UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE RUSSAS

CURSO DE ENGENHARIA DE SOFTWARE

EMERSON DIEGO RIBEIRO MARTINS

IDENTIFICAÇÃO DA VULNERABILIDADE DE USUÁRIOS A PARTIR DE SUAS POSTAGENS EM PÁGINAS BANCÁRIAS

RUSSAS

2018

EMERSON DIEGO RIBEIRO MARTINS

IDENTIFICAÇÃO DA VULNERABILIDADE DE USUÁRIOS A PARTIR DE SUAS POSTAGENS EM PÁGINAS BANCÁRIAS

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

Orientador: Profa. Dra. Marília Soares Mendes.

RUSSAS

2018

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)

M342i Martins, Emerson Diego.
Identificação da vulnerabilidade de usuários a partir de suas postagens em páginas bancárias. / Emerson Diego Martins. – 2018.
45 f. : il. color.

Trabalho de Conclusão de Curso (especialização) – Universidade Federal do Ceará, , Russas, 2018.
Orientação: Profa. Dra. Marília Soares Mendes.

1. Vulnerabilidade. 2. Páginas Bancárias. 3. Rede Sociais. 4. Engenharia Social. I. Título.
CDD

EMERSON DIEGO RIBEIRO MARTINS

IDENTIFICAÇÃO DA VULNERABILIDADE DE USUÁRIOS A PARTIR DE SUAS POSTAGENS EM PÁGINAS BANCÁRIAS

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Engenharia de Software do Centro de Ciências e Tecnologia Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Software.

Orientador: Profa. Dra. Marília Soares Mendes.

Aprovada em: ___/___/_____.

BANCA EXAMINADORA

_____
Profa. Dra. Marília Soares Mendes (Orientadora)
Universidade Federal do Ceará (UFC)

_____
Profa. Dra. Anna Beatriz dos Santos Marques
Universidade Federal do Ceará (UFC)

_____
Prof. Me. José Osvaldo Mesquita Chaves
Universidade Federal do Ceará (UFC)

A minha família, por sua capacidade de acreditar em mim e investir em mim. Aos meus pais, seu cuidado e dedicação foi que deu, em alguns momentos, a esperança para seguir.

A Maria Consuelo, sua presença significou segurança e certeza de que não estou sozinho nessa caminhada.

AGRADECIMENTOS

Primeiramente a Deus por me conceder saúde, força e sabedoria para superar os desafios não somente nestes anos como universitário, mas que em todos os momentos da minha vida.

Aos meus pais e irmão, Erivan, Maria Lúcia e Wallace, por sempre me apoiarem, incentivarem e acreditarem em mim!

A minha avó, Maria Consuelo, e tia Maria Nair por sempre cuidar de mim como se fosse seu filho, por incentivo e orientação e pelas orações em meu favor.

A meu amigo e supervisor de estágio e orientadora de estágio, Francisco Gilcélio e Anna Beatriz, por acreditar no meu potencial e ter contribuído imensamente para minha carreira profissional.

A esta universidade, seu corpo docente, direção e administração que oportunizaram a janela que hoje vislumbro um horizonte superior, eivado pela acendrada confiança no mérito e ética aqui presente.

A minha querida professora Marília Soares Mendes, pela orientação, motivação e dedicação para conclusão deste trabalho e pela oportunidade que me foi dada.

Ao professor Rafael, por ter disponibilizado seu tempo e pela grande ajuda me dada para conclusão deste trabalho.

Aos meus grandes amigos e companheiros, que fizeram parte da minha formação e que vão continuar presentes em minha vida com certeza. Matheus Oliveira, Luan, Matheus Diorgenes, Barbara e outros não citados, mas que também tenho grande carinho, o meu muito obrigado.

“Feliz aquele cujo conhecimento é livre de ilusões e superstições”.

Buda

RESUMO

A exploração das redes sociais na Internet, em especial a aplicação dessas redes como ferramentas para se realizar o relacionamento entre o banco e cliente de bancos, vem cada vez mais sendo uma opção diferenciada para os clientes bancários se relacionarem com seu banco com mais praticidade e conforto, como apoio inicial para tratar de assuntos como: dúvidas, reclamações, sugestões ou até mesmo solicitações relacionadas diretamente com o banco, obtendo respostas rápidas sem precisar se dirigir a uma agência de seu banco. São apresentados conceitos referentes à engenharia social, segurança da informação, acesso dos usuários em páginas bancárias, sistemas sociais e utilização de empresas nas páginas de redes sociais. Este trabalho aborda a comunicação entre clientes bancários e seus respectivos bancos, visando a segurança de suas postagens como forma de se estudar a vulnerabilidade a partir de seus textos em páginas de sistemas bancários em sistemas sociais. Neste trabalho foi realizado um experimento com aproximadamente 1.000 postagens extraídas de páginas bancárias na rede social Facebook. Essas postagens passaram por uma classificação e apresentaram os seguintes percentuais estatísticos para cada tipo de classificação: Postagens Vulneráveis (11,44%), Não Vulneráveis à quebra de sigilo do usuário (50,57%) e Postagem Reencaminhada para área privada de comunicação privada banco/cliente (38,09%). Além dessas postagens, não foram levadas em consideração as postagens relacionadas a publicidade e propaganda direcionadas aos bancos trabalhados (Banco do Brasil e Banco Bradesco).

Palavras-chave: Vulnerabilidade. Páginas bancárias. Redes sociais. Engenharia social.

ABSTRACT

The exploitation of social networks on the Internet, especially the application of these networks as tools for the relationship between the bank and bank customers, is increasingly being a differentiated option for bank clients to relate to their bank more conveniently and comfort, as initial support to deal with issues such as: doubts, complaints, suggestions or even requests directly related to the bank, getting quick answers without having to go to an agency from your bank. Concepts related to social engineering, information security, users' access to banking pages, social systems and the use of companies in social network pages are presented. This paper deals with the communication between bank clients and their respective banks, aiming the security of their posts as a way of studying vulnerability from their texts on pages of banking systems in social systems. In this work was carried out an experiment with approximately 1,000 posts extracted from bank pages in the social network Facebook. These posts had a classification and presented the following statistical percentages for each type of classification: Vulnerable Posts (11.44%), Not Vulnerable to user secrecy breach (50.57%) and Post Forwarded to private area of private communication bank / customer (38.09%). In addition to these postings, the postings related to advertising and publicity directed to the banks worked (Banco do Brasil and Banco Bradesco) were not taken into account.

Keywords: Vulnerability. Bank web pages. Social Networks. Social Engineering.

LISTA DE ILUSTRAÇÕES

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
API	Application Programming Interface
CPF	Cadastro de Pessoa Física
HTTP	Hyper Text Transfer Protocol
RG	Registro Geral
SS	Sistemas Sociais

SUMÁRIO

1 INTRODUÇÃO

Vivemos em uma era tecnológica onde o uso das redes sociais pelos smartphones se tornou algo comum no nosso dia a dia. De acordo com os dados do Banco Central, hoje 66% das transações bancárias são feitas por meio de Internet Banking, Aplicativos ou Call Center. Ainda de acordo com o levantamento apenas um terço das operações são feitas em pontos de atendimento. Com aproximadamente 25 bilhões de transações registradas o uso dos smartphones representa 35% desse total (G1, 2018). Tem-se, então os vários canais de atendimento para a resolução de problemas sendo que as redes sociais são uma das opções mais utilizadas.

As redes sociais permitem o relacionamento entre as pessoas, criar novas amizades, e manter contatos com velhos amigos. Ao interagir nesses sistemas, o usuário pode compartilhar fotos de família, lugares que frequenta, viagens, vídeos, comentários, sites visitados, e muitos outros dados, que podem ser preciosos nas mãos dos Engenheiros Sociais. Os Engenheiros Sociais são pessoas que manipulam outras pessoas psicologicamente para execução de ações ou divulgar informações confidenciais (HATFIELD, 2017). Eles podem ter acesso a uma série de informações de usuários a partir de seus dados coletados. Nos últimos anos, houve um grande aumento do número de ataques envolvendo engenharia social nas redes sociais. Perseguição e roubo de identidade são os principais tipos de ameaças que tornam a segurança neste ambiente um verdadeiro desafio para os responsáveis. O maior problema é que muitos desses ataques e ameaças são por parte de técnicas que desrespeitam “fatores humanos” e não a parte tecnológica como as falhas, faltas e erros de sistemas (OLIVEIRA, 2011).

Atualmente, para facilitar a comunicação e a troca de informações, adotou-se a metodologia de comunicação em massa, em que um emissor atinge vários receptores no mesmo instante (MENEZES, 2017). As redes sociais de internet não fogem a essa regra.

O Facebook é hoje a rede social com a maior quantidade de usuários ativos no mundo com 2.234 milhões de usuários (STATISTA, 2018). Dentre a diversidade de usuários que o Facebook tem, existem aqueles que utilizam páginas bancárias para se relacionar com o seu banco de forma rápida e prática. Tais usuários utilizam páginas de bancos no Facebook; ou Twitter; a fim de tirar dúvidas sobre as funcionalidades do sistema, bem como para solicitar apoio na realização de alguns serviços, como por exemplo: desbloqueio de conta, desbloqueio de cartão de crédito, informações a respeito de sua conta, e demais serviços. Os usuários postam suas eventuais dúvidas, solicitações, informações ou até mesmo reclamações

ao banco em questão a fim de ter uma solução para o assunto tratado.

Grande parcela das pessoas não tem optado em ir a agências bancárias e esperar por horas por um atendimento que seria possível fazer em casa. Um banco, universidade ou até mesmo mercado, somente consegue operar seu funcionamento devido à troca de conhecimentos e à disponibilização automática da informação. Isso só é possível via computação, sistemas e redes.

As redes sociais estão indo além de um relacionamento entre usuários, cada vez mais empresas investem nas redes sociais a fim de seus produtos se propagarem pela rede mais rapidamente, e fazerem pesquisas de suas marcas. Isso é demonstrado pelo aumento do conhecimento da população, possibilitado pelos computadores, pela melhoria da qualidade e expectativa de vida e pela velocidade com que se resolvem questões entre partes atualmente (MENEZES, 2017).

Existem diversos problemas que os usuários/clientes de bancos enfrentam,+ como, por exemplo, a falta de conhecimento de se utilizar as redes sociais de forma segura e eficiente, tomando conhecimento sobre o que deve ser postado a fim de não comprometer a segurança de seus dados.

Em uma breve análise pelo autor deste trabalho no Facebook, foi possível constatar que alguns usuários estão postando seus dados à procura de auxílio para o uso do sistema ou serviço bancário. Foram observadas entre os dados informados de forma pública: número da conta, CPF, RG, cartões sociais de bolsas do governo, dentre outros documentos que os usuários utilizam para passar seus dados pessoais de forma pública. As postagens com tais características são chamadas neste trabalho de “postagens vulneráveis”, e tem como objetivo investigar o comportamento dos usuários de páginas bancárias por meio de suas postagens com relação, revelando problemas de segurança e privacidade.

