INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
CAMPUS MACAPÁ
CURSO: TECNOLOGIA EM REDES DE COMPUTADORES

DEOCLEY PEDRADA PEREIRA

CRIMES CIBERNÉTICOS:

pequenos passos na prevenção de fraudes por meio de dispositivos móveis

MACAPÁ – AP
2021

DEOCLEY PEDRADA PEREIRA

CRIMES CIBERNÉTICOS:

pequenos passos na prevenção de fraudes por meio de dispositivos móveis

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Tecnologia em Redes de Computadores, do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores.

Orientador: Prof. Clayton Jordan Espindola do Nascimento.

MACAPÁ – AP
2021

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

P436c Pereira, Deocley Pedrada
Crimes Cibernéticos: pequenos passos na prevenção de fraudes por meio de dispositivos moveis. / Deocley Pedrada Pereira - Macapá, 2021.
31 f.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2021.

Orientador: Prof. Esp. Clayton Jordan Espíndola Nascimento.

1. Crimes ciberneticos. 2. tecnologia. 3. prevenção de fraudades em dispositivos moveis. I. Nascimento, Prof. Esp. Clayton Jordan Espíndola, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

DEOCLEY PEDRADA PEREIRA

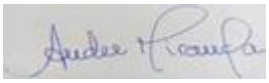
CRIMES CIBERNÉTICOS:

pequenos passos na prevenção de fraudes por meio de dispositivos móveis

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Tecnologia em Redes de Computadores, do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP, como requisito avaliativo para obtenção de título de Tecnólogo em Redes de Computadores.

Trabalho de Conclusão de Curso apresentado e aprovado em 11/05/2021 pela seguinte Banca Examinadora:

Prof. Esp. Gestão e Docência no Ensino Superior,
Clayton Jordan Espindola do Nascimento.
Orientador - Presidente
Instituto Federal de Educação, Ciência e Tecnologia do Amapá



Prof. Esp. Informática na Educação,
André Luiz Simão de Miranda Membro da banca - Examinadora
Instituto Federal de Educação, Ciência e Tecnologia do Amapá

Prof. Esp. Redes de Computadores com ênfase em segurança
Jairo Kássio Siqueira Barreto Membro da banca - Examinadora
Instituto Federal de Educação, Ciência e Tecnologia do Amapá

RESUMO

O presente trabalho apresentará uma reflexão sobre o tema “crime cibernético” e sua delimitação “Crimes cibernéticos: pequenos passos na prevenção de fraudes por meio de aplicativos móveis”. A consulta bibliográfica teve como objetivo geral, compreender o que é crimes cibernéticos e de que forma os usuários podem prevenir que fraudadores acessem os aplicativos móveis. Os objetivos específicos a serem alcançados foram: conhecer os tipos aplicativos móveis, analisar e inferir acerca da prevenção desses instrumentos digitais. De natureza básica, a consulta bibliográfica serviu para a produção do saber acerca da relevante temática. Buscou-se por meio de textos, um apoio teórico para produzir o trabalho de forma significativa. Estudos foram elaborados para colher as informações, os dados foram analisados, relacionados à teoria e apresentadas em forma de texto descritivo, apresentando características qualitativas. Assim, o referido trabalho deixará relevante saberes acerca de crime cibernético: pequenos passos na prevenção de fraudes por meio de aplicativos móveis.

Palavras-chave: Crime cibernético. Aplicativos móveis. Fraudes. Prevenção.

ABSTRACT

The present work will present a reflection on the theme “cyber crime” and its delimitation “Cyber crimes: small steps in the prevention of fraud through mobile applications”. The bibliographic consultation had the general objective of understanding what cybercrimes are and how users can prevent fraudsters from accessing mobile applications. The specific objectives to be achieved were: to know the types of mobile applications, to analyze and infer about the prevention of these digital instruments. Of a basic nature, the bibliographic consultation served to produce knowledge about the relevant theme. Theoretical support was sought through texts to produce the work in a meaningful way. Studies were developed to collect the information, the data were analyzed, related to the theory and presented in the form of descriptive text, presenting qualitative characteristics. Thus, this work will make relevant knowledge about cyber crime relevant: small steps in the prevention of fraud through mobile applications.

Keywords: Cyber crime. Mobile apps. Fraud. Prevention.

SUMÁRIO

1 INTRODUÇÃO

Este trabalho tem como viés ajudar, de forma significativa, na construção do conhecimento acerca da realidade vivenciada por muitas vítimas de crimes cibernéticos no tocante a fraudes em aplicativos como também trará orientações de prevenção desses crimes virtuais.

Para a sociedade, este estudo trará resultados positivos, pois no mundo digital a práxis será posto à prova, devido a utilização dos dispositivos moveis fazer parte do cotidiano como meio de comunicação.

Este estudo será de grande relevância, porque comprovará com veracidade, com pesquisa nas redes sociais e jornais, manifestar reflexões significativas acerca da temática enfatizada, inspirar a construção de novos conhecimentos a partir da pesquisa, podendo ser fonte do saber para estudos posteriores. Além disso, vai contribuir para alicerçar pensamentos, uma vez que, as comprovações inerentes aos objetos de estudos são fundamentadas a partir de situações da experiência humana.

O artigo que discutiu crimes cibernéticos: pequenos passos na prevenção de fraudes por meio de aplicativos móveis. Tem como objetivo compreender o que é crime cibernético. Quanto aos objetivos específicos: conhecer tipos de aplicativos móveis, analisar os tipos de fraudes e inferir acerca da prevenção de aplicativos.

Esta temática será de natureza básica e, serviu para a produção do saber acerca da relevante temática, pois considerando o crime cibernético, buscou-se através de diversos textos, um apoio teórico para esta proposta de trabalho. Os dados foram categorizados, analisados, relacionados à teoria e apresentadas em forma de texto descritivo, com características qualitativas.

Para melhor nortear a pessoa na leitura do trabalho, este foi divido em três tópicos. A primeira parte tem o aspecto teórico acerca de crime cibernético. O segundo momento contemplou o estudo de aplicativos móveis, o terceiro momento destacou os tipos de fraudes, e para finalizar apresentou crimes virtuais em aplicativos móveis. Logo, o presente trabalho propõe uma reflexão acerca de crime cibernético.

2 ASPECTO TEÓRICO

2.1 Cibernético

Pesquisas apontam que o uso da tecnologia tem sido muito frequente entre os sujeitos, visto que a internet tem ocupado um espaço de grande dimensão na vida dos indivíduos em que estabelecem comunicação, trocam experiências e informações por meio dos instrumentos capazes de facilitar a vida, mas também, pode causar muitos problemas quando usados de forma inadequada e ilícita. Segundo Cruz & Rodrigues (2018):

> Diariamente conectamos aparelhos à Internet, podendo assim afirmar que no século XXI a vida das pessoas está inteiramente interligada com a rede de computadores, seja para acessos a sistemas de interação como o Facebook, mensagens de e-mails, chamadas telefônicas, videoconferências ou para operações bancárias, sendo estes recursos vantajosos. Contudo nem tudo é vantagens, pois através da conexão, que conecta milhões de pessoas com à rede, indivíduos com altas capacidades técnicas ou sem a capacidade que através de alguns sites (endereço virtual, o qual são disponibilizadas informações) aprendem formas de praticar o ilícito. (CRUZ & RODRIGUES, 2018, p. 2).

