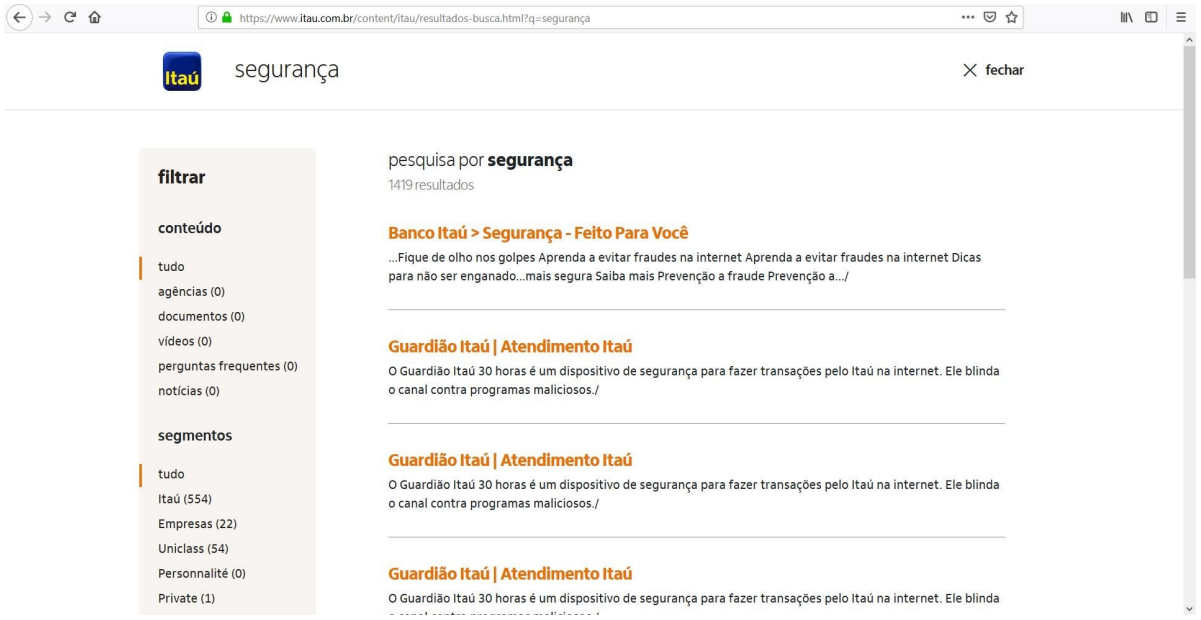


Fonte: (ITAU, 2019).

Quando foi usado a opção de "busca"com a seguinte palavra "segurança", foram retornados 1419 resultados da pesquisa, foram exibidos noticias relacionadas ao "guardião itaú", "atendimentos"entre outros tópicos para assegurar mais segurança do correntista que caso queira saber mais especificamente de algum desses tópicos terá mais como acessar o conteúdo clicando em algum dos link e sendo redirecionado para a página específica, é exibido também um menu lateral dividido em filtragem de "conteúdo"e "segmentos"contendo submenus com assuntos relacionados ao tema.

No rodapé da página, diante de várias opções são encontrados na categoria "ajuda"o quesito segurança, quando acessado é retornado um *slideshow* com alertas relacionados a liberação de *iToken* e como correntista consegue validar seu *itoken* para transações bancárias. É colocado um tópico "Canais Digitais"com seguintes assuntos: "Mais segurança para suas

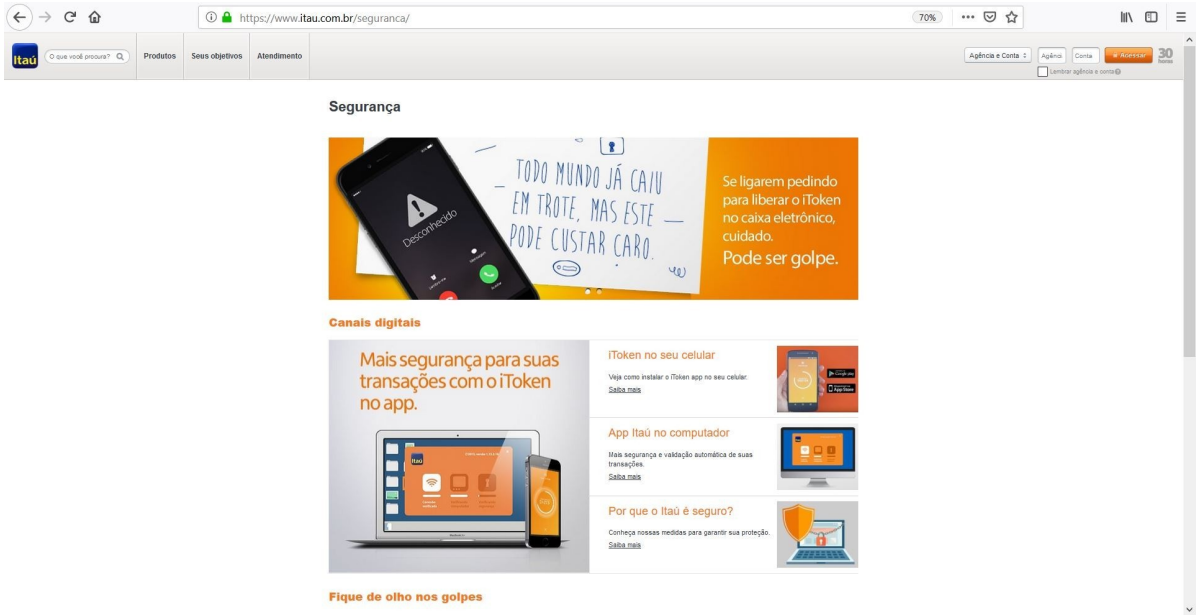
Figura 10 – Página inicial - Busca - Segurança



Fonte: (ITAU, 2019).

transações com o *iToken* no (app)", "*iToken* no seu celular", "App Itaú no computador"e "Por que o Itaú é seguro", todos eles levam a uma outra página explicando melhor cada ponto especificamente clicando em "Saiba mais".

Figura 11 – Página inicial - Rodapé - Ajuda - Segurança

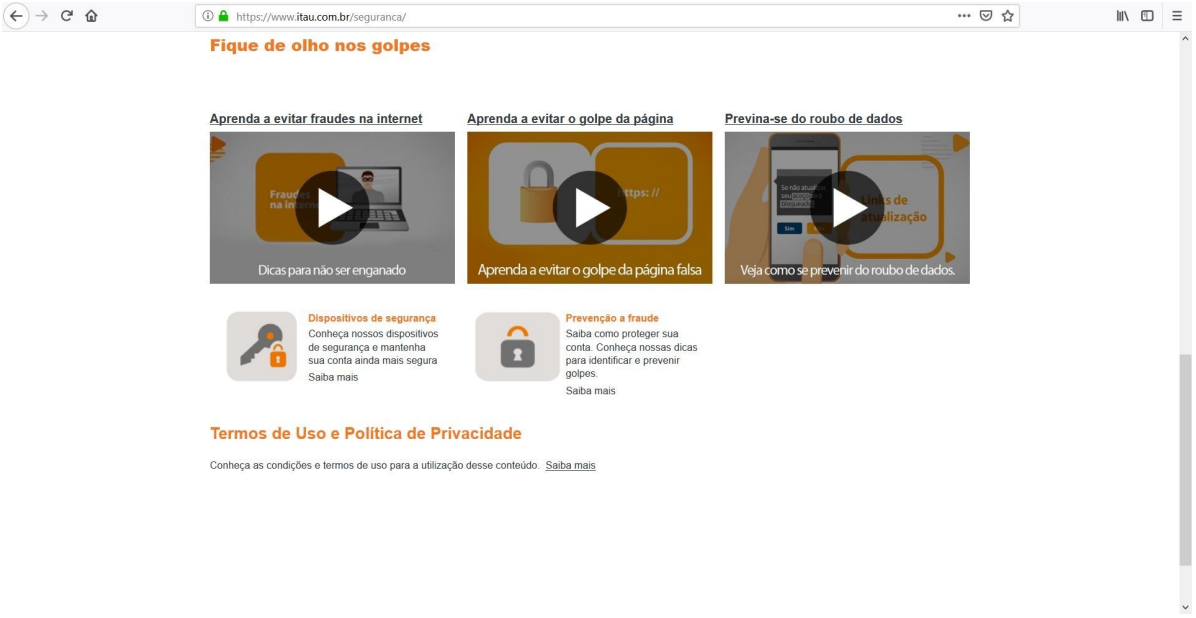


Fonte: (ITAU, 2019).

Um segundo tópico chamado "Fique de olho nos golpes"com três conteúdos em vídeo com os seguintes temas: "Aprenda a evitar fraudes na internet", "Aprenda a evitar o golpe da página", "Previna-se do roubo de dados"na qual caso o correntista queira saber mais é aberta

uma janela modal na página e então é exibido o vídeo explicando cada um de acordo com o selecionado. Mais abaixo é exibido um conteúdo relacionado a "Dispositivos de segurança"e "Prevenção a fraudes", para finalizar é exibido "Termos de Uso e Política de Privacidade".

Figura 12 – Página inicial - Rodapé - Ajuda - Segurança

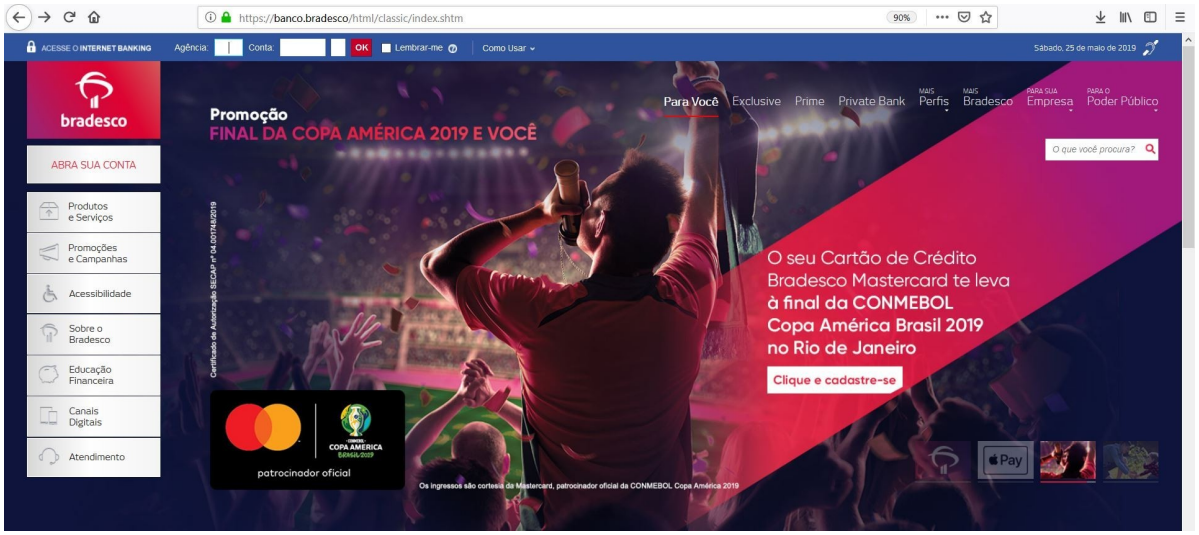


Fonte: (ITAU, 2019).

6.2.2 Site do Banco Bradesco

O *site* do banco Bradesco, no ano de 2019 pode ser acessado por usuários do banco ou não. Na página inicial é dada a opção de acesso "Para Você", "Exclusive", "Prime", "Private Bank", "Perfis(Aposentados, Crianças e etc)", "Para Empresa","Para o Poder Público". No menu superior é dado agência e conta para os correntistas logarem em suas respectivas contas, no menu lateral é exibido opções para "Abrir Conta","Produtos e Serviços","Promoções e Campanhas","Acessibilidade","Sobre o Bradesco","Educação Financeira","Canais Digitas","Atendimento".

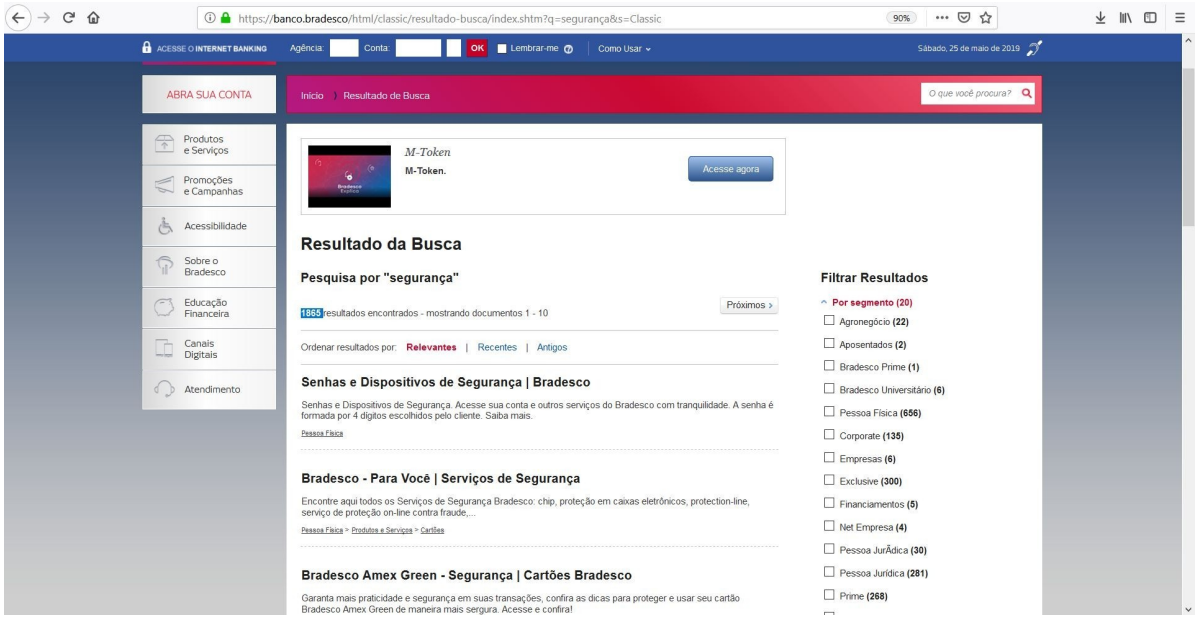
Figura 13 – Página inicial



Fonte: (BRADESCO, 2019).