A organização deste trabalho se dá da seguinte forma: no primeiro capítulo aborda uma breve introdução sobre o problema, objetivos e procedimentos metodológicos.

No segundo capítulo é abordado toda a fundamentação teórica, apresentando conceitos de engenharia social, segurança da informação, acesso dos usuários em páginas bancárias, sistemas sociais na utilização de páginas de empresas e análise de postagens nas redes sociais, e os trabalhos relacionados.

O terceiro capítulo apresenta o estudo de caso, uma investigação a partir de um experimento de extração e análise de postagens de páginas bancárias no Facebook. Os resultados da investigação e as considerações finais, contendo: as contribuições do trabalho; uma discussão sobre o trabalho; e os trabalhos futuros.

1.1 Objetivos

Investigar padrões de vulnerabilidade em postagens de usuários em páginas bancárias em uma rede social.

1.1.1 Objetivos específicos

a) Coletar e analisar postagens dos usuários em páginas bancárias nas redes sociais, tendo como a fonte de extração principal o Facebook;
b) Identificar postagens vulneráveis;
c) Identificar as estratégias adotadas pelas empresas ou redes sociais para fornecer privacidade aos usuários clientes de páginas bancárias.

1.2 Procedimentos metodológicos

Este trabalho seguiu uma abordagem teórica e outra prática. A abordagem teórica foi constituída do estudo da fundamentação teórica necessária para desenvolvimento deste trabalho (conceito e tecnologias). A abordagem prática foi constituída de uma investigação de postagens no Facebook, com as seguintes etapas:

a) Extração de Postagens;
b) Análise das Postagens Vulneráveis;
c) Análise de Resultados.

Tais etapas são explicadas na investigação apresentada neste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados os conceitos necessários para a compreensão deste trabalho. Em um primeiro momento é introduzido o conceito de Engenharia Social, seguido pela teoria da Segurança da Informação, como o acesso dos usuários tem sido nas páginas bancárias e, por fim, uma breve introdução sobre os sistemas sociais, especificando a utilização das empresas nas páginas de redes sociais e análise de postagens de usuários em redes sociais.

2.1 Engenharia Social

Engenharia Social compreende a prática utilizada para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio de enganação ou exploração da confiança das pessoas (LIM, 2012). A segurança da informação é um dos fatores relevantes para os usuários sentirem-se aptos para utilizar os sistemas colaborativos (LIM, 2012). Visando o bem-estar dos usuários será necessária a criação de metodologias integradas a esses sistemas para que pessoas de má fé não se utilizem de técnicas de Engenharia Social, como por exemplo: pessoas podem se passar por outras pessoas a fim de assumir falsas personalidades, fingir que é um profissional de determinada área, etc. Essas pessoas, também, garantem meios para entrar em determinadas áreas de privacidade do usuário que não necessitam da força bruta ou de erros de softwares; exploram falhas de segurança de outras pessoas que, quando não conscientizadas (treinadas) para esses ataques, podem ser facilmente induzidas a repassar informações sem a mera percepção no que pode acarretar a si próprio.

O grande sucesso das redes sociais criou um novo espaço para compartilhamento de informações, consequentemente, formou um “mural” no qual os engenheiros sociais são capazes de garimpar dados de forma anônima. Era necessária uma maior exposição do hacker pessoa que possui interesse e um bom conhecimento na área de informática, sendo capaz de fazer uma ou mais modificações, em algum sistema informático a fim de obter informações ou o acesso a estas. Por meio das redes sociais é possível realizar uma tarefa semelhante sem contato físico e sem deixar rastros (e-mails, grampos, filmagens). A grande maioria dos usuários não sabem o quanto as informações publicadas abertamente podem ser prejudiciais. Lim (2012) cita as características mais marcantes encontradas nestes indivíduos:

> - Necessidade de se expressar: muitos usuários, especialmente os mais jovens, sentem grande necessidade de se expressar publicamente;
> - Necessidade de atenção, Inerente do ser humano: muitos indivíduos utilizam o espaço virtual visando à atenção de outros usuários;
> - Necessidade de popularidade: esta característica também é conhecida no mundo real, em que se destacam as pessoas mais populares. No mundo virtual não é diferente, usuários postam fotos provocativas ou ostentando objetos de valor visando alcançar popularidade na rede.

Estas necessidades citadas por Lim (2012) são comuns em comunidades reais, entretanto levam a satisfação dos usuários de redes sociais, a estar conectados e compartilhando de sua vida com seus amigos de redes sociais, assim podendo gerar uma possível vulnerabilidade de suas informações pessoais e consequentemente abrir possibilidades para uma quebra de sigilo. Buscando estas características no mundo virtual, os usuários acabam expondo de maneira inconscientemente suas informações, assim repassando dados próprios que comprometem a quebra de sigilo bancário, muitas das vezes, que deveriam ser privadas. Por exemplo, completando todos os campos pertencentes ao Perfil, o usuário publicará informações valiosas para prática do phishing ou roubo de identidade, como: Nome, cidade, CPF, RG, conta bancária, agência e local de trabalho Lim (2012). É possível ainda preencher dados como telefone e endereço residencial que sozinhos já dão margens para a quebra de sigilo bancário.

As fotos postadas na *Timeline* (linha do tempo, em inglês) de um perfil, ou até mesmo fotos de documentos pessoais revelam um grande leque de informações a um engenheiro social como agência da conta, tipo de conta, dentre outras informações pessoais que levam ao comprometimento da segurança de dados.

2.2 Segurança da Informação

A segurança da informação é uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alteração indevida ou sua disponibilidade Sêmola (2003).

Com uma importância cada vez maior para as organizações, as informações são consideradas um ativo de elevado valor que deve ser adequadamente mantido e protegido, para que se mantenha a continuidade das atividades de negócio e até mesmo a existência da organização, como por exemplo, os bancos.

A informação é um recurso crítico não apenas para a realização de tarefas e concretização de negócios, mas também para a tomada de decisões, propagar informações, e

disseminar o conhecimento. Pelo fato de estarem armazenadas em meios eletrônicos e até mesmo conectadas as redes externas, as informações poderiam ser divulgadas a concorrentes, corrompidas, apagadas ou ate mesmo não estar disponíveis quando necessário para as atividades Ferreira (2003). "São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade, onde também tem a finalidade de contribuir com a privacidade de seus usuários". (ABNT, 2012).

Os sites de relacionamento investem constantemente em novas ferramentas e novos métodos de segurança da informação. Desde sua criação, o Facebook evoluiu muito na área da sociabilização, trazendo novos recursos a cada atualização do sistema. Com a segurança não foi diferente. Quando o Facebook tornou-se público, não havia opções de privacidade disponíveis aos usuários, o que permitia que qualquer indivíduo com um perfil cadastrado no site obtivesse acesso a todos os outros, mesmo sem vínculo algum. Antes de se tornar disponível para o público, o Facebook era um site de relacionamentos fechado, voltado somente para a sociedade acadêmica e umas poucas empresas convidadas. Desta forma, mesmo que todo perfil fosse aberto à comunidade, os outros membros eram conhecidos e não gerava preocupação no quesito da privacidade. A partir do momento que esta política foi abandonada, uma onda de novos usuários passou a integrar o site, trazendo, além de um grande crescimento da rede, pessoas de realidades diferentes e, no meio destas, pessoas de má índole, fraudadores e golpistas.

Para evitar possíveis problemas com privacidade, o Facebook, assim como outras redes sociais, implantou um sistema de permissão a nível de grupo, ou seja: todas as informações pessoais, posts, fotos, vídeos e comentários ficam disponíveis apenas para os usuários classificados como *friend* (amigo, em inglês). Existem diversas classificações de amigos previamente implantadas, usuários caracterizados como *coworker* (colega de trabalho, em inglês) ou *Acquaintances (conhecidos, em inglês)*, por exemplo, possuem um menor nível de detalhes do perfil em questão. Além dos níveis de permissão pré-definidos é possível criar novos grupos e impor a eles configurações personalizadas de privacidade, permitindo um acesso selecionado às informações publicadas. Fora do campo de amizades, também podem ser impostas outras regras como quem pode lhe enviar pedido de amizade e quais informações suas estão disponíveis ao público.

Muitas empresas hoje trabalham com a questão da segurança da informação já que essa é um bem de grande valor e a engrenharia social pesa sobre essa. De acordo com a Norma Brasileira NBR ISO/IEC 17799 de 2005 a informação deve ser adequadamente protegida. De acordo com a NBR ISO/IEC 17799 de 2005 os princípios básicos para se ter

uma segurança da Informação são: Confidencialidade, Integridade e Disponibilidade, explicadas a seguir:

a) Confidencialidade: garantia de que a informação esteja acessível somente a pessoas autorizadas e um sistema de autenticação, impedindo que pessoas não autorizadas possam ter acesso a ela;

b) Integridade: a informação não pode sofrer manipulação e deve retornar sempre que necessário em sua forma original.

c) Disponibilidade: A informação deve sempre estar disponível no momento em que for necessário.

Pode-se dizer que a confidencialidade se torna dependente da integridade pois uma vez que a mesma for perdida não existem mais mecanismos de controle que garantam que a informação é confiável, e assim a integridade se torna dependente da confidencialidade, pois se a mesma for perdida e qualquer usuário passar a ter acesso os mecanismos de integridade facilmente podem ser desativados.

2.3 Acesso dos usuários em páginas bancárias

A popularização da internet foi um evento que impactou a maneira como as empresas fazem seu marketing e disponibilizam suas informações. Assim as instituições cada vez mais observam que os sistemas sociais são um meio alternativo de propagar seus produtos de maneira mais acessível aos seus clientes Torres (2009).

Em uma investigação inicial deste trabalho foram observadas postagens dos usuários contendo informações como: RG, CPF, Cartão Social, dentre outros dados que comprometem a segurança do cliente bancário. Os bancos estão adotando a comunicação pelas páginas de redes sociais com o intuito de facilitar a comunicação com seu cliente e gerar uma maior rapidez em solucionar as eventuais dúvidas, solicitações, de modo que seus clientes estejam cada vez mais informados sobre seu banco e que tenham seus atendimentos os mais rápidos possíveis. Esse relacionamento entre cliente e banco acontece por meio de postagens nas páginas de bancos nas redes sociais.

As páginas em redes sociais proporcionam novas maneiras de conexões, com as quais as empresas podem não estar acostumadas a lidar Nakagawa; Gouvêa (2006). Entretanto, o mundo virtual e suas interações são reflexos da sociedade, apenas transferidos do mundo físico para interações eletrônicas Torres (2009).

No Apêndice B deste trabalho estão algumas imagens de postagens dos usuários observadas. Os nomes e imagens dos usuários foram ocultados para preservação de suas identidades.

