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

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

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.

2 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

2.1 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.

3 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 (2022) 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. 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.

   Além disso, segundo a pesquisa de uma grande empresa de cibersegurança , 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).

2. 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.

Ambos os tipos de ataques 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.

4 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.

5 Golpes comuns

Na clonagem de aplicativos de mensagem, tais como whatsapp e telegram, para conseguir instalar o aplicativo com a conta da vítima, o golpista sempre precisa da colaboração do usuário, uma vez que para a instalação o WhatsApp envia um código para o numero da vitima e o criminoso tenta convencer a vitima a revelar esse código, alegando ser algum funcionário que precisa daquele numero. Se o usuário enviar esse código, ela se torna uma vítima, porque perde completamente o acesso a sua conta do whatsapp e o criminoso fica livre para passar outros golpes se fingindo ser a pessoa que possuía o numero.

O acesso a contas bancarias via aplicativos, nesse tipo de golpe normalmente o golpista usa técnicos de *spoofing* para fingir ser um funcionário do banco e técnicas de engenharia social, para convencer a vítima que sua conta está sendo acessada por terceiros e que ela está sendo roubada. Após deixar a vitima assustada e nervosa ele a convence lhe passar o login e senha para supostamente impedir o roubo e obtém acesso total a conta.

6 Como evitar golpes

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 violação 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 se proteger ativamente de cair em golpes digitais é recomendado que:

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.

7 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.

8 O que fazer se for vítima de um golpe digital

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.

9 Aplicação

Inicialmente foi pensado um aplicativo que seria usado para auxiliar em uma palestra proporcionando uma demonstração dos conceitos vistos de forma mais fixadora, infelizmente a palestra em questão não foi realizada, contudo o aplicativo ainda foi desenvolvido com o proposito de ser usado como material informativo auxiliar para palestras de conscientização sobre fraude digitais

9.1 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.

Esta escolha também garante uma experiência de usuário fluida, a decisão de utilizar o React Native se alinhou com a busca por uma solução de desenvolvimento rápida, de alto desempenho e de custo efetivo, promovendo a disseminação do conhecimento e da educação de maneira eficaz e acessível.

9.2 Configurando o ambiente

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

9.2.1 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.

9.2.2 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 1 – Comando para instalar o Expo

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

Fonte: Elaborado pelo autor

9.2.3 Criar um projeto

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

Figura 2 – 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 3 – Comando entrar na pasta do projeto

```
cd tcc
```

Fonte: Elaborado pelo autor

9.2.4 Inicie o servidor de desenvolvimento

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

Figura 4 – Comando para iniciar o projeto

```
expo init tcc
```

Fonte: Elaborado pelo autor

9.2.5 MEmu

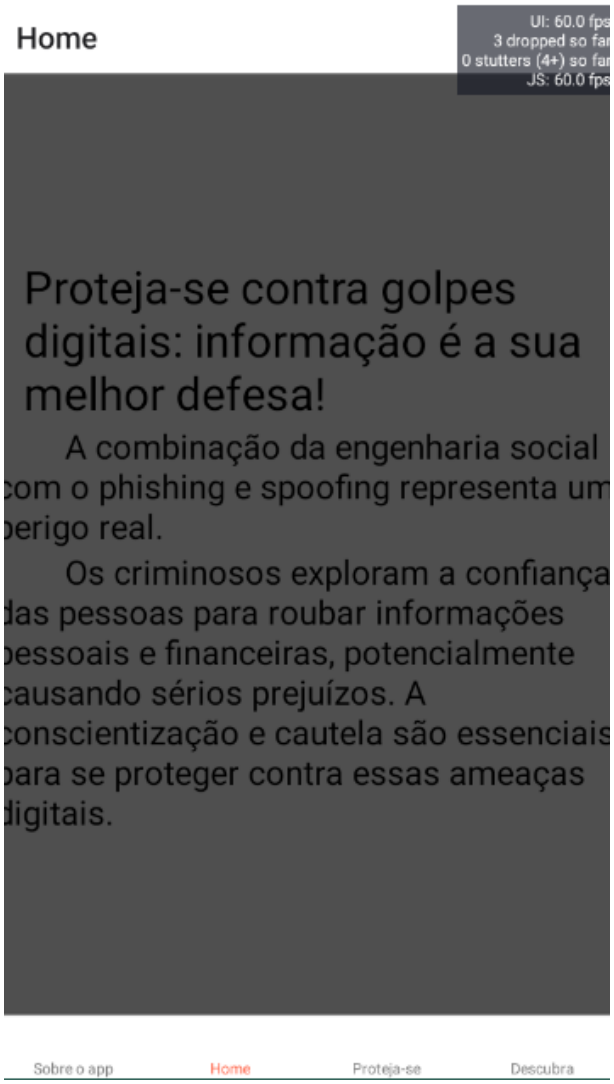
Foi usado a versão do **Android 9** por meio do emulador de Android **MEmu** para testar o projeto, por sua reputação de oferecer desempenho e velocidade consistentes,