Quando foi usado a opção "O que você procura"com a palavra "segurança", foram retornados 1865 resultado da pesquisa, o conteúdo principal está relacionado a senhas e dispositivos de segurança juntamente com algum tipo de segurança que o banco Bradesco oferece a seus correntistas. É exibido o mesmo menu no topo e lateral da página inicial, logo mais a direita é exibido um filtro com resultados específicos dado a busca separando-os por categoria como, por exemplo ("Pessoa Física","Empresas","Bradesco Universitário"entre outros).

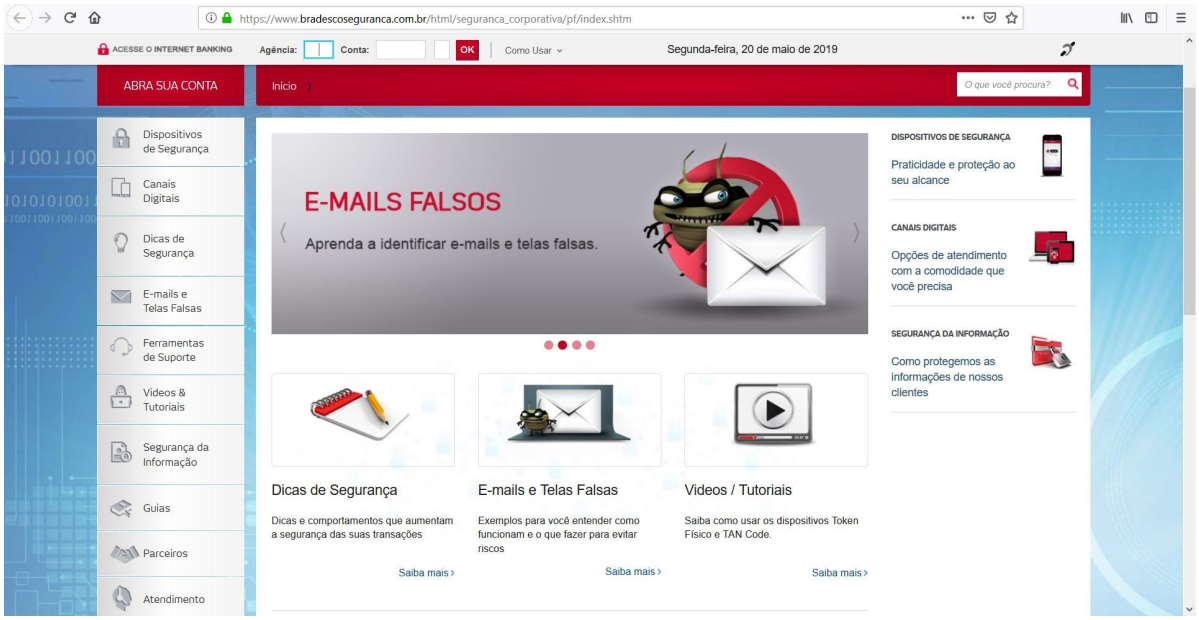
Figura 14 – Página inicial - Busca - Segurança



Fonte: (BRADESCO, 2019).

No rodapé da página são exibidos várias outras opções voltadas as informações que o banco pode passar para o cliente como, por exemplo "Fone Fácil", "Fale Conosco", "Trabalhe Conosco", "Direito dos consumidores","Informações de créditos"e logo mais abaixo tem uma opção "Segurança"na qual é redirecionada para a Figura 10. É exibido um menu lateral, *slideshow* e o conteúdo da página com informações de segurança: "Dispositivos de Segurança", "Canais Digitais", "Dicas de Segurança", "*E-mails* e Telas Falsas", "Ferramentas de Suporte", "Vídeos e tutoriais"e "Segurança da Informação".

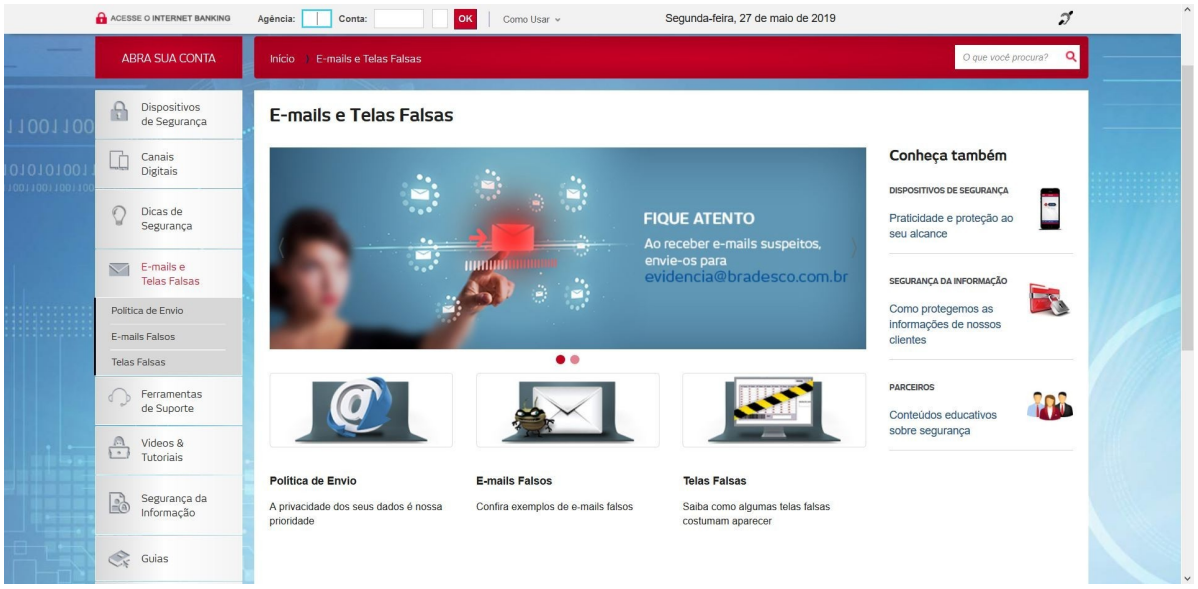
Figura 15 – Página inicial - Rodapé - Segurança



Fonte: (BRADESCO, 2019).

Ao clicar em alguns dos links o usuário é redirecionado para uma página na qual será especificado detalhadamente o conteúdo escolhido, com dicas de segurançaacompanhado por vários conteúdos relacionados.

Figura 16 – Página inicial - Rodapé - Segurança - Emails e telas falsas

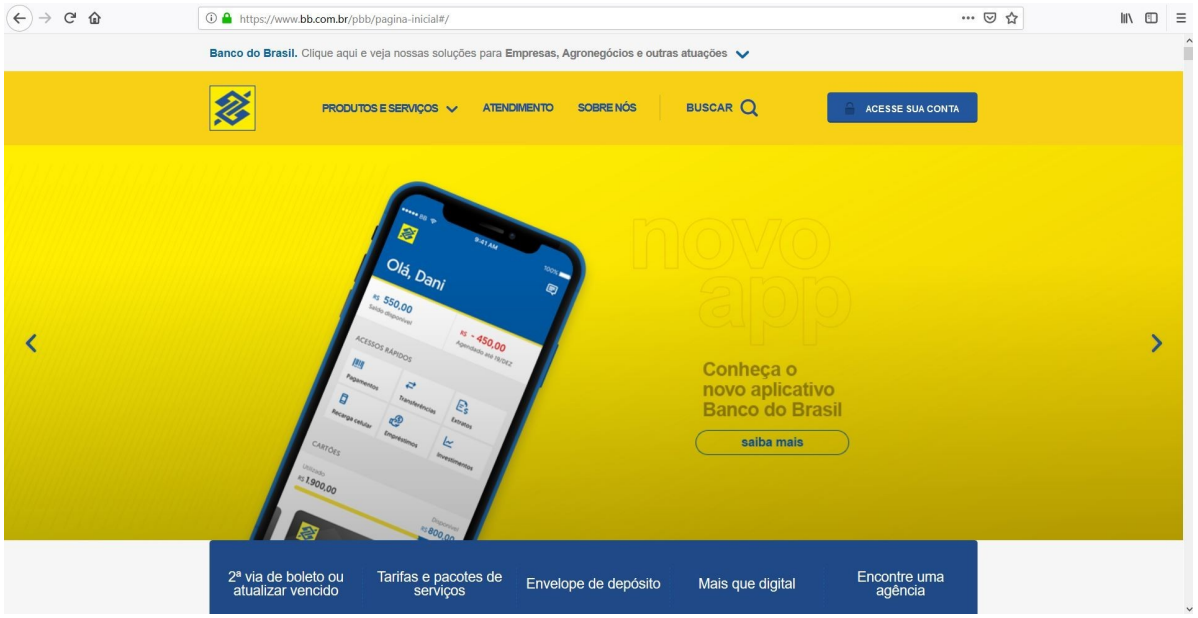


Fonte: (BRADESCO, 2019).

6.2.3 Site do Banco do Brasil

O *site* do banco do Brasil, no ano de 2019 pode ser acessado por usuários do banco ou não. Na página inicial é dada a opção de acesso para "Pessoa Física","Pessoa Jurídica","Setor Publico","Outras Atuações". É exibido um menu com opções "Produtos e Serviços","Atendimento","Sobre Nós"e o botão para "Acessar sua Conta", contem um *slideshow* exibindo algumas novidades do banco para os correntistas.

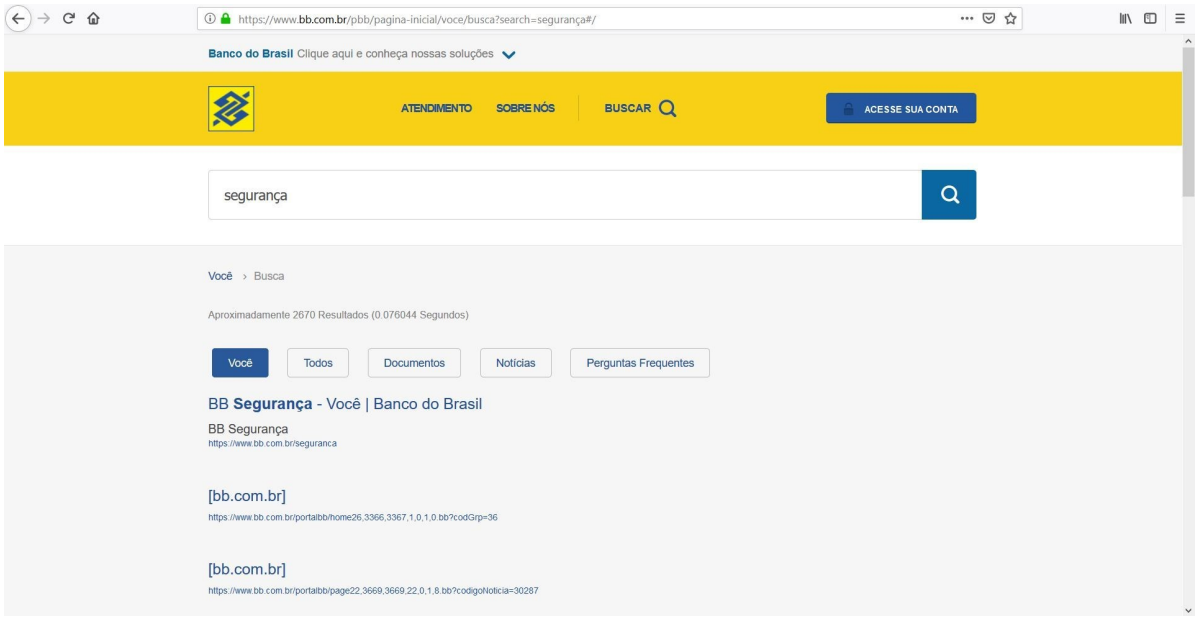
Figura 17 – Página Inicial



Fonte: (BRASIL, 2019).

Quando foi usado a opção "Buscar"com a palavra "segurança", foram retornados 2670 resultado da pesquisa. O conteúdo principal está relacionado a "Dicas de Segurança", "Segurança para patrimônio"e páginas com diversos alertas voltada a política de *e-mail*, sms e cartões de segurança. É exibido também um filtro com as opções "Você", "Todos", "Documentos", "Notícias", "Perguntas Frequente"para exibir notícias de acordo com cada opção dada.

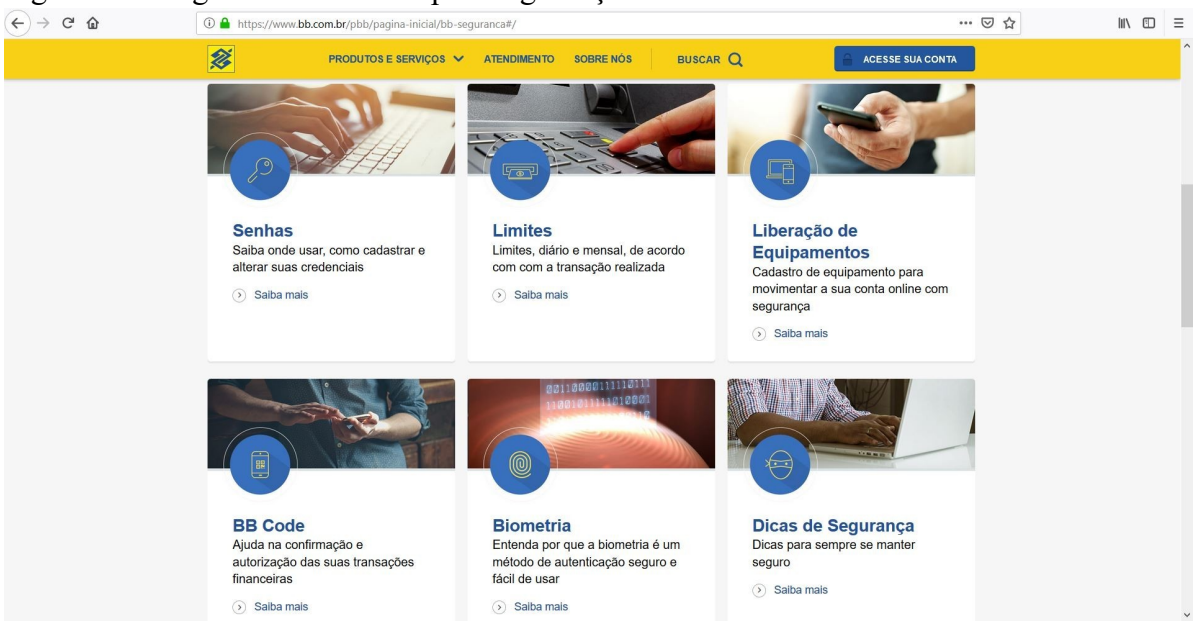
Figura 18 – Página Inicial - Busca - Segurança



Fonte: (BRASIL, 2019).

