UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
FACULDADE DE CIÊNCIAS - CAMPUS BAURU
DEPARTAMENTO DE COMPUTAÇÃO
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

GABRIEL CARVALHO POLIDO

ESTUDO SOBRE FRAUDES DIGITAIS E O DESENVOLVIMENTO DE APLICATIVO PARA SMARTPHONES ANDROID E IOS PARA USO EM PALESTRAS DE SENSIBILIZAÇÃO E ESCLARECIMENTO

BAURU
Novembro/2023

GABRIEL CARVALHO POLIDO

ESTUDO SOBRE FRAUDES DIGITAIS E O DESENVOLVIMENTO DE APLICATIVO PARA SMARTPHONES ANDROID E IOS PARA USO EM PALESTRAS DE SENSIBILIZAÇÃO E ESCLARECIMENTO

Trabalho de Conclusão de Curso do Curso de Ciência da Computação da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Faculdade de Ciências, Campus Bauru.
Orientador: Prof. Assoc Eduardo Martins Morgado

BAURU
Novembro/2023

P766e

Polido, Gabriel Carvalho
Estudo sobre fraudes digitais e o desenvolvimento de aplicativo para smartphones android e ios para uso em palestras de sensibilização e esclarecimento / Gabriel Carvalho Polido. -- Bauru, 2023
41 p.

Trabalho de conclusão de curso (Bacharelado - Ciência da Computação) - Universidade Estadual Paulista (Unesp), Faculdade de Ciências, Bauru
Orientador: Eduardo Martins Morgado

1. Ciência da computação. 2. Fraude na Internet. 3. Engenharia social. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Ciências, Bauru. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Gabriel Carvalho Polido

Estudo sobre fraudes digitais e o desenvolvimento de aplicativo para smartphones android e ios para uso em palestras de sensibilização e esclarecimento

Trabalho de Conclusão de Curso do Curso de Ciência da Computação da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Faculdade de Ciências, Campus Bauru.

Banca Examinadora

Prof. Assoc Eduardo Martins Morgado
Orientador
Universidade Estadual Paulista "Júlio de Mesquita Filho"
Faculdade de Ciências
Departamento de Ciência da Computação

Profa. Dra. Simone das Graças Domingues Prado
Universidade Estadual Paulista "Júlio de Mesquita Filho"
Faculdade de Ciências
Departamento de Ciência da Computação

Dr. João Pedro Albino
Universidade Estadual Paulista "Júlio de Mesquita Filho"
Faculdade de Ciências
Departamento de Ciência da Computação

Bauru, _____ de _____ de ____.

Resumo

Golpes e fraudes digitais são uma ameaça em constante evolução, principalmente quando utilizam três estratégias de ataque: ***Phishing***, ***Spoofing*** e **Engenharia Social**. Durante a pesquisa, foi destacada a natureza sofisticada dessas ameaças, que visam enganar os usuários e obter acesso a informações confidenciais. O estudo forneceu uma análise aprofundada de cada estratégia, explorando exemplos de casos e técnicas de mitigação. Além disso, foram estudadas as estratégias de ataque que são utilizadas atualmente para que seja possível enfrentar com êxito essas ameaças. tais estrategias de ataque tem o intuito de roubar informações e recursos, visando posteriormente utilizar tais informações para aplicar golpes e fraudes elaboradas na vítima. Assim sendo, foi enfatizada a importância da conscientização e da educação como estratégias cruciais para proteger indivíduos e organizações contra essas ameaças digitais em um ambiente cada vez mais interconectado, dependente da tecnologia e em constante evolução. Foi desenvolvido um aplicativo informático que incentiva as pessoas a tomarem medidas mais proativas para combater eficazmente os golpes e fraudes digitais, garantindo um ambiente cibernético mais seguro.

Palavras-chave: Golpes digitais, Fraudes digitais, Phishing, Spoofing, Engenharia Social.

Abstract

Digital scams and frauds are a constantly evolving threat, particularly when they specifically employ three attack tactics: Phishing, Spoofing, and Social Engineering. Throughout the research, the sophisticated nature of these threats was highlighted, which aim to trick users into gaining access to useful information. The study provided an in-depth analysis of each strategy, exploring case examples and mitigation techniques. Furthermore, the attack strategies that are currently used were studied so that it is possible to successfully deal with these threats. Such attack strategies have the intention of stealing information and resources, later using such information to apply elaborate scams and frauds on the victim. Therefore, the importance of awareness and education was emphasized as crucial strategies to protect individuals and organizations against these digital threats in an increasingly interconnected, technology-dependent and constantly evolving environment. A computer application has been developed that encourages people to take more proactive measures to effectively combat scams and digital fraud, ensuring a safer cyber environment.

Keywords: Digital scams, Phishing, Spoofing, Social Engineering.

Lista de figuras

Lista de abreviaturas e siglas

CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
DNS	*Domain Name System*

Sumário

1 Introdução

Este trabalho visa contribuir para aumentar o entendimento sobre golpes digitais, além de fornecer orientações para prevenir tais crimes virtuais. A sociedade se beneficiará com resultados positivos, já que tal prática no mundo digital é constantemente aprimorada.

Nos últimos anos, o grande aumento das fraudes digitais que estão ocorrendo, estão causando prejuízos financeiros e emocionais para empresas e pessoas. Os criminosos virtuais utilizam técnicas cada vez mais sofisticadas para enganar e lesar terceiros. Para combater essa ameaça, existem algumas soluções tecnológicas, como *softwares*, antivírus, *antimalwares*, sistemas de autenticação de acesso, que tentam proteger a privacidade e a segurança das informações *online*. Contudo, a ação mais eficaz é o envolvimento das pessoas na sua própria defesa, o que exige intensos e frequentes meios de conscientização e esclarecimento.

Com o passar do tempo e com a maioria das pessoas armazenando seus dados pessoais, sem o devido cuidado, em computadores, celulares, e sites, entre outros recursos tecnológicos. As autoridades brasileiras vem reconhecendo a importância da proteção dos dados pessoais para evitar fraudes, e estão implantando uma adequação e padronização das legislações através da implementação do Marco Civil da Internet e da Lei Geral de Proteção de Dados. Estas leis transformaram a proteção de dados em uma obrigação do Estado. Como resultado, os controladores e operadores de dados pessoais passaram a ser responsabilizados pelo tratamento e controle dessas informações, podendo enfrentar problemas que podem incluir o ressarcimento de danos e o pagamento de indenizações. Nesse contexto, a segurança e a confidencialidade dos dados emergem como os principais objetivos dessas legislações, promovendo uma maior proteção aos direitos individuais e à privacidade."

Diante desse cenário, ao aprimorar o conhecimento sobre as principais técnicas de fraudes digitais, será possível identificar as melhores práticas para prevenção e conscientização. Nosso projeto vai desenvolver um aplicativo para ***smartphones***, sejam eles Android ou iOS, que possam ser utilizados em palestras e eventos de esclarecimento sobre o tema. Espera-se que essa pesquisa possa contribuir para a redução dos índices de fraudes digitais e aumentar a segurança e o bem-estar das pessoas no mundo digital.

1.1 Contexto

Atualmente no mundo pode-se encontrar disponíveis na rede, as mais variadas informações sobre os mais diversos tipos de pessoas .

Para Tieso e Santo (2020) a informação é um dos ativos com mais valor em uma organização, exatamente por isso também é o mais visado e cobiçado por pessoas más intencionadas que tem como objetivo roubar informações, em outras palavras a informação obtida por criminosos pode ser usada para a prática de golpes

1.1.1 Redes sociais

O mundo das redes sociais online tem crescido com o desenvolvimento da internet, oferecendo uma ampla gama de serviços, que podem ser um eficaz meio de comunicação usado diariamente por parte da população.

No entanto, esse crescimento também proporcionou oportunidades para criminosos que exploram essas plataformas de forma anônima, e como resultado, crimes podem acontecer, vaiando de pequenos delitos a crimes internacionais, que agora ocorrem em comunidades virtuais.

Infelizmente, os usuários dessas redes muitas vezes se expõem excessivamente, tornando-se alvos fáceis para ataques contínuos, pois disponibilizam publicamente diversas informações que auxiliam a realização de golpes.

1.2 Problema

Nos últimos anos, a complexidade das fraudes digitais tem aumentado, e os criminosos virtuais utilizam técnicas cada vez mais sofisticadas para enganar e lesar pessoas e empresas, segundo o levantamento da Febraban (2022a) o número de vítimas de golpes ou tentativas de golpe em 2021, era 21% em setembro, 22% em dezembro e, em junho de 2022, subiu para 31%. Dentre as várias técnicas de ataques destacam-se:

1.2.1 *Phishing*

O *phishing*, que é uma das práticas mais recorrentes no ambiente virtual, e consiste na captação de dados pessoais da vítima, para isso, o criminoso se vale de falsos *e-mail* e mensagens, quase sempre informando que a pessoa é a ganhadora de algum prêmio e para recebê-lo é necessário enviar suas informações pessoais (WANDERLEY; COSTA; RIBEIRO, 2022).

A palavra *phishing* deriva do inglês e faz referencia ao ato de pescar, pois na analogia o criminoso equivale a um pescador que joga iscas na água esperando alguma vítima cair na armadilha.