facilidade de uso e suporte a recursos avançados, tornando-o uma opção eficaz para testar aplicativos Android em um ambiente de desenvolvimento Windows.

9.3 Telas

O aplicativo possui 4 telas informativas, a primeira 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 5 – Tela inicial do aplicativo

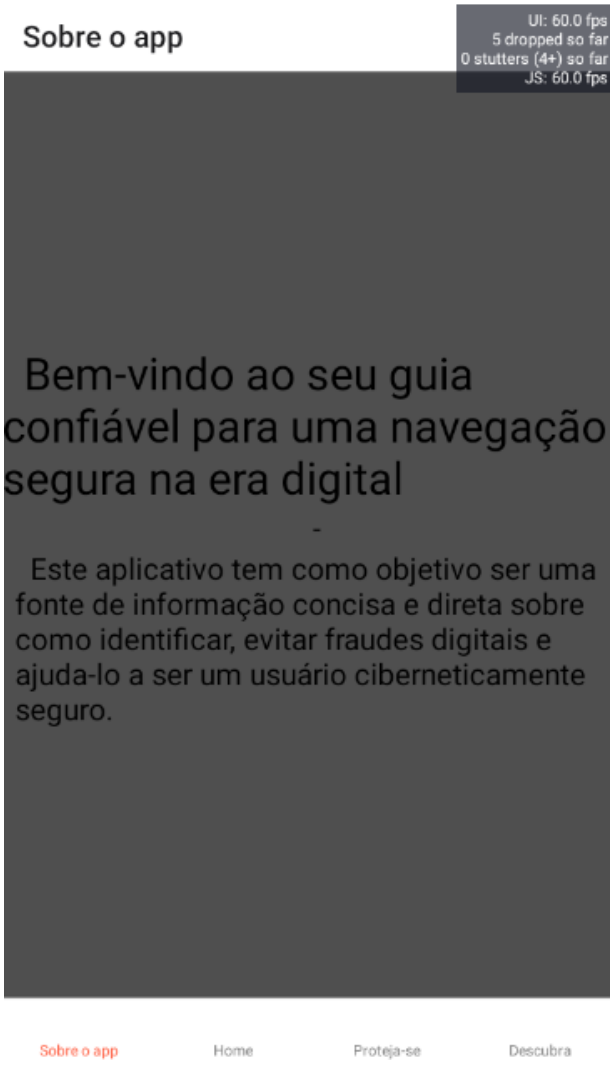


Fonte: Elaborado pelo autor

A segunda tela informa o usuário que ele está em perigo e a informação é o

melhor jeito dele se defender

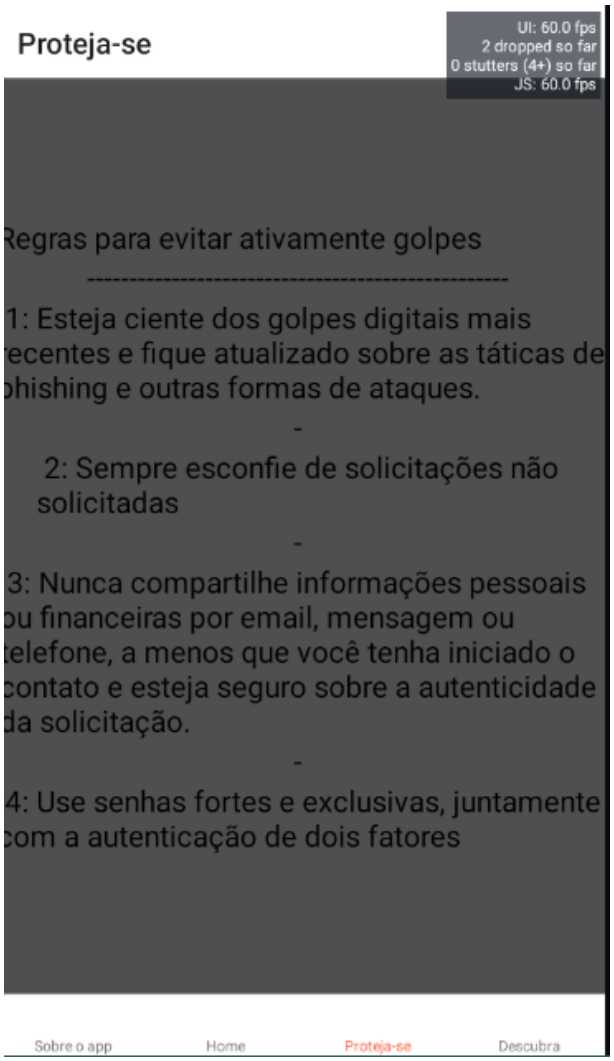
Figura 6 – Tela informativa do aplicativo



Fonte: Elaborado pelo autor