No rodapé é exibido o menu superior padrão, juntamente com alguns conteúdos sobre o banco e relacionado a formas diversas de atendimento ao cliente, na parte inferior temos as opções "Mapa do Site", "Segurança", "Ética e Integridade", "Políticas de uso e Privacidade", ao clicar em "Segurança", será redirecionado para a Figura 19. São exibidos várias metodologias que o banco do Brasil adquiriu para maior confiabilidade dos correntistas. Os conteúdosabordados são: "Senhas", "Limites", "Liberação de Equipamentos", "BB Code", "Biometria"e "Dicas de Segurança".

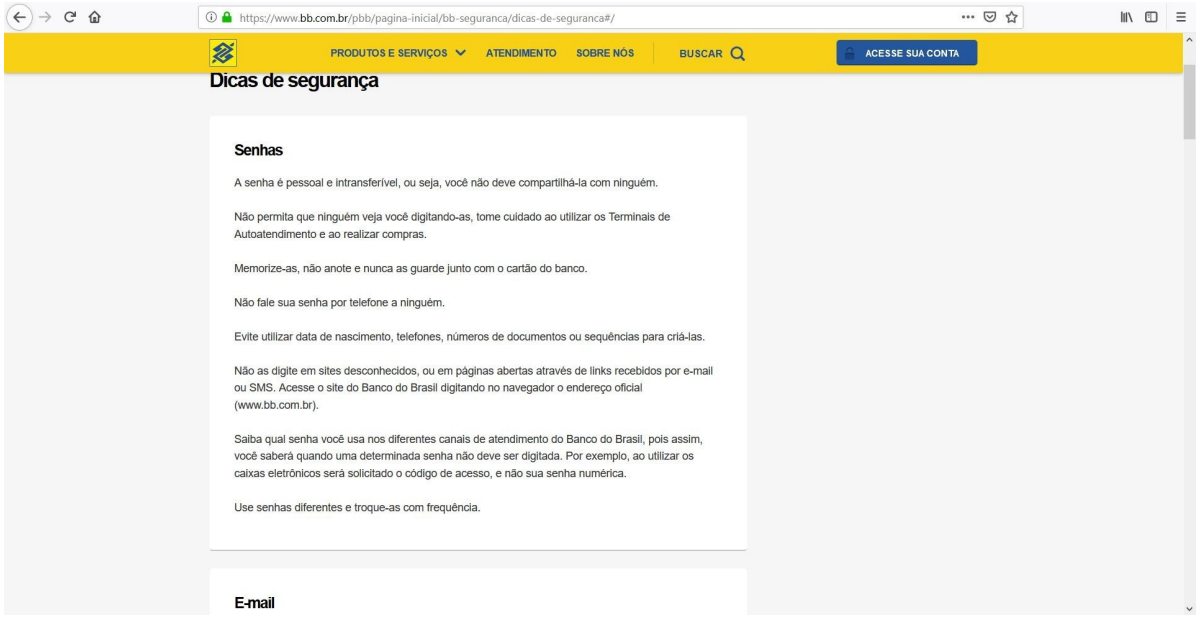
Figura 19 – Página Inicial - Rodapé - Segurança



Fonte: (BRASIL, 2019).

Ao clicar em "Saiba Mais"dos links o usuário é redirecionado para uma página na qual será especificado detalhadamente o conteúdo escolhido, com dicas de segurança acompanhado por vários conteúdos relacionados.

Figura 20 – Página Inicial - Rodapé - Segurança



Fonte: (BRASIL, 2019).

6.2.4 Comparativo das informações sobre seguranças disponíveis nos sites

A Quadro 4 apresenta como os *sites* que tratam o quesito “Segurança"em seus textitsites. Os bancos Itaú, Bradesco e Brasil não apresentam a opção “Segurança"no do topo de sua página web.

Quadro 4 – Aspecto comparativo da segurança nos *sites* das instituições bancárias

Banco	**Apresenta "Segurança" no topo da página**	**Buscar "Segurança" nos resultados**	**Apresenta "Segurança" no rodapé**	**Tem uma página que trata somente de "Segurança"**
Itaú	Não	1419	Sim	Sim
Bradesco	Não	1865	Sim	Sim
Brasil	Não	2670	Sim	Sim

Fonte: Elaborada pelo autor

Os bancos Itaú, Bradesco e Brasil não apresentam a opção "Segurança"no do topo de seu *website*. Ao inserir a palavra "Segurança"na busca de seus respectivos *site*, retornaram

"1419"resultados referente ao banco Itaú, "1865"resultados do Bradesco e "2670"resultados do banco do Brasil, todos esses conteúdos tem algo relacionado a segurança com as especificidade de cada instituição financeira abordada. Nos *websites* das instituições todas tinham a opção "Segurança"no rodapé, como exibido nas figuras anteriores, todas as três possuem uma página na qual trata exclusivamente do conteúdo. Pode ser visto que os *sites* apesar de ser diferentes bancos, no quesito "Segurança"são abordados com uma estrutura bem parecidas nos *websites*.

6.3 Técnicas de ataques

Nesta seção será exibido como os engenheiros sociais executam seus ataques, desde a criação dos *sites* até a manipulação dos dados de correntistas.

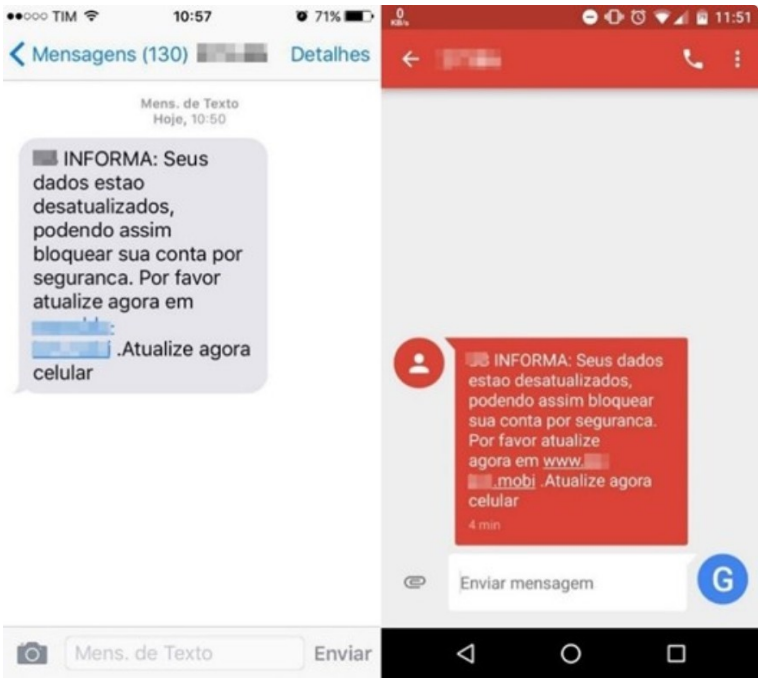
6.3.1 E-mails falsos de phishing

Os ataques de *phishing* são divididos em três fases. A primeira a vítima recebendo um *phish*. A segunda etapa é a vítima tomando a ação sugerida na mensagem, que geralmente é ir a um *site* falso, mas também pode incluir a instalação de *malware* ou a resposta a informações confidenciais. O terceiro passo é o criminoso monetizar informações roubadas. A maioria dos e-mails de *phishing* usa técnicas sociais em vez de truques técnicos para enganar os usuários finais. Por exemplo, transmitir a urgência é um método bem conhecido usado por criminosos para direcionar a atenção das pessoas de forma inadequada. Um exemplo é fingir ser um sistema administrador avisar as pessoas sobre um novo ataque e instalar o *patch* anexado outro exemplo é notificar as pessoas de que houve vários logins com falha em sua conta e que precisam verificar sua conta agora ou arriscar as consequências. Apelar para o sentimento de medo das pessoas é uma técnica antiga que foi adaptada ao mundo digital.

6.3.2 Mensagens falsas de smishing

Existe um tipo de técnica de *phishing* que rouba as informações pessoais de um usuário usando o serviço de mensagens curtas (SMS) de um telefone celular. Smishing (SMS + *phishing*), que foi nomeado pela McAfee, uma empresa de segurança da Internet. Ocorre quando um link de *site* é enviado via mensagem de texto para um usuário de smartphone, fazendo com que o receptor clique no link e acesse a página falsa de acordo como é exibido na figura 21.

Figura 21 – SMS falso



Fonte: https://www.tecmundo.com.br/acesso-a-banco/108006-novo-golpe-usa-sms-sites-falsos-bancos-roubar-dados.htm

6.3.2.1 Long number vs short code

De modo geral, o *long number* é representado por envios cuja origem vem de um número idêntico com a de uma linha normal. Tem se observado que as operadoras estão cada vez mais exigentes com campanhas que usam o *long number*, chegando até a parar de aceitar os envios, assim como as campanhas que usam “chipeiras”. "Chipeiras"são equipamentos que concentram um número determinado de chips e que permitem o roteamento direto entre redes IP, digitais e analógicas para as redes GSM de telefonia celular, ou seja, equipamentos conectados a um computador que permitem o envio de um grande número de SMS. Conhecido como SMS Pirata, o serviço não é regulamentado sendo praticado de forma ilegal no Brasil. A exigência das operadoras e da Anatel, é que o envio seja feito por *short code*, que é inclusive a forma de envio utilizada por bancos, pelas próprias operadoras e pelo SGP (software para políticos e candidatos).

Diferentemente do *long number*, o "*short code*"tem de 5 a 6 dígitos. Usá-lo traz diversas vantagens em relação ao *long number*. Uma das principais é a possibilidade de resposta e as métricas, que dão retorno sobre quem recebeu o SMS, facilitando as análises. Além dessas vantagens, o serviço *short code* é regulamentado pela Anatel, garantindo segurança no uso.

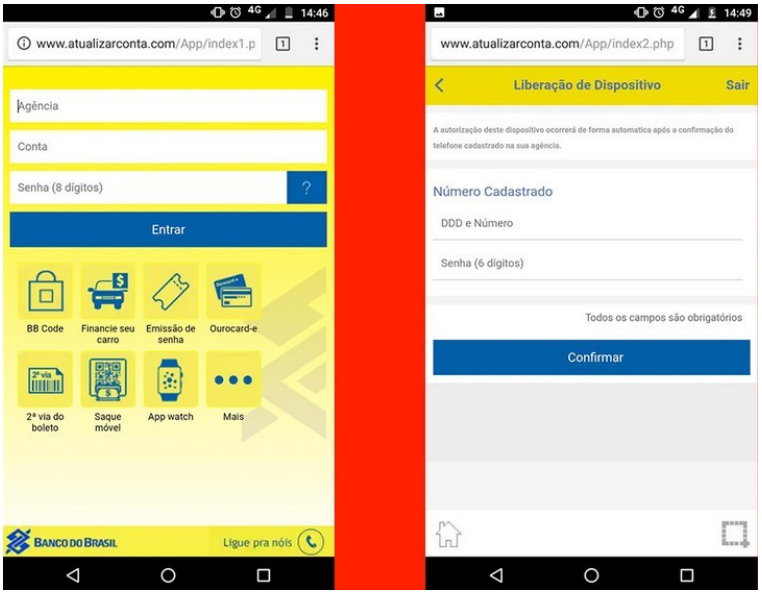
6.3.3 Configurando sites falsos

A maioria dos ataques de *phishing* tentam convencer os internautas a acessarem *sites* falsos, na qual as informações pessoais podem ser coletadas. Para hospedar um *site*, os golpistas usam plataformas de hospedagem que são disponibilizadas na web, geralmente usam servidores virtuais privados (VPS) para hospedar *sites*, pois, as hospedagens compartilhadas tem um maior critério de avaliação devido ser a mais usada para hospedagem de *sites*. A VPS é bem mais difícil de ser instalada comparada com hospedagens comuns devido ser um servidor virtual no qual o acesso só é possível através da virtualização do servidor, sendo necessário ter um bom conhecimento para fazer a sua configuração.

Ao registrar novos domínios, os criminosos tentam obter nomes semelhantes ao *site* em que estão tentando simular. Por exemplo, para simular ser o banco itaú, os golpistas podem registrar o domínio "itau-login.com". Os criminosos também usam ataques homográficos que exploram a semelhança visual dos personagens. Por exemplo, ltaucard.com, usam "l"para se parecer com um i, nomes de domínios internacionalizados facilitam esse tipo de ataque, pois, caracteres em diferentes conjuntos de idiomas podem parecer idênticos. A abordagem mais inovadora até agora é o fluxo rápido, que usa um grande conjunto de *proxies* e nomes de domínio para ocultar a verdadeira localização de um *phishing*. O fluxo rápido torna mais difícil a lista negra de *sites*, devido, existirem muitos (URLs) que precisam ser verificados manualmente. Encontrar e remover *sites* ofensivos também é difícil, pois, é preciso mais trabalho para encontrar o servidor real.