Em vista desse pressuposto, é possível inferir que no século XXI, o sujeito não está alheio a tecnologia, especialmente no que tange ao uso de internet. São vários aplicativos que podem ser usados a rede de computadores. Vale enfatizar que o uso da internet é algo necessário, mas também quando usado de forma errada pode causar muitos prejuízos à usuários com a criação de códigos maliciosos com o intuito de cometer crimes.

Conforme Cruz & Rodrigues (2018), a principal forma e meio utilizado para cometer crimes é a criação de um programa com código malicioso conhecido como *Malware* que é projetado para adentrar um sistema sem seu conhecimento, com intenção de repassar informações a outrem ou causar danos ao sistema operacional de dispositivos eletrônicos, ele é muitas vezes baixado e instalado de forma inequívoca, em alguns casos os criminosos espalham esse vírus por meio de serviços *peer-to-peer* que é uma rede que disponibiliza arquivos pela internet, onde esses usuários baixam um arquivo e os disponibilizam em seu próprio computador novamente para download, esses arquivos já vem incorporados muitas das vezes com o malware, nesse sistema não há um servidor geral que armazene esses arquivos e sim um sistema onde cada computador funciona como servidor e cliente

ao mesmo tempo, pode-se também carregar esse código malicioso na firmware de um pen-drive ou na unidade flash USB, e já que está armazenado de forma interna e não no sistema de arquivos, ele acaba se tornando imperceptível. Há alguns tipos que são bastante comuns de malwares, são eles: ramsoware, cavalo de troia, spyware, worms, adware, botnets, etc.

Embasado nesse pensamento é possível observar que, o dispositivo *Malware* representa um perigo para os usuários, haja vista que, pode prejudicar quem for vítima, pois pode levar o vírus para o dispositivo e assim, causar sérios danos.

Ainda conforme Cruz & Rodrigues (2018), além do vírus, existe também os *Worms*, (*malware* que ao contrário do vírus depende de interação da pessoa, este aproveita falhas do dispositivo e se hospeda no sistema). Ou seja, os *Malwares* são a principal fonte de repasse de informações que originam os cyber crimes. Como se não bastasse os *malwares*, criminosos utilizam-se da rede para assediar pessoas, realizar discriminações, vender produtos ilegais como drogas, bem como realizar calúnia, injúria e difamação, apologia ao crime, pedofilia, espionagem, estelionato, roubo de identidade e inclusive terrorismo.

Em vista desse aporte teórico se pode imaginar o quanto o vírus é capaz de destruir e causar males as pessoas suscitáveis a esses tipos de crimes os quais se tornam cada vez mais frequentes entre as pessoas, especialmente pela impunidade que, na maioria das vezes, acontece.

Sobre essa assertiva os autores acima mencionados enfatizam que, as práticas dos crimes cibernéticos estão se tornando muito comuns, em razão de uma falsa sensação de impunidade que se tem, no qual os indivíduos que realizam transgressões da lei possuírem uma ilusão de que o ato, por se consumar ser a longa distância e de que os instrumentos utilizados para as práticas do ilícito não fornecerem identidade.

Logo, o crime cibernético é prejudicial às pessoas e a sociedade em geral, que são vítimas desse tipo de vírus, e, além disso, que tem sido muito praticado pela falta de punição aos usuários que se aproveitam das informações e dados de outras pessoas para tirarem vantagens e se beneficiarem de forma ilícita. De maneira mais esclarecedora se pode dizer que, Crime cibernético é uma atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou um

dispositivo conectado em rede. Sendo que, na sua maioria os crimes cibernéticos são cometidos por *ciber* criminosos ou hackers que querem ganhar dinheiro.

2.1.1 Principais crimes digitais

Há várias classificações acerca de crimes digitais, nesse sentido, surgem diversas abordagens de diferentes autores para explicar tal fenômeno. Para isso, estudos foram realizados para melhor entender sobre essa temática. Briat (1985) tece as seguintes explicações sobre esse assunto.

> a) Manipulação de dados e/ou programas a fim de cometer uma infração já prevista pelas incriminações tradicionais;
> b) Falsificação de dados ou programas;
> c) Deterioração de dados e de programas e entrave à sua utilização;
> d) Divulgação, utilização ou reprodução ilícitas de dados e de programas;
> e) Uso não autorizado de sistemas de informática;
> f) Acesso não autorizado a sistemas de informática (BRIAT, 1985, p. 22).

Perante essa explicação é possível analisar que, são várias as classificações de crime digitais, todos com grandes proporções de risco para as vítimas, que podem até responder por crimes não cometidos, pois muitas vezes a pessoa tem seus dados roubados por hackers que invadem sua conta e praticam crimes virtuais, causando embaraços e prejuízos as pessoas.

Nesse sentido, é preciso ficar atento aos golpes virtuais que podem ser praticados pela internet, causando prejuízos à vida dos usuários vítimas desses crimes virtuais. Segundo Bertho (2018):

> Ao navegar na internet é preciso ficar atento aos *links* onde clica os arquivos que baixa e sites onde irá cadastrar suas informações pessoais ou bancárias. Isso porque existem diferentes crimes virtuais sendo aplicados por criminosos que buscam obter vantagens à custa das vítimas desatentas. O importante é o entendimento de que em todos os golpes já aplicados o problema foi acarretado por descuidos com a segurança, como pouco cuidado nos sites acessados, ou falta de malícia para identificar falsas informações, promoções ou ofertas de emprego irrealistas. (BERTHO, 2018, p. 1).

Percebe-se a importância de ficar atento aos acessos aos links para que os dados pessoais e bancários não sejam roubados e também para não se tornar vitima desses crimes virtuais. Sobre crimes da internet Bertho (2018) enfatiza o *site* malicioso:

> Por falta de segurança, alguns *sites* acabam expostos a ações de criminosos que os invadem e colocam códigos maliciosos para prejudicar a empresa, gestores ou o público que os acessam. Além disso, há sites criados exclusivamente com o objetivo de enganar o público. Geralmente eles exibem ofertas muito tentadoras para atrair usuários e podem se valer do nome e identidade visual de um *e-commerce* que tenha boa reputação. Na ânsia de comprar o produto a um preço muito baixo, o consumidor esquece-se de checar fatores básicos como a URL correta do site e selos de segurança, como o Selo *Site* Blindado, e acaba caindo em um golpe. (BERTHO, 2018, p. 1).

Com base nesse embasamento é possível perceber que os usuários estão sujeitos a diversos golpes virtuais, inclusive induzidos a realizar compras de produtos por preços baixos, uma forma de enganar e tirar proveito da situação e da falta de atenção em checar o site e se é confiável. Além dos sites maliciosos crime conhecido como “phishing”, Bertho (2018) enfatiza sobre eles “*phishing”* e o roubo de identidade e tece as seguintes explicações.

> O termo *phishing* é uma referência à *fish*, “pescar”, em inglês.Trata-se de um artifício onde os golpistas se passam por empresas confiáveis ou contatos pessoais da vítima para enganá-las e obter acesso a informações sigilosas dessa pessoa ou para que ela realize algum tipo de ação desejada como: baixar um arquivo, preencher um formulário com dados pessoais, fazer uma transferência e etc. Assim como no ambiente *offline*, existem golpes na internet focados em roubar a identidade digital de outra pessoa para obter algum tipo de privilégio ou realizar uma ação. Os criminosos podem abrir um perfil social em nome da vítima, enviar e-mails em nome de outra pessoa e etc. Neste caso, elas podem se apropriar da confiança que há em relação à vítima para se passar por ela, pedindo ajuda em dinheiro aos amigos, enviando arquivos com vírus e etc. Dependendo das informações obtidas, pode ser ainda que outras pessoas façam cadastros e compras no nome da vítima. (BERTHO, 2018, p. 1).