No último ano, o Brasil foi o país mais atacado por *phishing* pelo WhatsApp, com mais de 76 mil tentativas de fraudes. A pesquisa também mostra que o país é o quarto no mundo que mais sofre *phishing* via e-mail(KASPERSKY, 2023).

1.2.1.1 *Spear phishing*

É um tipo de phishing que é direcionado a um alvo específico, podendo ser um indivíduo, instituição ou empresa, assim os criminosos juntam informações sobre a vítima e executam o ataque utilizando esses dados obtidos, para que faça parecer o mais legítimo possível o que está sendo enviado, aumentando as chances do golpe ser bem sucedido. (LIPU et al., 2021)

As mensagens de *spear phishing* costumam parecer mais legítimas, pois são personalizadas para parecerem vindas de fontes confiáveis, como colegas de trabalho, superiores hierárquicos ou empresas conhecidas. Podem solicitar informações confidenciais, induzir o destinatário a baixar um arquivo infectado ou a clicar em um link malicioso.

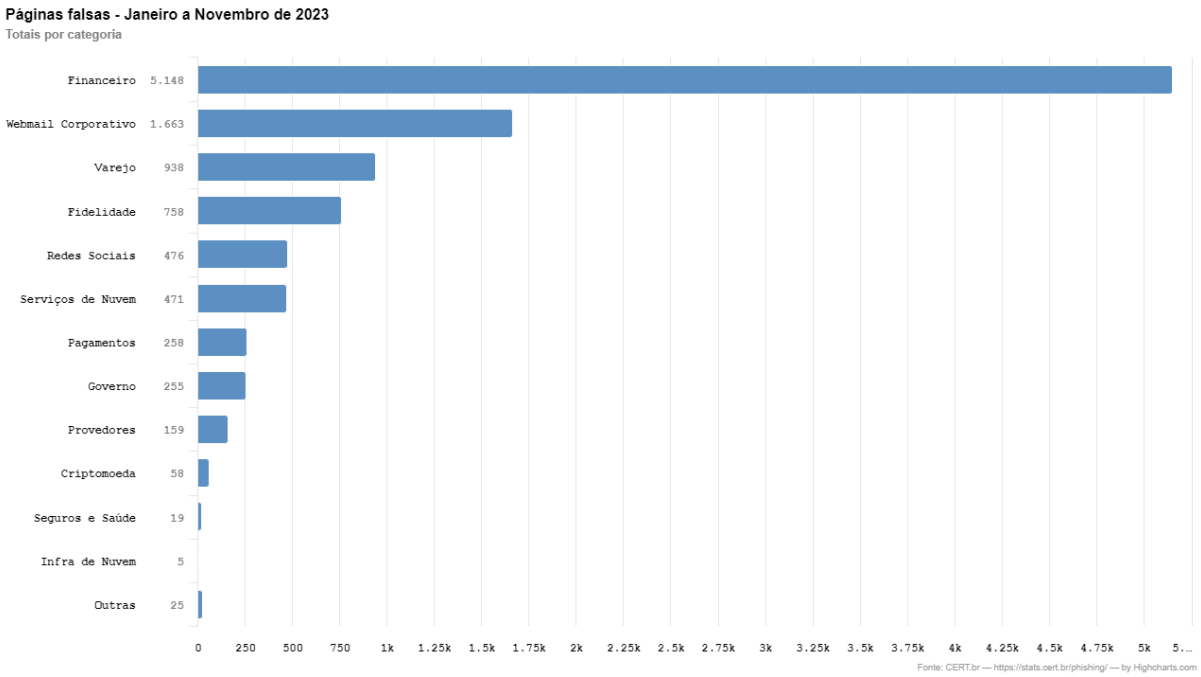
Devido à sua natureza altamente direcionada, o *spear phishing* pode ser ainda mais perigoso do que o *phishing* tradicional, pois é mais difícil de ser detectado por sistemas de segurança convencionais. A defesa contra esse tipo de ataque requer não apenas tecnologias de segurança robustas, mas também uma cultura de conscientização e treinamento para que os usuários estejam alertas e capacitados para identificar e evitar essas tentativas de ataque direcionadas.

1.2.1.2 Páginas falsas utilizadas em tentativas de *phishing*

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um grupo que tem como missão Aamentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à internet no Brasil.

Para CERT (2023) essas estatísticas de páginas falsas são utilizadas em tentativas de *phishing* relativas tanto a golpes com intuito de obter vantagem financeira direta (envolvendo bancos, cartões de crédito, meios de pagamento e sites de comércio eletrônico), quanto a tentativas de fraude em geral envolvendo serviços de *webmail*, acessos remotos corporativos, credenciais de serviços de nuvem, entre outros.

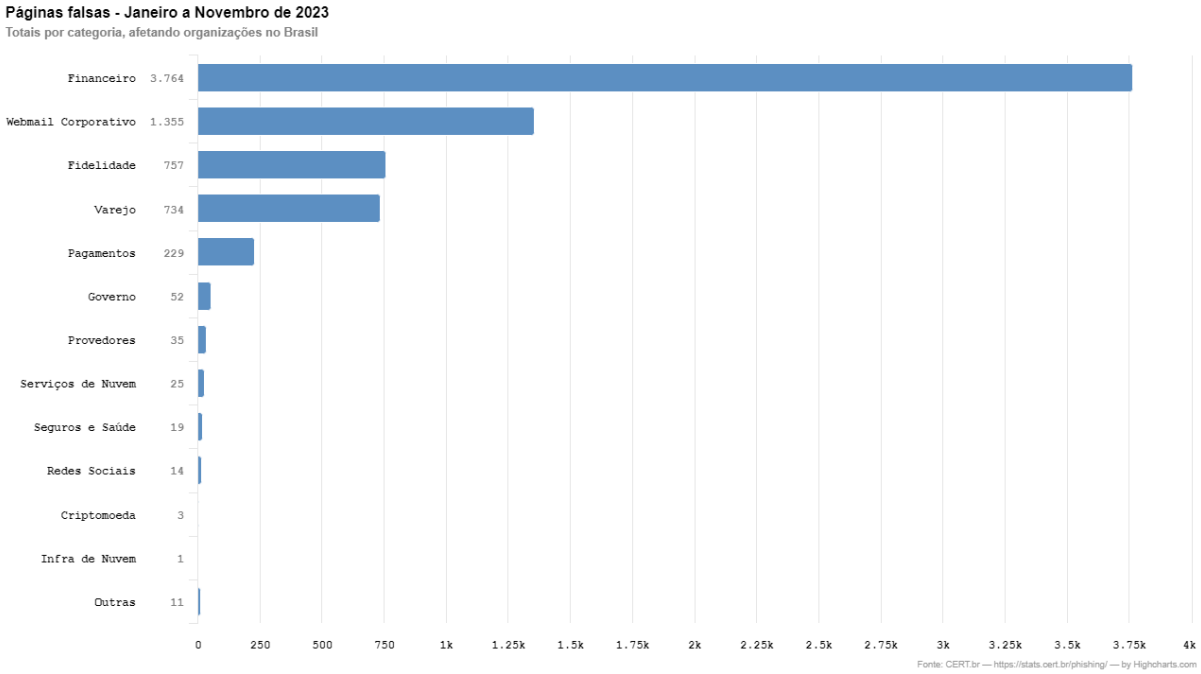
Figura 1 – Páginas falsas de janeiro a novembro de 2023



Fonte: CERT.br

Na análise da figura 1, torna-se evidente que a maior parte das páginas falsas criadas estão estrategicamente projetadas para imitar plataformas financeiras legítimas. Essa observação é crucial, uma vez que revela a direção estratégica dos golpistas, eles miram diretamente as instituições financeiras e seus usuários, explorando a confiança e a falta de familiaridade que as pessoas têm com esses sites. A predominância dessas imitações de sites financeiros ressalta a gravidade do problema, pois não se trata apenas de uma questão de simples clonagem, mas sim de um ataque direto à privacidade e à segurança das informações pessoais e financeiras dos indivíduos. Essa estratégia reflete a sofisticação crescente dos golpes de *phishing*, exigindo medidas cada vez mais abrangentes e adaptáveis para proteger os usuários contra tais ataques maliciosos.

Figura 2 – Páginas falsas de janeiro a novembro de 2023 afetando organizações no brasil

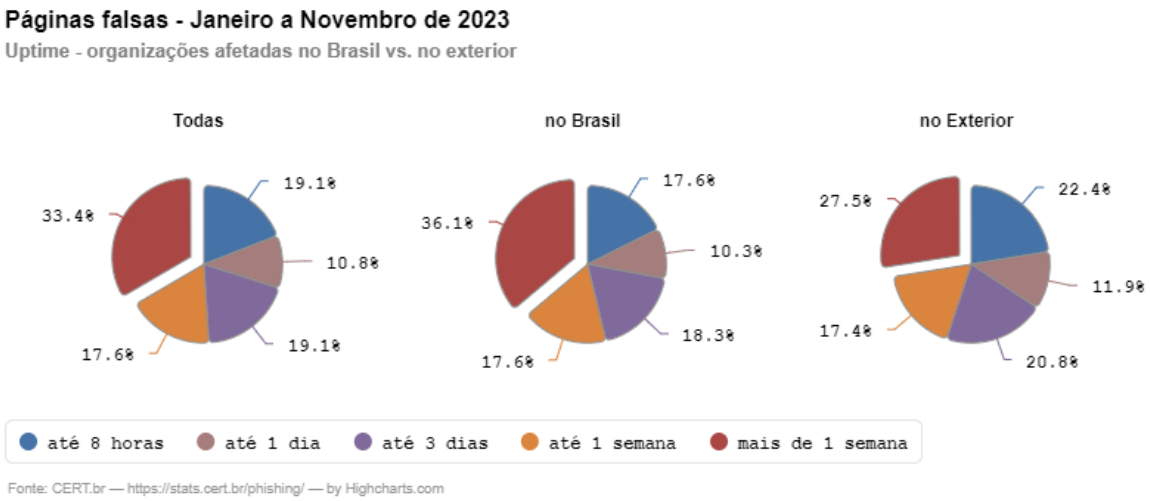


Fonte: CERT.br

Na análise da figura 2, é possível observar que o Brasil enfrenta impactos semelhantes aos de outras regiões afetadas pelos golpes digitais de *phishing*. Isso demonstra que o país não está imune a essa ameaça crescente e global. A representação gráfica evidencia que as estratégias de ataque e os padrões de imitação de sites financeiros são recorrentes no contexto brasileiro, corroborando a natureza disseminada e indiscriminada desses golpes.