2.4 Sistemas Sociais

Ellison (2007) define Sistemas Sociais como serviços baseados na web que permitem aos indivíduos construir um perfil público ou semipúblico dentro de um sistema limitado, articular uma lista de outros usuários com quem eles compartilham uma conexão, e visualizar e percorrer a sua lista de conexões e aquelas feitas por outros dentro do sistema. Segundo Baranauskas et al. (2010), o surgimento dos Sistemas Sociais (como Twitter, Facebook, Youtube e Instagram) colaborou para uma mudança de paradigma: mais do que interligar documentos, páginas ou recursos, a Web hoje interliga pessoas, organizações e conceitos, dando origem à chamada Web Social.

As pessoas se voltam para SS para expressar seus sentimentos em relação a grandes acontecimentos de suas vidas, como aniversários, casamentos, encontros, etc (BRUBAKER et al., 2012 apud MENDES, 2015). Porém, por ser totalmente dependente dos usuários, o êxito desses sistemas depende fortemente de aspectos da Interação Humano Computador-IHC relacionados, por exemplo, com fatores emocionais, socioculturais e técnicos, incluindo a forma como os recursos de interface são empregados (BARANAUSKAS; PEREIRA; SILVA, 2010).

2.4.1 Análise de postagens de usuários em Redes Sociais

Existem muitos trabalhos que têm investigado postagens de usuários em redes sociais, seus objetivos são desde sua opinião sobre algum assunto, como saúde, jogos esportivos, política, até mesmo sobre o uso do sistema (Mendes, 2015). No entanto, existem poucos estudos de vulnerabilidades de usuários a partir de suas postagens. Mao *et al*.,(2011 apud MENDES, 2015) para destacar as ameaças às privacidades enfrentadas pelos usuários:

> Segundo os autores, tais ameaças são os próprios conteúdos postados pelos usuários, como os seguintes temas sensíveis a privacidade: férias/viagens, postagens sob a influência de álcool e postagens de doenças. Eles utilizaram uma ferramenta de extração de postagem e coletaram 575.689 postagens sobre férias, 21.297 postagens sobre bebidas e 149.636 postagens sobre doença, concluindo o quão os usuários estão expondo sua privacidade.

De acordo com a empresa Forrester Research, 75% dos usuários da Internet acessaram Sistemas Sociais no Verão de 2008, acima dos 56% em 2007 (KAPLAN; HAENLEIN, 2010). Números mais recentes indicam que entre 79% (Europa) e 86% (US) dos adultos online se envolvem com Sistemas Sociais, onde o Facebook, atualmente o site mais popular dentre eles, reporta mais de 900 milhões de usuários ativos mensais (KARNIK et al., 2013).

Neste trabalho são analisadas as postagens de usuários com objetivo de investigar a vulnerabilidade de dados que estão sendo expostos nas páginas bancárias em redes sociais.

2.5 Trabalhos relacionados

As vulnerabilidades do ser humano em relação à segurança da informação têm sido frequentemente pesquisadas nos últimos anos. Capistrano (2013), em seu trabalho intitulado “Redes sociais virtuais como ambiente de exposição de dados pessoais para a engenharia social”, apresentou que, embora a crescente utilização da internet possibilite a resolução de problemas de forma rápida e prática, cresce também o fluxo de informações pessoais expostas por parte de pessoas despreparadas para atuar nestes ambientes.

Oliveira (2011), em seu trabalho intitulado “Quantificação de vulnerabilidades em segurança da informação avaliando maturidade de pessoas” apresenta um instrumento que quantifica as vulnerabilidades e ao mesmo tempo avalia a maturidade das pessoas no que diz respeito a ameaças como exemplo por e-mail.

Sêmola (2013), em seu trabalho intitulado “Gestão da Segurança da Informação: uma visão executiva da segurança da informação” considera a Segurança da Informação como a prática de gestão de riscos e incidentes que impliquem no comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação.” A segurança da informação é um dos fatores relevantes para o usuário sentir-se apto a utilizar os sistemas colaborativos. O trabalho apresenta como as empresas têm administrado as informações de forma segura e privativas no meio empresarial.

Laureano e Moraes (2005), em seu trabalho intitulado “Uma Abordagem Para a Proteção de Detectores de Intrusão Baseadas em Máquinas Virtuais” apresentam que, embora possa ser dado esse critério de valor a informação, nem toda informação é relevante ou crucial a ponto de merecer uma maior atenção. Não obstante existem informações que podem ser tão

cruciais e importantes que o custo da sua integridade será menor que qualquer outro custo se não dispor dela adequadamente. De acordo com os autores, uma informação pode ser classificada pelo seu nível de sigilo que seria pública, interna, confidencial e secreta (Laureano; Moraes, 2005):

> a) Pública - informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;
> b) Interna - o acesso a esse tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital;
> c) Confidencial - informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;
> d) Secreta - informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a companhia

Rezende e Abreu (2000), em seu trabalho intitulado "Tecnologia da informação aplicada a sistemas de informação empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas." define que informação é o dado com uma interpretação lógica ou natural é agregada pelo usuário. Pode-se classificar a informação como um ativo da empresa uma vez que traz valor a empresa. Uma informação já seria um ou mais dados organizados de maneira compreensível ao qual baseado nessa organização consegue revelar algum significado. O trabalho apresenta como a informação nos dias de hoje tem um valor altamente significativo e pode representar um grande poder para quem a possui, seja pessoa, seja instituição. Ela possui seu valor, pois está presente em todas as atividades que envolvem pessoas, processos, sistemas, recursos financeiros, tecnologias, etc.

Pereira e Fonseca (1997), em seu trabalho "Faces da Decisão: as mudanças de paradigmas e o poder da decisão.", tem a visão que os sistemas de informação *(management information systems)* são mecanismos de apoio a gestão, desenvolvidos com base na tecnologia de informação e com suporte da informática para atuar como condutores das informações que visam facilitar, agilizar e otimizar o processo decisório nas organizações. A gestão empresarial precisa cada dia mais do apoio de sistemas, pois estes dão segurança, agilidade e versatilidade para a empresa no momento em que se processam as decisões. Assim como nos bancos, hoje os sistemas sociais tem sido uma alternativa para os mesmos propagar suas informações como meio abrangente e um mecanismo estratégico de divulgar suas informações.

Laureano e Moraes (2005), em seu trabalho intitulado “Uma Abordagem Para a Proteção de Detectores de Intrusão Baseadas em Máquinas Virtuais” apresenta o conceito de engenharia da informação – que é um conjunto empresarial de disciplinas automatizadas, dirigindo ao fornecimento da informação correta para a pessoa certa no tempo exato et al. (MARTIN, 1991; FELICIANO NETO, FURLAN E HIGO, 1988) – já demonstrava a importância da segurança da informação para as instituições. Os bancos não contam com um sistema automatizado que possa filtrar as informações através dos sistemas sociais, neste trabalho de Laureano e Moraes é feita uma abordagem para se determinar possíveis vulnerabilidades que pode levar a quebra de sigilo de dados de usuários.

Quadro 1 – Quadro comparativo dos trabalhos relacionados

Autor	Objetivo do Trabalho	Utiliza de Rede Social?	Critérios Investigados	Faz Análise de Postagens?
Capistrano (2013)	Investiga as redes sociais virtuais como ambiente de exposição de dados pessoais para a engenharia social.	Sim Facebook	Privacidade	Sim
Oliveira (2011)	Quantificando as vulnerabilidades em segurança da informação avaliando maturidade de pessoa.	Sim Facebook	Privacidade	Sim
Sêmola (2013)	Trabalha a gestão da Segurança da Informação, com uma visão executiva da segurança da informação.	Não	Privacidade	Não
Laureano e Moraes (2005)	Abordando a Proteção de Detectores de Intrusão Baseadas em Máquinas Virtuais	Não	Privacidade	Não
Resende e Abreu (2000)	Tratando de tecnologia da informação aplicada a sistemas de informação empresariais, com o papel estratégico da informação e dos sistemas de informação nas empresas.	Não	Privacidade	Não
Martins (2018)	Trata-se de investigar o quão vulnerável/ suscetível a quebra do sigilo dos clientes bancários de se expõe nas redes sociais.	Sim Facebook	Vulnerabilidade	Sim

Fonte: elaborado pelo autor.

Não foi encontrado nenhum trabalho que investigasse a vulnerabilidade dos dados dos usuários em páginas bancárias de um sistema social. Este trabalho apresenta dados estatísticos reais a partir de uma coleta de dados, de aproximadamente 1.000 postagens coletadas da rede social: Facebook, retirada de páginas do Banco do Brasil e Banco Bradesco

para demonstrar o quão os usuários destes bancos estão utilizando a ferramenta como uma opção para realizar procedimentos como reclamações, informações, sugestões e tirar dúvidas a respeito de seus interesses junto ao seu banco. Os trabalhos encontrados até então correlacionados com este trabalho apresentam alternativas de como os usuários têm se exposto perante as redes sociais, e como os hackers têm levado em considerações para ter acesso às informações pessoais, assim focando mais na parte da segurança e não exposição por parte de usuários/clientes bancários. O intuito deste trabalho é apresentar como os clientes dos bancos onde possuem contas bancárias ou quaisquer interesse no banco, estejam expostos a tal ponto que se abra margens para uma possível quebra de sigilo de suas informações pessoais.

3 INVESTIGAÇÃO: BANCO DO BRASIL E BANCO BRADESCO

3.1 Contextualização

Esta etapa consiste na extração de postagens de usuários em uma rede social. A rede social utilizada foi o Facebook. O Facebook foi escolhido por ser uma rede social com maior número de usuários, aproximadamente 2,13 bilhões de usuários em todo mundo (ESTADÃO, 2018). As páginas bancárias analisadas neste trabalho foram de um banco público e um privado: Banco do Brasil e Bradesco, respectivamente. Nos capítulos anteriores foi apresentado, de forma teórica, o comportamento dos usuários comuns de sites de relacionamento. Este estudo de caso visa levantar dados de forma prática, a fim de definir o quanto estão expostos os dados pessoais e as informações publicadas pelo próprio cliente bancário, bem como os usuários que utilizam das redes sociais para interagir com seus bancos estão expondo de forma consciente e inconscientemente seus dados pessoais.

No Apêndice B deste trabalho estão algumas imagens de postagens dos usuários observadas. Os nomes e imagens dos usuários foram ocultados para preservação de suas identidades.

