



Estudo sobre fraudes digitais e desenvolvimento de aplicativo para smartphone Android e iOS para uso em palestras de sensibilização e esclarecimento



Aluno: Gabriel Carvalho Polido
Orientador: Eduardo Martins Morgado

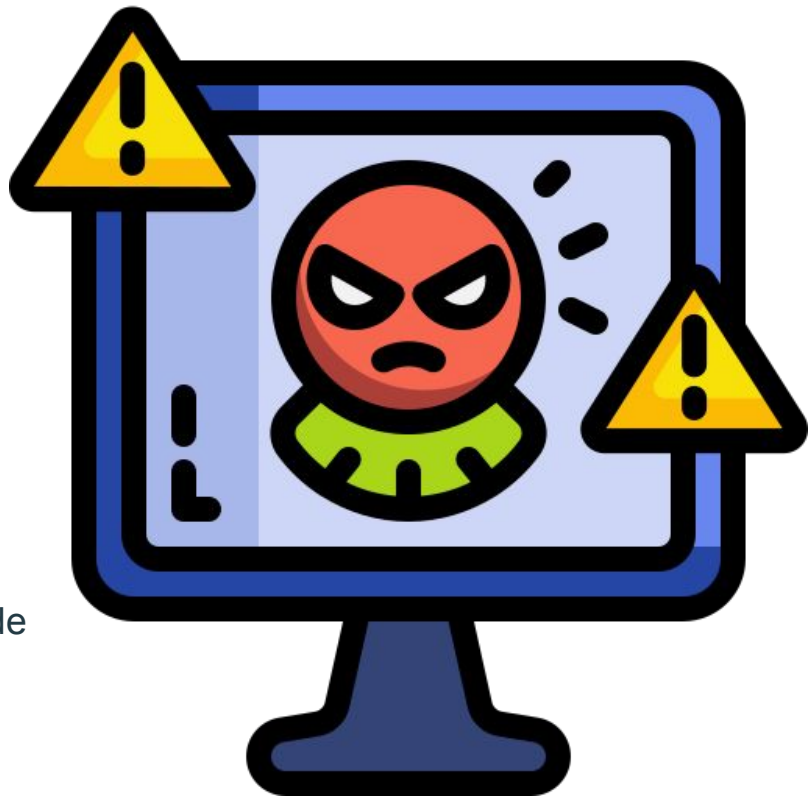


Introdução

Alto número de golpes e fraudes

FEBRABAN - 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%.

Fortinet - Registrou 31,5 bilhões de ataques cibernéticos no Brasil no primeiro semestre do ano de 2022.



Introdução

Ainda segundo a Febraban, 33% dos homens se declaram mais atingidos além de 35% daqueles com mais de 60 anos

A FEBRABAN estima que os golpes alcançaram R\$ 2,5 bilhões de reais em 2022.

Introdução

Celulares foram adotados por quase toda a população brasileira.

Segundo IBGE de 2021, temos:

- 84,4% dos brasileiros com celular de uso pessoal;
- 90% deles com acesso à Internet

Introdução

A informação é um dos ativos com mais valor e o mais cobiçado por pessoas más intencionadas que tem como objetivo aplicar golpes..

As redes sociais permitem que o usuário se exponha excessivamente, tornando-se alvos fáceis para ataques contínuos, pois disponibilizam publicamente diversas informações que auxiliam a realização de golpes..

Falta de conhecimento

Muitas pessoas não estão cientes dos riscos associados à divulgação de informações pessoais online, por vezes por não entender completamente como seus dados podem ser usados, compartilhados ou explorados por terceiros mal-intencionados.

Pessoas induzidas por um golpista são prejudicadas por desconhecimento das reais consequências que os seus comportamentos podem causar.

Problema

Nos últimos anos, o aumento vertiginoso das fraudes digitais tem causado prejuízos financeiros e emocionais para empresas e pessoas.

Segundo uma pesquisa da KASPERSKY, no ano de 2022 o brasil foi o país mais atacado do mundo, por phishing pelo WhatsApp

Técnicas de ataque: phishing, spoofing.

Soluções tradicionais: Antivírus, Anti-malwares, sistemas de autenticação.



Objetivos

Estudar as fraudes digitais e demonstrar o perigo que as técnicas, como phishing e spoofing, podem representar para as vítimas.

- Identificar as principais formas de fraudes digitais no Brasil.
- Desenvolver um aplicativo para smartphones que possa ser usado em palestras para informar aos usuários a facilidade de sofrer ataques cibernéticos.
- Desenvolvimento de um material para auxiliar na identificação de mensagens suspeitas

Pilares da segurança da informação

Confidencialidade: qualquer informação não é revelada para terceiros.

Integridade: os dados chegam de forma íntegra ao destino sem a ocorrência de alterações e/ou modificações durante o trajeto.

Disponibilidade: a informação está sempre disponível.



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.

Exemplo de phishing

Utilizam o URL da página, copiando o link original, mas adicionam, removem ou embaralham letras para confundir os usuários. Se o usuário clicar vai parar numa página falsa

Link falso 1: <https://www.caiixa.gov.br>

Link falso 2: <https://www.calxa.gov.br>



Phishing e Spoofing

Essas mensagens sms ou e-mails podem conter um link direto para um site fraudulento que, em muitos casos, é visualmente semelhante à página web verdadeira.