Essa similaridade de impacto reforça a necessidade de abordagens específicas e adaptadas à realidade brasileira no que tange à proteção contra esses golpes. Além disso, ressalta a importância de políticas e medidas de segurança mais robustas, juntamente com a conscientização pública, visando mitigar os riscos associados à engenharia social e à proteção da privacidade dos dados pessoais no país.

Figura 3 – Tempo de existência das páginas falsas de janeiro a novembro de 2023



Fonte: CERT.br

A análise da figura 3 revela um padrão consistente e alarmante: tanto no contexto global quanto no Brasil, a maioria das páginas falsas criadas como parte desses golpes de engenharia social têm uma vida útil extremamente curta, durando menos de uma semana. Esse dado, por si só, ressalta a natureza efêmera e fugaz dessas tentativas maliciosas.

Essa rápida desativação das páginas falsas pode ser interpretada como uma estratégia deliberada dos golpistas para evitar detecção e ações de mitigação por parte das autoridades ou das equipes de segurança. A brevidade dessas páginas ressalta a necessidade urgente de respostas igualmente ágeis por parte das instituições e usuários, como sistemas de detecção precoce, atualizações constantes de medidas de segurança e educação contínua dos usuários sobre os riscos associados a esses golpes.

Esses dados reforçam a dinâmica veloz e evolutiva desses ataques, exigindo estratégias de proteção ágeis e adaptativas para enfrentar essa realidade em constante mutação.

1.2.2 *Spoofing*

Já o ***spoofing*** é outro tipo de técnica amplamente utilizada por cibercriminosos no Brasi, e consiste em falsificar informações de identificação, como endereços de ***e-mail*** ou **números de telefone**, para enganar as vítimas e fazê-las acreditar que estão interagindo com pessoas ou organizações legítimas.

O *spoofing* é uma técnica utilizada por criminosos que consiste na falsificação

da identidade e de aparelhos no meio digital. Esta técnica, assim como o *phishing*, tem o objetivo de roubar dados, disseminar malware ou contornar controles de acesso. Suas formas mais comuns são *spoofing* de e-mail, DNS e identificador de chamadas(LIPU et al., 2021).

1.2.2.1 DNS *Spoofing*

Para Espínula e Cruz (2020) quando o Domain Name System (DNS) Spoofing é aplicado ele redireciona as solicitações de um endereço DNS específico da rede para outro endereço, ou melhor dizendo, quando o site “X” é solicitado pelo usuário, o atacante o redireciona para o site “Y”, porém com o mesmo endereço de URL na rede, o que faz com que o usuário pense que realmente está no site que deveria estar, quando na realidade o invasor está no controle da situação.

1.2.2.2 Spoofing de identificador de chamadas

Espínula e Cruz (2020) ainda define o Spoofing de identificador de chamadas como um ataque que é ainda mais fácil de ser feito do que o primeiro. Ele consiste na troca do numero da ligação, o atacante pode ligar para o celular da vítima passando-se por uma operadora telefônica (com o mesmo número de ramal), o que representa uma falsa credibilidade para a vítima.

A simplicidade e a eficácia desse método aumentam sua periculosidade, essa vulnerabilidade ressalta a importância de conscientizar as pessoas sobre os riscos associados à confiança cega na identificação de chamadas e na necessidade de adotar medidas adicionais de verificação e segurança ao lidar com chamadas de fontes desconhecidas ou suspeitas.

1.2.2.3 Spoofing de email

Spoofing de e-mail é um termo usado para descrever atividades de e-mail (geralmente fraudulentas) nas quais o endereço do remetente e outras partes do cabeçalho do e-mail são alteradas para parecer que o e-mail foi originado. de uma fonte diferente(PANDOVE; JINDAL; KUMAR, 2010).

O spoofing de e-mail é uma prática que evolui constantemente, desafiando as medidas de segurança existentes. Uma análise das tendências atuais nessa área revela uma sofisticação crescente nos métodos utilizados, como o uso de técnicas de falsificação mais avançadas e a exploração de vulnerabilidades em sistemas de autenticação de e-mail. Compreender a natureza dinâmica dessas estratégias é crucial para desenvolver defesas eficazes e proativas contra esses ataques, destacando a necessidade de soluções que vão além das abordagens convencionais de segurança cibernética.

1.2.3 Engenharia social

Ambos os tipos de ataques anteriores têm sido cada vez mais comuns nos últimos anos, e podem causar danos financeiros além de prejudicar a privacidade e a segurança dos usuários da internet. Além dos dois ataques já citados, ainda existe uma ferramenta usada pelos cibercriminosos, para Piovesan et al. (2019) ela é uma ameaça, que além de perigosa é desconhecida por muitos, a engenharia social, que busca obter informações enganando usuários. para aumentar suas chances de efetuarem um golpe, esta ferramenta é chamada de **engenharia social**.

Para Piovesan et al. (2019) uma ameaça, que além de perigosa é desconhecida por muitos é a engenharia social, que busca obter informações enganando usuários.

Segundo Souza (2019) a engenharia social é considerada uma das grandes ameaças a serem enfrentadas na segurança da informação, principalmente por que é focada no fator humano.

Na **engenharia social**, os fraudadores, utilizando contato por voz, buscam conquistar a confiança de suas vítimas e enganá-las a fim de extrair dados pessoais, utilizando diversos meios, como **telefonemas**, **mensagens**, e **e-mails**. Os hackers exploram as vulnerabilidades associadas com o comportamento das pessoas, que seriam técnicas derivadas da psicologia. Empregando uma ampla gama de canais de comunicação, incluindo chamadas telefônicas e redes sociais, esses invasores convencem as pessoas a colaborar e fornecer informações confidenciais.

É amplamente reconhecido que a proteção da rede de computadores de uma empresa é de suma importância, a fim de mitigar ameaças, como o roubo de dados por meio de engenharia social. Este desafio representa uma das principais preocupações para os gerentes de TI e os profissionais de segurança da informação na atualidade, devido à crescente habilidade dos criminosos na obtenção de informações para a execução de golpes digitais, contudo no âmbito da vida pessoal as pessoas ainda não tomam os devidos cuidados para mitigar esse tipo risco.

A ameaça de hackers que buscam incessantemente informações sobre suas vítimas com a intenção de cometer atos criminosos tem se tornado cada vez mais premente.

2 Fundamentação Teórica

2.1 Exemplos

Para fortalecer as defesas contra os crescentes riscos de golpes digitais, é essencial não apenas reconhecer, mas também compreender em detalhes os diferentes tipos de golpes aplicados na atualidade, afinal a evolução tecnológica proporcionou aos golpistas uma gama diversificada de táticas enganosas e métodos sofisticados para explorar a vulnerabilidade das pessoas.

Esses golpes digitais abrangem uma ampla gama de estratégias onde podem ser categorizados, como *phishing*, ataques de engenharia social, *spoofing*, entre outros.

Segundo a Anatel (2023), os golpes e fraudes mais comuns são Sequestro da linha, obtenção de dados de celular roubado, chamadas falsas, golpe da falsa central de atendimento, golpe de engenharia social furto de contas de redes sociais e aplicativos e golpe do WhatsApp falso

Segundo a Febraban (2021), a incidência do golpe do falso motoboy, fraude muito comum durante a pandemia, se mantém como uma das principais investidas dos criminosos e registrou aumento de 271%.

Alguns exemplos brasileiros de fraudes mais comuns são apresentados a seguir, segundo a Febraban (2022b) e a Anatel (2023)

2.1.1 Golpe da falsa central de atendimento

O golpista faz contato com a pessoa se passando por um representante do banco ou empresa com a qual ela mantém um relacionamento ativo. Ele informa à vítima que sua conta foi comprometida de alguma forma, como invadida ou clonada, e a partir daí solicita informações pessoais e financeiras. Em alguns casos, instrui a vítima a ligar para a central do banco, utilizando o número encontrado no verso do cartão, porém o fraudador permanece na linha para simular o atendimento da central e solicitar os dados da conta, informações dos cartões e a senha.