O e-mail ou SMS falsificado pode então utilizar engenharia social e informações contextuais sobre os alvos para direcionar os usuários a uma página da web falsa. Uma página da web falsa e é ilustrada na figura 22, embora a página original é visualmente semelhante, a versão da imagem 22 difere da legítima em vários aspectos: sua (URL) contém HTTP em vez de HTTPS que é uma conexão segura que criptografa dados por um certificado seguro conhecido como SSL, segundo um ícone de cadeado no início da (URL) está faltando, indicando que o *site* que está sendo acessado não é seguro; e por fim o próprio (URL) contém um domínio falso (http://www.atualizarconta.info), o da verdadeira página do banco do Brasil é (https://www.bb.com.br/).

Figura 22 – Tela falsa banco do brasil



Fonte: https://exame.abril.com.br/tecnologia/site-falso-do-bb-e-quase-convincente-para-roubar-seus-dados/

6.3.4 Monetizando informações roubadas

Atualmente, muitos *phishers* vendem credenciais através de redes clandestinas para outros criminosos. Esses compradores por sua vez, pode recrutar pessoas desavisadas como “laranjas” para lavar dinheiro e bens, reduzir o risco que os criminosos enfrentam e contornar as contramedidas existentes. Por exemplo, alguns envolvem receber transferências de dinheiro para a conta bancária do "laranja", com os fundos realmente provenientes de uma conta bancária hackeada, então é feito o saque mantendo uma pequena comissão para ele e o restante distribuído para os integrantes do furto.

Quando obtida as informações roubadas, na maioria das vezes, são monetizadas devido à especialização e ao risco de rastreio uma pessoa que é boa em criar *sites* de *phishing* pode não necessariamente ser boa em roubar dinheiro dessas contas, especialmente dada uma maior vigilância por parte dos bancos. Assim, em vez de correr o risco de ser rastreado, um *phisher* pode optar por vender informações roubadas a outras pessoas menos avessas ao risco. Geralmente o canal de vendas utilizados são aplicativos bastantes conhecidos como: ("telegram", "whatsapp", "youtube", "facebook"entre outros).

6.3.5 Como os phishers tiram dinheiro das contas ?

No Banco do Brasil, com as informações bancárias em sua posse (Agência, Conta, Senha de 6 dígitos, senha de 8 digitos e Número telefônico), o *phisher* com um *smartphone* para acessa á conta, é preciso fazer a liberação do dispositivo. Nesse caso ele tem ajuda de pessoas que trabalham em operadoras para fazer o "resgate"da linha telefônica da vítima. Essa ação é uma forma de cancelar a linha que a vítima usa, obtendo o seu número no novo chip. Então é solicitado o SMS para liberar o celular, após confirmado o código enviado pelo banco, o *smartphone* estará habilitado para fazer as transações bancárias.

No banco Itaú, as informações bancárias em sua posse (agência, conta, senha eletrônica, senha da conta e número telefônico), o *phisher* com um *smartphone* acessa no aplicativo e faz a solicitação para realizar transferências pelo celular na qual é a liberação do "Itoken", para fazer isso algumas vezes os golpistas ligam para as vítimas se passando por funcionários do banco e pedem para ir ao caixa fazer a liberação ou simplesmente esperam os correntistasirem ao caixa e de forma desatenta liberarem, pois, assim que inserido o cartão no caixa o sistema pergunta se o correntista quer liberar o *Itoken* para fazer transações, fazendo uma dessas duas maneiras o celular ficará habilitado para transações bancárias.

No banco Bradesco, é usado como método de liberação chave de segurança, não foi encontrada a maneira que *phishers* fazem para liberar celulares para fazer transferência nessa instituição.

Após a liberação do "APP", os *phishers* conseguem fazer transferências para contas de "laranjas", pagamentos de boletos, usam valores que estão disponíveis no cartão de crédito (gerando cartão virtual), quando possível usam de empréstimos e resgatam aplicações de valores dos correntistas para pegar mais dinheiro das contas.

6.3.6 Perfis dos atacantes

Segundo (ROHR, 2011), a polícia tem uma grande dificuldade em encontrar quem realiza golpes de "*phishing*", pois as transações são feitas das contas de vítimas para a de "laranjas", então sua real identidade é muito difícil de ser achada devido não ter nenhuma relação com o responsável por executar a ação criminosa. Quando os golpistas são aprendidos geralmente são quadrilhas entre quatro a oito integrantes do gênero masculino. As idades e nomes não são divulgados, não revelam fotos, mas geralmente mostram qual equipamento foi usado no crime.

Na grande maioria dos casos, os golpistas são identificados pelas ostentações diárias em redes sociais, denúncia de vizinhos que suspeitam de algo e quando são realizadas compras de valores altíssima em lojas físicas de forma frequente.

6.3.7 Phishing nos bancos digitais

Assim como nos bancos físicos, os correntistas de bancos digitais também são vítimas de ataques de *phishing*. No começo dos bancos digitais, as validações de contas não eram tão rigorosas facilitando a abertura de contas, somente com os dados digitais de terceiros. Conforme (JACOMINI, 2018) atualmente há uma verificação maior como, por exemplo a solicitação completa de documentação do indivíduo como: CPF, endereço, nome completo, data nascimento além das fotos da documentação e *selfie* com a própria documento. Os bancos digitais também são alvo do recebimento de pagamentos através de transferência *on-line* ou pagamento através de boletos gerados. Quem tem conta no banco digital também está sendo vítima de tentativas de ataques do *phishing* através de *e-mail* e sms, com as mesmas táticas já citadas anteriormente nos bancos físicos.

6.3.8 Como solicitar o cadastro no banco digital

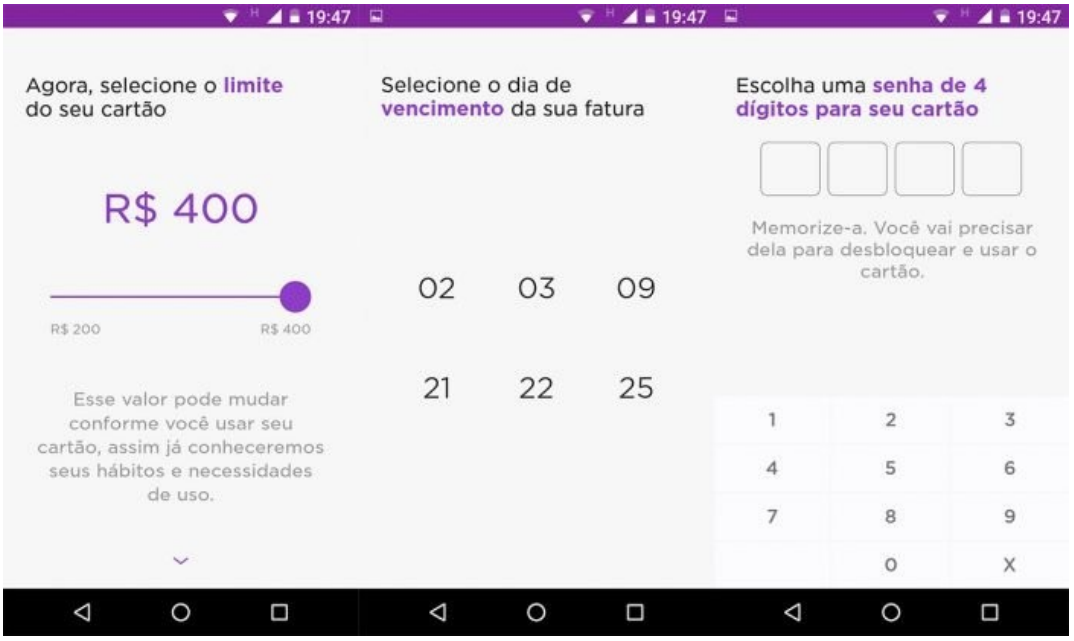
Serão analisadas as etapas necessárias para cadastrar uma nova conta no banco. Por esse motivo, será limitado apenas até a etapa de análise de documentos.

6.3.9 Nubank

1. Baixe e instale o (app) do Nubank para Android ou iPhone.
2. Toque em “Quero Ser Nubank” e Caso tenha um convite "Já tenho Convite".
3. Inicie o cadastro no (app). O Nubank vai pedir os seguintes dados:
   - Número do documento, que pode ser RG, CNH ou RNE (para estrangeiros).
   - Em caso de RG, o órgão emissor e estado.
   - Endereço de residência, incluindo número, complemento e bairro.
   - Foto da frente e verso do documento (assegure que esteja visível).
   - Uma *selfie* usando o aplicativo, segurando o documento para atestar a veracidade.
   - Rendimento mensal.
4. Quando aparecer “Experimentar Nubank Rewards”, toque em Continuar apenas

com cartão.

Figura 23 – Tela de cadastro do Nubank



Fonte: https://tecnoblog.net/242090/pedir-solicitar-cartao-nubank-convite/

5. Escolha um limite de acordo com o limite pré-estabelecido do Nubank.
6. Selecione uma data de vencimento para a sua fatura.
7. Coloque uma senha de quatro dígitos para o cartão de crédito.
8. Assine a tela do aplicativo com o dedo.

Depois de colocar todos esses dados, o Nubank deverá responder em até cinco dias úteis, seja pedindo mais informações ou confirmando a emissão do cartão.

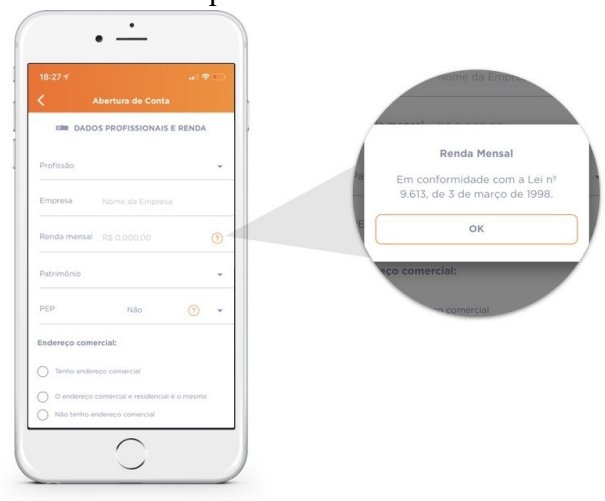
6.3.9.1 Inter

1. Baixe e instale o (app) do Inter para Android ou iPhone.
2. Digite seu CPF.
3. Abertura da Contas seguintes dados:
   - CPF, Nome, Telefone e e-mail.
4. Informações Básicas.
   - Nome da mãe e pai.
   - Sexo, Data Nascimento e Estado Civil.
   - Documento de Identificação e Data de Emissão e Validade.
5. Endereço Residencial.

- CEP, Número, Complemento.

6. Dados profissionais e Renda.

Figura 24 – Tela de cadastro do Inter- Etapa dados profissionais



Fonte: https://usemobile.com.br/analise-cadastro-aplicativo-do-banco-inter/

7. Referência Pessoal.
8. Modelo do Cartão.
9. Foto *Selfie* utilizando o aplicativo.

Após receber a solicitação, os documentos serão analisados e dentro do prazo de 10 dias terá uma resposta do banco inter.

6.3.9.2 Criação de contas fraudulentas nos bancos digitais

Os *phishers* só precisam do RG, CPF, ou até mesmo telefone das vítimas. Através de *softwares* de consultas conseguem obter todos dados(Nome Completo, Telefone, RG, CPF, nome pai e mãe , endereços e etc) da vítima. Com os dados necessários em sua posse, podem fazer identidades ou cnh falsas com fotos de laranjas, o mesmo bater a *selfie* para comprovar que são os titulares dos documentos e então conseguirem que seja realizado todo procedimento exigido pelos bancos digitais.

Com cartão aprovado, basta esperar o dia exato para fazer a liberação com a senha escolhida pelos *phishers* e então usar o limite de crédito que foi liberado pela instituição bancária. Outra forma também que está sendo bastante usada é a de receber valores com essas contas digitais. Os *phishers* que tem acesso a contas de vítimas conseguem fazer transferências para

essas contas e logo em seguida os valores são sacados.

Pelo registro do banco central, é possível consultar os seus limites de crédito e também a descrição de todas as instituições financeiras que possuem conta bancária com seu cpf. Caso o consumidor desconheça a abertura de conta em uma determinada agência e conta, deve procurar imediatamente a instituição financeira para evitar que a conta seja utilizada para aplicar golpes. Existem casos de consumidores que ficam com o nome sujo por conta de dívidas contraídas em conta digitais abertas de maneira fraudulenta. (BANCOCENTRAL, 2017).

6.4 Técnicas de defesa e estudo dos perfis das vítimas

Nesta seção serão exibidos táticas de defesa ao *phishing* e os resultados da pesquisa feita com os correntistas que foram fraldados por engenheiros sociais.

6.4.1 Como podemos identificar tentativas de phishing?

Dados os riscos do *phishing*, os indivíduos e organizações tem que tomar certas decisões a primeira linha de defesa e impedir ataques de *phishing* de alcançar usuários finais. De acordo com (HONG, 2012), as soluções neste espaço incluem filtragem e-mails de *phishing*, bloqueio e remoção de *sites* falsos:

1. Suspeitar da gramática e pontuação: redatores profissionais esforçam-se ao máximo para criar e-mails com conteúdo testado, linha de assunto, apelo à ação, etc. É muito provável que qualquer e-mail que contenha gramática, pontuação ou mostre um fluxo ilógico de conteúdo seja provavelmente escrito por pessoas inexperientes.

2. Solicitam informações pessoais: marcas estabelecidas nunca solicitam informações confidenciais por e-mail. Qualquer mensagem que solicite a inserção ou verificação de dados pessoais, ou informações bancárias / de cartão de crédito deve ser tratada como uma grande bandeira vermelha.

3. Conteúdo alarmante, cheio de avisos e possíveis consequências: os hackers podem enviar mensagens que causam alarme dizendo coisas como uma de suas contas foi invadida, sua conta está expirando e que você pode perder alguns benefícios críticos imediatamente ou outra condição extrema que a deixa em pânico. Esse conteúdo geralmente é formatado para criar alarme e um senso de urgência com a intenção de levar o usuário a tomar uma açãoimediata.