Para que fosse possível a constatação de usuários passíveis de ser quebrado seu sigilo bancário, foram coletadas postagens usando uma biblioteca (*Application Programming Interface – API Graph*)[1] de onde foram coletadas exatamente 1.000 postagens, que depois passaram por uma classificação em postagens vulneráveis, não vulneráveis e reencaminhadas, sendo definidas assim:

1. **Postagens Vulneráveis:** postagem que passa diretamente algum tipo de dado ou informação como por exemplo: RG, CPF, Agência Bancária, Tipo de Conta, dentre outros dados que comprometem a segurança do cliente, conforme a Figura 1.
2. **Postagens Não Vulneráveis:** postagem que não passa nenhum tipo de dado diretamente ou indiretamente em sua descrição, conforme a Figura 2.
3. **Postagens Reencaminhadas para Área de Conversa Restrita:** postagem que indiretamente pode comprometer algum tipo de dado, ou seja, em alguma etapa pode ser preciso solicitar algum dado para confirmação, como por exemplo: solicitar informações a respeito do proprietário da conta, agência do cliente, etc. A área restrita é um ambiente onde somente o cliente e o banco se relacionam de

[1] https://developers.facebook.com/docs/graph-api/

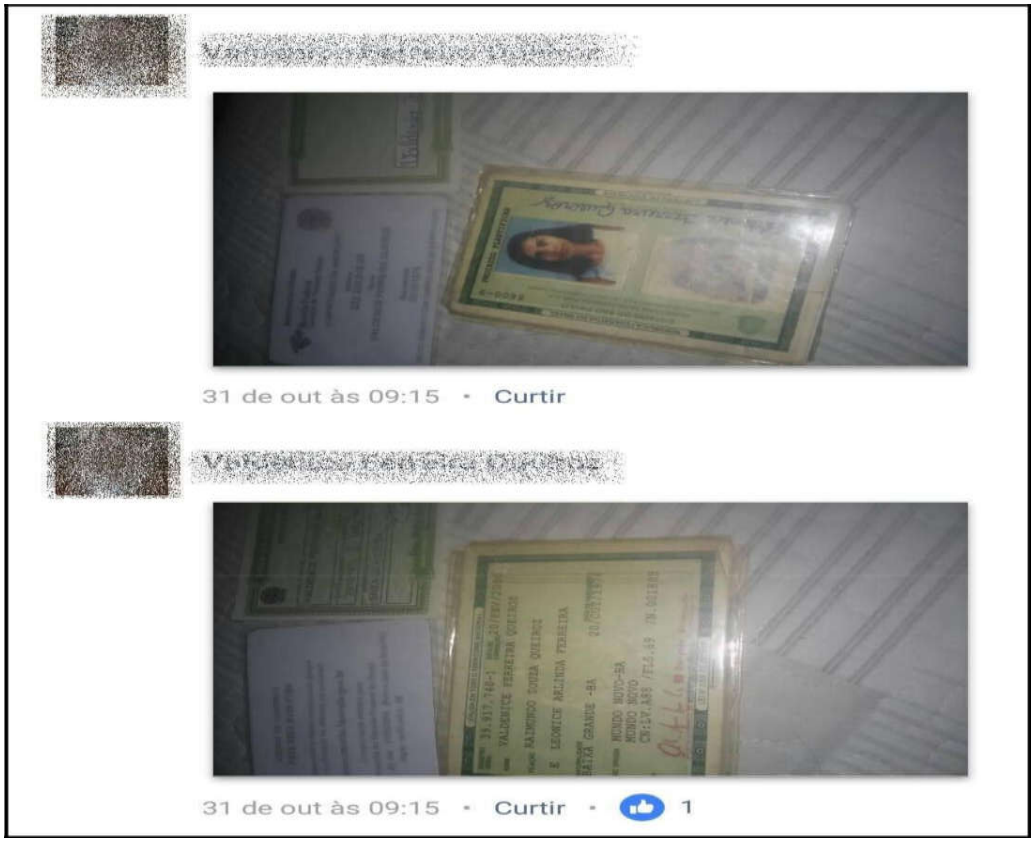
forma direta, sem a visualização dos demais usuários da página bancária na rede social, um exemplo pode ser visto no Quadro 2

Quadro 2 – Quadro exemplo de postagem

Usuário:	Meu nome é Maria Gisele de Sousa, tenho CC 30248-8 na Ag: 2094-8 no BB e gostaria de solicitar um cartão de crédito do BB livre de anuidade. Obrigado!
BB:	Sr(a): Maria redirecionaremos nossa conversa para uma área privada para confirmação de alguns de seus dados pessoais.

Fonte: elaborado pelo o autor

Figura 1 – Postagem vulnerável de usuários no Facebook



Fonte: Facebook, 2018. Adaptado pelo autor.

Figura 2 – Postagem não vulnerável de usuários no Facebook.

Fonte: Facebook, 2018. Adaptado pelo autor.

3.2 Extração de postagens

A forma de extração das postagens foi feita por um processo automatizado, utilizando a Application Programming Interface (API) denominada Graph. O período de extração das postagens foi de 01 de abril a 01 de outubro de 2018, quando foram extraídas em dias aleatórios por se tratar de que a Graph API captava somente um limite das 25 últimas postagens e seus devidos comentários. Esta API é a principal forma de os aplicativos lerem e gravarem no gráfico social do Facebook. Durante o desenvolvimento de extração de postagens, as postagens dos usuários foram catalogadas da seguinte forma: Vulneráveis, Não Vulneráveis e Reencaminhadas para área privada entre o banco e seu cliente.

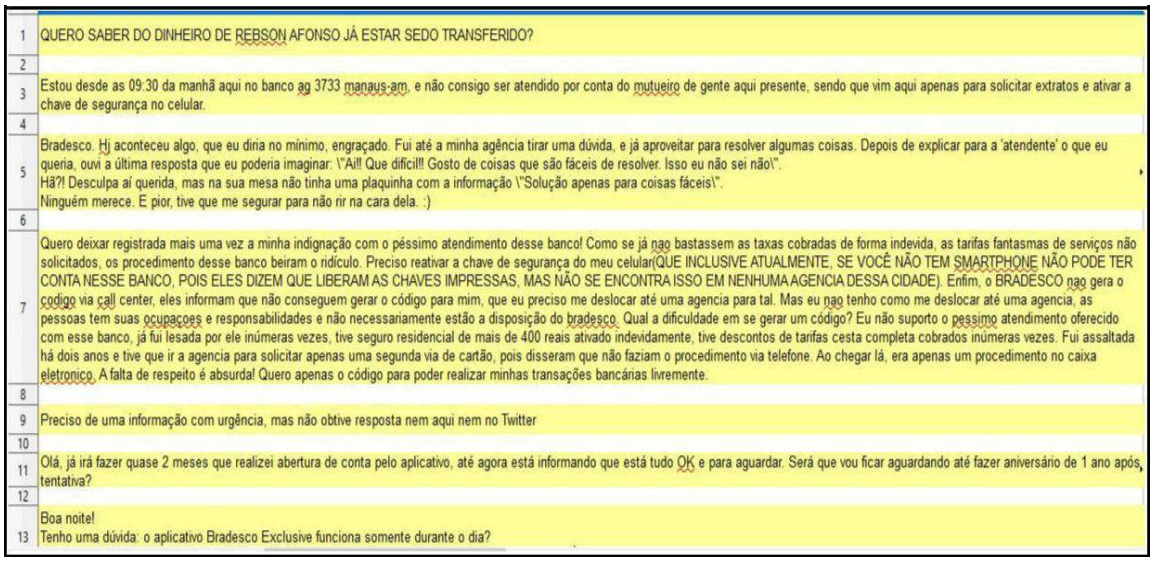
Para uma melhor organização das postagens, foi-se coletando e armazenando em uma tabela os parâmetros correlacionados as devidas postagens, conforme demonstrado pelas Figuras 3, 4 e 5 , a seguir:

Figura 3 – Parâmetros da postagem

	A
1	2018-04-05T20:30:39+0000
2	
3	2018-04-05T16:27:30+0000
4	
5	2018-04-05T14:48:07+0000
6	
7	2018-04-05T03:06:00+0000

Fonte: Elaborado pelo autor.

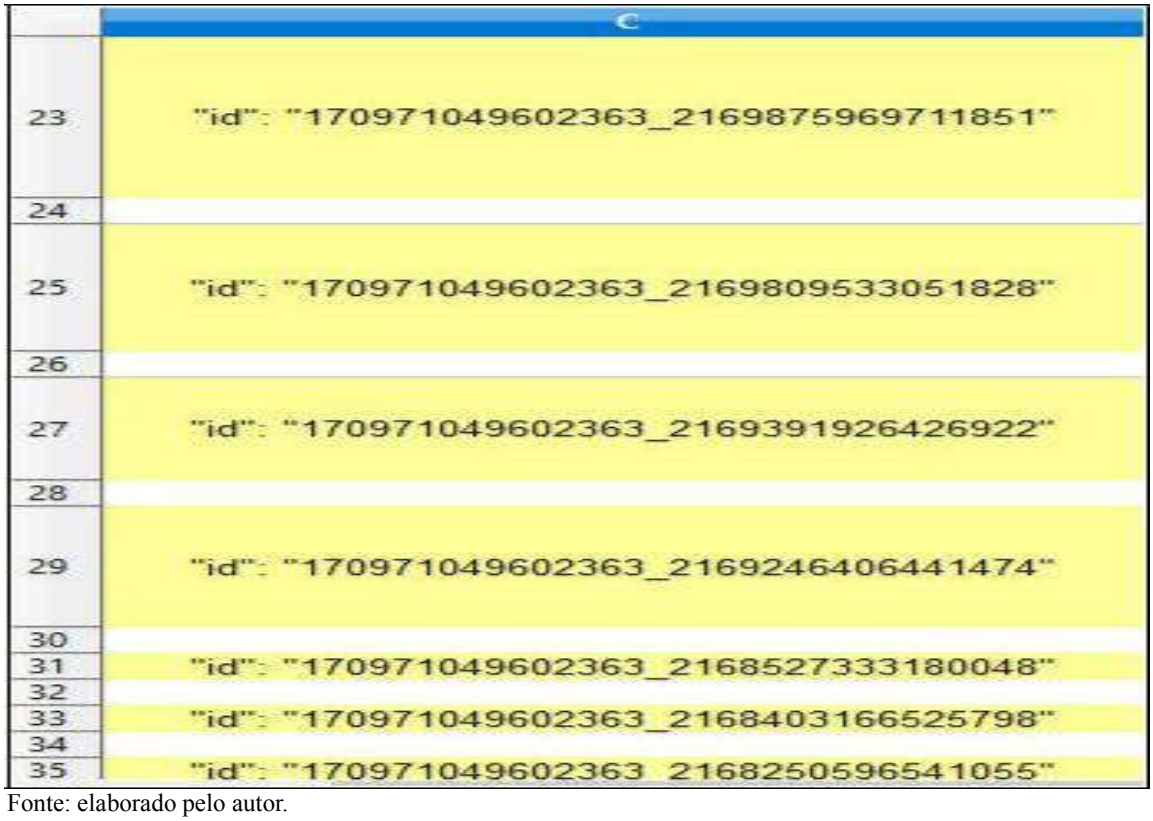
Figura 4 – Descrição das postagens do usuário/cliente bancário.