Todo cuidado é pouco perante a esperteza e maldade dos hackers quanto aos golpes e crimes na internet que podem transformar os usuários inocentes e vítimas em criminosos e culpados por golpes que não cometeram, visto que, ao roubar sua identidade podem enganar e cometer golpes em nomes de pessoas inocentes.

Ainda conforme o autor acima citado há também golpes como falsas oportunidades de empregos, falsos boletos de faturas e sites com promessas de dinheiro fácil.

Receber para fazer algo muito desejado, como degustar ovos de Páscoa, ou ganhar grandes quantias de dinheiro apenas fazendo determinado curso, ou trabalhando em casa, estas são algumas artimanhas utilizadas para atrair e enganar as vítimas.

É muito importante checar se aquele boleto ou fatura é realmente esperado e se os dados são legítimos. É possível checar os números iniciais do código de barra, por exemplo, para ver se eles conferem com o do banco correspondente que é citado no boleto, e os números finais são o valor de pagamento do boleto, o restante são números definidos pelas instituições financeiras, uma outra forma de se ter mais segurança ao pagar um boleto, é procurar uma agencia bancaria e pedir ativação do serviço *DDA* (Debito direto autorizado) que seria um serviço que permite com que o usuário receba boletos direto em sua conta bancária, entrando em sua conta pessoal você tem uma visão muito mais ampla desses boletos, e tem como saber se o boleto é duplicado ou falso sendo que para cair em sua conta pessoal o boleto deve ser registrado, isso torna muito mais seguro o pagamento de qualquer boleto.

São muitas as formas de enganar as pessoas que fazem uso da internet, e cada vez mais os criminosos criam artimanhas para tirar proveito e lucrar à custa dos sujeitos, especialmente daqueles mais desatentos. Cabendo a todos buscar ficar mais atentos com relação às propostas que recebe via modo virtual para não cair em ciladas e se tornar vítima de crimes na internet. Bertho (2018), ainda enfatiza, *Romance Scammer* e *Fake News*:

> *Romance scammer* é um dos crimes virtuais que têm sido utilizados em sites como Facebook e sites de encontros românticos. Nestes golpes da internet, a pessoa mal-intencionada irá seduzir a vítima em busca de um romance cultivando uma relação de confiança e intimidade com ela. Depois, os golpistas sentem maior liberdade de começar a pedir dinheiro a quem seduziram ou informações pessoais e bancárias. Mensagens falsas espalhadas por *apps* de mensagens, redes sociais ou *e-mails* também podem ter um viés ainda maior que o de enganar os usuários. Em alguns casos, além da mentira e intenção de influenciar a opinião da vítima, a abordagem polêmica do título pode ser apenas uma maneira de atrair cliques para instalação de vírus no computador ou celular das pessoas. Esses vírus podem trazer concessões de acesso que permitem que o golpista roube dados pessoais, bancários ou mesmo fotos e vídeos da vítima. (BERTHO, 2018, p. 1).

Como observado os golpes partem das mais diferentes formas, as vítimas podem ser do gênero masculino ou feminino, pessoas novas ou com mais idades são seduzidas seja de maneira emocional ou financeira, enganadas e com prejuízos físicos, morais ou financeira.

Portanto, os principais crimes digitais são verdadeiras armadilhas às

pessoas de bem que por sua inocência ou falta de conhecimento acerca dos riscos que correm no que se refere aos crimes virtuais, podem se tornar vítimas dos *sites* maliciosos e sua vida pessoal ou profissional prejudicada.

2.2 Os tipos de fraudes

O avanço tecnológico tem colaborado de forma significativa para que o homem e a sociedade de modo geral cresçam em vários aspectos sociais, econômicos, culturais e históricos. Todavia, essa mesma tecnologia que tanto contribui pode ser uma aliada dos criminosos virtuais, mas inimiga dos usuários inocentes. Visto que em pouco tempo, por meio de mecanismos muitas informações são obtidas. Segundo Giavaroto & Santos (2013):

> Através das informações do Google, Yahoo e outros mecanismos de busca, em poucas horas conseguimos uma gama de informações potencializando nosso *pentest*. A disseminação de informações importantes nos sites de relacionamento como *Facebook*, Orkut, etc, facilita sobre maneira a obtenção dos dados desejados. Diretores, gerentes e administradores de redes, de uma forma geral, chegam a publicar informações desnecessárias que comprometem toda uma estrutura organizacional e, muitas das vezes, isto é feito apenas pelo ego e prazer pessoal, não levando em conta o sigilo necessário e a preservação dos dados de uma empresa. (GIAVAROTO, SANTOS, 2013, p. 21).

Observa-se que, para satisfazer seu ego, muitas vezes, o usuário permite que seus dados sejam expostos, correndo o risco de ter invadido o sigilo de sua vida pessoal ou da empresa em que trabalha.

Logo, é necessário que o usuário esteja atento a todas as situações para não pôr em risco a empresa em que trabalha e também, preservar a sua vida pessoal, principalmente na utilização dos aplicativos, onde sua particularidade pode ficar mais exposta e vulnerável aos acessos de suas informações.

2.2.1 Aplicativos de uso pessoal

Os aplicativos de uso pessoal são fundamentais para manter a rotina de trabalho organizada, visto que, nos dias atuais essa organização é um grande desafio, principalmente quando se tem inúmeras obrigações e compromissos a serem cumpridos em pouco tempo. No entanto, com a transformação digital nas empresas e o uso cada vez mais disseminado dos aplicativos na nuvem, a

tecnologia pode ser a solução para isso. Andrade (2017) enfatiza doze aplicativos de organização pessoal:

- **Google Keep**

Um aplicativo (app) intuitivo e fácil de usar que te ajuda a fazer *checklists* e organizar anotações de forma simples e rápida. O Google Keep é bastante personalizável, além de permitir vários tipos de formatos (incluindo fotos e áudios!). A interface do *app* é bonita e o programa é gratuito.

- **Trello**

O Trello é uma ferramenta de gerenciamento de tarefas que pode ser utilizada pelo desktop ou pelo *app*. Ele divide as tarefas por cartões e é um ótimo jeito de visualizar o progresso das suas atividades. Você separa seus projetos entre *a* fazer, fazendo e feito e é possível compartilhar com toda a equipe. Você também pode adicionar etiquetas, prazos e *checklists* para acompanhar o progresso da tarefa para organizar melhor ainda.

- **Evernote**

É um aplicativo que possibilita capturar, organizar e sincronizar anotações, fotos e listas com todos os seus dispositivos. O Evernote, por estar sincronizado na nuvem, garante maior segurança para seus dados.

- **Habitica**

Já pensou em usar a gamificação não apenas para gerenciar seu trabalho, mas também para se motivar? O Habitica é um app para organização diária que usa a lógica dos videogames para te motivar, usando personagens e “poderes” que você vai adquirindo e desenvolvimento conforme atinge seus objetivos.