2.1.2 Como evitar

Ao receber mensagens desse tipo, mantenha-se alerta e busque os canais oficiais da empresa mencionada na suposta ligação para verificar a autenticidade do problema. Nunca compartilhe informações pessoais ou bancárias por telefone ou mensagem de texto com desconhecidos. Lembre-se de que as histórias dos golpes

frequentemente se alteram para parecerem mais convincentes. Desconfie sempre de solicitações repentinas e inesperadas.

2.1.3 Como resolver

Caso seja vítima desse tipo de golpe, entre imediatamente em contato com a empresa, órgão ou instituição por meio de seus canais oficiais para relatar o incidente. Além disso, é recomendado alterar suas senhas imediatamente e verificar se há atividades suspeitas em suas contas bancárias. Essas ações ajudarão a minimizar os danos causados pelo golpe e a proteger suas informações pessoais.

2.1.4 Obtenção de dados de celular roubado

Quando um criminoso rouba ou furta um celular, diversas possibilidades se abrem. O aparelho pode ser vendido no mercado ilegal para obtenção de lucro rápido. No entanto, há também a prática de reter o dispositivo para acessar informações pessoais e profissionais da vítima. Isso inclui a busca por senhas, exploração de aplicativos e invasão de contas, resultando em um potencial uso indevido dos dados.

2.1.4.1 Como evitar

A segurança do seu celular deve ser uma prioridade constante, não apenas após o roubo, furto ou perda. Adote medidas preventivas, como a criação de uma senha robusta para desbloquear o aparelho. Além disso, faça backups regulares de informações importantes e evite armazenar senhas de forma desprotegida no dispositivo. Manter a opção de localização ativada é crucial para rastrear o aparelho, mesmo se estiver desligado, em caso de situações desse tipo.

2.1.4.2 Como resolver

Se você foi vítima de roubo ou furto de celular, é essencial registrar um boletim de ocorrência na polícia civil imediatamente. Também é crucial informar ao banco e à operadora do celular sobre o ocorrido. O bloqueio do aparelho pode ser solicitado no momento do registro do boletim de ocorrência, enquanto o bloqueio da linha deve ser requisitado à operadora.

2.1.5 Chamadas falsas

Os criminosos se aproveitam da adulteração de equipamentos de telecomunicações para originar chamadas utilizando números falsos. Essa prática permite que eles simulem ligações provenientes de empresas, bancos ou instituições conhecidas. Ao receber a ligação, a vítima pode acreditar estar conversando com um representante

legítimo, o que facilita a obtenção de dados pessoais. O objetivo é coletar informações sensíveis para perpetrar fraudes ou causar danos financeiros à vítima.

2.1.5.1 Como evitar

É crucial manter um nível elevado de desconfiança ao receber ligações supostamente de empresas ou instituições. Se houver solicitação de dados pessoais, senhas, informações bancárias ou pagamento de tarifas, é importante não fornecer essas informações de imediato. Antes de compartilhar qualquer dado, verifique a autenticidade da ligação por meio dos canais oficiais de atendimento da empresa ou instituição em questão. Em caso de dúvida, encerre a chamada e confirme sua veracidade utilizando os canais oficiais de atendimento.

2.1.6 Como resolver

Se você foi vítima desse tipo de golpe, é fundamental registrar um Boletim de Ocorrência para documentar o ocorrido. Além disso, comunique imediatamente o problema à empresa, órgão ou instituição mencionada pelo fraudador, utilizando os canais oficiais de comunicação. Essa ação é crucial para alertar a instituição sobre o incidente e iniciar procedimentos para minimizar os danos causados pela fraude.

2.1.7 Falso motoboy

O golpe se inicia com uma ligação fraudulenta, onde o cliente é contatado por alguém que se faz passar por um funcionário bancário. Esse impostor alega a ocorrência de uma fraude com o cartão da vítima. Fingindo ser um representante legítimo da instituição, o fraudador solicita a senha do cartão e instrui a vítima a cortar o plástico, mantendo o chip intacto. Em seguida, o falso funcionário informa que um mensageiro será enviado à residência do cliente para retirar o cartão supostamente para "análise".

2.1.7.1 Como evitar

Mantenha-se alerta para chamadas inesperadas. Não forneça informações pessoais ou senhas por telefone, especialmente se a ligação vier de fontes não verificadas. Os bancos geralmente não solicitam senhas por telefone. Caso haja suspeita, entre em contato diretamente com o banco utilizando os canais oficiais de atendimento ao cliente para confirmar a veracidade da situação.

2.1.7.2 Como resolver

Se você for vítima desse tipo de golpe, é crucial agir rapidamente. Registre um Boletim de Ocorrência na delegacia mais próxima e entre em contato imediatamente com seu banco para relatar o ocorrido. Informe-os sobre a situação, incluindo todos os detalhes do golpe. Além disso, monitore suas contas bancárias em busca de atividades suspeitas e solicite o bloqueio do cartão afetado para evitar possíveis prejuízos financeiros adicionais.

2.1.8 Golpe do WhatsApp copiado

Os criminosos obtêm uma foto da vítima, muitas vezes a foto de perfil usada em aplicativos, e usam-na para enviar mensagens aos contatos da vítima com histórias variadas, buscando ganhos financeiros. Eles podem solicitar dinheiro sob falsos pretextos, como resolver problemas urgentes ou alegando bloqueio de contas em instituições financeiras. Para se aproximar da vítima sem levantar suspeitas, os golpistas começam o contato com frases como: "Oi, este é meu novo número. Salva aí"ou "Oi, tudo bem? Vou deixar meu número antigo para questões profissionais. Anota meu novo número particular."Dessa forma, tentam evitar que a vítima identifique a tentativa de fraude, mesmo usando um número totalmente diferente do da vítima.

2.1.8.1 Como evitar

Mantenha sua foto de perfil oculta nos aplicativos para que apenas seus contatos possam vê-la. Essa configuração pode ser ajustada nas opções de privacidade. Além disso, tenha cuidado com as publicações em redes sociais, protegendo suas fotos nas configurações de privacidade. Instrua seus contatos mais próximos a estarem alertas para esses golpes. Evite adicionar novos contatos sem verificar previamente a identidade deles.

2.1.8.2 Como resolver

Registre um Boletim de Ocorrência na Polícia Civil e alerte seus contatos sobre a má utilização de sua foto em tentativas de golpes. Oriente-os a denunciar o contato suspeito no WhatsApp, clicando no número e selecionando a opção de denúncia. Além disso, envie um e-mail para support@whatsapp.com, informando sobre a prática criminosa. No corpo do e-mail, forneça o número de telefone no formato internacional (+55 + DDD + número do telefone) e explique que a conta está usando sua imagem indevidamente para aplicar golpes, solicitando a desativação da conta devido à prática criminosa.

2.1.9 Golpe do WhatsApp clonado

Os golpistas conseguem obter o número de celular e o nome da vítima que visam a clonagem da conta do WhatsApp. Utilizando essas informações, os criminosos tentam registrar o WhatsApp da vítima em seus próprios dispositivos. Para efetivar essa ação, é necessário inserir o código de segurança enviado pelo aplicativo via SMS sempre que uma nova instalação é feita em um dispositivo diferente.

Os fraudadores iniciam o procedimento enviando uma mensagem pelo WhatsApp, fingindo representar o serviço de atendimento ao cliente de um site de vendas conhecido ou da empresa na qual a vítima tem cadastro. Eles requisitam o código de segurança, previamente enviado pelo aplicativo, alegando ser necessário para uma suposta atualização, manutenção ou confirmação de cadastro. Com posse desse código, os criminosos conseguem replicar a conta do WhatsApp em outro celular, obtendo acesso ao histórico completo de conversas e à lista de contatos da vítima.

A partir desse ponto, os golpistas enviam mensagens aos contatos, se passando pela vítima, e solicitam empréstimos de dinheiro, induzindo os contatos a acreditarem estar falando com a pessoa real. Essa tática visa enganar os contatos próximos da vítima para obter ganhos financeiros ilícitos.

2.1.9.1 Como evitar

Mantenha-se atento a solicitações de dinheiro ou dados pessoais por aplicativos de mensagens, especialmente se houver urgência ou pressão para realizar depósitos ou transferências via Pix para contas de terceiros. Desconfie de mensagens solicitando códigos de segurança enviados por SMS, principalmente se não estiver esperando por nenhuma atualização ou confirmação de cadastro. Sempre verifique a legitimidade do pedido de informações antes de compartilhar qualquer dado sensível.

2.1.9.2 Como resolver

Caso suspeite que sua conta do WhatsApp foi clonada ou que você tenha sido vítima desse golpe, é essencial agir rapidamente. Entre em contato imediato com o suporte do WhatsApp para relatar o ocorrido e recuperar o acesso à sua conta. Altere imediatamente sua senha e configure a autenticação em duas etapas no WhatsApp para aumentar a segurança. Informe seus contatos sobre o ocorrido para evitar que sejam enganados por mensagens fraudulentas. Além disso, registre um Boletim de Ocorrência na delegacia mais próxima para documentar o incidente e buscar assistência legal, se necessário.