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

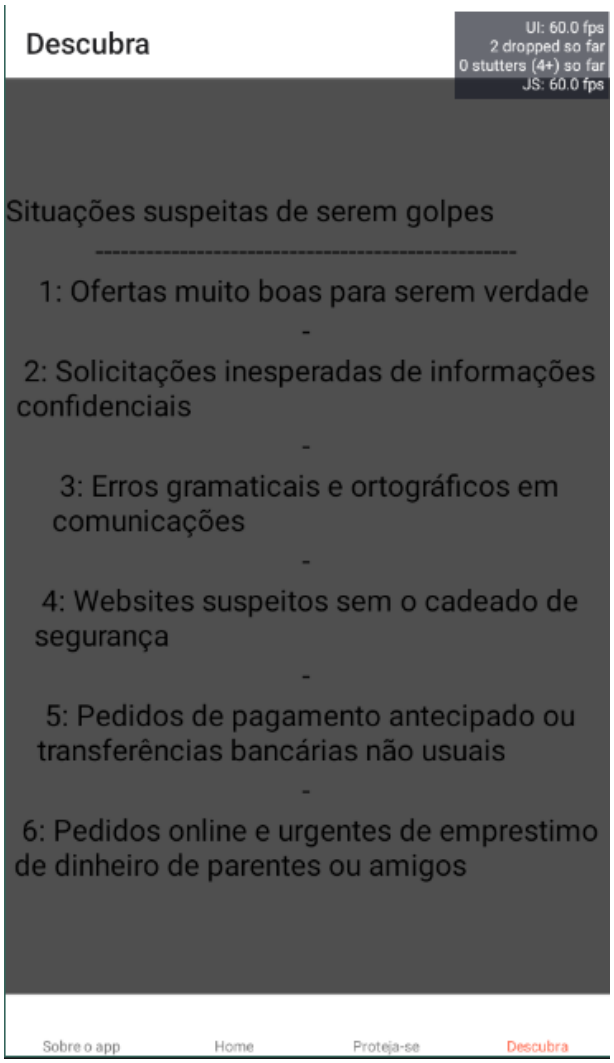
Figura 7 – Tela como evitar golpes digitais



Fonte: Elaborado pelo autor

A quarta tela 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 8 – Tela como identificar mensagens e situações suspeitas



Fonte: Elaborado pelo autor

10 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.

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

Referências

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.

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.

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.