- **Any.do**

Esse app é um gerenciador de tarefas, que pode ser utilizado tanto no desktop como no celular. Assim como o Trello, ele permite com que sua equipe veja e interaja com suas anotações. Nele você tem acesso a uma agenda mensal, na

qual é possível adicionar eventos, tarefas e checklists. Um detalhe interessante do Any.do é que ele disponibiliza lembretes para suas tarefas.

- **Pocket**

Você vê muitos links, fotos e vídeos pela Internet e não tem tempo para prestar atenção a todos eles na hora? Com o Pocket você consegue salvar as publicações em um lugar só para conferir depois. O app pode ser utilizado pelo computador e pelo celular, para que você não perca nada de interessante.

- **Todoist Karma**

Além de controlar suas tarefas, este é mais um daqueles apps de organização pessoal que tem uma proposta de desenvolvimento pessoal. Assim, toda vez que uma tarefa é completada seu perfil no aplicativo evolui pouco a pouco, destravando funcionalidades.

- **Daylio**

Nosso humor e rotina diária também são importantes de serem mensurados para conseguirmos nos tornar mais produtivos. Com o Daylio, você contabiliza seus hábitos e descreve suas atividades de forma personalizada, gerando estatísticas interessantes que podem te ajudar a criar hábitos mais saudáveis.

- **Pomodoro Timer**

Esse app se baseia na técnica de Pomodoro, que é um método para gerenciamento de tempo e aumento da produtividade. Os apps que são focados nessa técnica contam com um temporizador que contabiliza 25 minutos de trabalho intenso para 5 minutos de descanso. Ele é útil para evitar a procrastinação e ajudar na finalização de tarefas, evitando distrações.

- **Scanbot**

Imagina ter um scanner portátil? O Scanbot é um app que te ajuda a digitalizar todos os documentos que você precisa ter em mãos diretamente pelo seu celular e com boa qualidade. É bastante simples e fácil de utilizar o app, que captura

e logo disponibiliza o arquivo em PDF.

- **Mobills**

Controle seu orçamento com esse app de gerenciamento financeiro, que permite que você anote todos os seus gastos diários (como alimentação, contas etc.) e administre melhor o que entra e o que sai. Com o Mobills, você pode sincronizar dados de cartões de crédito e acompanhar seu fluxo orçamentário por gráficos interativos e de simples visualização.

- **HashTrack**

De nada adianta ter aplicativos de organização pessoal individuais se a equipe como um todo não está em sintonia sobre suas tarefas. Por isso, Se você quer estender os controles de atividade sobre toda a equipe, o **HashTrack** pode ser a solução. Esse aplicativo para organização diária centraliza as informações e, além disso, tem funcionalidades que auxiliam a fazer o cálculo do custo de horas trabalhadas, facilitando a elaboração de orçamentos, por exemplo.

Portanto, na perspectiva de organizar melhor a vida existem alguns aplicativos de organização pessoal que ajudam a simplificar as tarefas e colocar as ideias em ordem, para que o sujeito possa ser cada vez mais produtivo e ter mais tempo livre.

2.3 Prevenção de fraudes em aplicativos

Diante dos diversos crimes virtuais que traz sérias consequências a vida pessoal e a vida profissional dos usuários são necessárias buscas de mecanismos para a prevenção de fraudes em aplicativos, permitindo certa segurança as pessoas que fazem usos desses recursos tecnológicos. Para Giavaroto & Santos (2013) A tríade da segurança da informação se baseia nos princípios da Confidencialidade, Integridade e Disponibilidade. Como enfatizado abaixo, a concepção teórica desses estudiosos.

Princípio da confidencialidade: define que somente pessoas autorizadas poderão acessar determinada informação. Isto significa que, se alguém, intencionalmente ou não, acessar determinado sistema sem autorização, estará

violando o princípio da confidencialidade. Um exemplo de quebra de confidencialidade seria a invasão de um sistema computacional, protegido por senha ou não, em que o atacante pudesse obter informações confidenciais a respeito de determinada pessoa ou empresa.

Princípio da integridade: uma informação que esteja íntegra e sem alterações pode ser considerada confiável. Porém, a quebra da integridade pode ocorrer quando a informação é adulterada, intencionalmente ou não, e, com isto, a informação perde a confiabilidade, como exemplo de quebra de integridade poderíamos citar um aluno que tenta mudar sua média em um sistema de notas, de tal forma, estará comprometendo a integridade da informação de forma intencional.

Princípio da disponibilidade: define que a informação deverá estar disponível a quem esteja autorizado sempre que for necessário. Podemos citar como quebra da disponibilidade um ataque de negação de serviço contra um servidor, tal ataque faria com que o equipamento parasse de funcionar e, com isto, a informação ficaria indisponível.

Esses são alguns mecanismos de segurança que podem ser usados para evitar as fraudes em empresas ou nos aplicativos de uso pessoal, preservando os dados e informações dos usuários para não cair nos golpes dos criminosos virtuais.

2.4 Engenharia de rede social

Sabe-se da necessidade de proteger a rede de computadores de uma empresa para isso é preciso não a expor a ameaças, como o roubo de dados via engenharia social, este é um dos principais desafios dos gerentes de TI e dos profissionais de segurança da informação atualmente, pois cada vez mais os criminosos estão habilidosos na captação de informações para aplicar golpes digitais.

Nesse contexto, na engenharia social, o fraudador obtém a confiança da vítima e engana-a para extrair dados pessoais, seja por telefone, mensagem, sms ou e-mail. Os hackers, nesse caso, exploram a única fraqueza encontrada em toda e qualquer organização: a psicologia humana. Usando uma variedade de mídias, incluindo chamadas telefônicas e mídias sociais, esses invasores induzem as pessoas a oferecerem informações confidenciais. Há cada vez mais hackers tentando coletar informações sobre vítimas e, com isso, cometer atos criminosos.

Eles tentam copiar detalhes de cartões, hackear computadores e pesquisam dados para obter o máximo possível de informações a fim de realizar transações financeiras em nome da vítima.

Mesmo com as mais avançadas tecnologias, existe o risco de um funcionário ser enganado e passar os dados da empresa via engenharia social e, assim, perder informações importantes para o mercado, como dados de clientes.

Conforme escreve Mitnick e Simon (2003) um engenheiro social vive da sua capacidade de manipular as pessoas para que elas façam coisas que o ajudem a atingir o seu objetivo, mas o sucesso quase sempre requer uma grande dose de conhecimento e habilidade com os sistemas de computador e telefonia. Esta é uma amostragem dos golpes da engenharia social nos quais a tecnologia teve um papel importante.

Com base nisso é possível observar que, engenheiro social é uma pessoa inteligente que se apropria da tecnologia para atender aos seus interesses. Enquanto os ataques tradicionais alavancam vulnerabilidades de sistemas baseados em tecnologia, como erros de software e configurações incorretas, os ataques de engenharia social tiram proveito das vulnerabilidades humanas. Usam o engano para fraudar as vítimas, que são direcionadas a realizar ações prejudiciais.

A maioria desses golpes funciona porque as vítimas acreditam que se trata de algo verdadeiro e, então, entregam aos criminosos suas informações com mais facilidade. O principal objetivo do criminoso, nesse caso, é convencer a vítima a entregar suas informações voluntariamente em vez de usar ameaças ou intimidação forçada.