2.1.10 Golpe da troca do cartão

Os golpistas que atuam como vendedores observam atentamente quando você digita sua senha na máquina de pagamento e, em seguida, trocam o cartão na devolução. Ao obter acesso ao seu cartão e senha, realizam compras fraudulentas utilizando o seu dinheiro. Essa mesma tática pode ser empregada por desconhecidos que oferecem ajuda no caixa eletrônico. Aproveitando-se de qualquer dificuldade que você possa enfrentar no terminal eletrônico, eles rapidamente pegam o seu cartão e o substituem por outro que não lhe pertence, ao mesmo tempo em que observam furtivamente a digitação da sua senha. Essas ações visam obter acesso aos seus dados financeiros e possibilitar transações não autorizadas utilizando as informações capturadas.

2.1.10.1 Como evitar

Mantenha-se vigilante durante as compras. Verifique se o nome no cartão devolvido é realmente o seu e, sempre que possível, faça o procedimento de passar o cartão na máquina pessoalmente, evitando entregá-lo a terceiros. Ao utilizar caixas eletrônicos, certifique-se de buscar ajuda apenas de funcionários bancários uniformizados e nunca aceite auxílio de pessoas desconhecidas.

2.1.10.2 Como resolver

Se você se encontrar em uma situação em que suspeita ter sido vítima desse tipo de golpe, é crucial agir prontamente para minimizar o potencial impacto financeiro. Primeiramente, entre em contato imediatamente com o seu banco ou instituição financeira para relatar o ocorrido. Informe-os sobre a possível troca do seu cartão e a suspeita de acesso não autorizado à sua conta.

Registre um Boletim de Ocorrência na delegacia mais próxima. Esse passo é essencial para documentar o incidente e colaborar com as autoridades na investigação do crime. Detalhe todos os eventos, descrevendo o momento e o local em que a possível troca de cartões ocorreu, além de quaisquer informações relevantes que possam auxiliar na identificação dos golpistas.

Monitore regularmente suas transações bancárias para identificar atividades suspeitas ou não autorizadas. Caso identifique compras ou movimentações desconhecidas, informe imediatamente o banco sobre essas transações para contestá-las.

É importante, também, revisar as políticas de segurança do banco e seguir as orientações fornecidas para proteger suas informações financeiras. Considere solicitar o bloqueio imediato do cartão suspeito e a emissão de um novo.

Ao adotar essas medidas rapidamente, você estará colaborando para reduzir possíveis prejuízos financeiros e contribuindo para a investigação do incidente.

2.1.11 Golpe do link falso

Um golpe comum acontece por meio de ofertas tentadoras enviadas por e-mail ou redes sociais, visando atrair os usuários para compartilhar informações sensíveis, como números de CPF, dados bancários, informações de cartões e senhas. Além disso, essas mensagens podem conter links maliciosos que, quando clicados, instalam vírus e aplicativos projetados para roubar dados pessoais. Essa ação criminosa concede aos golpistas acesso não autorizado a todas as contas do indivíduo, comprometendo tanto a segurança quanto a privacidade de suas informações financeiras e pessoais.

2.1.11.1 Como evitar

Desconfie de ofertas irresistíveis recebidas por e-mail ou redes sociais, especialmente aquelas que solicitam informações pessoais ou financeiras. Sempre verifique a legitimidade dessas mensagens, confirmando diretamente com a empresa ou instituição, utilizando os canais oficiais de comunicação, se a oferta é real. Evite clicar em links suspeitos e verifique sempre a autenticidade das fontes antes de fornecer dados pessoais ou financeiros online.

2.1.11.2 Como resolver

Se você caiu em um golpe desse tipo, aja imediatamente. Primeiramente, informe o ocorrido ao seu banco ou instituição financeira, relatando a possível exposição de suas informações sensíveis. Mude todas as senhas e códigos de acesso relacionados às contas afetadas e monitore regularmente suas transações bancárias. Se identificar qualquer atividade suspeita, comunique imediatamente seu banco para contestar as transações não autorizadas. Além disso, registre um Boletim de Ocorrência na delegacia mais próxima para documentar o incidente e, se possível, relate o ocorrido às autoridades responsáveis por crimes cibernéticos. Isso ajudará na investigação e pode prevenir futuros ataques similares.

2.1.12 Golpe do falso leilão

Os golpistas desenvolvem sites falsos de leilão, promovendo uma variedade de produtos a preços significativamente abaixo do valor de mercado. Em seguida, solicitam transferências bancárias, depósitos e até mesmo dinheiro via Pix para garantir a compra dos itens anunciados. Usualmente, apelam para a urgência na finalização da transação, alegando que os descontos oferecidos podem expirar rapidamente, induzindo a vítima a agir rapidamente. Entretanto, após o pagamento, os fraudadores nunca realizam a entrega dos produtos adquiridos.

Além do prejuízo financeiro, os golpistas também buscam roubar informações sensíveis, como números de CPF e de conta das vítimas. Essa ação criminosa compromete a segurança e a privacidade dos dados pessoais dos indivíduos lesados, expondo-os a riscos significativos de roubo de identidade e fraudes financeiras.

2.1.12.1 Como evitar

Desconfie de ofertas extremamente vantajosas em sites desconhecidos ou leilões online. Antes de efetuar qualquer pagamento, pesquise sobre a credibilidade do site e verifique se há avaliações ou reclamações de outros usuários. Prefira realizar transações em plataformas reconhecidas e seguras, que ofereçam garantias de proteção ao consumidor. Evite a pressão para finalizar compras rapidamente, pois essa urgência pode ser um sinal de alerta.

2.1.12.2 Como resolver

Se você se viu envolvido em um golpe desse tipo, é crucial agir prontamente para minimizar os danos. Primeiramente, entre em contato com o seu banco ou instituição financeira para relatar a fraude e solicitar orientações sobre a contestação do pagamento. Registre um Boletim de Ocorrência na delegacia mais próxima, detalhando o incidente e fornecendo todas as informações disponíveis sobre o site falso. Além disso, monitore suas contas bancárias para identificar quaisquer atividades suspeitas e considere acionar órgãos de defesa do consumidor para buscar assistência adicional. Esteja atento a possíveis sinais de roubo de identidade e tome medidas preventivas, como o monitoramento regular de seus dados pessoais e financeiros.

2.2 Cibercriminosos

O modo usual de agir desses golpistas é automatizar os ataques de forma a atingir milhares de usuários por vez, tornando as soluções tradicionais de defesa, incapazes de detectar e reagir a tais ameaças com a rapidez necessária. Quanto aos smartphones, os principais métodos de ataques tem como alvo obter senhas e informações enganando o usuário por meio de engenharia social. Como não é possível instalar aplicativos perigosos remotamente, é necessária a colaboração do usuário, seja fornecendo o aparelho telefônico ao golpista diretamente ou seguindo instruções para baixar algum aplicativo suspeito.

Os golpes digitais de engenharia social são vistos de forma estereotipada, onde os golpistas agem isoladamente ou de forma desorganizada. Pelo contrário, a realidade desmistifica essa imagem, esses agentes são indivíduos elegantes, educados

e perspicazes, operando em grupos compactos, colaborando mutuamente para alcançar seus objetivos nefastos.

Eles constituem associações criminosas altamente articuladas que operam em rede, empregando estratégias de cooperação em ambientes que se assemelham a espaços de trabalho compartilhados, conhecidos como *coworking*. Essas organizações se dedicam a criar contas falsas, muitas vezes utilizando informações verdadeiras de pessoas reais, para construir uma fachada de autenticidade e credibilidade.

Essa abordagem coletiva e estruturada confere a esses grupos criminosos uma eficiência e uma adaptabilidade notáveis. Eles se movem habilmente nos domínios digitais, aproveitando-se da interconexão global para disseminar suas atividades fraudulentas. Essa realidade revela uma sofisticação surpreendente por trás das ações aparentemente discretas, exigindo uma abordagem mais ampla e coordenada para enfrentar essa ameaça à segurança digital e à privacidade dos indivíduos.

A compreensão desses padrões de comportamento e organização é fundamental para o desenvolvimento de estratégias de defesa mais eficazes. É imperativo não apenas abordar os aspectos técnicos desses golpes, mas também desmantelar suas estruturas organizacionais, reduzindo assim a eficácia dessas redes criminosas e protegendo de maneira mais abrangente os usuários e suas informações pessoais.

2.3 Princípios para evitar golpes

Segurança, em geral, pode ser alcançada através da prevenção, preensão, inibição, desvio, bem como, detecção de ataques e contramedidas de proteção e eliminação de intrusão. E a detecção de intrusão é baseada nas crenças de que o comportamento de um intruso será noticiavelmente diferente do de um usuário legítimo e de que muitas ações não-autorizadas são detectáveis(MUKHERJEE et al., 1994).

Assim sendo, uma forma de evitar ser vitima de um golpe digital é utilizar ferramentas reconhecidamente seguras por especialistas no setor.

Para garantir a segurança no uso de quaisquer aplicações conectadas a rede, é necessário seguir as práticas corretas e ortodoxas em relação a segurança da informação. A tríade confidencialidade, integridade e disponibilidade representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger(SILVA; JÚNIOR, 2013).

Princípio da confidencialidade: Estabelece que somente pessoas com autorização apropriada têm permissão para acessar informações específicas. Isso implica que qualquer acesso não autorizado, seja intencional ou acidental, constitui uma viola-

ção do princípio da confidencialidade. Um exemplo de quebra desse princípio ocorre quando alguém invade um sistema de computador, independentemente de proteção por senha, e obtém informações confidenciais sobre uma pessoa ou empresa.