Resultando na vítima sendo induzida a passar informações voluntariamente para o criminoso.



Engenharia Social

A Engenharia Social é o processo pelo qual se tenta convencer alguém algo falso, explorando a ingenuidade do alvo.

O fraudador obtém a confiança da vítima e engana-a para extrair dados pessoais, seja por telefone, mensagem, sms ou e-mail.

De acordo com o Centro Nacional de Cibersegurança a Engenharia Social é um dos maiores riscos de segurança das pessoas e das organizações.

Engenharia Social

A engenharia social é usada em conjunto com técnicas de phishing e spoofing, tornando mais fácil explorar a vítima.

A engenharia social é uma grande ameaça, principalmente por que é focada no fator humano.

De acordo com a Febraban, houve aumento de 165% nesse tipo de golpe desde o início da pandemia

Mais exemplos golpes

Existem os golpes de relacionamento on-line ou “golpes de romance”:

Ocorrem quando alguém acredita que conseguiu amizade ou amor através de um site de relacionamento.

Mas a pessoa com quem você fala é, na verdade, um golpista usando um perfil falso.

O golpista manipula a vítima para ganhar sua confiança ao longo do tempo e, por fim, pedir dinheiro ou obter informações suficientes para roubar sua identidade.

Mais exemplos golpes

- O golpista pede dinheiro para pagar voos ou um passaporte para visitar o seu país de origem ou o país da vítima (no caso de existir um relacionamento).
- O golpista precisa que a vítima pague sua conta de telefone, água, condomínio. E manda uma cobrança falsa - fishing
- O golpista precisa de dinheiro para pagar um tratamento médico, seja para si mesmo ou para um familiar próximo.

Mais exemplos golpes

- O golpista diz que possui itens valiosos presos na alfândega e precisa pagar os impostos para recuperá-los e poder entrar no país da vítima e ter primeiro encontro.
- O golpista precisa de dinheiro para concluir alguma coisa – curso, estágio, negócio, antes de visitar a vítima.

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.

Golpes aplicativos de celulares

Nos principais golpes para celulares é necessária a colaboração do usuário, fornecendo códigos de segurança, logins e senhas

Uma segurança significativa pode ser obtida se o usuário não compartilhar tais informações relevantes com terceiros

Exemplos de golpes no celular

Clonagem de aplicativos de mensagem

Para funcionar o golpista precisa de um código, que apenas o proprietário original tem acesso

Acesso a contas bancárias via aplicativos

Usam muitos truques para a vítima passar login e senha



Cuidados com aplicativos de celulares

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.

Como identificar golpes digitais

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.

Consequências

Difícilmente a vítima vai conseguir ser ressarcida ou conseguir que os criminosos sejam pegos, então o que deve ser feito é:

- Entrar imediatamente em contato com a empresa relacionada e com a polícia

- Alterar todas as senhas das contas online

- Avisar amigos e familiares do ocorrido

O aplicativo

O aplicativo foi desenvolvido em react native com o propósito de ser usado como material informativo auxiliar para palestras de conscientização sobre fraude digitais

A ideia é que qualquer pessoa com um celular com Android ou iOS possa acessar um resumo das informações relevantes sobre os golpes digitais na palestra ou depois dela

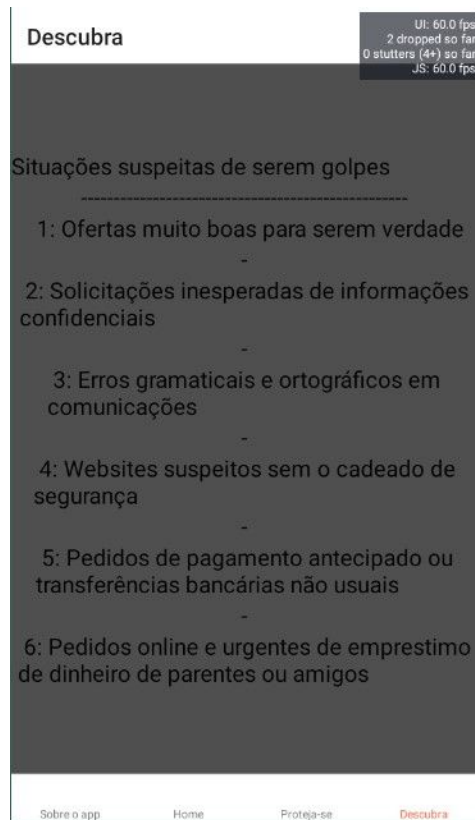
O aplicativo

O aplicativo visa ajudar o usuário a se defender das ameaças da rede.

A informação é apresentada usando frases simples que podem ser facilmente compreendidas pelo público geral.

O aplicativo

Apresenta características comuns que aparecem em interações fraudulentas e que ao identificadas podem ajudar indivíduos a cessarem o contato com os golpistas



O aplicativo

Apresenta princípios que ao serem seguidos ajudam a evitar os principais golpes digitais contra os indivíduos.

Proteja-se

UI: 60.0 fps
2 dropped so far
0 stutters (4*) so far
JS: 60.0 fps

Regras para evitar ativamente golpes

1: Esteja ciente dos golpes digitais mais recentes e fique atualizado sobre as táticas de phishing e outras formas de ataques.

2: Sempre 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

[Sobre o app](#)

[Home](#)

[Proteja-se](#)

[Descubra](#)



Dúvidas?

Obrigado!