1	QUERO SABER DO DINHEIRO DE REBSON AFONSO JÁ ESTAR SEDO TRANSFERIDO?
2	
3	Estou desde as 09:30 da manhã aqui no banco ag 3733 manaus-am, e não consigo ser atendido por conta do mutueiro de gente aqui presente, sendo que vim aqui apenas para solicitar extratos e ativar a chave de segurança no celular.
4	
5	Bradesco. Hj aconteceu algo, que eu diria no mínimo, engraçado. Fui até a minha agência tirar uma dúvida, e já aproveitar para resolver algumas coisas. Depois de explicar para a 'atendente' o que eu queria, ouvi a última resposta que eu poderia imaginar: \"Ai!! Que difícil!! Gosto de coisas que são fáceis de resolver. Isso eu não sei não\". Hã?! Desculpa aí querida, mas na sua mesa não tinha uma plaquinha com a informação \"Solução apenas para coisas fáceis\". Ninguém merece. E pior, tive que me segurar para não rir na cara dela. :)
6	
7	Quero deixar registrada mais uma vez a minha indignação com o péssimo atendimento desse banco! Como se já nao bastassem as taxas cobradas de forma indevida, as tarifas fantasmas de serviços não solicitados, os procedimento desse banco beiram o ridículo. Preciso reativar a chave de segurança do meu celular(QUE INCLUSIVE ATUALMENTE, SE VOCÊ NÃO TEM SMARTPHONE NÃO PODE TER CONTA NESSE BANCO, POIS ELES DIZEM QUE LIBERAM AS CHAVES IMPRESSAS, MAS NÃO SE ENCONTRA ISSO EM NENHUMA AGENCIA DESSA CIDADE). Enfim, o BRADESCO nao gera o codigo via call center, eles informam que não conseguem gerar o código para mim, que eu preciso me deslocar até uma agencia para tal. Mas eu nao tenho como me deslocar até uma agencia, as pessoas tem suas ocupaçoes e responsabilidades e não necessariamente estão a disposição do bradesco. Qual a dificuldade em se gerar um código? Eu não suporto o pessimo atendimento oferecido com esse banco, já fui lesada por ele inúmeras vezes, tive seguro residencial de mais de 400 reais ativado indevidamente, tive descontos de tarifas cesta completa cobrados inúmeras vezes. Fui assaltada há dois anos e tive que ir a agencia para solicitar apenas uma segunda via de cartão, pois disseram que não faziam o procedimento via telefone. Ao chegar lá, era apenas um procedimento no caixa eletronico. A falta de respeito é absurda! Quero apenas o código para poder realizar minhas transações bancárias livremente.
8	
9	Preciso de uma informação com urgência, mas não obtive resposta nem aqui nem no Twitter
10	
11	Olá, já irá fazer quase 2 meses que realizei abertura de conta pelo aplicativo, até agora está informando que está tudo OK e para aguardar. Será que vou ficar aguardando até fazer aniversário de 1 ano após, tentativa?
12	
13	Boa noite! Tenho uma dúvida: o aplicativo Bradesco Exclusive funciona somente durante o dia?

Fonte: Elaborado pelo o autor.

Figura 5 – ID referente às postagens



	C
23	"id": "1709710496023 63_2169875969711851"
24	
25	"id": "1709710496023 63_2169809533051828"
26	
27	"id": "1709710496023 63_2169391926426922"
28	
29	"id": "1709710496023 63_2169246406441474"
30	
31	"id": "1709710496023 63_2168527333180048"
32	
33	"id": "1709710496023 63_2168403166525798"
34	
35	"id": "1709710496023 63_2168250596541055"

Fonte: elaborado pelo autor.

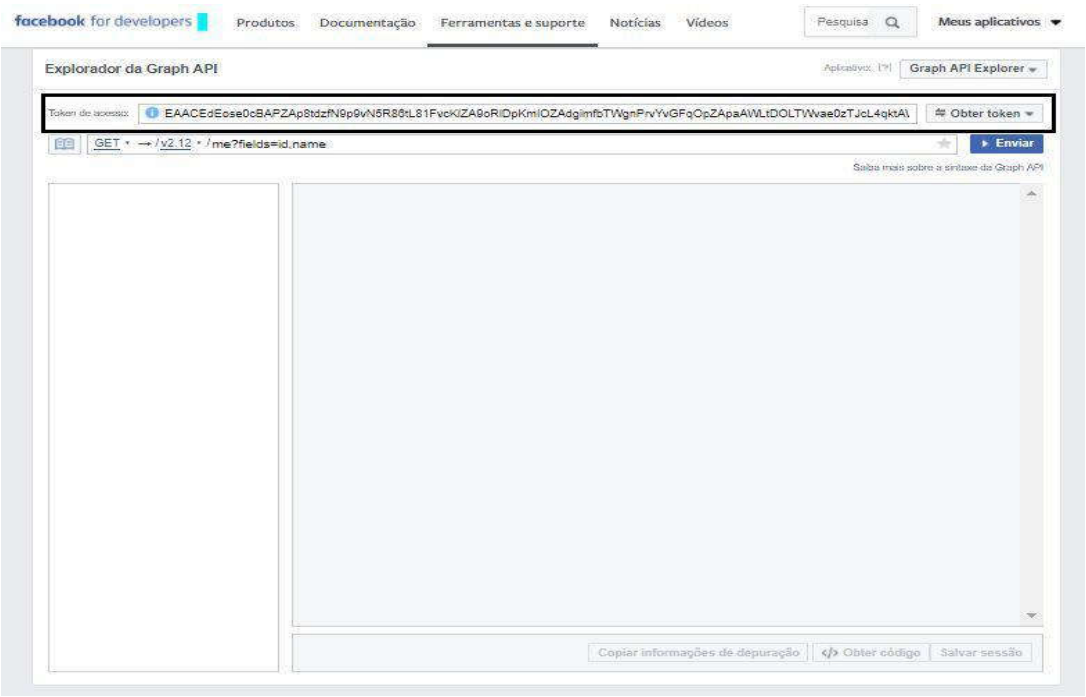
Para a extração das postagens, foi utilizada A Graph API, que é a principal forma de inserir e extrair dados da plataforma do Facebook. É uma API baseada em HTTP (

HyperText Transfer Protocol) de nível inferior que os aplicativos podem usar para consultar dados de forma programática, para publicar novas histórias, gerenciar anúncios, carregar fotos e realizar diversas outras tarefas.

Sua forma de utilização no Facebook permite que certos dados sejam coletados, permitindo com que a análise seja feita em qualquer linguagem de programação. O uso dela é bastante simples, bem documentado e possui um ambiente de teste, que permite formular e testar as *querys, querys é um t*ermo em inglês para representar uma linguagem de consulta, a uma linguagem de computador usada para realizar consultas em bancos de dados e sistemas de informação a serem utilizadas.

Antes de solicitar qualquer dado, obviamente é necessário uma identificação, e a Graph API utiliza um token como autenticação. Para gerar ele, basta entrar na Graph API Explorer e clicar no botão 'Get Token' => 'Get User Access Token' e marcar as opções que você quer que a API tenha acesso, conforme apresentado a seguir pela Figura 6, que apresenta um código de endereço para representar o responsável pela coleta de dados na plataforma.

Figura 6 – Endereço de Token de acesso

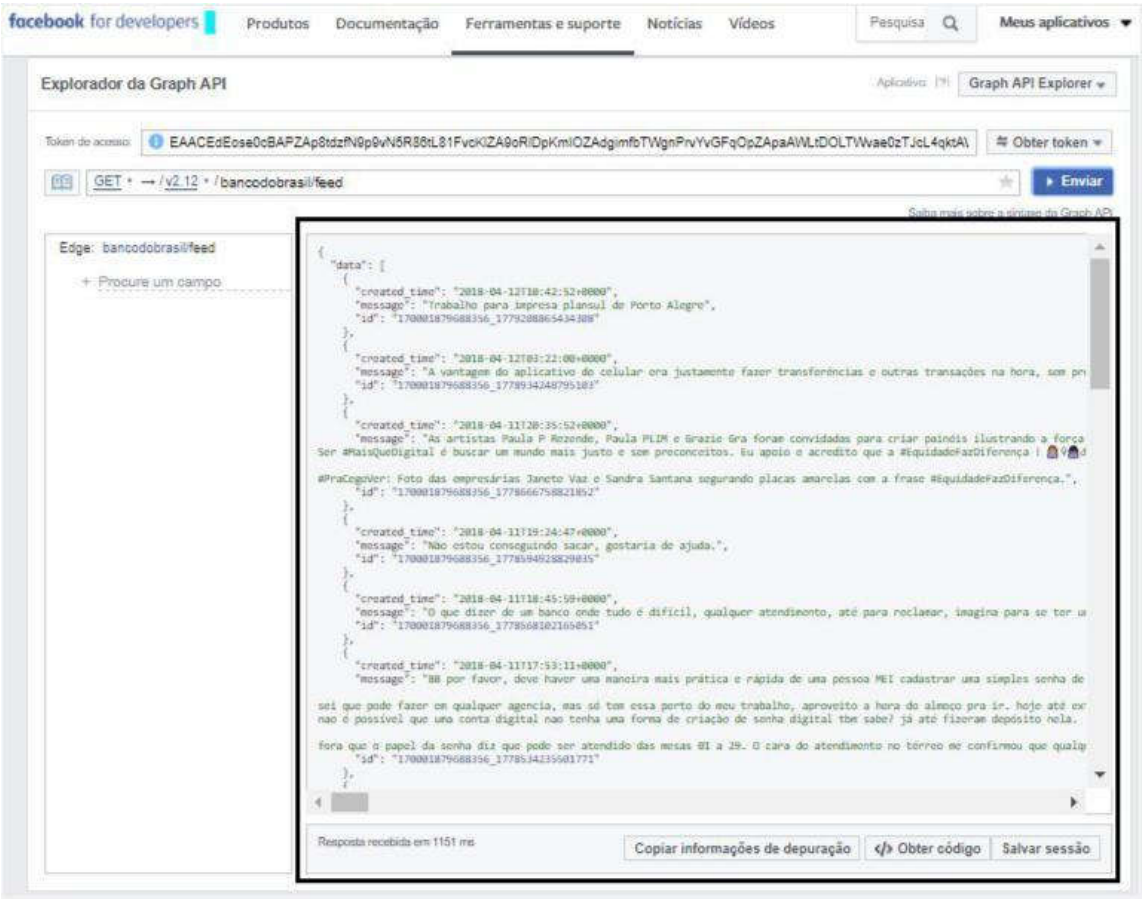


Fonte: elaborado pelo autor.