Princípio da integridade: A integridade de uma informação significa que ela não foi alterada de forma não autorizada e, portanto, pode ser considerada confiável. Qualquer modificação intencional ou não autorizada de informações compromete sua integridade. Um exemplo de violação da integridade ocorre quando um aluno tenta alterar sua própria média em um sistema de notas, comprometendo deliberadamente a precisão e a integridade das informações.

Princípio da disponibilidade: Este princípio afirma que as informações devem estar disponíveis para aqueles que têm a devida autorização sempre que necessário. Um exemplo de violação da disponibilidade ocorre em um ataque de negação de serviço contra um servidor, que leva à interrupção de seu funcionamento e torna as informações inacessíveis para os usuários autorizados.

Para Espínula e Cruz (2020) algumas medidas que deixam alguem mais seguro são evitar o uso de redes de internet públicas, manter o computador e celular sempre atualizados, instalar (e manter) algum software de proteção (antivírus), manter a navegação em sites conhecidos e com certificado de segurança, evitar o download de arquivos e programas desconhecidos e sempre desconfiar de alguma mensagem suspeita independente de como a recebeu.

Para se proteger ativamente de cair em golpes digitais esses principios gerais podem auxiliar:

1. Esteja ciente dos golpes digitais mais recentes e fique atualizado sobre as táticas de *phishing* e outras formas de ataques.
2. Desconfie de solicitações não solicitadas.
3. Nunca compartilhe informações pessoais ou financeiras por email, mensagem ou telefone, a menos que você tenha iniciado o contato e esteja seguro sobre a autenticidade da solicitação.
4. Use senhas fortes e exclusivas, juntamente com a autenticação de dois fatores.

2.3.1 Sinais para identificar um possível golpe digital

Muitos golpes apresentam mesma estrutura e características que podem ser identificadas e usadas para convencer a vítima de que ela deve encerrar qualquer contato com os golpistas.

1. Ofertas muito boas para serem verdade.

2. Solicitações inesperadas de informações confidenciais.
3. Erros gramaticais e ortográficos em comunicações.
4. Websites suspeitos sem o cadeado de segurança.
5. Pedidos de pagamento antecipado ou transferências bancárias não usuais.

2.3.2 O que fazer se for vítima de um golpe digital novo

Ao sofrer um golpe digital, dificilmente a vítima vai conseguir ser ressarcida ou conseguir que os criminosos sejam pegos, justamente por isso que a prevenção é tão importante para evitar esse tipo de crime. Mesmo assim, ainda existem medidas que devem ser tomadas para evitar maior prejuízos.

Entrar imediatamente em contato com a agencia bancária e com a polícia ou com uma delegacia especializada em crimes digitais para relatar o golpe e fornecer todas as informações pertinentes é essencial para ajudar a polícia em prender os criminosos.

Notificar as instituições financeiras tais como o banco e a operadora do cartão de crédito sobre o golpe, para que medidas possam ser tomadas para proteger a conta violada e evitar perdas financeiras adicionais.

É essencial alterar todas as senhas das contas online e monitorar as contas financeiras regularmente para identificar qualquer atividade suspeita.

Por fim, é importante avisar amigos e familiares do ocorrido para evitar que mais pessoas se tornem vítimas desses crimes.

3 Aplicação

O aplicativo foi desenvolvido com o proposito de ser usado como material informativo auxiliar para palestras de conscientização sobre fraude digitais, essa finalidade direcionada do aplicativo o posiciona como uma ferramenta valiosa e complementar para ampliar o alcance e a eficácia dessas palestras educativas.

Um aplicativo foi cuidadosamente feito com o propósito explícito de servir como um recurso informativo essencial e complementar para palestras de conscientização sobre fraudes digitais. Cada detalhe, desde a seleção dos tópicos abordados até a forma de apresentação, foi meticulosamente pensado para oferecer uma compreensão abrangente e clara dos perigos e das estratégias utilizadas por golpistas virtuais. Compreende-se a importância fundamental de educar e capacitar as pessoas para reconhecerem e evitarem situações de risco online. Portanto, cada linha, cada exemplo e cada conceito incluído neste material foram estrategicamente escolhidos para oferecer um conhecimento prático e acessível, fornecendo orientações claras e práticas sobre como se proteger contra ameaças cibernéticas. A abrangência deste recurso se destina não apenas a informar, mas também a motivar indivíduos a adotarem medidas proativas e preventivas em suas interações diárias na internet, promovendo uma cultura de segurança digital e minimizando os riscos de cair em golpes e fraudes virtuais.

As campanhas de sensibilização sobre fraudes reduzem a vulnerabilidade apenas a curto prazo(BULLEE et al., 2016, tradução nossa).

Portanto essas campanhas têm um impacto imediato e podem reduzir a vulnerabilidade a curto prazo. Isso ocorre porque a conscientização é uma etapa inicial no processo de proteção contra fraudes digitais.

Além das campanhas de conscientização, é crucial investir em educação contínua, desenvolver habilidades específicas para identificar e evitar golpes, além de promover uma cultura de segurança digital no longo prazo. Isso pode incluir programas educacionais mais extensos, treinamentos especializados e a integração de medidas de segurança digital nas práticas cotidianas. Ao fazer isso, é possível ampliar o impacto das campanhas de conscientização, reduzindo a vulnerabilidade não apenas a curto, mas também a longo prazo.

O reconhecimento de que as campanhas de conscientização têm um impacto mais imediato reforça a importância contínua dessas iniciativas. As palestras educativas oferecem um espaço valioso para abordar tópicos atuais, compartilhar exemplos práticos e interagir diretamente com o público para promover uma compreensão mais profunda dos desafios das fraudes digitais.

Além disso, o desenvolvimento de aplicativos informativos pode complementar essas palestras, proporcionando um recurso acessível e informativo para reforçar o conhecimento adquirido. Esses aplicativos podem oferecer atualizações regulares, dicas de segurança, exemplos de casos reais, testes interativos e guias passo a passo para lidar com situações de risco online. Eles são uma ferramenta valiosa para manter o engajamento do público e incentivar a aplicação prática das informações aprendidas.

Portanto, a combinação de palestras educativas com aplicativos informativos oferece uma abordagem abrangente e adaptável para promover a conscientização e a educação contínua sobre fraudes digitais. Juntos, esses recursos podem ajudar a manter o interesse, o entendimento e a prática de medidas de segurança digital, reduzindo assim a vulnerabilidade tanto a curto quanto a longo prazo.

3.1 Tecnologia escolhida

A tecnologia escolhida foi o **React Native** por sua capacidade de oferecer uma experiência multiplataforma eficiente. O **React Native** permite a criação de aplicativos para Android e iOS a partir de uma **única base de código**, economizando tempo e recursos. Além disso, sua comunidade ativa, a facilidade de reutilização de código e a capacidade de criar interfaces de usuário nativas foram considerações cruciais para atender à meta de disponibilizar um aplicativo informativo amplamente acessível e eficaz.

A escolha de utilizar o React Native para desenvolver o aplicativo foi cuidadosamente ponderada e alinhada com uma série de critérios fundamentais. A busca por uma solução eficiente e ágil de desenvolvimento de aplicativos desempenha um papel vital, principalmente quando se trata de uma plataforma que visa fornecer uma experiência de usuário fluida e consistente. O React Native, por sua vez, emergiu como uma escolha estratégica, não apenas por sua capacidade de criar aplicativos com aparência e funcionalidades similares às de aplicativos nativos, mas também por sua eficácia em termos de tempo e custo.

A decisão de adotar essa tecnologia foi impulsionada pela necessidade de um desenvolvimento rápido, mantendo um alto desempenho e, ao mesmo tempo, sendo uma solução de custo efetivo. O **React Native** oferece um ambiente de desenvolvimento unificado que permite aos desenvolvedores criar aplicativos para múltiplas plataformas (iOS e Android) com uma base de código comum. Isso não apenas agiliza o processo de desenvolvimento, reduzindo o tempo necessário para a criação de aplicativos para diferentes sistemas operacionais, mas também otimiza os recursos, reduzindo custos associados ao desenvolvimento e manutenção de aplicativos separados para cada plataforma.

Além disso, ao optar pelo React Native, a escolha foi em direção a uma solução altamente escalável, que não apenas garante a disseminação mais ampla do conhecimento e da educação, mas também oferece uma abordagem mais acessível para usuários finais. A eficiência no desenvolvimento de aplicativos permite que mais recursos sejam direcionados para a melhoria da experiência do usuário, agregando valor ao produto final e, por consequência, facilitando a disseminação de informações, educação e conhecimento de forma eficaz e acessível para um público mais amplo.

Ao considerar trabalhos futuros e novas iterações do aplicativo, a versatilidade do React Native oferece a vantagem de simplificar e acelerar o processo de implementação de novos recursos e conteúdos. Isso inclui a capacidade de divulgar imediatamente os golpes mais recentes, atualizando o aplicativo com informações vitais sobre novas ameaças, táticas de golpes emergentes e medidas de segurança adicionais.

A natureza modular e escalável do React Native permite que a equipe de desenvolvimento adicione e modifique facilmente conteúdos informativos, recursos de segurança e funcionalidades relevantes para educar os usuários sobre as últimas tendências em fraudes digitais. Dessa forma, o aplicativo pode permanecer atualizado e oferecer orientações relevantes e confiáveis, mantendo os usuários informados e protegidos contra os golpes mais recentes, consolidando sua posição como uma ferramenta dinâmica e confiável na prevenção e conscientização sobre fraudes online.