4. Prazos urgentes: Nesse padrão, os hackers enviam um e-mail sobre algum prazo

pendente. Por exemplo, um hacker pode enviar um e-mail de renovação sobre uma apólice de seguro vencida ou um desconto de validade limitado em alguma transação que possa ser do interesse do alvo. Normalmente, esses e-mails levam os usuários a *sites* de coleta de dados que acabam roubando informações pessoais ou financeiras valiosas.

5. Oferecer grandes recompensas financeiras: esse padrão inclui e-mails afirmando que você ganhou na loteria quando nunca compra uma, oferece um grande desconto em dinheiro em algo que você nunca comprou, um grande prêmio em dinheiro em um concurso para o qual você nunca se inscreveu e assim por diante. A intenção real é geralmente direcioná-lo para um *site* onde os golpistas podem obter suas informações pessoais ou financeiras.

6. Links encurtados: não mostram o nome real de um *site* e podem ser usados com mais facilidade para induzir o destinatário a clicar. Os hackers podem usar links reduzidos para redirecioná-lo para *sites* parecidos e capturar informações confidenciais. Sempre coloque o cursor no link reduzido para ver a localização do alvo antes de clicar nele.

7. Verifique as credenciais *SSL* do *site* de destino: A tecnologia *SSL* garante a transmissão segura e criptografada de dados pela Internet. Se você clicar em um link de e-mail e acessar um *site*, sempre verifique suas credenciais *SSL* . Uma técnica altamente eficaz para evitar *phishing* é nunca fornecer informações confidenciais (senhas, detalhes de cartão de crédito, respostas a perguntas de segurança, etc.) em *sites* que não possuem um certificado *SSL* válido instalado.

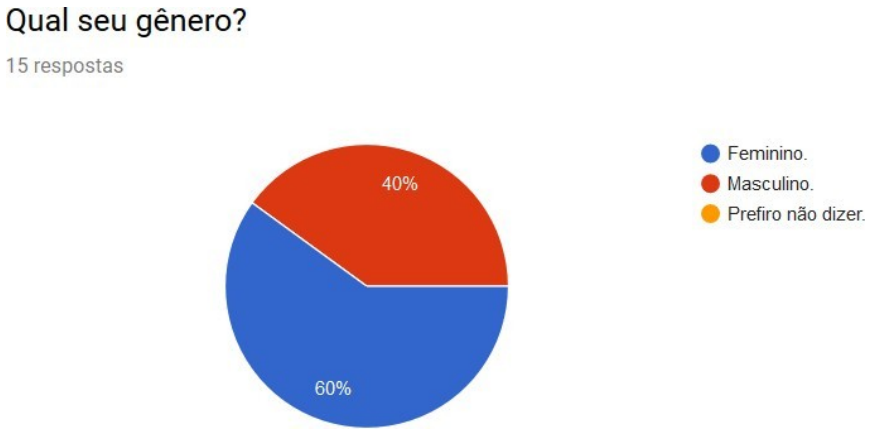
8. Cuidado com os pop-ups: usando a tecnologia *Iframe*, os *pop-ups* podem capturar facilmente informações pessoais e enviar para um domínio diferente daquele que aparece na barra de ferramentas do navegador. *sites* reconhecidos e estabelecidos raramente pedem para inserir informações confidenciais em *pop-ups* e, como regra geral, nenhuma informação pessoal deve ser inserida em *pop-ups*, mesmo que apareçam em domínios com *SSL* válido e tenham passado em todas as outras verificações de *phishing*.

6.4.2 Informações sobre as características comuns dos correntistas fraudados – resultados e repercussões

As variáveis estudadas com objetivo de identificar as principais características dos correntistas vítimas da engenharia social, implicando em fraudes eletrônicas foram: o gênero, idade, grau de escolaridade, renda mensal. Do total das fraudes eletrônicas, 15 ocorreram com pessoas físicas, considerando as variáveis que foram estudadas, os dados a seguir estão relacionados à esses correntistas.

As fraudes eletrônicas se concentraram no gênero feminino com 9 correntistas fraudados, representando 60%. Em contrapartida, 6 mulheres foram fraudadas correspondendo a 40% do total das fraudes, como segue na imagem 25:

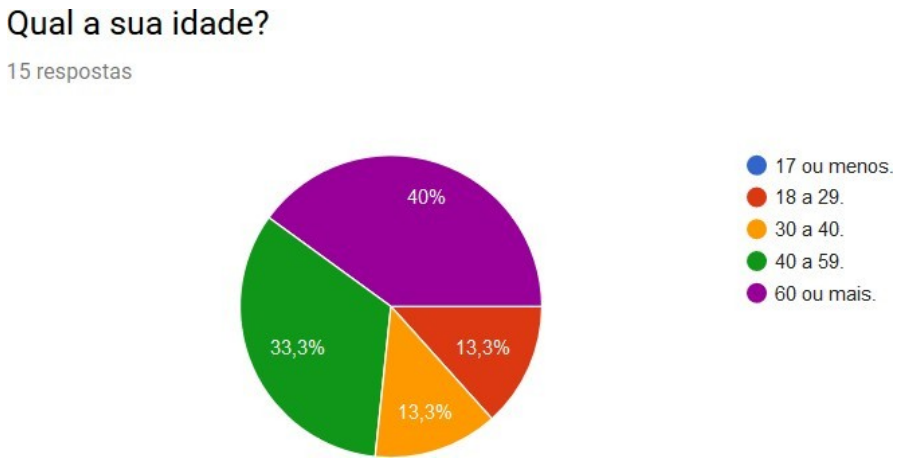
Figura 25 – Correntistas fraudados - gênero



Fonte: Elaborada pelo autor - dados obtidos do formulário

Para a variável "faixa etária", 6 pessoas com mais de 60 anos foram vítimas de fraude, representando 40%, seguidas dos classificados entre 40 a 59 anos, com 5 pessoas, ou seja, 33,3%, seguidamente dos classificados entre 30 a 40 anos, com 2 pessoas, ou seja, 13,3%, sucessivamente dos classificados entre 18 a 29 anos, com 2 pessoas, ou seja, 13,3% e dos classificados com 17 ou menos, com 0 pessoas, ou seja, 0%, cujos detalhes podem ser observados na figura 26.

Figura 26 – Correntistas fraudados - Faixa etária



Fonte: Elaborada pelo autor - dados obtidos do formulário

Os resultados colhidos demonstraram que 9 correntistas vítimas de fraudes eletrônicas, possuem ensino médio, representando 60%, 3 pessoas, contem ensino superior, representando 20% , seguidas dos que tem ensino fundamental, representando 20%, observados no gráfico. 27.

Figura 27 – Correntistas fraudados - Grau de escolaridade

Fonte: Elaborada pelo autor - dados obtidos do formulário

Considerando a variável "renda"da pesquisa, utilizaram-se os parâmetros seguidos pelo (SAE) em 2014 que divide suas amostras para efeito de pesquisa em 5 faixas de renda ou classes sociais, conforme o Quadro 5:

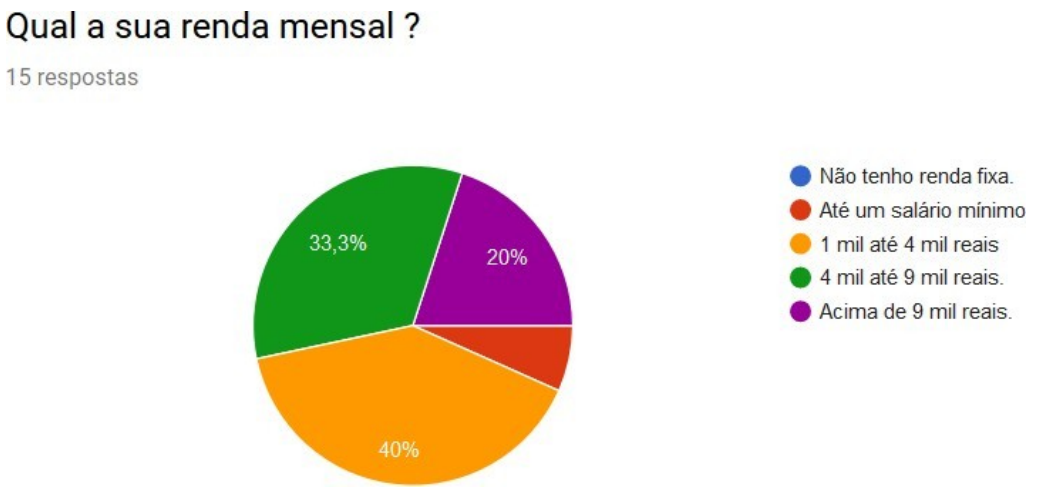
Quadro 5 – Grupo de renda da população

Classificação	**Renda**	**Grupo**
Extremamente pobre	Menor de R$ 854	1
Pobre,mas não extremamente pobre	Até R$ 1.013	2
Baixa classe média	Acima de R$ 1.484 até R$ 4.081	3
Média classe média	Acima de R$ 4.081 até R$ 9.097	4
Alta classe média	Acima de R$ 9.097	5

Fonte: Elaborada pelo autor

Tendo como parâmetro o critério de definição do SAE para a variável renda, pode ser notado que o grupo 1, sem renda fixa, não teve nenhum correntista que sofreu alguma fraude, a pesquisa também revelou que o grupo 3 é aquela que apresenta a maior concentração de fraude eletrônica, representada pelos correntistas da Instituição Bancária com renda mensal entre 01 a 04 salários mínimos, seguida dos grupos 2, 4 e 5 como podemos observar:

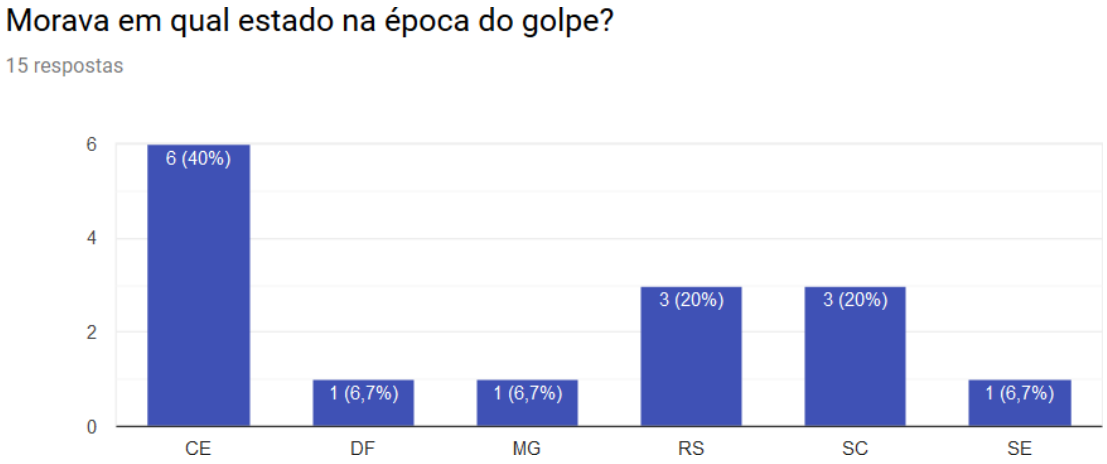
Figura 28 – Correntistas fraudados - Renda Mensal



Fonte: Elaborada pelo autor - dados obtidos do formulário

Os correntistas que foram fraudados, estão distribuídos nos estados brasileiros no qual o principal foi o Ceará, representando 6 pessoas, seguidas de Rio Grande do Sul e Santa Catarina com 3 pessoas e Sergipe, Minas Gerais e Brasília com uma pessoa para cada estado, conforme a figura 29.

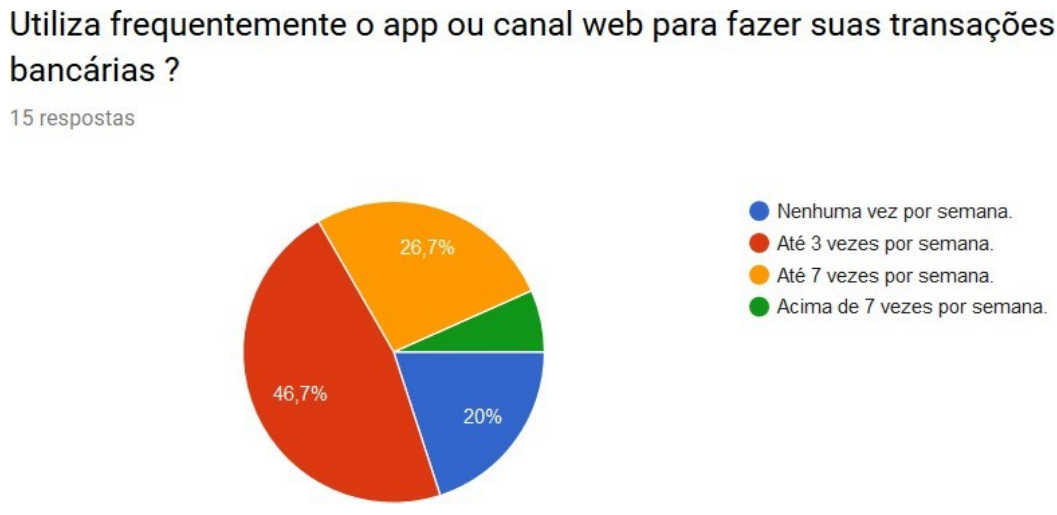
Figura 29 – Correntistas fraudados - Região



Fonte: Elaborada pelo autor - dados obtidos do formulário

Para a variável "Frequência no uso do (app)", 7 correntistas utilizam até 3 vezes por semana utilizam o (app), ou seja, representando 46,7%, seguidas por 4 pessoas que utilizam até 7 vezes por semana utilizam o (app), ou seja, representando 26,7%, seguidamente 3 correntistas utilizam acima de 7 vezes por semana utilizam o (app), seguidas por 1 pessoa que não utilizam o aplicativo nenhuma vez durante a semana, como é ilustrado na imagem 30.