O formato de saída do Graphh API é um JSON *(Javascript Object Notation)*, que possui as postagens de usuários da rede social utilizada(Facebook), bem como suas postagens e seus respectivos comentários a serem analisados. É um objeto em notação JavaScript, em

um formato universal para estruturar dados e representar estes como objeto. A Figura 8 apresenta as postagens em formato JSON, organizadas por data, seguida de uma descrição da postagem e do código ID da postagem. A saída pode ser manipulada de diversas formas, tanto utilizando programação para manipular e apresentar os dados, como também utilizando sites que disponibilizam de uma interface para exibição e manipulação de JSONs.

Figura 7 – Código de extração de postagens API Graph



Fonte: elaborado pelo autor.

A Figura 7 ilustra as postagens de usuários de rede social utilizada(Facebook), bem como suas postagens e seus respectivos comentários a serem trabalhados, e analisados. A saída é um objeto em notação JavaScript, considerado um formato universal para estruturar dados e representá-los como objeto, conforme apresentada nas Figuras 8 e 9.

Figura 8 – Transformando JSON para modo de exibição em itens

Fonte: elabora pelo autor.

Figura 9 – JSON em modo de exibição em itens

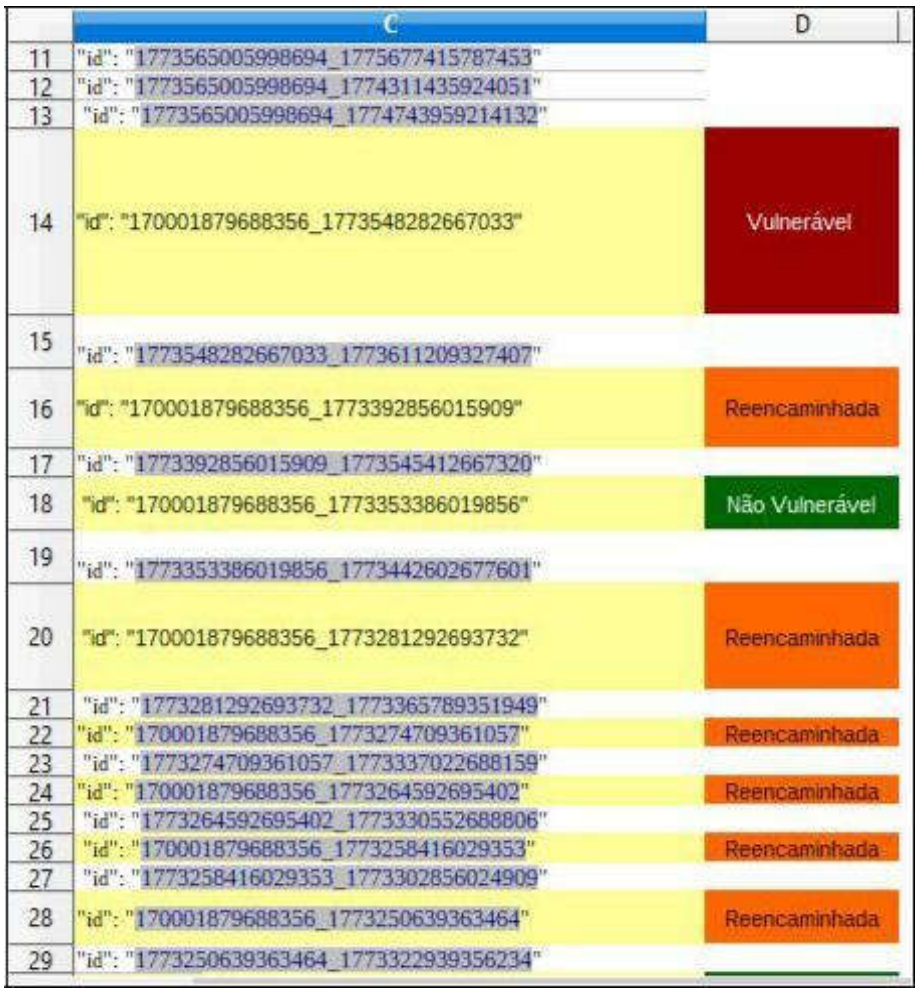
Fonte: elaborado pelo autor.

3.3 Análise das postagens

A classificação de postagens foi realizada por somente uma pessoa, o autor deste trabalho, no período de 03 de Abril a 01 de outubro de 2018 em postagens do tipo: Vulnerável; Não Vulnerável e Reencaminhada para o suporte da entidade bancária. A validação desta classificação de postagens se deu pela orientadora desse trabalho.

Um trecho da planilha de classificação pode ser visto na Figura 10. Outros exemplos desta classificação são expostos no Apêndice A deste trabalho.

Figura 10 – Classificação das postagens



Fonte: elaborado pelo autor.

3.4 Resultados

A Tabela 1 ilustra o resultado obtido dos dois bancos investigados: Banco do Brasil e Bradesco. O total de postagens classificadas foram 360 do Banco do Brasil, 408 do Branco Bradesco, totalizando 768 postagens. Vale ressaltar que foram excluídas 232 postagens relacionadas a publicidade e propaganda, como por exemplo: Neste dia das crianças aproveite para abrir a conta poupança do seu filho, e garanta uma renda extra em seu futuro.

Tabela 1 – Resultado obtido Banco do Brasil x Banco Bradesco

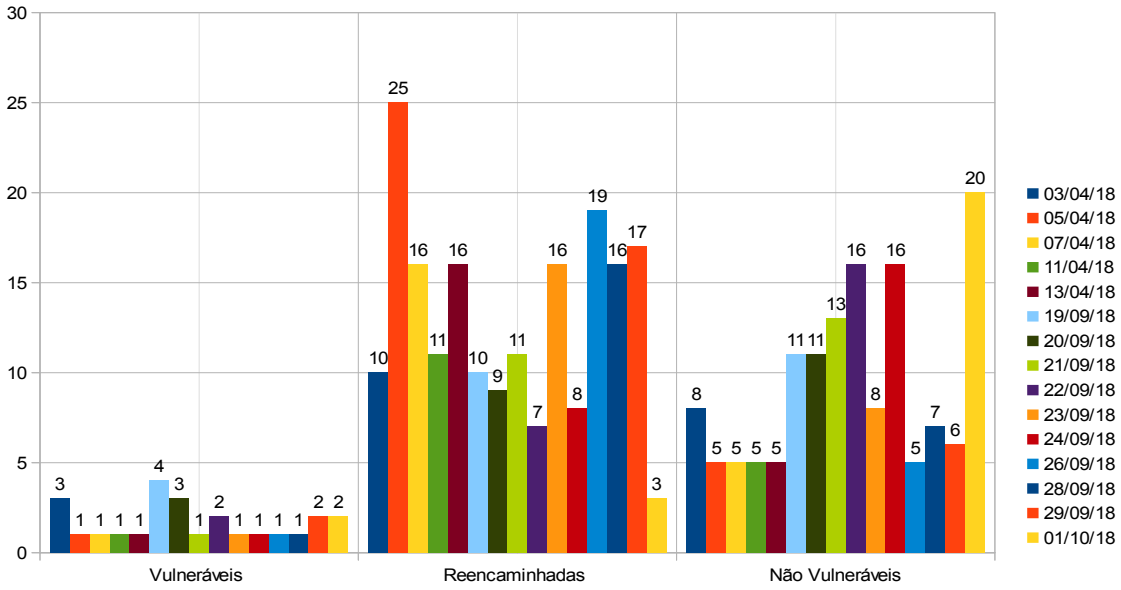
DADOS ESTATÍSTICOS			
BANCO DO BRASIL	**VULNERÁVEL**	**REENCAMINHADA**	**NÃO VULNERÁVEL**
%	6,9%	53,9%	39,2%
BANCO BRADESCO	**VULNERÁVEL**	**REENCAMINHADA**	**NÃO VULNERÁVEL**
%	15,9%	22,3%	61,8%
MÉDIA PERCENTUAL	11,7%	37,1%	51,2%
ANALISE DE DADOS COLETADOS			
TOTAL DE POSTAGENS COLETADAS	TOTAL DE POSTAGENS COLETADAS COM PUBLICIDADE E PROPAGANDAS	TOTAL DE POSTAGENS COLETADAS BANCO DO BRASIL	TOTAL DE POSTAGENS COLETADAS BRADESCO
100%	23,2%	36%	40,8%
1.000 POSTAGENS	232 POSTAGENS	360 POSTAGENS	408 POSTAGENS

Fonte: elaborado pelo autor.

Os gráficos 1 e 2 mostram o quão os clientes de bancos privados e públicos têm se exposto na Internet, deixando margens para uma exposição dos dados dos usuários, identificando suas vulnerabilidades, como roubo de informações em sistemas sociais.

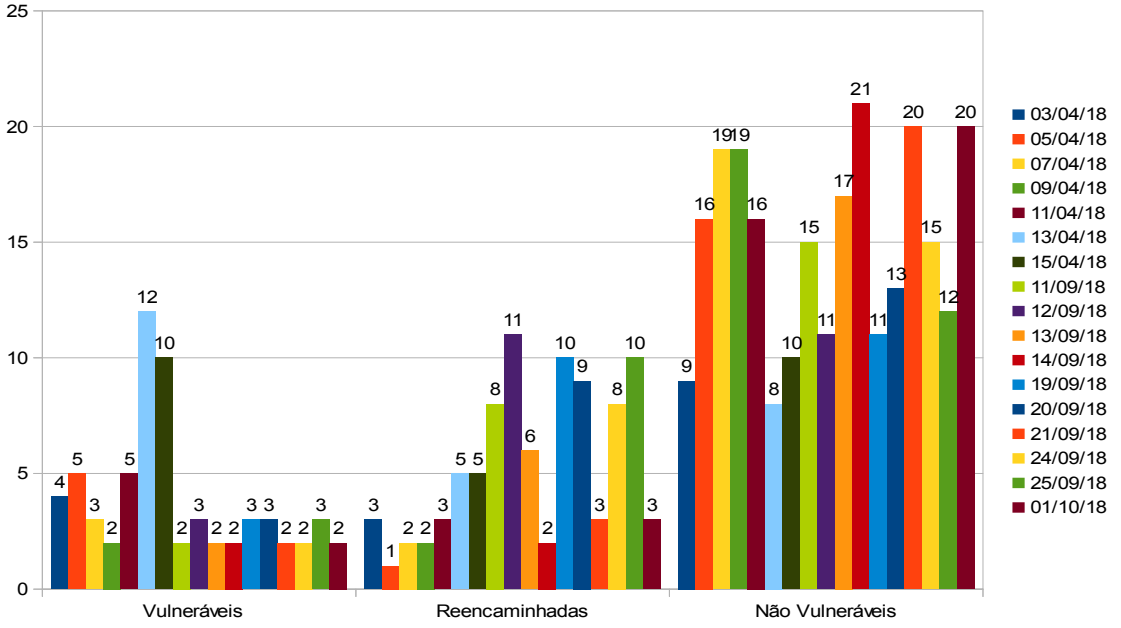
Os gráficos 1 e 2 - ilustra detalhadamente os relatórios de como as postagens coletadas entre os dias 03/04/2018 ao dia 01/10/2018 se comportam, em dias alternados, dos Banco do Brasil e Banco Bradesco.