3.2 Configurando o ambiente

O aplicativo foi desenvolvido em um ambiente Windowns 10 usando o **Visual Studio Code** para a programação.

O Visual Studio Code é uma ferramenta bastante versátil e popular entre desenvolvedores, oferecendo uma ampla gama de recursos e suporte para diversas linguagens de programação, o que o torna uma escolha sólida para o desenvolvimento de aplicativos.

Desenvolver o aplicativo nesse ambiente proporciona uma interface familiar e amigável para o desenvolvimento, facilitando a codificação, depuração e implementação do aplicativo. Além disso, o Windows 10 oferece um ambiente estável e bem integrado para o desenvolvimento de software, fornecendo recursos que podem facilitar o processo de criação do aplicativo.

Essa escolha de ambiente de desenvolvimento oferece um conjunto de ferramentas eficientes para criar e gerenciar o projeto, permitindo a implementação de funcionalidades, a realização de testes e a aplicação de atualizações de forma ágil e eficaz. Com o Visual Studio Code e o ambiente Windows 10, os desenvolvedores

têm à disposição recursos robustos para garantir o desenvolvimento e aprimoramento contínuo do aplicativo.

3.2.1 Instalar o Node.js

Primeiro, foi baixado o Node.js em nodejs.org. O Node.js é uma parte essencial da infraestrutura do React Native.

3.2.2 Instalar o Expo CLI

Expo é uma ferramenta que simplifica o desenvolvimento de aplicativos React Native. Para instalá-lo foi aberto o terminal do **Visual Studio Code** e executado o seguinte comando:

Figura 4 – Comando para instalar o Expo

```
npm install -g expo-cli
```

Fonte: Elaborado pelo autor

3.2.3 Criar um projeto

Foi usado o comando Expo CLI para criar o projeto projeto:

Figura 5 – Comando para criar o projeto

```
expo init tcc
```

Fonte: Elaborado pelo autor

Após criar o projeto fomos até o diretório do projeto usando o comando cd:

Figura 6 – Comando entrar na pasta do projeto

```
cd tcc
```

Fonte: Elaborado pelo autor

3.2.4 Inicie o servidor de desenvolvimento

Foi iniciado o servidor de desenvolvimento do Expo com o seguinte comando:

Figura 7 – Comando para iniciar o projeto

```
expo init tcc
```

Fonte: Elaborado pelo autor

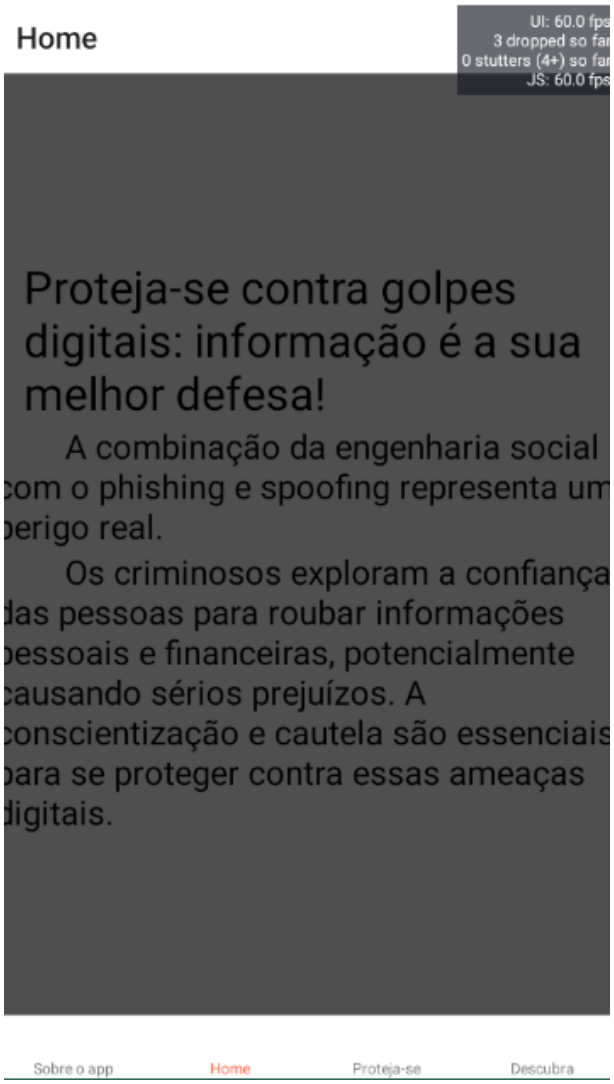
3.2.5 MEmu

Foi usado a versão do **Android 9** por meio do emulador de Android **MEmu** para testar o projeto, por sua reputação de oferecer desempenho e velocidade consistentes, facilidade de uso e suporte a recursos avançados, tornando-o uma opção eficaz para testar aplicativos Android em um ambiente de desenvolvimento Windows.

3.3 Telas

O aplicativo possui 4 telas informativas, a primeira corresponde a figura 4 e informa o usuário que ele está em um aplicativo que visá ajuda-lo a se defender das ameaças da rede Foi pensada mais uma tela para informar o que se deve fazer em caso de golpes, contudo como esses golpes são aplicados por criminosos e organizações profissionais quase não existe meio de recuperar os dados causados, a única informação relevante seria informar parentes e amigos para evitar mais vítimas

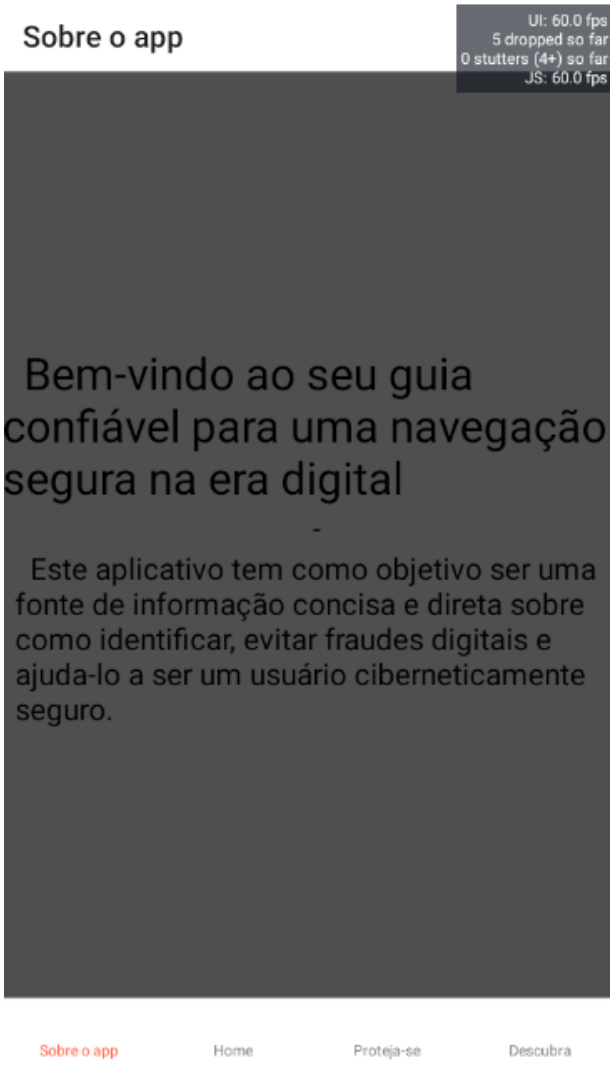
Figura 8 – Tela inicial do aplicativo



Fonte: Elaborado pelo autor

A segunda tela corresponde a figura 4 e informa o usuário que ele está em perigo e a informação é o melhor jeito dele se defender

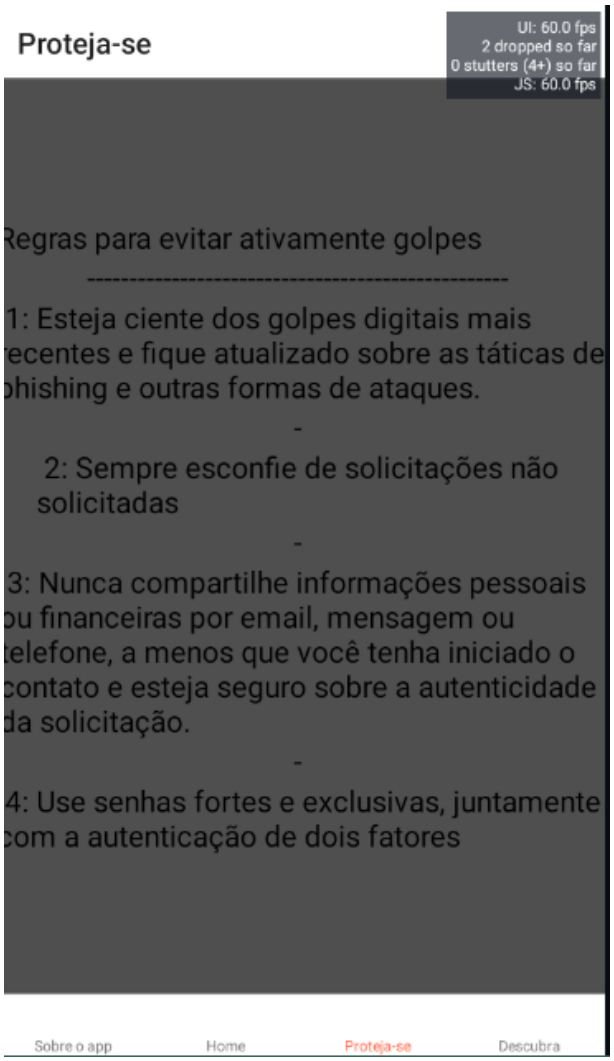
Figura 9 – Tela informativa do aplicativo