Figura 30 – Correntistas fraudados - Frequência no uso do app

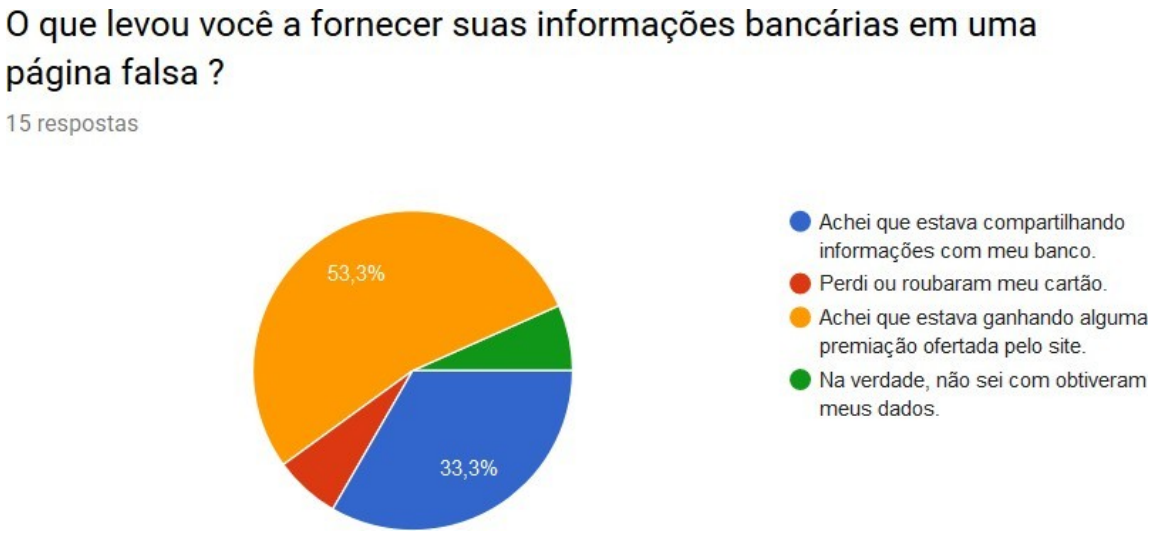


Fonte: Elaborada pelo autor - dados obtidos do formulário

Um dos principais construtos da sustentação de qualquer negócio, é a confiança, assim, a perda de confiança no canal pode vir a restringir o crescimento da Instituição Bancária,

podendo causar a diminuição de seus ativos. A segurança corresponde a uma percepção, uma sensação, dessa forma, caso as pessoas não venham a se sentir seguras, dificilmente virão a mudar esta percepção, fato este confirmado pela pesquisa. Para avaliar o grau de satisfação dos entrevistados em relação às orientações recebidas da Instituição Bancária sobre as fraudes as quais estariam sujeitos, 8 correntistas pensavam que estivesse ganhando alguma premiação ofertada pelo *site*, ou seja, representando 53,3%, seguidas por 5 pessoas no qual informou que achava que estivesse compartilhando informações com a instituição responsável, ou seja, representando 33,3%, sucessivamente 1 correntista perdeu ou roubaram seu cartão, representando 6,7%, seguida por 1 usuário no qual informou que não sabe como obtiveram os seus dados bancários, representando 6,7%, como ilustrado na figura 31.

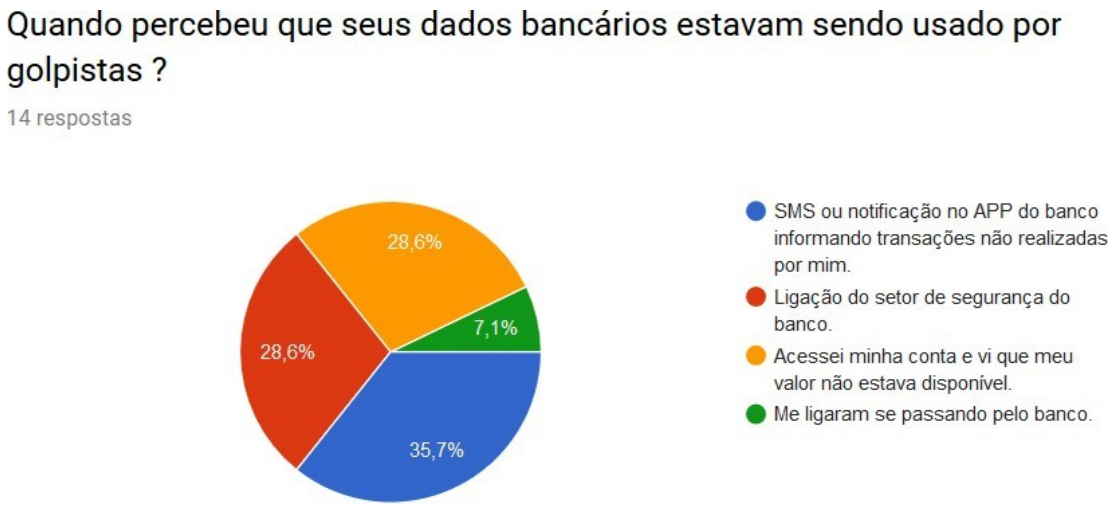
Figura 31 – Correntistas fraudados - Fornecimento das informações



Fonte: Elaborada pelo autor - dados obtidos do formulário

Para o quesito "Quando o correntista percebeu que seus dados bancários estavam sendo utilizado por outra pessoa", no qual 35.7% foram notificados por SMS ou *app*, ou seja, 6 correntistas, seguindo de 28,6% receberam ligação do setor de segurança do banco, ou seja, 4 pessoas, sucessivamente 28,6% acessaram suas respectivas contas e viram que o valor não estava disponível, ou seja 4 correntistas, seguidas de 7,1% que receberam ligações de engenheiros sociais se passando pelo banco, ou seja, somente 1 usuário, como pode ser exibido na figura 32.

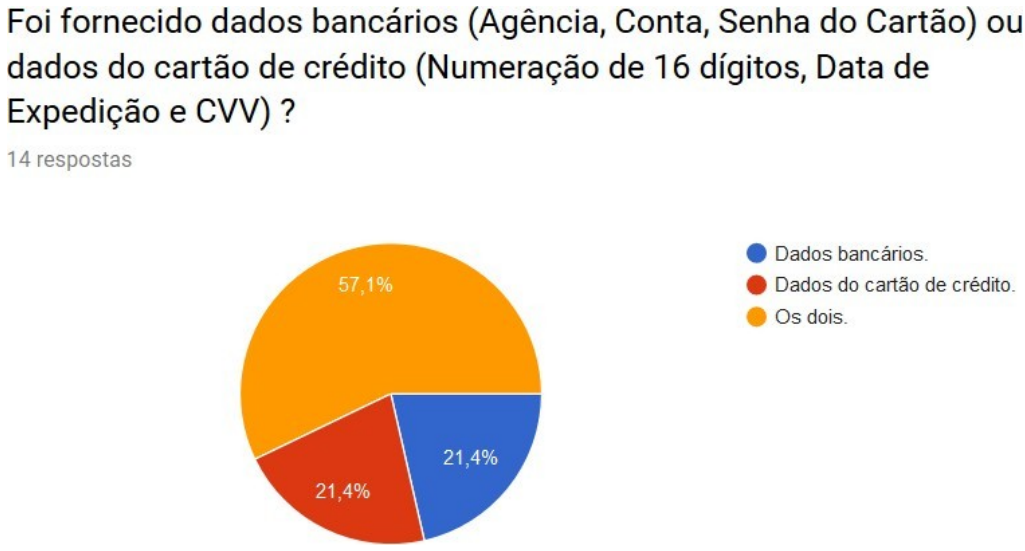
Figura 32 – Correntistas fraudados - Dados usados por golpistas



Fonte: Elaborada pelo autor - dados obtidos do formulário

Os resultados colhidos demonstraram que 9 correntistas vítimas de fraudes eletrônicas, informaram os dois que seria tanto os dados bancários como os dados do cartão de crédito, representando 57,1%, 3 pessoas, forneceram somente dados do cartão de crédito, representando 21,4%, 3 correntistas, informaram somente dados bancários, representando 21,4%, observados na imagem 33.

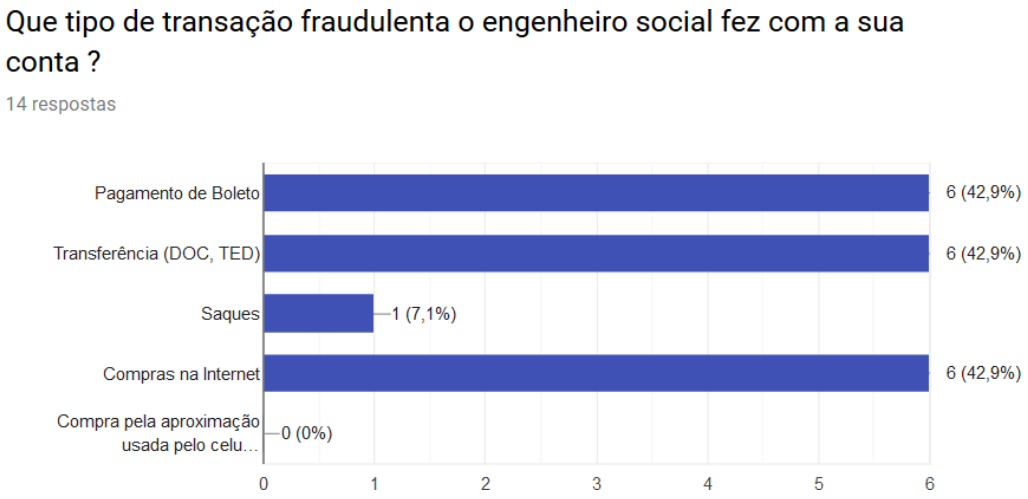
Figura 33 – Correntistas fraudados - Dados bancários fornecidos



Fonte: Elaborada pelo autor - dados obtidos do formulário

Os tipos de transações realizadas pelos engenheiros sociais após obterem as informações sigilosas dos correntistas da Instituição Bancária foram: pagamento de boletos, com um total de 6 transações fraudulentas, seguidas de 6 transferências (doc e ted), logo após aparecem os saques, no total de um, e as compras com cartão pela internet, com 6 registros, sucessivamente não teve nenhum registro de compras pela aproximação, tais dados assim se apresentam no na figura 34.

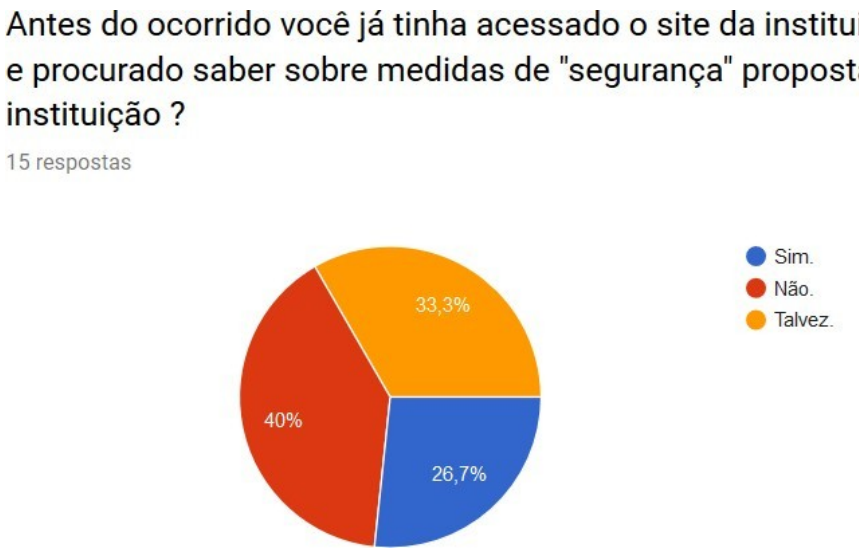
Figura 34 – Correntistas fraudados - Tipo de transação fraudulenta



Fonte: Elaborada pelo autor - dados obtidos do formulário

O mapeamento das tipologias dos canais de informação utilizados, sendo estes internos ou externos à Instituição Bancária, é essencial para se identificar quais os canais mais utilizados pelos correntistas, podendo inclusive ser alicerce para futuras pesquisas voltadas ao desenvolvimento da melhoria de tais meios. Sobre este aspecto, a questão formulada foi assim descrita: “Quando procurou sobre informações de segurança, a instituição bancária lhe orientou sobre o cuidado com informações sigilosas”. Identificou-se que os correntistas fraudados na grande maioria não procurou ou tem dúvidas sobre segurança antes de cair no golpe, uma pequena parte dos correntistas já tinham acessado o *site* da instituição e procurado saber sobre medidas de segurança, como ilustrado na figura 35.

Figura 35 – Correntistas fraudados - Medidas de segurança



Fonte: Elaborada pelo autor - dados obtidos do formulário

Após o registro da contestação de débito, a instituição realiza a análise das informações elencadas pelo correntista, confrontando-as com os dados da transação contestada, histórico das transações reconhecidas pelo correntista, para identificar o seu padrão de comportamento e características, além das imagens das câmeras instaladas nas agências e nos caixas eletrônicos. Em seguida, as contestações são processadas como "procedentes", com ônus para a Instituição Bancária, quando é confirmada a fraude eletrônica, ou "improcedentes", com ônus para o correntista, quando as informações recuperadas descartam a fraude. A figura 36 mostra que o ressarcimento foi realizado para os 14 correntistas, apenas um correntista não teve o ressarcimento no qual seu relato foi:

> Disseram que eu que entreguei meus dados e não tive provas. Fui injustiçado.(ENTREVISTADO)

Figura 36 – Correntistas fraudados - Perdas financeiras

Fonte: Elaborada pelo autor - dados obtidos do formulário

Com a intenção de identificar se o correntista vítima de fraude eletrônica estaria suscetível novamente a ser fraudado, foi elaborada a questão: depois do ocorrido você acha que cairia novamente em algum tipo de fraude na internet? Uma fração significativa dos entrevistados, ou seja, 6 deles, relataram que estariam suscetíveis a cair novamente no engodo da engenharia social, enquanto que 3 deles declararam que não seriam novamente vítimas, no entanto, 6 responderam que poderiam ser vítimas sim de nova engenharia social e com isso terem prejuízos financeiros, como mostrado na figura 37.