3 METODOLOGIA

Estudos sobre metodologia comprovam que o procedimento metodológico é o caminho traçado para se alcançar os objetivos definidos em qualquer situação ou trabalho. A consulta bibliográfica aqui exposta a respeito de crime cibernético e fraudes em aplicativos pessoais apresentaram os caminhos para a sua elaboração.

Primeiro fundamentou-se na revisão da literatura, a partir da utilização de obras acadêmicas, artigos eletrônicos e revistas especializadas que tratam da temática no contexto da tecnologia. Em seguida a sistematização das informações com revisão da literatura, apresentado os debates no campo das ideias e comparando teorias significativas na construção do saber.

Além disso, o trabalho criado teve características bibliográficas, embasado nos referenciais teóricos que tratam do assunto em questão, construindo, assim, uma pesquisa qualitativa. Destacando as principais formas de fraudes de email e WhatsApp e telegrama utilizando casos conhecidos como do juiz Moro do telegrama, e outros, mas nosso olhar será no método que eles utilizaram. Conforme enfatiza Ventura (2020):

> O MPF/PR (Ministério Público Federal do Paraná) diz em comunicado que foi vítima de um hacker que “invadiu telefones e aplicativos de procuradores da Lava Jato usados para comunicação privada e no interesse do trabalho”. O órgão explica: “não se sabe exatamente ainda a extensão da invasão, mas se sabe que foram obtidas cópias de mensagens e arquivos trocados em relações privadas e de trabalho”. Por isso, o MPF tomou medidas de segurança para evitar futuros ataques: “em face da agressão cibernética, foram adotadas medidas para aprimorar a segurança das comunicações dos integrantes do Ministério Público Federal, assim como para responsabilizar os envolvidos no ataque hacker”. (VENTURA, 2020, p. 1).

De acordo com Ventura (2020), Ainda não se sabe como as mensagens foram vazadas, mas é possível arriscar um palpite: alguém pode ter roubado a linha de celular de Dallagnol. O invasor teria acesso ao histórico de conversas dele com Moro e com o grupo da Lava Jato através do Telegram se o procurador não tivesse ativado a autenticação por dois fatores.

O Telegram não utiliza criptografia de ponta a ponta como padrão, somente nos chats secretos. Além disso, o serviço exige apenas um código enviado por SMS para fazer login. Feito isso, você — ou um invasor — tem acesso a todo o histórico de mensagens armazenado na nuvem. É um dos motivos pelos quais a autenticação

por SMS é uma péssima ideia.

Vale lembrar que isso não exige acesso ao celular da vítima: se o invasor roubar a linha, consegue receber o código SMS e fazer *login* até mesmo pelo navegador ou cliente desktop — o Telegram funciona de forma independente do smartphone.

Diante disso, observa-se que, que o uso de aplicativos é frágil diante da habilidade dos criminosos, sendo que o usuário deve se cercar de todos os cuidados para não ter suas informações vazadas como aconteceu com o juiz Sérgio Moro.

4 LOCAL DE REALIZAÇÃO DO ESTUDO

Para entender melhor a temática enfatizada, buscou-se por informações em site a respeito de como os invasores roubam os dados e aplicam golpes por meio da clonagem do WhatsApp, roubo do *chip*. Sobre essa temática Souza (2019), destaca alguns golpes como:

> 1) Chip roubado Um dos golpes mais difíceis de serem identificados pelas vítimas é o do chip perdido. Isso porque o golpista rouba o número de telefone de uma pessoa, bloqueia a linha original e se passa pela vítima para extorquir dinheiros dos contatos dela. Mas como isso é feito? Primeiro, o golpista compra um chip novo e liga para a operadora se passando pelo dono do chip original. Ele diz que perdeu o celular ou teve o aparelho roubado. Assim, a central reativa o antigo número no novo chip. Com isso, o golpista tem acesso aos grupos e à lista de contatos da pessoa no WhatsApp. Quando o novo chip é ativado, o original é bloqueado. Os criminosos fazem isso sem precisar invadir nenhum dispositivo e correndo pouco risco. (SOUZA, 2019, p. 1).

Percebe-se que esse golpe é muito comum de realizar pela facilidade que o criminoso tem de adquirir os dados e as informações do usuário do chip roubado. E de como pode se fazer passar pela pessoa que tinha o chip anteriormente e aplicar os crimes digitais.

Outro golpe muito conhecido citado por Souza (2019) é o da recarga ilimitada, mais comum em grupos públicos, essa fraude ocorre quando o usuário também quer levar algum tipo de vantagem. A fraude ocorre quando os estelionatários oferecem um serviço de recarga para celular ilimitada a um preço até dez vezes menor que o praticado pelo mercado. Algumas ofertas prometem planos ilimitados de telefonia durante um ano por um valor fixo. Também há golpistas que oferecem serviços de IPTV - um programa capaz de liberar até 18 mil canais de TV aberta e fechada do mundo inteiro.

A análise que se faz é que os criminosos buscam de toda forma lesar e enganar as pessoas, iludindo com promoções e recarga ilimitada, roubando a confiança e causando prejuízos morais e financeiros, pois a pessoa na sua inocência, ao tornar-se alvo desses estelionatários são vítimas de seus crimes e golpes virtuais.

Um dos golpes mais antigos da internet se reinventou e se tornou um dos preferidos dos golpistas durante a Black Friday: o phishing. São técnicas usadas para enganar e roubar os dados dos usuários. Uma das maneiras de fazer isso é

criar sites falsos para que os clientes repassem, sem saber, dados a golpistas.

No Brasil, eles criam correntes falsas e a distribuem massivamente por meio de correntes de WhatsApp. Geralmente, são promoções de eletrodomésticos e eletrônicos vendidos a preços muito menores que o habitual.

Ao clicar no link com a suposta promoção, o usuário é redirecionado para um site idêntico ao de grandes lojas brasileiras de departamento. Na página, ele tem a opção de colocar seus dados e comprar o produto, quando finalmente esses dados são enviados aos bandidos.

Portanto, há muitas maneiras do criminoso virtual praticar seus golpes, seja por meio de roubos de dados ou por meio de enganar, se aproveitar da falta de conhecimento ou da inocência do usuário. São bandidos que enriquecem ilicitamente gerando um déficit e causando prejuízos às pessoas de bem e a sociedade em geral.

5 SOLUÇÕES PROPOSTAS

Embora os golpistas digitais tenham suas artimanhas, há também muitas possibilidades do usuário se proteger dessas armadilhas combatendo o crime cibernético e evitando problemas em vários aspectos como sociais, morais e financeiros. Entres tantas maneiras de se proteger, especialistas dão algumas dicas e informações.

Quanto ao chip roubado, especialistas em bancos de dados explicam que a solução é ativar a verificação em duas etapas. Com isso, a pessoa que ativa um novo chip precisará de uma segunda confirmação, por e-mail ou SMS, caso ela tente acessar o aplicativo de mensagens. Os especialistas ressaltam que esse golpe só é possível quando os bandidos tiveram acesso aos dados pessoais da vítima de alguma forma. Para evitar que isso ocorra, ele indica cuidado na hora de passar essas informações online.

Nesse caso, os funcionários das operadoras pedem uma série de dados pessoais antes de ativar um novo chip. O ideal é fazer cadastros apenas em sites conhecidos para evitar que seus dados caiam em mãos erradas. Informações como nome, endereço, telefone e CPF são suficientes para cometer diversas fraudes.