Gráfico 1 – Percentual por postagens Banco do Brasil



Fonte: elaborado pelo autor.

Gráfico 2 – Distribuição dos documentos analisados por programa de pós-graduação



Fonte: elaborado pelo autor.

Pela análise dos Gráficos, observou-se que o Banco do Brasil apresentou uma preocupação bem maior em redirecionar os usuários para um ambiente privado em relação ao Banco Bradesco, visto que no Banco do Brasil 67,25% das postagens foram redirecionadas enquanto somente 13,20% do Branco Bradesco. Isso tem sido um ponto positivo do Banco do Brasil, pois é de compreensão que ao direcionar a comunicação para o ambiente privado a segurança é aumentada em relação a comunicação pública.

Os dados de postagens apresentadas graficamente a seguir foram extraídas das postagens nos seguintes dias: do dia 03/04/2018 a 01/10/2018, conforme apresentado na Tabela abaixo.

Tabela 2 – Quantidades de postagens Banco do Brasil

BANCO DO BRASIL			
QUANTIDADE DE POSTAGENS POR CLASSIFICAÇÃO			
DATA DE COLETA	**VULNERÁVEL**	**REENCAMINHADA**	**NÃO VULNERÁVEL**
03/04/2018	3	10	8
05/04/2018	1	25	5
07/04/2018	1	16	5
11/04/2018	1	11	5
13/04/2018	1	16	5
19/09/2018	4	10	11
20/09/2018	3	9	11
21/09/2018	1	11	13
22/09/2018	2	7	16
23/09/2018	1	16	8
24/09/2018	1	8	16
26/09/2018	1	19	5
28/09/2018	1	16	7
29/09/2018	2	17	6
01/10/2018	2	3	20
TOTAL	25	194	141
%	6,9%	53,9%	39,2%
TOTAL DE POSTAGENS	360		

Fonte: elaborado pelo autor.

Conforme apresentado na Tabela 2, o total de postagens selecionadas, foram 360 postagens, onde dessas 360 postagens, 25 postagens são do tipo vulneráveis, 141 postagens do tipo não vulneráveis e 194 postagens são do tipo redirecionadas a uma área privativa de conversa.

Os dados de postagens apresentadas graficamente a seguir foram extraídas das postagens nos seguintes dias: do dia 03/04/2018 a 01/10/2018, conforme apresentado na Tabela abaixo.

Tabela 3 – Quantidades de postagens Banco Bradesco

BANCO BRADESCO			
QUANTIDADE DE POSTAGENS POR CLASSIFICAÇÃO			
DATA DE COLETA	**VULNERÁVEL**	**REENCAMINHADA**	**NÃO VULNERÁVEL**
03/04/2018	4	3	9
05/04/2018	5	1	16
07/04/2018	3	2	19
09/04/2018	2	2	19
11/04/2018	5	3	16
13/04/2018	12	5	8
15/04/2018	10	5	10
11/09/2018	2	8	15
12/09/2018	3	11	11
13/09/2018	2	6	17
14/09/2018	2	2	21
19/09/2018	3	10	11
20/09/2018	3	9	13
21/09/2018	2	3	20
24/09/2018	2	8	15
25/09/2018	3	10	12
01/10/2018	2	3	20
TOTAL	65	91	252
%	15,9%	22,3%	61,8%
TOTAL DE POSTAGENS	408		

Fonte: elaborado pelo autor.

4 CONCLUSÃO

Muitos dos usuários podem se expor nos sistemas sociais de forma inconsciente. Embora o resultado de postagens não vulneráveis seja maior do que as vulneráveis, ainda assim é possível detectar postagens vulneráveis em ambos os bancos analisados. Pode-se concluir que as postagens reencaminhadas, uma vez pré analisadas pelos bancos, estão passíveis de se tornar uma postagem de vulnerabilidade para o cliente. Como mencionado neste trabalho, a engenharia social explora diversas características humanas a fim de atingir objetivos, como: exploração de confiança, auto confiança, amizade e persuasão. Deste modo, não foi possível contar com um software capaz de inibir estas ações que podem levar aos usuários que utilizam de páginas bancárias a garantia de que seus dados estão totalmente seguros.

O foco principal abordado neste estudo foi a demonstração da vulnerabilidade de usuários, que utilizam das páginas bancárias para realizar procedimentos junto ao seu banco, e têm se exposto perante outros usuários da rede social, e como usuários leigos do Facebook publicam informações privadas, que podem ser garimpadas e posteriormente utilizadas por pessoas de má fé. Este problema poderia ser facilmente minimizado se os bancos ou a própria rede social oferecessem ferramentas de segurança que o usuário ao escrever sua postagem, fosse feito um tratamento dela antes mesmo de ser publicada para visualização dos demais usuários.

O problema de vulnerabilidade dos usuários vai além do amparo tecnológico, ao afirmar que o problema poderia ser facilmente minimizado, esbarra-se em condições culturais que interferem na busca por uma solução para este problema. As redes sociais, como o Facebook, poderiam ofertar um sistema de segurança para os usuários, de forma a guiar para uma área de segurança de dados, ou oferecer um tutorial sobre como proteger suas informações.

Durante a investigação apresentada, verificou-se que a maioria das postagens é reencaminhada para uma área privada entre cliente e banco, pois um atendente bancário visualiza que o procedimento pode levar ao usuário em um determinado momento da comunicação à exposição de seus dados. As postagens Classificadas como Não Vulneráveis, ou seja, aquelas que em sua postagem não passou nenhuma informação ou dado pessoal do cliente pode, em um dado momento, se tornar Vulnerável ao longo do desenvolvimento da postagem, assim podendo comprometer em algum dado pessoal, passando de Não Vulnerável a Vulnerável.

Foi de percepção do autor deste trabalho que a vulnerabilidade dos usuários está também diretamente ligada ao seu grau de conhecimento, pois, muitos usuários não têm a devida noção de como se expressar nos sistemas sociais, e a forma adequada para que não comprometa sua privacidade pessoal. Das postagens coletadas 38,09% delas são reencaminhadas para uma área privada, 50,57% corresponde postagens não vulneráveis e 11,44% vulneráveis.

Observa-se, também, que se for feita a soma das postagens reencaminhadas com o percentual das postagens vulneráveis, verifica-se que o número é bem maior que o percentual das postagens não vulneráveis, assim é possível chegar em um resultado maior parte dos usuários que utilizam de páginas bancárias para interagir com seu banco a maioria tem sua segurança comprometida.

4.1 Trabalhos futuros

Desenvolver um software para analisar postagens e informar o nível de vulnerabilidade dos usuários, como forma de contribuir para uma classificação automatizada e mais robusta, contendo parâmetros de dados definidos que podem levar a quebra de sigilo do usuário que utiliza os sistemas sociais como meio para realizar uma comunicação com seu banco. Fazer uma investigação com um volume maior de dados de postagens, pois quanto maior o número de postagens coletadas, mais preciso será o percentual de confiança da pesquisa. Expandir para mais bancos a pesquisa e a outras redes sociais, visto que este trabalho somente teve em seu escopo dois bancos, um privado e um público e uma rede social. Quanto maior o número de bancos e redes sociais, maior será o nível de confiança na pesquisa e mais segura será à amostra real dos dados apresentados.

REFERÊNCIAS

66% DAS TRANSAÇÕES bancárias são feitas por internet banking, aplicativos ou call centers, diz BC. **G1.** Disponível em: http://g1.globo.com/economia/noticia/2018/11/07/66-das-transacoes-bancarias-sao-feita-por-internet-banking-aplicativos-ou-call-diz-bc.ghtml/. Acesso em: 08 nov. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISSO/IEC 27002:** Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação. Rio de Janeiro, 2013.

_____. **NBR ISO/IEC 17799**: Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2003.

_____. **NBR ISO/IEC 17799**: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

BARANAUSKAS, M.; PEREIRA, R.; SILVA, S. D. Softwares sociais: uma visão orientada a valores. In: SIMPOSIO BRASILEIRO DE FATORES HUMANOS SISTEMAS COMPUTACIONAIS, 9, 2010. Belo horizonte. **Anais**... Belo Horizonte.: UFMG, 2010.

BRUBAKER, J. R.; KIVRAN-SWAINE, F.; TABER, L.; HAYES, G. R. Grief-stricken in a crowd: the language of bereavement and distress in social media. In: ICWSM, 6, 2012. Dublin. **Anais...** Dublin: AAAI, 2012.

CAMBRIDGE Analytica anuncia fim de suas operações. **G1.** Disponivel em: https://g1.globo.com/economia/noticia/cambridge-analytica-anuncia-fim-de-suas-operacoes.ghtml. Acesso em: 20/08/2018.

CROSBY, Philip B. **Qualidade é Investimento**. 5 ed. Rio de Janeiro: José Olympio, 1992.

ELLISON, N. B. et al. Social network sites: definition, history, and scholarship. **Journal of Computer-Mediated Communication**, Nova Jersey, v. 13, n. 1, p. 210–230, 2007.

ENTENDA o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **BBC.** Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 20 ago. 2018.

FACEBOOK chega a 2,13 bilhões de usuários em todo mundo. **Estadão.** Disponivel em: https://link.estadao.com.br/noticias/empresas,facebook-chega-a-2-13-bilhoes-de-usuarios-em-todo-o-mundo,70002173062. Acesso em: 01 dez. 2018.

FACEBOOK e Cambridge Analytica Trabalharam para Trump após vazamento de dados. **O Globo.** Disponível em: https://oglobo.globo.com/mundo/facebook-cambridge-analytica-trabalharam-para-trump-apos-vazamento-de-dados-1-22510991. Acesso em: 20 ago. 2018.

FELICIANO NETO, Acácio; FURLAN, José Davi e HIGO, Wilson. **Engenharia da Informação**: metodologia, técnicas e Ferramentas. São Paulo: McGrawHill, 1988.

FERREIRA, Fernando Nicolau Freitas. **Segurança da informação**. Rio de Janeiro: Ciência Moderna, 2003.

HATFIELD, Joseph M. Social engineering in cybersecurity: The evolution of a concept, **Computers & Security**, Amsterdã, v. 73, 2018. p. 102-113. Disponível em: https://doi.org/10.1016/j.cose.2017.10.008. Acesso em: 01 ago. 2018.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 17799:2005:** Environmental management – Life cycle assessment – Principles and framework. Genebra, 2005.

KAPLAN, A. M.; HAENLEIN, M. Users of the world, unite! The challenges and opportunities of social media. **Business horizons**, Amsterdã, v. 53, n. 1, p. 59–68, 2010.