Figura 37 – Correntistas fraudados - Ser Vítima novamente no phishing

Fonte: Elaborada pelo autor - dados obtidos do formulário

7 CONSIDERAÇÕES FINAIS

Para a finalização da pesquisa serão descritas a seguir as considerações finais, sistematizadas segundo os objetivos estabelecidos na pesquisa.

7.1 Conclusões

O objetivo geral deste trabalho é analisar a segurança da informação de correntistas de Instituições Bancárias a partir da perspectiva da engenharia social mediante apresentação de suas táticas de ataques.

A análise do estudo apresentou perfis das vítimas da engenharia social e através dos estudos foram feitas verificações, concluindo que a principal vulnerabilidade da segurança da informação são as pessoas, pois não há recursos tecnológicos suficientes para garantir a segurança da informação mediante usuários que as desconhecem ou as utilizam de forma inadequada.

Foi observado nessa pesquisa o gênero que mais são enganados nesse golpe é o feminino e com idade superior a 60 anos, nessa situação os bancos têm que procurar formas de alertar os correntistas de idades mais elevadas, pois geralmente são os que fornecem as informações acreditando que seja a instituição bancária solicitando. Com relação à frequência na utilização do (app), tanto os que utilizavam diariamente como os que não usavam com frequência tiveram porcentagens bem parecidas, ou seja, não impactou do usuário reconhecer a página e não cair na tentativa de golpe. As notificações (SMS e aplicativo) hoje em dia são de fundamental importância e com referência a alertas bancários foi a que mais auxiliou os correntistas, alertando na identificação de pagamentos e compras onlines.

A desinformação das normas de segurança pelos correntistas, também é observado na pesquisa, considerando a maneira como são divulgadas pelos bancos, na qual, o usuário precisa ir em busca da informação, não havendo interatividade. Esta vulnerabilidade é classificada como vulnerabilidade humana da segurança da informação, explorada pela engenharia social. Como melhoria da segurança da informação as Instituições Bancárias poderiam dispor em seus *sites* as informações já existentes sobre a política de segurança da informação, porém, de forma mais interativa, não dependendo da ação única e exclusiva dos usuários, através de alertas de segurança antes de realizarem uma transação financeira, além de concordância com tais políticas no primeiro acesso realizado pelo usuário.

A técnica de *phishing* apresenta grande efetividade com relação ao comprometimento

da segurança da informação relacionada aos correntistas, na qual o engenheiro social, de forma indireta, conduz o usuário a acessar *sites* falsos como se fossem os verdadeiros, permitindo em tal ambiente a obtenção das suas informações confidenciais. A educação voltada para a gestão da segurança da informação nas organizações e de seus usuários, como correntistas de Instituições Bancárias é um importante aliado ao enfrentamento desta ameaça social, a engenhariasocial.

Com base no estudo dos métodos de ataques dos engenheiros sociais nas três instituições bancárias a única instituição que não teve formas de invasão utilizadas pelos *phishers* foi a do Bradesco, ou seja, não se achou formas que são utilizadas para tirar dinheiro dos correntistas nessa instituição devido ao fator de segurança utilizado pelo Bradesco, porém Banco do Brasil e Itaú é possível fazer a monetização da conta com os dados em posse como exibido na seção 6.3.5.

Para a hipótese levantada foi possível chegar à conclusão que a engenharia social compromete a segurança da informação dos usuários de Instituições Bancárias. A segurança da informação é uma preocupação dos usuários de Instituições Bancárias e estas divulgam em seus *sites* orientações relacionadas ao assunto. O tópico inicial da pesquisa demonstrou os conceitos norteadores do tema e a sua interação relacionando-os e evidenciando o desafio da segurança da informação em proteger informações valoradas disponíveis nas Instituições Bancárias.

Desta forma, ao confirmar o estudo conclui-se que a proteção das informações confidenciais dos correntistas de um banco é de responsabilidade de tais organizações, independente do banco escolhido para obtenção de serviço. Porém, as pessoas detentoras de tais informações pertencem ao processo de proteção e, para tanto, precisam ser orientadas.

,Induz-se também, que os bancos desenvolvem em seus *sites* a publicação de alertas voltados à segurança de informações, atingindo assim, o segundo objetivo específico da pesquisa. Porém, o acesso à tais informações dependem da iniciativa do correntista em procurar a informação.

Com relação aos engenheiros sociais, sempre estarão trazendo novas formas de golpes, pois utilizam dessas táticas como forma principal de trabalho, ou seja, tiram sua renda através desses crimes. Da mesma maneira que os bancos se atualizam eles também sempre procuram novos *bugs* no sistema ou métodos para ludibriar correntistas de maneira simples e objetiva. Por esse motivo, a maioria dos usuários que já caíram em golpes de *phishing* chegaram a conclusão que poderia ser vítima novamente devido acreditar que existem várias formas de serem enganados.

As invasões de sistemas e a disseminação de programas espúrios são as atividades de maior relevância dos engenheiros sociais que ameaçam a segurança da sociedade da informação. Estes atores sociais se beneficiam de informações sigilosas e a sua presença no ciberespaço impulsiona o desenvolvimento de instrumentos tecnológicos que venham a neutralizar a sua ameaça, fazendo parte também do dinamismo da rede Klettenberg (2016).

7.2 Trabalhos futuros

Identificar os principais canais de comunicação sobre segurança da informação fornecido pelas Instituições Bancárias, considerando o atendimento pessoal nas agências bancárias e remotos como *sites*, *folders*, caixas eletrônicos, centrais de atendimento, smartphones, entre outros.

Realizar uma comparação entre *Phishing* e *Smishing* com o objetivo de determinar qual dos dois ataques é mais utilizado, mais efetividade e de maior alcance.

Analisar os sentimentos aflorados no correntista após serem vítimas de fraudes eletrônicas, considerando que os resultados da pesquisa identificaram sentimentos como o medo, insegurança e descrédito do canal utilizado e a perda da confiança na InstituiçãoBancária.

Realizar um estudo dos *sites* de bancos que são atacados com maior frequência por engenheiros sociais e entender as causas desses ataques.

REFERÊNCIAS

ALENCAR, F. **O que é spam?** 2016. Disponível em: https://www.techtudo.com.br/noticias/ noticia/2016/07/o-que-e-spam.html. Acesso em 5 jul. 2019.

ALMEIDA, M. **Aplicação de ontologias em segurança da informação**. [S.l.: s.n.], 2007. 13 p.

ALSAYED, A. O. Segurança de e-banking internet hacking phishing attacks. **International Journal of Emerging Technology and Advanced Engineering**, 2017.

BANCOCENTRAL. **Como evitar abertura de conta digital indevidamente em seu nome?**. 2017. Disponível em: https://www.conta-corrente.com/bancos/banco-central/como-evitar-abertura-decontadigital-indevidamente-em-seu-nome/. Acesso em 12 fev de 2019.

BENETTI, T. **Segurança da Informação(CID)**. 2015. Disponível em: https://www.profissionaisti.com.br/2015/07/seguranca-da-informacao-confidencialidade-integridadeedisponibilidade-cid. Acesso em: 20 jul. 2019.

BRADESCO, B. **Pagina Bradesco**. 2019. Disponível em: https://banco.bradesco/html/classic/ index.shtm.

BRASIL, B. do. **Pagina do Brasil**. 2019. Disponível em: https://www.bb.com.br/pbb/ paginainicial/voce#.

BRAGA, P. H. C. **Técnicas de engenharia social**. Rio de Janeiro: UFRJ.2011.Disponivel em: https://securityinformationnews.files.wordpress.com/2014/02/tecnicas_de_engenharia_ social.pdf. Acesso em: 17 dez. 2019.

CASTRO, G. de. **Engenharia Social**: as técnicas de ataques mais utilizadas. Profissionais ti., 2013. Disponível em: https://www.profissionaisti.com.br/2013/10/ engenharia-social-as-tecnicasde-ataquesmais-utilizadas. Acesso em: 09 mar. 2019.

CENTRAL, B. **Cresce uso de internet banking no Brasil**. Encontro digital, 2018. Disponível em: https://www.revistaencontro.com.br/canal/economia/2018/11/ cresce- uso-de-internet-bankingnobrasil.html. Acesso em: 11 abr. 2019.

FEBRABAN. **Investimentos dos bancos brasileiros crescem acima da média mundial**. Deloitte, 2018. Disponível em: https://www2.deloitte.com/br/pt/pages/financial-services/articles/pesquisadeloittefebraban-tecnologia-bancaria.html. Acesso em: 02 agos. 2019.

GANDINI, J. A. D.; SALOMÃO, D. P. d. S.; JACOB, C. **A validade jurídica dos documentos digitais**. Texto capturado em [2004 mai 06]. Disponível em: http://www1. jus. com. br/doutrina/texto. asp, 2002.

GLOBO, O. **Os cinco maiores bancos do Brasil**. 2018. Disponível em: https://oglobo.globo.com/economia/os-cinco-maiores-bancos-do-brasil-20938419. Acesso em: 13 mar. 2019.

HONG, J. **The current state of phishing attacks**. figshare, 2012.

ITAU, B. **Pagina Itau**. 2019. Disponível em: https://www.itau.com.br/.

JACOMINI, L. **Como abrir Conta Digital e economizar com ela**. 2018. Disponível em: https://www.foregon.com/blog/como-abrir-conta-digital-economizar.

KASPERSKY. **Brasileiros são maiores vítimas de golpes phishing no mundo**. 2017. Disponível em: https://www.kaspersky.com.br/blog/phishing-klsec-brasil-assolini/10642. Acesso em: 01 abril. 2019.

KLETTENBERG, J. **Um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de instituições bancárias**. Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências da Educação, Programa de Pós-Graduação em Ciência da Informação, Florianópolis.

MITNICK, Kevin D, and William L. SIMON. **A arte de enganar**. (2003).

MOUTON M. MALAN, L. L. F.; VENTER, H. social engineer attack framework. **IEEE Conference on Information Security for South Africa**, p. 1–9, 2014.

OLIVEIRA, Roberto A . O **internet banking e os habitos de uso entre os clientes**. Dissertação de mestrado - Universidade Federal do Rio Grande do Sul. Escola de Administração. Programa de PósGraduação em Administração. 2000.

PROMOBIT. **Os 5 melhores bancos digitais do brasil.** 2019. Disponível em: https: de //www.promobit.com.br/blog/os-5-melhores-bancos-digitais-do-brasil-411.

RAZAK, L. The effect of security and privacy perceptions on customers trust to accept internet banking services: An extension of tam'mohammed a. **Journal of Engineering and Applied Science**, v. 100, p. 545–552, 2016.

RFC8846. **(TLS) Protocol Version 1.3**. 2018. Disponível em: https://tools.ietf.org/html/ rfc8446.

ROHR, A. **Pena para hackers pode chegar a 5 anos de prisão, dizem espe- cialistas**. 2011. Disponível em: http://g1.globo.com/tecnologia/noticia/2011/06/ pena-para-hackerspodechegar-5-anos-de-prisao-dizem-especialistas.html.

RUSSELL, A. **O que é SSL?** 2019. Disponível em: https://www.ssl.com/faqs/faq-what-is-ssl/.

SAFEENA, R. **Internet banking adoption in an emerging economy:** Indian consumer's perspective. 2010. Disponível em: https://www.researchgate.net/publication/50367436_ Internet_Banking_Adoption_in_an_Emerging_Economy_Indian_Consumer's_Perspective.

SANTIAGO, S. **Técnicas de segurança em internet banking**. 2013. Disponível em: http://blog.newtonpaiva.br/pos/wp-content/uploads/2013/04/PDF-E6-SI53.pd.

SOUZA, A. G., SCHEFLER. C. M. S. **Envio de Spam – é ilegal?** 2014. Disponível em: http://www.gaiofatoegalvao.com.br/artigos/envio-de-spam-e-ilegal. Acesso em: 26 set. 2019.

SERAFIM. V. S. **Introdução à criptografia**: criptografia e criptoanálise. 2014.

SILVA, A.O.Engenharia social: o fator humano na segurança da informação. [S.l.]: **Coleção Meira Mattos Revista das Ciências Militares**, 2011.

STALLINGS, W. **Cryptography and network security**. [S.l.]: Pearson, 2006.