Com relação à recarga ilimitada, a primeira coisa a ser feita é ativar o duplo fator de autenticação para evitar o acesso ao aparelho. Nesse sentido, as pessoas precisam se atentar aos detalhes dos links e aplicativos que elas clicam e compartilham.

Para evitar ser enganado por sites falsos antes de tudo deve-se ter um antivírus de qualidade contra vírus ou qualquer tipo malware indesejado, há muitos softwares antivírus com licença gratuita: Avast antivírus, AVG, kaspersky internet secuty. O recomendado é utilizar um antivírus com licença pois possui uma infinidade de recursos que podem ajudar e muito em sua segurança doméstica, o recomendado é o “kaspersky internet secuty, o software possui licença grátis por 30 dias, depois disso você pode adquirir um plano mensal, ele possui um varredura de sistema poderosa sendo executada constantemente procurando malwares e outros tipos de pragas virtuais, ele detecta quase que instantaneamente essas pragas virtuais, ele possui ainda gerenciador de senhas, conexão VPN segura, privace cleaner, recurso esse que permite que você exclua toda a sua atividade do seu navegador. desse modo o kaspersky torna-se um antivirus recomendado para a

proteção do seu dispositivo. Há ainda sites e extensões para navegadores, como: Google transparency report safe browsing, safe web, vírus total, esse é uma extensão disponível para mozilla Firefox e google chrome, e há também o site, essa ferramenta faz varredura de arquivos individuais em buscas de vírus como também faz analises de sites malicioso em busca de worms, cavalo de troia e muitos outros tipos de malware.

Há ainda perigo de URL encurtadas, para esse tipo de fraude usamos alguns sites, como: URL x-ray e Unshorten.com, que são sites especializados nesse tipo de crime, basta copiar o link em alguns dos sites, ele em seguida irá visualizar de forma antecipada o link que foi encurtado.

O usuário deve ter calma e paciência ao receber oferta tentadora pela internet, para verificar se a oferta é verdadeira e se a empresa tem uma boa reputação. Você também deve verificar atentamente uma sequência de fatores que podem indicar se o site é falso, você pode digitar o site manualmente diretamente no browser para evitar sites clonados, Se a loja realmente estiver fazendo a promoção ira constar no site, o cliente deve entrar em sites que comprovem a reputação da empresa, como a plataforma consumidor.gov.br, do Ministério da Justiça, e o Reclame Aqui.

Logo, estas são algumas orientações que devem ser consideradas para combater e evitar crimes cibernéticos e fraudes no uso de aplicativos móveis.

6 CONSIDERAÇÕES FINAIS

O estudo realizado é de suma relevância no contexto atual em que o homem vive, visto que, com o avanço da tecnologia, que trouxe muitos benefícios a sociedade, ampliando o conhecimento conectando pessoas e diminuindo a distância entre os sujeitos, levou também os indivíduos a viverem situações de vulnerabilidade perante os crimes cibernéticos causados por hackers que roubam dados e informações importantes dos usuários e cometem crimes virtuais, deixando sérias consequências para a vida pessoal e profissional de quem faz uso de aplicativos móveis.

Nesse sentido, o que se pode inferir é que o mundo digital apresenta duas facetas, a primeira trata das vantagens e da comodidade de usar a tecnologia por meio dos aplicativos móveis, que contribuem muito para que as pessoas possam arquivar organizar e selecionar informações de uso pessoal e profissional. Todavia esse mesmo instrumento representa um perigo, pois pessoas com más intenções pode se apropriar de informações relevantes, e que podem ser usadas contra a própria pessoa, causando, assim, desconforto e problemas na vida pessoal ou de trabalho.

Porém, por mais que o homem queira viver alheio a esse instrumento tecnológico, isso é quase que impossível, porque as mudanças no cenário do mundo atual tornam necessário que algumas ações sejam executadas usando esse mecanismo, que são os aplicativos móveis.

Os aplicativos móveis têm colaborado de forma significativa para que as informações verdadeiras ou falsas, *fakenews*, sejam proliferadas com maior rapidez. Porém, é nesse momento que falsas notícias e informações, conhecidas como *fakenews*, circulam nas redes.

O falso conteúdo compartilhado nos perfis das redes sociais gera um grande transtorno para parte da população que acaba sendo convencida pela mentira e repassa a *fakenews* adiante, sendo que, as pessoas de tanto ler ou ouvir as falsas notícias acabam por reproduzi-las com verdade.

Outra situação com relação as notícias falsas é que as consequências da sua divulgação podem ser graves como incentivo ao preconceito e à violência, aumento de surtos de doenças, prejuízos morais ou financeiros de pessoas e empresas.

Há muitas informações falsas relacionadas com a saúde. Nos últimos tempos, o Corona Vírus tem sido o seu alvo de predileção.

Os dispositivos móveis como os *tablets e* smartphones também executam aplicativos. Estes aplicativos são feitos especialmente para facilitar a realização de tarefas e disponibilizar em nosso pequeno dispositivo muitas ferramentas e acessórios que utilizamos em nossa vida cotidiana.

Existem muitos aplicativos móveis gratuitos para serem baixados. Se o seu dispositivo móvel tem conexão com a internet, poderá fazer o download de aplicativos diretamente nele, e também pode baixá-los no seu computador e em seguida transferi-los para o móvel.

Sendo, então, a utilização dos aplicativos móveis realizada pelos indivíduos de grande relevância para desenvolver tarefas simples e complexas é importante que se tenha o conhecimento acerca desse recurso tecnológico para melhor compreender o contexto em que está inserido.

A partir das leituras realizadas e da sistematização das ideias acerca da temática enfatizada foi possível compreender por meio das respostas aos questionamentos que, o crime cibernético acontece quando criminosos virtuais se apropriam de informações de dados pessoais dos usuários para roubar, enganar o dono dos dados ou em seu nome cometer crimes, causando prejuízos moral e financeiro aos usuários.

Muitas vezes, os crimes cometidos atingem várias pessoas ao mesmo tempo, causando prejuízos coletivos e irreversíveis. Por isso, é de fundamental importância que ao utilizar os aplicativos móveis, os usuários busquem as formas de evitar que seus dados sejam acessados e usados de má fé.

Ficou conhecido que os aplicativos móveis são vários e servem para guardar informações pessoais ou de trabalho para que os usuários tenham mais tempo livre, organizam melhor e ajudam a simplificar as tarefas e colocar as ideias em ordem, para que o sujeito possa ser cada vez mais produtivo.

Esses aplicativos que normalmente são vistos em celular ou tablet. São aplicativos simples e amigáveis para a interface de um pequeno dispositivo. No entanto, o que começou nos telefones celulares e *tablets* agora se espalhou para relógios inteligentes, televisores e carros também.

Além disso, no mundo dos aplicativos móveis, existem vários tipos de aplicativos. É importante saber diferenciar o tipo de aplicativo móvel, principalmente se estiver pensando em criar um. Poderá encontrar uma grande diferença entre orçamentos e, entre outras coisas, a tecnologia com que são feitos é um fator determinante.

Ao analisar os tipos de fraudes foi possível inferir que, esses golpes acontecem de várias formas, os criminosos podem se apropriar dos dados das pessoas por meio do roubo do chip, de recargas ilimitadas e sites maliciosos que enganam as pessoas com propostas tentadoras.

Observa-se que, os criminosos são estrategistas e encontram formas de seduzir e enganar o usuário, são propostas tentadoras, verdadeiras armadilhas do mundo virtual.