KARNIK, M.; OAKLEY, I.; VENKATANATHAN, J.; SPILIOTOPOULOS, T.; NISI, V. Uses & gratifications of a facebook media sharing group. In: ACM. **Proceedings of the 2013 conference on Computer supported cooperative work**. [S.l.], 2013. p. 821–826.

LAUREANO, Marcos Aurelio Pchek. **Uma Abordagem Para a Proteção de Detectores de Intrusão Baseadas em Máquinas Virtuais**. 2004. Dissertação (Mestrado em Informática aplicada) - Pontifícia Universidade Católica do Paraná, Curitiba.

MARTIN, James. **Engenharia da Informação**: Introdução. Rio de Janeiro: Editora Campus, 1991.

MENEZES, Adriano Paulino. **Realização de negócios bancários nas redes sociais**: o atendimento a clientes do Banco do Brasil via Facebook. 2017. Dissertação (Mestrado) – Universidade Católica de Brasília, Brasília.

MINISTÉRIO Público do Distrito Federal pede indenizações de R$ 10 milhões ao Banco Inter por vazamento de dados de clientes. **G1.** Disponivel em: hhttps://g1.globo.com/df/distrito-federal/noticia/2018/07/31/mp-do-df-pede-indenizacao-de-r-10-milhoes-ao-banco-inter-por-vazamento-de-dados-de-clientes.ghtml. Acesso em: 01 ago. 2018.

NAKAGAWA, Sandra Sayuri Yamashita; GOUVÊA, Maria Aparecida. Marketing de relacionamento sob a influência da Internet. **Revista de Gestão USP**, São Paulo, v. 13, n. 1, p. 57-73, jan./mar. 2006.

OLIVEIRA M. C. **Quantificação de vulnerabilidades em segurança da informação avaliando maturidade de pessoas**. 2011. 20 f. TCC (Bacharelado em Redes de Computadores) – Universidade Luterana do Brasil (Ulbra), Canoas, Rio Grande do Sul.

PEREIRA, Maria José Lara de Bretãs; FONSECA, João Gabriel Marques. **Faces da Decisão**: as mudanças de paradigmas e o poder da decisão. São Paulo: Makron Books, 1997.

REZENDE, Denis Alcides; ABREU, Aline França de. **Tecnologia da informação aplicada a sistemas de informação empresariais**: o papel estratégico da informação e dos sistemas de informação nas empresas. São Paulo: Atlas, 2000

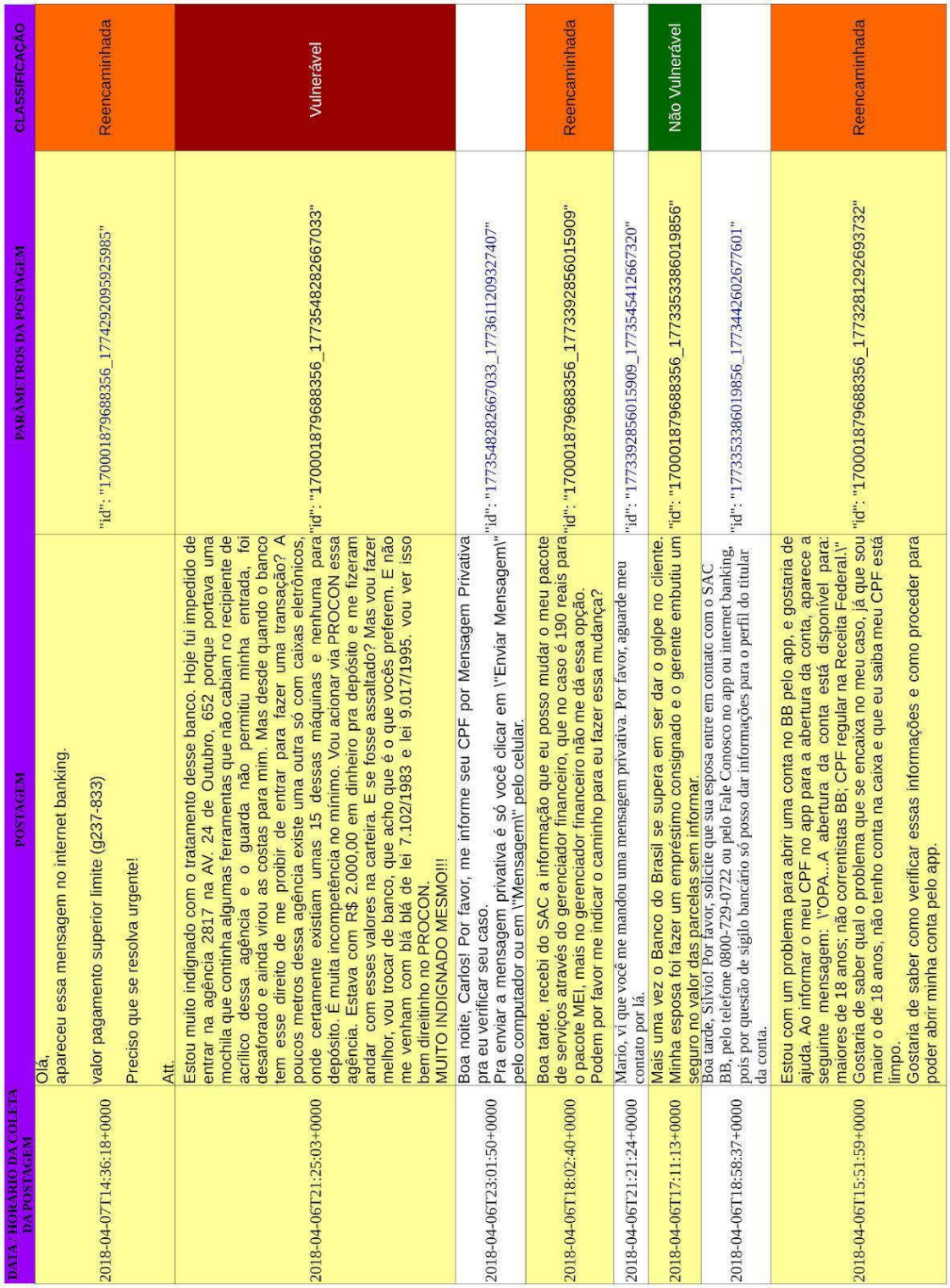
SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2003

STATISTA. Disponível em: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. Acesso em: 03 nov. 2018.

SILVA, D. R. P.; STEIN, L. M. Segurança da informação: uma reflexão sobre o componente humano. **Sumários**. Porto Alegre, v. 10, p. 46-53, mar. 2007. Disponível em: http://www.sumarios.org/sites/default/files/pdfs/52416_6138.PDF. Acesso em: 10 nov. 2011.

TORRES, Cláudio. **A bíblia do marketing digital**: tudo o que você queria saber sobre marketing e publicidade na Internet e não tinha a quem perguntar. São Paulo: Novatec, 2009.

APÊNDICE A – CLASSIFICAÇÃO DE POSTAGENS DE REDES SOCIAIS



DATA/HORÁRIO DA COLETA DA POSTAGEM	POSTAGEM	PARÂMETROS DA POSTAGEM	CLASSIFICAÇÃO
2018-04-07T14:36:18+0000	Olá, apareceu essa mensagem no internet banking. valor pagamento superior limite (g237-833) Preciso que se resolva urgente! Att.	"id": "1700018796883 56_1774292095925985"	Reencaminhada
2018-04-06T21:25:03+0000	Estou muito indignado com o tratamento desse banco. Hoje fui impedido de entrar na agência 2817 na AV. 24 de Outubro, 652 porque portava uma mochila que continha algumas ferramentas que não cabiam no recipiente de acrílico dessa agência e o guarda não permitiu minha entrada, foi desaforado e ainda virou as costas para mim. Mas desde quando o banco tem esse direito de me proibir de entrar para fazer uma transação? A poucos metros dessa agência existe uma outra só com caixas eletrônicos, onde certamente existiam umas 15 dessas máquinas e nenhuma para depósito. É muita incompetência no mínimo. Vou acionar via PROCON essa agência. Estava com R$ 2.000,00 em dinheiro pra depósito e me fizeram andar com esses valores na carteira. E se fosse assaltado? Mas vou fazer melhor, vou trocar de banco, que acho que é o que vocês preferem. E não me venham com blá blá de lei 7.102/1983 e lei 9.017/1995. vou ver isso bem direitinho no PROCON. MUITO INDIGNADO MESMO!!!	"id": "1700018796883 56_1773548282667033"	Vulnerável
2018-04-06T23:01:50+0000	Boa noite, Carlos! Por favor, me informe seu CPF por Mensagem Privativa pra eu verificar seu caso. Pra enviar a mensagem privativa é só você clicar em \"Enviar Mensagem\" pelo computador ou em \"Mensagem\" pelo celular.	"id": "1773548282667033_1773611209327407"	
2018-04-06T18:02:40+0000	Boa tarde, recebi do SAC a informação que eu posso mudar o meu pacote de serviços através do gerenciador financeiro, que no caso é 190 reais para o pacote MEI, mais no gerenciador financeiro não me dá essa opção. Podem por favor me indicar o caminho para eu fazer essa mudança?	"id": "1700018796883 56_1773392856015909"	Reencaminhada
2018-04-06T21:21:24+0000	Mario, vi que você me mandou uma mensagem privativa. Por favor, aguarde meu contato por lá.	"id": "1773392856015909_1773545412667320"	
2018-04-06T17:11:13+0000	Mais uma vez o Banco do Brasil se supera em ser dar o golpe no cliente. Minha esposa foi fazer um empréstimo consignado e o gerente embutiu um seguro no valor das parcelas sem informar.	"id": "1700018796883 56_1773353386019856"	Não Vulnerável
2018-04-06T18:58:37+0000	Boa tarde, Silvio! Por favor, solicite que sua esposa entre em contato com o SAC BB, pelo telefone 0800-729-0722 ou pelo Fale Conosco no app ou internet banking, pois por questão de sigilo bancário só posso dar informações para o perfil do titular da conta.	"id": "1773353386019856_1773442602677601"	
2018-04-06T15:51:59+0000	Estou com um problema para abrir uma conta no BB pelo app, e gostaria de ajuda. Ao informar o meu CPF no app para a abertura da conta, aparece a seguinte mensagem: \"OPA...A abertura da conta está disponível para: maiores de 18 anos; não correntistas BB; CPF regular na Receita Federal.\" Gostaria de saber qual o problema que se encaixa no meu caso, já que sou maior o de 18 anos, não tenho conta na caixa e que eu saiba meu CPF está limpo. Gostaria de saber como verificar essas informações e como proceder para poder abrir minha conta pelo app.	"id": "1700018796883 56_1773281292693732"	Reencaminhada

Fonte: elaborado pelo autor.

APÊNDICE B – POSTAGEM DE USUÁRIOS

Fonte: Facebook, adaptado pelo autor.