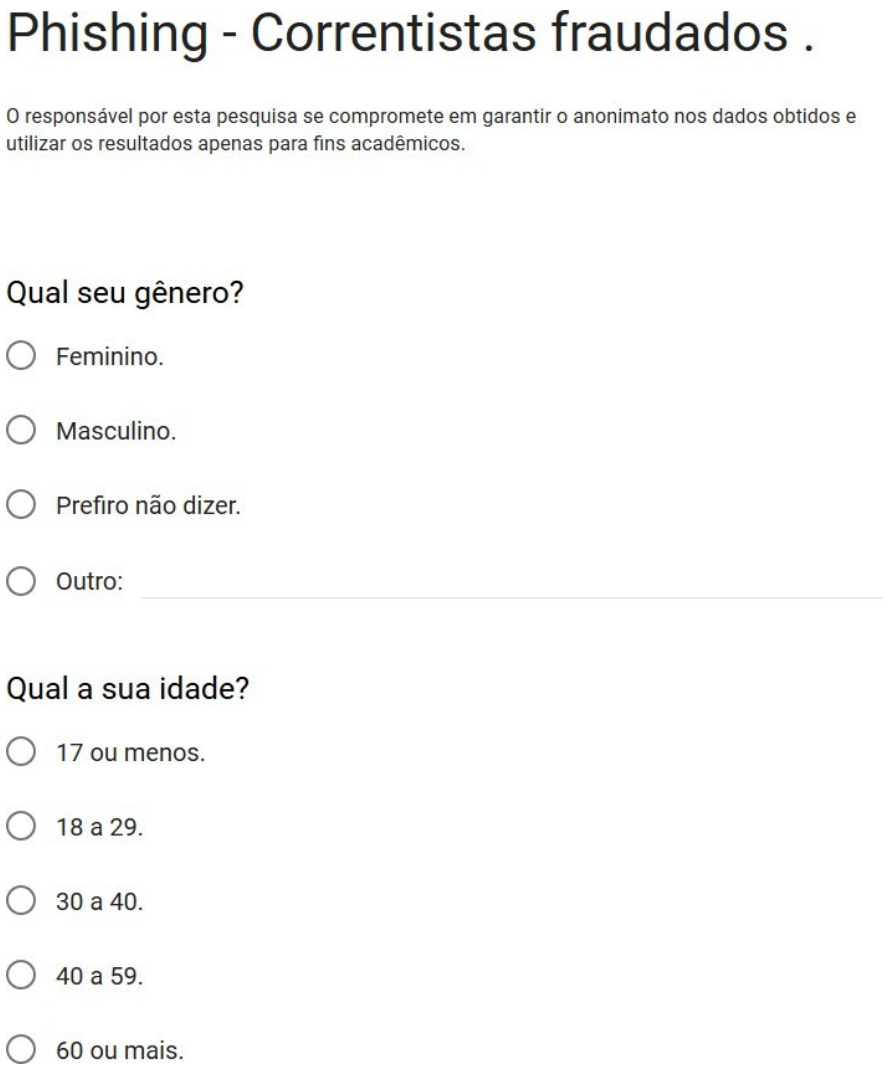
VIVIAN, D. **Como funciona o fluxo de infraestrutura de chaves públicas no Brasil?** 2019. Disponível em: https://www.bry.com.br/blog/infraestrutura-chaves-publicas. Acesso em: 23 out. 2019.

YEBOAH-BOATENG, E. O. Smishing ameação contra dispositivos moveis. **Journal of Emerging Trends in Computing and Information Sciences**, 2014.

ANEXO –FORMULÁRIO DE PESQUISA

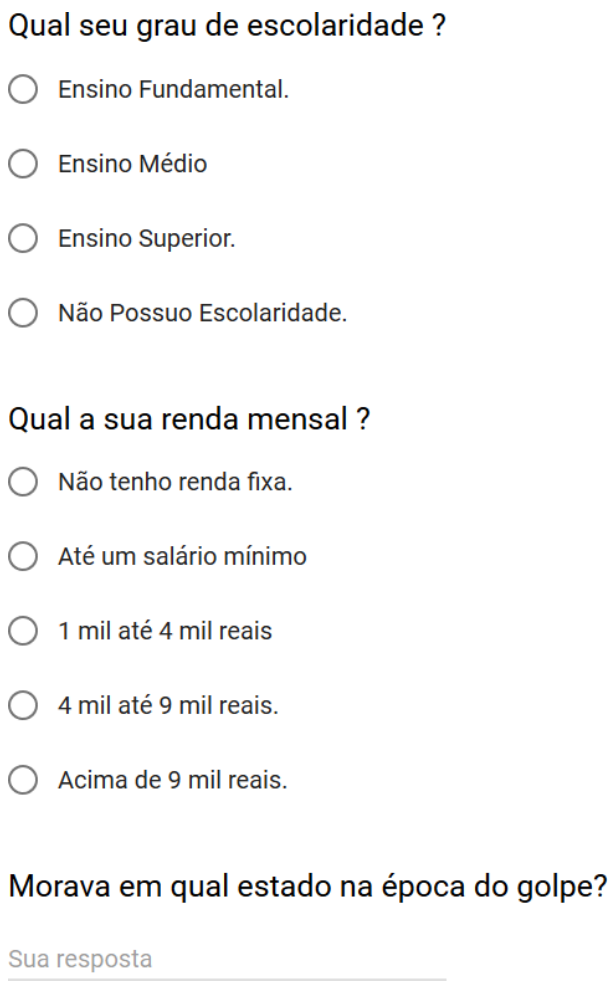
Pesquisa “SEGURANÇA DA INFORMAÇÃO”: um estudo sobre o uso da engenharia Social para capturar informações sigilosas de usuários de Instituições Bancárias. O objetivo da coleta de dados é fundamentar o desenvolvimento da dissertação de graduação em Engenharia de Software da Universidade Federal do Ceará . Os dados obtidos são de uso confidencial, sendo garantido o anonimato dos participantes da pesquisa, o sigilo bancário e o da informação.

Figura 38 – Informações pessoais dos correntistas 1



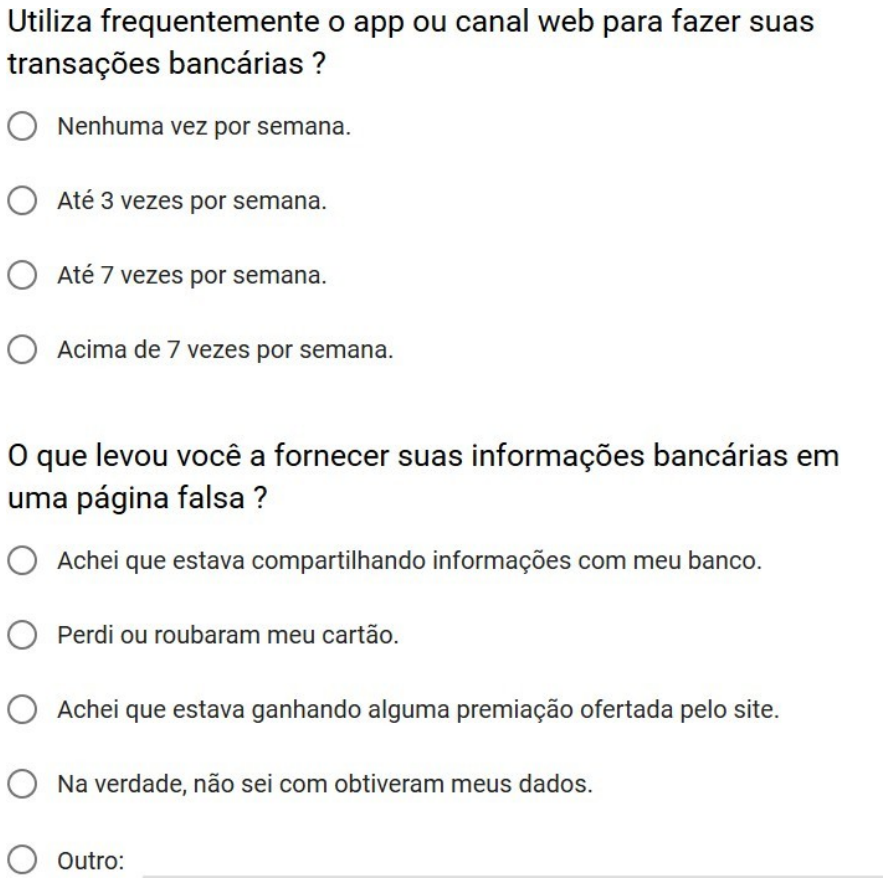
Fonte: Elaborada pelo autor

Figura 39 – Informações pessoais dos correntistas 2



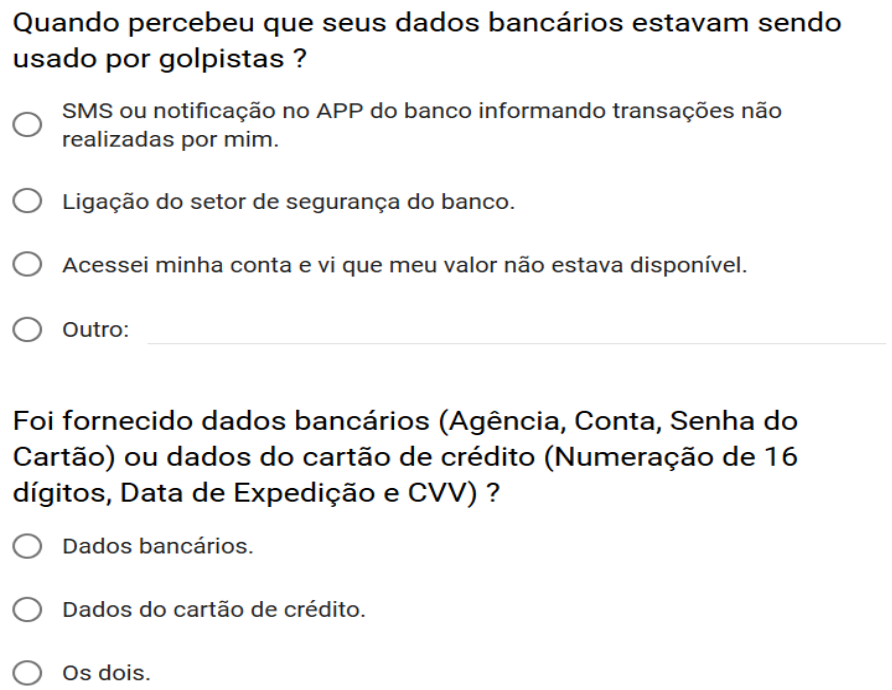
Fonte: Elaborada pelo autor

Figura 40 – Informações bancárias



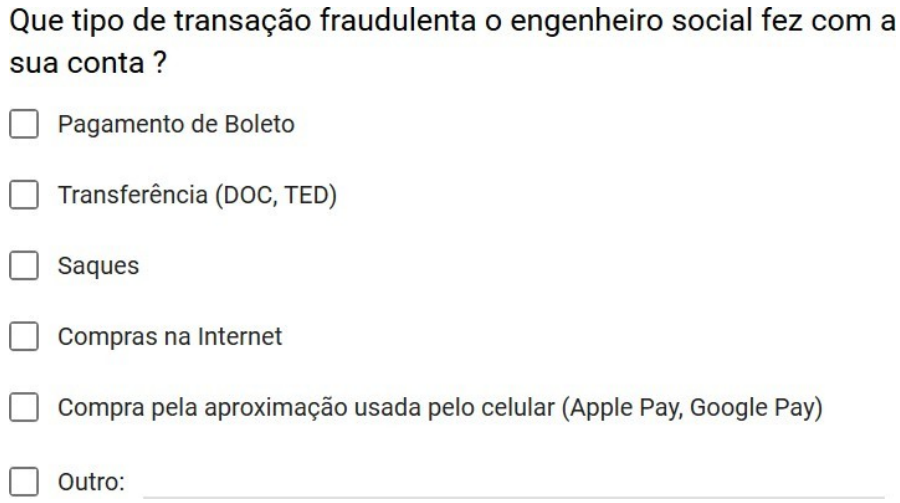
Fonte: Elaborada pelo autor

Figura 41 – Informações dos ataques



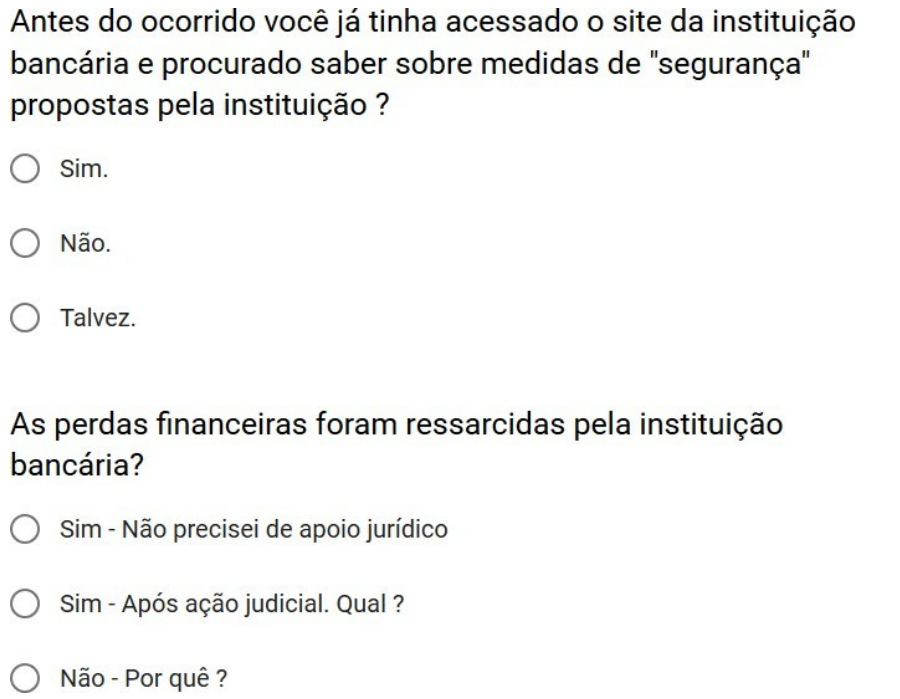
Fonte: Elaborada pelo autor

Figura 42 – Segurança nos bancos 1



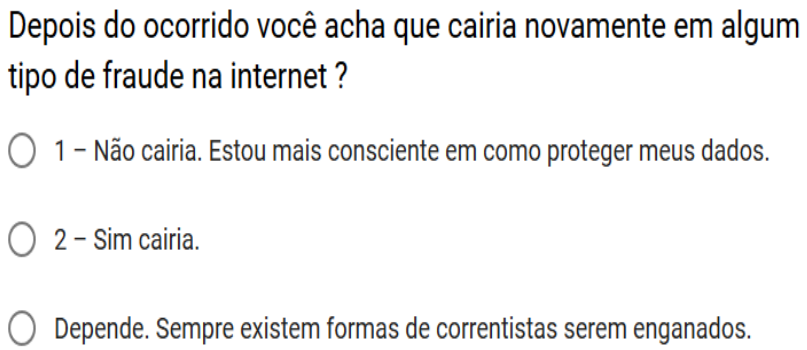
Fonte: Elaborada pelo autor

Figura 43 – Segurança nos bancos 2



Fonte: Elaborada pelo autor

Figura 44 – Vítimas de um novo golpe



Fonte: Elaborada pelo autor