Todavia, existem formas de combater e evitar que hackers acessem seus dados, o ideal é fazer cadastros apenas em sites conhecidos para evitar que seus dados caiam em mãos erradas. Informações como nome, endereço, telefone e CPF são suficientes para cometer diversas fraudes.

Portanto, a construção do presente estudo foi de fundamental relevância, pois abriu um leque de possibilidades e conhecimentos acerca do mundo tecnológico, e de como é o mergulho nesse campo virtual pode se tornar perigoso e cheio de problemas quando se tem os dados rackeados por fraudadores que se apropriam de informação para prejudicar suas vítimas.

REFERÊNCIAS

ANDRADE, Luiza. **Os 12 melhores apps de organização pessoal**. Disponível em: https://www.siteware.com.br/blog/produtividade/apps-de-organizacao-pessoal/. 2017. Acesso em: 12/12/2020.

BERTHO, Audrey. **7 crimes virtuais já registrados – principais golpes da internet.** Disponível em: https://blog.siteblindado.com/crimes-virtuais-golpes-da-internet. Acesso em: 12/12/2020.

BRIAT, M. (1985). **La fraude informatique**: une approche de droit compare. Bruxelas, 4.

CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade.** Revista Científica Eletrônica do Curso de Direito, 13ª ed., Jan. 2018. Disponível em: http://faef.revista.inf.br/imagens_arquivos /arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em: 21/12/2020.

GIAVARATO, Sílvio César Roxo. SANTOS, Gerson Raimundo dos. **Backtrack Linux**. Auditoria e teste de invasão em redes de computadores. Rio de Janeiro. Editora Ciência moderna Ltda. 2013. Disponível em: https://drive.google.com/file/d/198Ib5gmvRU8SvOI1RJJQf7LbGwOg8qV1/view. Acessa em: 27/12/2020.

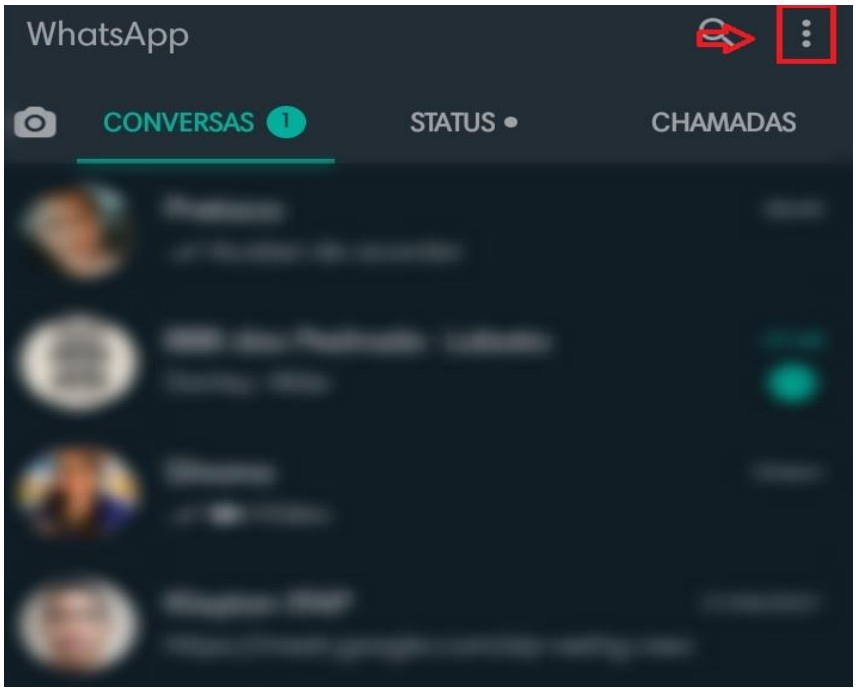
MITNICK Kevin D.; SIMON William L. MITNICK - **A arte de enganar**/. 2003. Disponível em: https://drive.google.com/file/d/1KQ7tSQ44ysIKKZQKhjTYi5mOT_KUkUVo/view. Acesso em: 18/01/2021.

SOUZA, Felipe. **Uma das principais precauções é configurar a autenticação em duas etapas, mas há uma maneira ainda mais eficaz..** https://www.uol.com.br/tilt/noticias/bbc/2019/11/10/veja-quais-sao-os-golpes-mais-comuns-no-whatsapp-e-como-se-proteger. Acesso em: 19/01/2021.

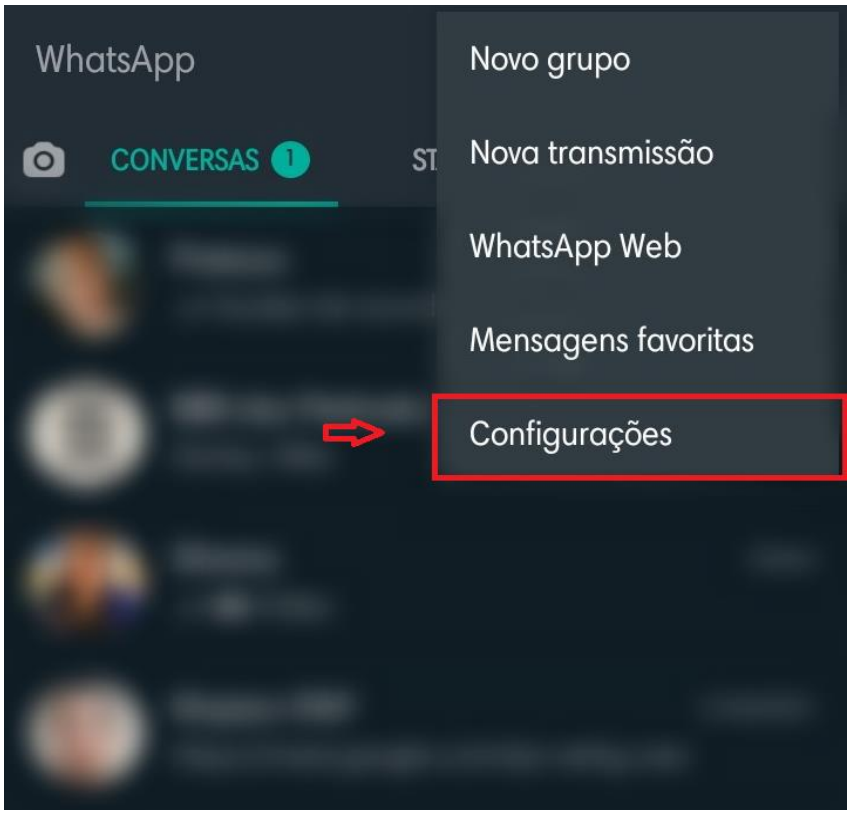
VENTURA, Felipe. **Como foram vazadas as conversas no Telegram entre Moro e Dallagnol?** Disponível em: https://tecnoblog.net/293880/vazamento-mensagens-telegram-sergio-moro-deltan-dallagnol/. Acesso em: 18/01/2021.