Fonte: Elaborado pelo autor

A terceira tela corresponde a figura 5 e informa regras e princípios que se seguidos podem ajuda-lo a evitar cair em um golpe

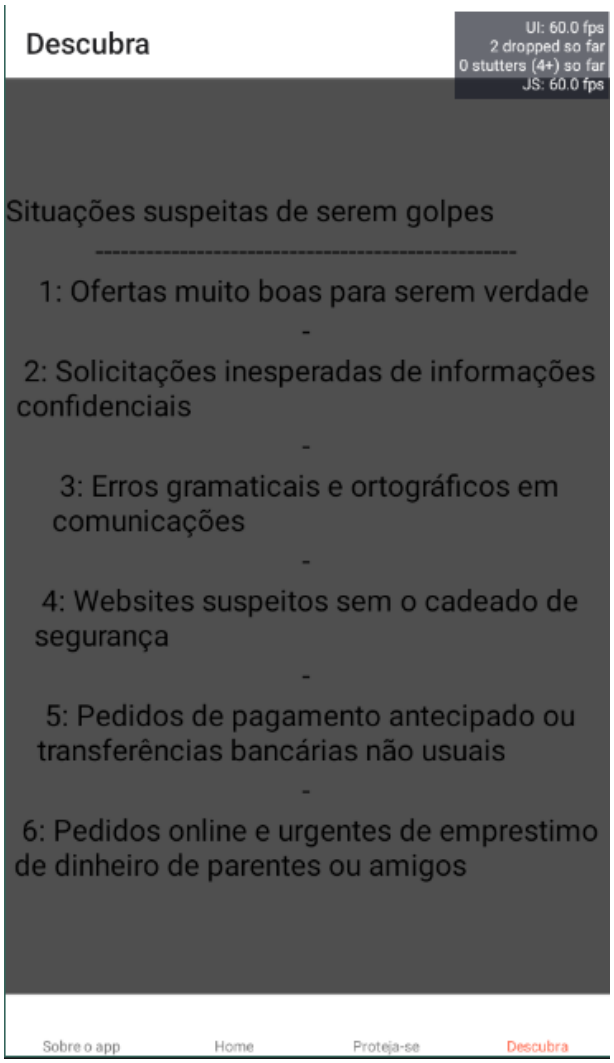
Figura 10 – Tela como evitar golpes digitais



Fonte: Elaborado pelo autor

A quarta tela corresponde a figura 6 e informa o usuário meio de conseguir identificar se uma mensagem é suspeita, ajudando ele a concluir que aquele contato visá aplicar-lhe um golpe ajudando-o a evitar e informar seus conhecidos e família, assim como as empresas relevantes como bancos e as de cartões de credito

Figura 11 – Tela como identificar mensagens e situações suspeitas



Fonte: Elaborado pelo autor

4 Conclusão

Nesse contexto, é evidente que o mundo digital apresenta uma dicotomia. Por um lado existem vantagens e conveniências oferecidas pela tecnologia por meio de aplicativos móveis, que desempenham um papel fundamental na capacidade das pessoas de armazenar, organizar e acessar informações para uso pessoal e profissional. No entanto, esse mesmo instrumento também representa uma ameaça, já que indivíduos mal-intencionados podem se apropriar de informações sensíveis, as quais podem ser usadas de maneira prejudicial contra o próprio indivíduo, resultando em desconforto e problemas tanto na esfera pessoal quanto no âmbito profissional.

A relevância deste estudo reside na análise do fenômeno sociotécnico dos golpes digitais de engenharia social, os quais representam uma ameaça à privacidade dos dados pessoais. Este trabalho integra disciplinas da comunicação e da computação para abordar essa questão de forma colaborativa. A necessidade de adotar medidas de proteção nos meios digitais é evidente, seja denominada como segurança da informação, segurança digital ou cuidados digitais. Essas medidas se tornam urgentes e, muito provavelmente, serão indispensáveis no futuro e devem fazer parte dele.

Golpes digitais são um problema sério e cada vez mais comum na era da tecnologia. Para se proteger, é importante estar atento, informado e seguir práticas sólidas de segurança cibernética. Lembre-se de que a prevenção é a melhor forma de se proteger contra golpes digitais. Adotar os cuidados necessários permite que se aproveite o mundo digital com segurança.

Dessa forma o ideal é fazer cadastros apenas em sites conhecidos para evitar que seus dados caiam em mãos erradas. Informações como nome, endereço, telefone e o numero do cadastro de pessoas físicas são suficientes para cometer diversas fraudes. Assim sendo quanto menos informações forem disponibilizas para terceiros, menor é a chance de uma pessoa se tornar uma vítima desses golpistas digitais

Os impactos financeiros dos golpes são claramente reconhecidos pela sociedade. Contudo, a análise sob o ponto de vista de impactos a privacidade ainda apresenta um longo caminho a ser percorrido para seu amadurecimento.

Os impactos financeiros dos golpes digitais são amplamente reconhecidos pela sociedade, porém, a análise dos impactos sobre a privacidade dos dados ainda carece de um aprofundamento significativo. Este estudo enfatizou a urgência de se considerar não apenas as consequências monetárias, mas também os efeitos intrusivos na esfera privada dos indivíduos. É crucial que futuras pesquisas e práticas se empenhem em explorar mais profundamente essa dimensão, visando um entendimento mais completo

e abrangente dos danos causados pelos golpes de engenharia social. Essa abordagem mais holística será fundamental para o desenvolvimento de estratégias mais eficazes na proteção da privacidade digital.

Referências

ANATEL. *Golpes atuais mais comuns*. 2023. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/dicas-contra-fraudes/golpes-atuais-mais-comuns. Acesso em: 25 nov 2023.

CERT. *CERT.br - Estatisticas*. 2023. Disponível em: https://stats.cert.br/phishing/. Acesso em: 25 nov 2023.

ESPÍNULA, S. G.; CRUZ, L. C. M. Segurança na Internet:Problemas e soluções para o usuário comum. *Anais do Congresso Nacional Universidade, EAD e Software Livre*, v. 1, n. 11, 2020.

FEBRABAN. *Crescem golpes envolvendo manipulação de vítimas para roubo de informações pessoais*. 2021. Disponível em: https://portal.febraban.org.br/noticia/3704/pt-br/. Acesso em: 25 nov 2023.

FEBRABAN. *3 em cada 10 brasileiros já foram vítimas de golpes ou tentativas de fraude*. 2022. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/3-em-cada-10-brasileiros-ja-foram-vitimas-de-golpes-ou-tentativas-de-fraude. Acesso em: 11 abr. 2023.

FEBRABAN. *FEBRABAN relança campanha nacional antifraudes*. 2022. Disponível em: https://portal.febraban.org.br/noticia/3836/pt-br/. Acesso em: 25 nov 2023.

KASPERSKY. *Brasil é o país com mais ataques de phishing por WhatsApp no mundo em 2022*. 2023. Disponível em: https://www.kaspersky.com.br/about/press-releases/2023_brasil-e-o-pais-com-mais-ataques-de-phishing-por-whatsapp-no-mundo-em-2022-aponta-kasper
Acesso em: 20 maio 2023.

LIPU, J. Y. G. et al. Crimes de informática. Universidade Federal da Grande Dourados, 2021.

MUKHERJEE, B.; HEBERLEIN, L. T.; Karl; Levitt. Network intrusion detection. *IEEE Network*, v. 8, n. 3, p. 26–41, 1994.

PANDOVE, K.; JINDAL, A.; KUMAR, R. Email spoofing. *International Journal of Computer Applications*, Citeseer, v. 5, n. 1, p. 27–30, 2010.

PIOVESAN, L. G.; SILVA, E. R. C.; SOUSA, J. F. d.; TURIBUS, S. N. ENGENHARIA SOCIAL: Uma abordagem sobre phishing. *REVISTA CIENTÍFICA UNIBALSAS*, v. 10, n. 1, p. 45–59, 2019.

SILVA, F. d. B. e.; JÚNIOR, S. M. C. d. J. Análise dos aspectos de segurança da informação em um ambiente de comunicações unificadas. 2013.

SOUZA, R. C. d. *Prevenção para ataques de engenharia social: um estudo sobre a confiança em segurança da informação em uma ótica objetiva, social, estrutural e interdisciplinar utilizando fontes de dados abertos*. Tese (Doutorado), ago. 2019.

TIESO, I. H. d. S.; SANTO, F. d. E. ATAQUES DE ENGENHARIA SOCIAL. *Rev. Interface Tecnol.*, v. 17, n. 2, p. 206–218, 2020.

WANDERLEY, C. A. C.; COSTA, R. S. da; RIBEIRO, L. de P. Crimes cibernéticos em tempos de pandemia: O isolamento social como propulsor da vulnerabilidade da população e do aumento dos casos. *Facit Business and Technology Journal*, v. 1, n. 37, 2022.