ANEXO A: VERIFICAÇÃO EM DUAS ETAPAS NO WHATSAPP

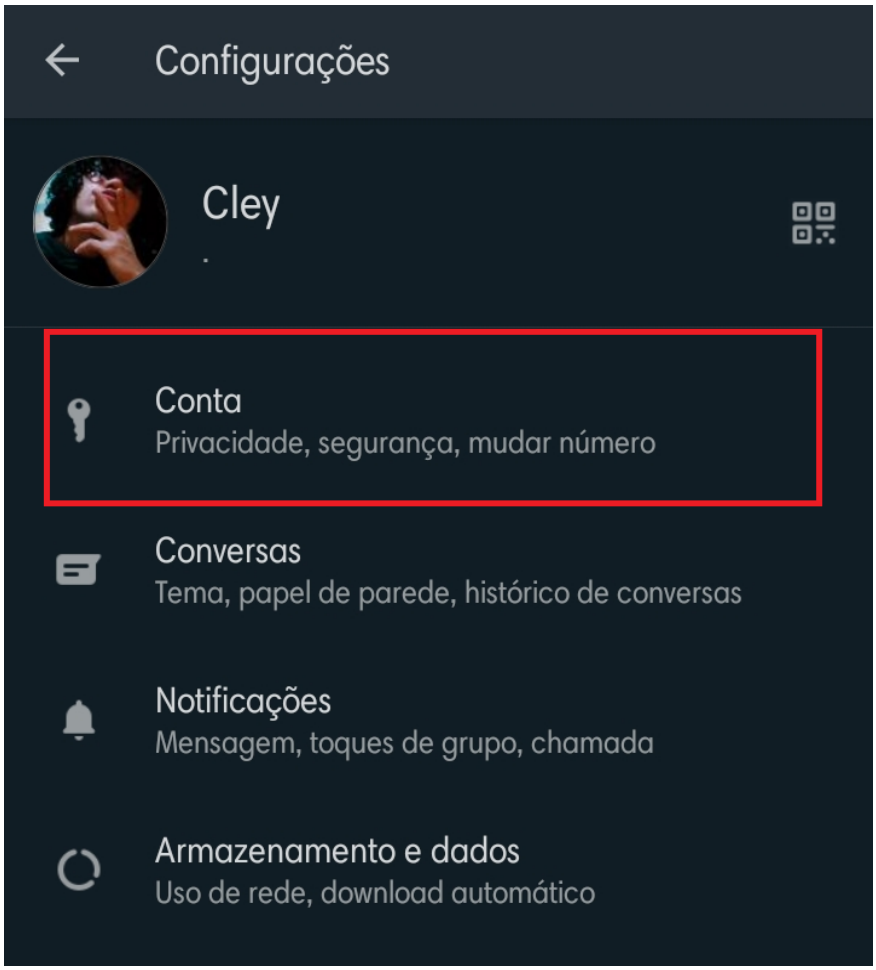
- Clique nos “**três pontinhos**” no canto superior direito.



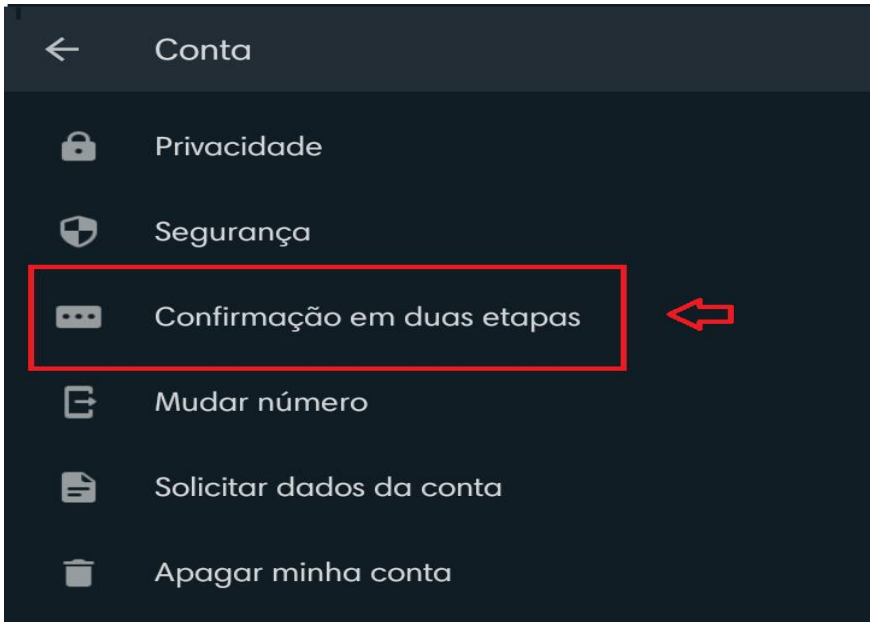
- No menu aberto em seguida “**clique em configurações**”.



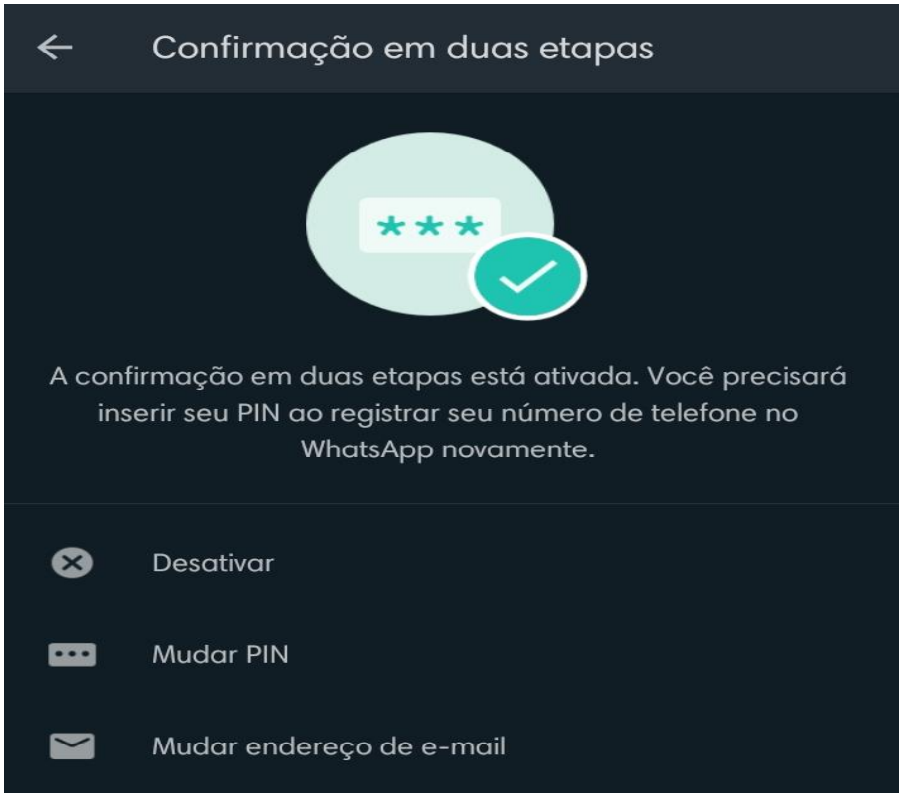
- Feito isso toque sobre “**conta**”



- Agora selecione “**confirmação em duas etapas**”



- Depois que você clicar em confirmação em duas etapas irá aparecer a opção “**ativar**” para você começar a configurar, mas como o meu já estava ativado não aparece essa opção, porém é só ativar e começar a configurar.



- Você pode configurar um **e-mail** para verificação em duas etapas caso você esqueça o código PIN você pode redefinir pelo e-mail cadastrado, hoje só vamos configurar o PIN. Nesse passo basta clicar na opção desejada e configurar.